UNIVERSIDAD DE CASTILLA - LA MANCHA

GUÍA DOCENTE

1. DATOS GENERALES

Asignatura:	SEGURIDAD EN LAS COMUNICACIONES	**Código:**	59664
Tipología:	OPTATIVA	**Créditos ECTS:**	6
Grado:	385 - GRADO EN INGENIERÍA DE TECNOLOGÍAS DE TELECOMUNICACIÓN	**Curso académico:**	2018-19
Centro:	308 - ESCUELA POLITECNICA DE CUENCA	**Grupo(s):**	30
Curso:	4	**Duración:**	Primer cuatrimestre
Lengua principal de impartición:	Español	**Segunda lengua:**	
Uso docente de otras lenguas:		**English Friendly:**	S
Página web:	Campus Virtual: campusvirtual.uclm.es	**Bilingüe:**	N

Profesor: **JOSE ANTONIO BALLESTEROS GARRIDO** - Grupo(s): **30**

Edificio/Despacho	Departamento	Teléfono	Correo electrónico	Horario de tutoría
E. Politécnica Cuenca (2.16)	INGENIERÍA ELÉCTRICA, ELECTRÓNICA, AUTOMÁTICA Y COMUNICACIONES	926053863	josea.ballesteros@uclm.es	

2. REQUISITOS PREVIOS

Se recomienda haber cursado con aprovechamiento las asignaturas "Redes de Comunicaciones I", "Redes de Comunicaciones II" y "Procesado y Transmisión".

3. JUSTIFICACIÓN EN EL PLAN DE ESTUDIOS, RELACIÓN CON OTRAS ASIGNATURAS Y CON LA PROFESIÓN

La seguridad en las comunicaciones es una de las ramas con mayor demanda laboral tanto en el sector privado como en el público, fruto del aumento de los ciberataques a particulares, compañías, administraciones, estados, etc.

4. COMPETENCIAS DE LA TITULACIÓN QUE LA ASIGNATURA CONTRIBUYE A ALCANZAR

Competencias propias de la asignatura

Código	Descripción
E26	Capacidad para 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 sistemas de transmisión.
E31	Capacidad para analizar, codificar, procesar y transmitir información multimedia empleando técnicas de procesado analógico y digital de señal.
G02	Una correcta comunicación oral y escrita.
G06	Conocimiento de materias básicas y tecnologías, que le capacite para el aprendizaje de nuevos métodos y tecnologías, así como que le dote de una gran versatilidad para adaptarse a nuevas situaciones.
G07	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 en el ámbito de las tecnología específicas de Sonido e Imagen y/o de Sistemas de Telecomunicación.
G08	Conocimientos para la realización de mediciones, cálculos, valoraciones, tasaciones, peritaciones, estudios, informes, planificación de tareas y otros trabajos análogos en su ámbito específico de la telecomunicación.
G13	Capacidad de buscar y entender información, tanto técnica como comercial, en varias fuentes, relacionarla y estructurarla para integrar ideas y conocimientos. Análisis, síntesis y puesta en práctica de ideas y conocimientos.

5. OBJETIVOS O RESULTADOS DE APRENDIZAJE ESPERADOS

Resultados de aprendizaje propios de la asignatura

Descripción

Análisis, síntesis y comprensión de documentación técnica y dominio del vocabulario específico.

Conocimiento y respecto de la ética y deontología profesional.

Aplicación de los sistemas de telecomunicación en ámbitos diversos de la ingeniería.

Uso correcto de la expresión oral y escrita para transmitir ideas, tecnologías, resultados, etc.

Uso de las TICs para alcanzar los objetivos específicos fijados en la materia.

Síntesis de capacidades de varios ámbitos de la ingeniería de telecomunicaciones.

