Escuela Técnica Superior de Ingenieros Industriales y de Telecomunicación

GUÍA DOCENTE DE LA ASIGNATURA

G1498 - Seguridad en Redes de Comunicación

Grado en Ingeniería de Tecnologías de Telecomunicación
Optativa. Curso 4

Curso Académico 2018-2019

1. DATOS IDENTIFICATIVOS					
Título/s	Grado en Ingeniería de Tecnologías de Telecomunicación			Tipología y Curso	Optativa. Curso 4
Centro	Escuela Técnica Superior de Ingenieros Industriales y de Telecomunicación				
Módulo / materia	ASIGNATURAS OPTATIVAS DE MENCIÓN MENCIÓN EN TELEMÁTICA				
Código y denominación	G1498 - Seguridad en Redes de Comunicación				
Créditos ECTS	6	Cuatrimestre		Cuatrimestral (2)	
Web	http://www.tlmat.unican.es				
Idioma de impartición	Español	English friendly	No	Forma de impartición	Presencial

Departamento	DPTO. INGENIERIA DE COMUNICACIONES
Profesor responsable	JORGE LANZA CALDERON
E-mail	jorge.lanza@unican.es
Número despacho	Edificio Ing. de Telecomunicación Prof. José Luis García García. Planta: - 2. DESPACHO (S227)
Otros profesores	LUIS SANCHEZ GONZALEZ

2. CONOCIMIENTOS PREVIOS

La asignatura presupone el conocimiento de algoritmos criptográficos y su aplicación, así como protocolos y servicios en redes de comunicaciones. Recomendable haber cursado la asignatura de 'Criptografía y Seguridad en Redes y Servicios' de 4º curso, impartida en el 1º cuatrimestre.

3. COMPETENCIAS GENÉRICAS Y ESPECÍFICAS DEL PLAN DE ESTUDIOS TRABAJADAS
Competencias Genéricas
Conocimiento, comprensión y capacidad para aplicar la legislación necesaria durante el desarrollo de la profesión de Ingeniero Técnico de Telecomunicación y facilidad para el manejo de especificaciones , reglamentos y normas de obligado cumplimiento.
Capacidad de resolver problemas con iniciativa, toma de decisiones, creatividad, y de comunicar y transmitir conocimientos, habilidades y destrezas, comprendiendo la responsabilidad ética y profesional de la actividad del ingeniero técnico de telecomunicación.
Facilidad para el manejo de especificaciones, reglamentos y normas de obligado cumplimiento.
Pensamiento crítico y reflexivo.
Pensamiento lógico.
Uso de las TIC.
Búsqueda de información.
Manejo del Inglés.
Creatividad.
Innovación.
Competencias Específicas
Capacidad para aprender de manera autónoma nuevos conocimientos y técnicas adecuados para la concepción, el desarrollo o la explotación de sistemas y servicios de telecomunicación.
Capacidad de concebir, desplegar, organizar y gestionar redes, sistemas, servicios e infraestructuras de telecomunicación en contextos residenciales (hogar, ciudad y comunidades digitales), empresariales o institucionales responsabilizándose de su puesta en marcha y mejora continua, así como conocer su impacto económico y social.
Conocimiento y utilización de los fundamentos de la programación en redes, sistemas y servicios de telecomunicación.
Capacidad para aplicar las técnicas en que se basan las redes, servicios y aplicaciones telemáticas, tales como sistemas de gestión, señalización y conmutación, encaminamiento y enrutamiento, seguridad (protocolos criptográficos, tunelado, cortafuegos, mecanismos de cobro, de autenticación y de protección de contenidos), ingeniería de tráfico (teoría de grafos, teoría de colas y teletráfico) tarificación y fiabilidad y calidad de servicio, tanto en entornos fijos, móviles, personales, locales o a gran distancia, con diferentes anchos de banda, incluyendo telefonía y datos.
Capacidad de describir, programar, validar y optimizar protocolos e interfaces de comunicación en los diferentes niveles de una arquitectura de redes.
Capacidad de seguir el progreso tecnológico de transmisión, conmutación y proceso para mejorar las redes y servicios telemáticos.
Capacidad de programación de servicios y aplicaciones telemáticas, en red y distribuidas.
Capacidad de construir, explotar y gestionar las redes, servicios, procesos y aplicaciones de telecomunicaciones, entendidas éstas como sistemas de captación, transporte, representación, procesado, almacenamiento, gestión y presentación de información multimedia, desde el punto de vista de los servicios telemáticos.

