DESCRIPCIÓN DE LA ASIGNATURA

Grado/Máster en:	Master Universitario en TELEMÁTICA Y REDES DE TELECOMUNICACIÓN por la Universidad de Málaga
Centro:	Escuela Técnica Superior de Ingeniería de Telecomunicación
Asignatura:	SEGURIDAD EN REDES Y APLICACIONES MÓVILES
Código:	114
Tipo:	Optativa
Materia:	INTERNET DE LAS COSAS Y SEGURIDAD
Módulo:	ESPECIALIZACIÓN
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: MARIA CRISTINA ALCARAZ TELLO	alcaraz@uma.es	95951952915	3.2.50 - E.T.S.I. INFORMÁTICA	

RECOMENDACIONES Y ORIENTACIONES

Se recomienda haber cursado previamente alguna asignatura sobre seguridad informática y gestión o administración de redes, además de tener conocimientos básicos de programación orientada a objetos, idealmente en Java o lenguajes de programación similares. En caso de tener poca experiencia con los lenguajes de programación orientado a objetos, es recomendable que el alumno haya cursado la asignatura obligatoria del primer cuatrimestre de "Tecnologías Avanzadas de Desarrollo Software".

CONTEXTO

La asignatura cubre aspectos relacionados con la seguridad en redes en sentido amplio, principalmente cubriendo la problemática actual de las redes WLAN, WMAN y redes móviles, como 4G/5G, así como también los servicios básicos de seguridad existentes para su protección, incluyendo desde servicios mínimos como autenticación, confidencialidad y control de acceso, a servicios avanzados como la delegación de acceso o la privacidad.

Por lo tanto, el objetivo general de esta asignatura es que el alumno conozca los problemas y vulnerabilidades que se plantean durante la construcción de redes de telecomunicaciones de gran alcance y móvil, y tenga una visión mucho más clara y objetiva de cómo construir sistemas de red complejas en base a un conjunto de tecnologías y servicios de seguridad mínimos para su protección. Entre los servicios de seguridad de alto nivel, destacamos aquellos relacionados con la seguridad en pagos móviles, en VoIP y en comunicaciones multimedia, ofreciendo un soporte especial a las actuales aplicaciones de las tecnologías de comunicación.

COMPETENCIAS

CONTENIDOS DE LA ASIGNATURA

SEGURIDAD EN WLAN Y WMAN

- Amenazas y ataques a la seguridad en Redes
- Servicios y mecanismos básicos de protección en Redes
- Seguridad en IEEE 802.11
- Seguridad en IEEE 802.16 y WIMAX

SEGURIDAD EN REDES MÓVILES

- Problemática de Seguridad en Redes 3G
- Seguridad en Redes 4G: LTE
- Seguridad en Redes 5G: SDN y NFV

TÉCNICAS DE PROTECCIÓN PARA APLICACIONES MÓVILES

- Seguridad en pagos móviles
- Seguridad en VoIP
- Seguridad en comunicaciones multimedia

ACTIVIDADES FORMATIVAS

Actividades Presenciales

Actividades expositivas
Lección magistral

Otras actividades presenciales
Otras actividades presenciales

ACTIVIDADES DE EVALUACIÓN

Actividades de evaluacion Presenciales

Actividades de evaluación del estudiante
Examen final
Realización de trabajos y/o proyectos

RESULTADOS DE APRENDIZAJE / CRITERIOS DE EVALUACIÓN

Al finalizar la asignatura el alumno deberá ser capaz de:

RA.1 Identificar los problemas de seguridad en redes fijas y de dispositivos móviles.

RA.2 Conocer el diseño de los servicios de seguridad avanzados relacionados con la gestión de identidad, confianza y privacidad.

RA.3 Ser capaz de integrar soluciones de seguridad en aplicaciones de usuario y servicios de red.

Estos RAs cubren las competencias específicas de esta asignatura (2.8 y 2.9), en concreto:

- Los resultados RA1, RA2 desarrollan la competencia específica 3 (2.8).
- El resultado RA3 desarrolla la competencia específica 4 (2.9).

El Examen Final en su parte teórica evalúa los resultados RA1 y RA2.
El Examen Final en su parte práctica evalúa los resultados de aprendizaje RA3.

La realización de trabajos prácticos y proyectos sirve para evaluar los resultados RA1 y RA3.

De forma no presencial y soportada por las herramientas del campus virtual, se evalúa mediante varios cuestionarios (test) todos los resultados de aprendizaje.

Similarmente, el alumnado debe realizar una serie de prácticas e informes a lo largo del curso que permitan evaluar los resultados de aprendizaje RA1 y RA3.

PROCEDIMIENTO DE EVALUACIÓN

Para la evaluación y superación de la asignatura, se tendrá en cuenta: la participación activa en las diversas actividades propuestas y la realización de trabajos prácticos, ambas partes corresponderán al 60% de la nota final. El 40% restante, corresponderá a un examen final teórico.

Los alumnos a tiempo parcial deberán realizar una prueba final que corresponderá al 100% de la nota.

Si lo desea, el alumno podrá guardar hasta la convocatoria de Septiembre (pero no para la de Diciembre) la calificación (superada del 60% correspondiente) obtenida de la evaluación continua y las prácticas. Si no desea guardar esa calificación, entonces habrá de superar las preguntas (teórico-práctico) incluidas en el examen relativas a la parte práctica de la asignatura. Del mismo modo, si el alumno también desea renunciar a su calificación en la Evaluación Continua en Junio, podrá realizar un examen teórico-práctico, que de superarlo le permitirá aprobar la asignatura

BIBLIOGRAFÍA Y OTROS RECURSOS

Básica

AAA and Network Security for Mobile Access, Wiley, 2005.; Madjid Nakhjiri

Cryptography and network security, principles and practicesPractice Hall, 2013; Stallings, W.

Mobile and Wireless Network Security and Privacy, Springer, 2007.; S. Kami Makki

Security in computing, Prentice Hall, 2007; Pfleeger, C. UMTS Security, Wiley, 2003.; V. Niemi, K. Nyberg

Wireless Personal Area Networks: Performance, Interconnection, and Security with IEEE 802.15.4, Wiley, 2008.; Jelena Misic

Wireless Security Handbook, Auerbach, 2005.; Aaron E. Earle

Complementaria

Foundations of Modern Networking: SDN, NFV, QoE, IoT and Cloud, 2015; Stallings, W., Pearson Education.

DISTRIBUCIÓN DEL TRABAJO DEL ESTUDIANTE

ACTIVIDAD FORMATIVA PRESENCIAL

Descripción	Horas	Grupo grande	Grupos reducidos
Lección magistral	12	☑	☐
Otras actividades presenciales	21,8	☑	☐
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**		