6. TEMARIO

Tema 1: Introducción

- **Tema 1.1** Marco Legal
- **Tema 1.2** Introducción a los ciberataques
- **Tema 1.3** Aplicaciones de la criptografía

Tema 2: Pentesting

Tema 2.1 Introducción al pentesting
Tema 2.2 Recolección de información
Tema 2.3 Confeccionando el ataque
Tema 2.4 Recomendaciones del proceso
Tema 2.5 Realización del informe
Tema 2.6 Dispositivos de pentesting
Tema 2.7 Ejemplo Práctico: Pentesting Web

Tema 3: OSINT y Hacking con buscadores
Tema 3.1 OSINT
Tema 3.2 Google hacking
Tema 3.3 Bing hacking
Tema 3.4 Shodan

Tema 4: Ataques en redes de datos
Tema 4.1 Seguridad en redes de área local
Tema 4.2 Seguridad en redes WiFi

Tema 5: Prácticas
Tema 5.1 Uso de técnicas criptográficas
Tema 5.2 Herramientas de Pentesting
Tema 5.3 Pentesting Web
Tema 5.4 Investigación con técnicas OSINT y Hacking con Buscadores
Tema 5.5 Ataques en redes de datos
Tema 5.6 Ataques en redes WiFi

COMENTARIOS ADICIONALES SOBRE EL TEMARIO

Software: Packet Tracer, Kali linux.

Equipos: Router, Switch, dispositivos de pentesting.

7. ACTIVIDADES O BLOQUES DE ACTIVIDAD Y METODOLOGÍA

Actividad formativa	Metodología	Competencias relacionadas (para títulos anteriores a RD 822/2021)	ECTS	Horas	Ev	Ob	Rec	Descripción
Enseñanza presencial (Teoría) [PRESENCIAL]	Método expositivo/Lección magistral	E26 E31 G02 G06 G08	0.75	18.75	N	-	-	
Resolución de problemas o casos [PRESENCIAL]	Resolución de ejercicios y problemas	E31 G02 G06 G07 G08	0.7	17.5	S	N	S	
Elaboración de informes o trabajos [AUTÓNOMA]	Resolución de ejercicios y problemas	E31 G02 G06 G07 G08	1	25	S	N	S	
Prácticas de laboratorio [PRESENCIAL]	Prácticas	E26 E31 G02 G06 G07 G08 G13	0.7	17.5	S	N	N	
Elaboración de memorias de Prácticas [AUTÓNOMA]	Prácticas	E26 E31 G02 G06 G07 G08 G13	0.5	12.5	S	N	N	
Estudio o preparación de pruebas [AUTÓNOMA]		E26 E31 G02 G06 G07 G08 G13	2.1	52.5	N	-	-	
Tutorías individuales [PRESENCIAL]		E26 E31 G02 G06 G07 G08 G13	0.08	2	N	-	-	
Pruebas de progreso [PRESENCIAL]	Pruebas de evaluación	E26 E31 G02 G06 G07 G08 G13	0.17	4.25	S	N	S	Las pruebas de progreso consistirán en un exámen práctico (CTF) y un exámen de teoría
		Total:	**6**	**150**				
		Créditos totales de trabajo presencial: 2.4						**Horas totales de trabajo presencial: 60**
		Créditos totales de trabajo autónomo: 3.6						**Horas totales de trabajo autónomo: 90**

Ev: Actividad formativa evaluable
Ob: Actividad formativa de superación obligatoria
Rec: Actividad formativa recuperable

8. CRITERIOS DE EVALUACIÓN Y VALORACIONES

	Valoraciones		
Sistema de evaluación	**Estudiante presencial**	**Estud. semipres.**	**Descripción**
Resolución de problemas o casos	10.00%	0.00%	Recogida de una o más entregas durante el semestre
Realización de prácticas en laboratorio	65.00%	0.00%	Se tendrán en cuenta tanto el trabajo desarrollado en el laboratorio (observación directa), así como las memorias entregadas que resuman el mismo e incluso la presentación oral de las prácticas.
Pruebas de progreso	25.00%	0.00%	Consistirán en un exámen práctico (CTF) y un exámen de teoría
Total:	**100.00%**	**0.00%**	

Criterios de evaluación de la convocatoria ordinaria:
Los indicados en la tabla de 'valoraciones'.

Particularidades de la convocatoria extraordinaria:

Las prácticas de laboratorio no son recuperables. Se podrán recuperar las 'pruebas de progreso' mediante un examen práctico (CTF) y otro teórico en la fecha que fije la subdirección de estudios y la 'resolución de problemas o casos' mediante la entrega de lo que se indique antes de la fecha mencionada. Se aplicarán las mismas ponderaciones que en la convocatoria ordinaria.