3.1 RESULTADOS DE APRENDIZAJE
- Conocer la arquitectura de seguridad de protocolos empleados en la Internet, desde las tecnologías de comunicaciones hasta los servicios desplegados e inferir las tendencias de seguridad futuras.
- El alumno tendrá capacidad de diseñar, especificar y desarrollar una red/servicio de comunicación segura en base a supuestos y problemáticas específicas
- El alumno será capaz de evaluar prácticamente la operativa de las diferentes soluciones de seguridad estudiadas y sus implicaciones y requerimientos técnicos.
- El alumno será capaz de informar de incidencias de seguridad y razonar la aplicación de medidas para tratarlas y evitar su ocurrencia en un futuro.

4. OBJETIVOS
Ampliar los conocimientos teórico-prácticos de los sistemas de redes de comunicación actuales, profundizando en los aspectos de seguridad que se aplican según las necesidades de cada entorno.
Adquirir los conocimientos sobre los mecanismos necesarios para garantizar el cumplimiento de las políticas de seguridad definidas para una red (evaluando los riesgos e incidencias) y asegurar el transporte de la información a través de ellas.
Adquirir el conocimiento sobre la legislación y las recomendaciones de gestión y auditoria de seguridad vigentes tanto a nivel nacional como internacional.

5. MODALIDADES ORGANIZATIVAS Y MÉTODOS DOCENTES

ACTIVIDADES	HORAS DE LA ASIGNATURA
ACTIVIDADES PRESENCIALES	
HORAS DE CLASE (A)	
- Teoría (TE)	38
- Prácticas en Aula (PA)	6
- Prácticas de Laboratorio (PL)	16
- Horas Clínicas (CL)	
Subtotal horas de clase	60
ACTIVIDADES DE SEGUIMIENTO (B)	
- Tutorías (TU)	9
- Evaluación (EV)	6
Subtotal actividades de seguimiento	15
Total actividades presenciales (A+B)	75
ACTIVIDADES NO PRESENCIALES	
Trabajo en grupo (TG)	45
Trabajo autónomo (TA)	30
Tutorías No Presenciales (TU-NP)	
Evaluación No Presencial (EV-NP)	
Total actividades no presenciales	75
HORAS TOTALES	150

6. ORGANIZACIÓN DOCENTE

CONTENIDOS		TE	PA	PL	CL	TU	EV	TG	TA	TU-NP	EV-NP	Semana
1	Tema I: INTRODUCCIÓN A LA SEGURIDAD EN REDES. Concepto de seguridad. Terminología. Política de seguridad. Seguridad lógica, física y personal. Riesgos y vulnerabilidades	3,00	0,00	0,00	0,00	1,00	0,00	4,00	2,00	0,00	0,00	1
2	Tema II: AUTENTICACIÓN Y GESTIÓN DE CLAVES. Introducción a los servicios de autenticación. Autenticación criptográfica. Kerberos. Certificación digital. Infraestructura de clave pública.	16,00	3,00	8,00	0,00	3,00	3,00	16,00	12,00	0,00	0,00	2-8
3	Tema III: PROTOCOLOS Y MECANISMOS DE SEGURIDAD. Seguridad en redes cableadas e inalámbricas. Seguridad a nivel de red (IPSec, tunnelling, VPN). Seguridad a nivel de transporte (SSL, TLS). Seguridad en los servicios (HTTPS, SSH).	15,00	3,00	6,00	0,00	4,00	2,00	17,00	11,00	0,00	0,00	8-14
4	Tema IV: CONTROL DE ACCESO Y SEGURIDAD PERIMETRAL. Control de acceso, protocolos de identificación, autorización y autenticación. Arquitecturas y configuración de cortafuegos.	4,00	0,00	2,00	0,00	1,00	1,00	8,00	5,00	0,00	0,00	14-15
TOTAL DE HORAS		38,00	6,00	16,00	0,00	9,00	6,00	45,00	30,00	0,00	0,00	

Esta organización tiene carácter orientativo.

