GUÍA DOCENTE ABREVIADA DE LA ASIGNATURA

G1498 - Seguridad en Redes de Comunicación

Grado en Ingeniería de Tecnologías de Telecomunicación

Curso Académico 2019-2020

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

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.

6. ORGANIZACIÓN DOCENTE

	CONTENIDOS
1	Tema I: INTRODUCCIÓN A LA SEGURIDAD EN REDES. Concepto de seguridad. Terminología. Política de seguridad. Seguridad lógica, física y personal. Riesgos y vulnerabilidades
2	Tema II: AUTENTICACIÓN Y GESTIÓN DE CLAVES. Introducción a los servicios de autenticación. Autenticación criptográfica. Kerberos. Certificación digital. Infraestructura de clave pública.
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).
4	Tema IV: CONTROL DE ACCESO Y SEGURIDAD PERIMETRAL. Control de acceso, protocolos de identificación, autorización y autenticación. Arquitecturas y configuración de cortafuegos.

7. MÉTODOS DE LA EVALUACIÓN

Descripción	Tipología	Eval. Final	Recuper.	%
Evaluación Continua	Otros	No	Sí	17,00
Laboratorio	Evaluación en laboratorio	Sí	No	30,00
Final teórico-practico	Examen escrito	Sí	Sí	53,00
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 * 0.7 + PRAC * 0.3

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

Esta es la Guía Docente abreviada de la asignatura. Tienes también publicada en la Web la información más detallada de la asignatura en la Guía Docente Completa.