Particularidades de la convocatoria especial de finalización:

Para la convocatoria de especial finalización el alumno deberá tener el laboratorio aprobado el curso anterior y los criterios de evaluación serán 70% laboratorio y 30% la prueba de progreso

9. SECUENCIA DE TRABAJO, CALENDARIO, HITOS IMPORTANTES E INVERSIÓN TEMPORAL

No asignables a temas

Horas	Suma horas
Estudio o preparación de pruebas [AUTÓNOMA][]	52.5
Tutorías individuales [PRESENCIAL][]	2
Pruebas de progreso [PRESENCIAL][Pruebas de evaluación]	4.25

Comentarios generales sobre la planificación: Los temas se impartirán secuencialmente. La duración de las actividades puede sufrir ligeras variaciones.

Tema 1 (de 5): Introducción

Actividades formativas	Horas
Enseñanza presencial (Teoría) [PRESENCIAL][Método expositivo/Lección magistral]	4
Resolución de problemas o casos [PRESENCIAL][Resolución de ejercicios y problemas]	3.5
Elaboración de informes o trabajos [AUTÓNOMA][Resolución de ejercicios y problemas]	5

Tema 2 (de 5): Pentesting

Actividades formativas	Horas
Enseñanza presencial (Teoría) [PRESENCIAL][Método expositivo/Lección magistral]	4
Resolución de problemas o casos [PRESENCIAL][Resolución de ejercicios y problemas]	3.5
Elaboración de informes o trabajos [AUTÓNOMA][Resolución de ejercicios y problemas]	5

Tema 3 (de 5): OSINT y Hacking con buscadores

Actividades formativas	Horas
Enseñanza presencial (Teoría) [PRESENCIAL][Método expositivo/Lección magistral]	4
Resolución de problemas o casos [PRESENCIAL][Resolución de ejercicios y problemas]	3.5
Elaboración de informes o trabajos [AUTÓNOMA][Resolución de ejercicios y problemas]	5

Tema 4 (de 5): Ataques en redes de datos

Actividades formativas	Horas
Enseñanza presencial (Teoría) [PRESENCIAL][Método expositivo/Lección magistral]	6.75
Resolución de problemas o casos [PRESENCIAL][Resolución de ejercicios y problemas]	7
Elaboración de informes o trabajos [AUTÓNOMA][Resolución de ejercicios y problemas]	10

Tema 5 (de 5): Prácticas

Actividades formativas	Horas
Prácticas de laboratorio [PRESENCIAL][Prácticas]	17.5
Elaboración de memorias de Prácticas [AUTÓNOMA][Prácticas]	12.5

Actividad global

Actividades formativas	Suma horas
Enseñanza presencial (Teoría) [PRESENCIAL][Método expositivo/Lección magistral]	18.75
Resolución de problemas o casos [PRESENCIAL][Resolución de ejercicios y problemas]	17.5
Elaboración de informes o trabajos [AUTÓNOMA][Resolución de ejercicios y problemas]	25
Prácticas de laboratorio [PRESENCIAL][Prácticas]	17.5
Elaboración de memorias de Prácticas [AUTÓNOMA][Prácticas]	12.5
Estudio o preparación de pruebas [AUTÓNOMA][]	52.5
Tutorías individuales [PRESENCIAL][]	2
Pruebas de progreso [PRESENCIAL][Pruebas de evaluación]	4.25
Total horas:	150

10. BIBLIOGRAFÍA, RECURSOS

Autor/es	Título/Enlace Web	Editorial	Población	ISBN	Año	Descripción
González Pérez, Pablo (1976-)	Ethical Hacking : Teoría y práctica para la realización de u	OxWord Computing,		978-84-617-0576-4	2014	
González Pérez, Pablo (1976-)	Pentesting con Kali 2.0 /	0xWORD Computing,		978-84-608-3207-2	2015	
Molenaar, René	How to master CCNA	GNS3 Vault		978-1482364873	2013	
Ramos Varón, Antonio Ángel	Hacking práctico de redes wifi y radiofrecuencia /	Ra-Ma,		978-84-9964-296-3	2015	
Ramos Varón, Antonio Ángel	Seguridad perimetral, monitorización y ataques en redes /	Ra-Ma,		978-84-9964-297-0	2014	
Rando González, Enrique.	Hacking con buscadores : Google, Bing & Shodan /	ZeroXword Computing,		978-84-616-7589-0	2014	