TE	Horas de teoría
PA	Horas de prácticas en aula
PL	Horas de prácticas de laboratorio
CL	Horas Clínicas
TU	Horas de tutoría
EV	Horas de evaluación
TG	Horas de trabajo en grupo
TA	Horas de trabajo autónomo
TU-NP	Tutorías No Presenciales
EV-NP	Evaluación No Presencial

7. MÉTODOS DE LA EVALUACIÓN

Descripción	Tipología	Eval. Final	Recuper.	%
Evaluación Continua	Otros	No	Sí	20,00

Calif. mínima	0,00
Duración	1 hora
Fecha realización	Durante el desarrollo de cada bloque teórico
Condiciones recuperación	En examen final tanto en la convocatoria ordinaria como en la extraordinaria.
Observaciones	Pruebas de tipo test o ejercicios a resolver en el aula sobre los contenidos de cada bloque teórico.

Laboratorio	Evaluación en laboratorio	Sí	No	25,00

Calif. mínima	0,00
Duración	Durante el desarrollo de la práctica
Fecha realización	Durante el desarrollo de la práctica
Condiciones recuperación	
Observaciones	La evaluación se adaptará a las características de las prácticas realizadas, teniendo en cuenta la consecución de hitos durante la realización de las mismas. Adicionalmente, podrán plantearse cuestiones durante la realización de las prácticas. La asistencia a las prácticas en el laboratorio es obligatoria.

Final teórico-practico	Examen escrito	Sí	Sí	55,00

Calif. mínima	4,00
Duración	3 horas
Fecha realización	Al finalizar la asignatura, en la fecha que establezca la dirección de la escuela
Condiciones recuperación	En la convocatoria extraordinaria de Septiembre
Observaciones	El examen incluirá cuestiones relativas a los conceptos impartidos durante las sesiones teóricas y de laboratorio. El examen se realizará sin apuntes y podrá incluir tanto cuestiones a desarrollar como preguntas tipo test.

TOTAL	100,00

Observaciones

La realización de las prácticas es obligatoria.

La nota final de la asignatura se obtiene aplicando la siguiente fórmula, en la que TEOR es la nota de teoría y PRAC la de prácticas:

NOTA_FINAL = TEOR * 0.75 + PRAC * 0.25

La nota teórica TEOR se calculará partir de las calificaciones de las pruebas de seguimiento Evaluación Continua (EC) y de la del Examen Final (EF). En cualquier caso, será necesario obtener un 4.0 en dicho examen. Además, la nota de la EC no damnificará la calificación final, resultando por tanto:

TEOR = max{ 0.75 * EF + 0.25 * EC ; EF}

Las pruebas de evaluación continua tienen como objetivo que el alumno siga la asignatura de manera continuada y no en intervalos marcados por las evaluaciones. Por ello, solo se podrán consultar las notas de dichas pruebas durante la revisión de exámenes fijada tras el examen final.

Observaciones para alumnos a tiempo parcial

La evaluación continua no es de carácter obligatorio; los alumnos que no la hagan tendrán su calificación de la parte de Evaluación en Laboratorio y Examen Final.

8. BIBLIOGRAFÍA Y MATERIALES DIDÁCTICOS

BÁSICA
W. Stallings, L. Brown, Computer Security: Principles and Practice, Prentice Hall, 2007
S. Northcutt et all, Inside Network Perimeter Security: The Definitive Guide to Firewalls, Virtual Private Networks (VPNs), Routers, and Intrusion Detection Systems, Sams, 2005

Complementaria
D. W. Davies, W. L. Price, Security for Computer Networks, Wiley, 1989
Charles P. Pfleeger, Shari Lawrence Pfleeger, Security in computing, Prentice Hall, 2003
E. Rescorla, SSL and TLS: Designing and Building Secure Systems, Reading, MA: Addison-Wesley, 2000
C. Adams, S. Lloyd., Understanding PKI: Concepts, Standards, and Deployment Considerations, Addison Wesley, 2002
L. Spitzner, Honeypots: Tracking Hackers, Addison Wesley
J. Pastor et all, Criptografía Digital: Fundamentos y aplicaciones, 1999
Recomendaciones de la ITU RFC (Request for Comments) de la IETF

9. SOFTWARE

PROGRAMA / APLICACIÓN	CENTRO	PLANTA	SALA	HORARIO
OpenSSL: The Open Source toolkit for SSL/TLS	ETSIIT	+1	106/128	Lab. Telemática

10. COMPETENCIAS LINGÜÍSTICAS

☑ Comprensión escrita ☐ Comprensión oral
☐ Expresión escrita ☐ Expresión oral
☐ Asignatura íntegramente desarrollada en inglés

Observaciones