

FICHA TÉCNICA DE LA ASIGNATURA

Datos de la asignatura	
Nombre completo	Seguridad en Sistemas de Comunicación
Código	DTC-MIT-512
Título	Máster Universitario en Ingeniería de Telecomunicación por la Universidad Pontificia Comillas
Impartido en	Grado en Administración y Dirección de Empresas y Máster Univ. en Ingeniería de Telecomunicación [Quinto Curso] Máster Universitario en Ingeniería de Telecomunicación [Primer Curso] Máster Universitario en Ingeniería de Telecomunicación y Máster en Ciberseguridad [Primer Curso] Máster Universitario en Ingeniería de Telecomunicación y Mást. Univ. en Administración de Empresas [Primer Curso] Máster Universitario en Ingeniería de Telecomunicación + Máster Big Data.Tecnología y Anal. Avanzada [Primer Curso]
Nivel	Postgrado Oficial Master
Cuatrimestre	Semestral
Créditos	4,5 ECTS
Carácter	Obligatoria
Departamento / Área	Departamento de Telemática y Computación
Responsable	Rafael Palacios Hielscher
Horario de tutorías	Contactar por email con el profesor

Datos del profesorado	
Profesor	
Nombre	Ángel Prado Montes
Departamento / Área	Departamento de Telemática y Computación
Correo electrónico	aprado@comillas.edu
Profesor	
Nombre	Javier Jarauta Sánchez
Departamento / Área	Departamento de Telemática y Computación
Correo electrónico	jarauta@comillas.edu

DATOS ESPECÍFICOS DE LA ASIGNATURA

Contextualización de la asignatura
Prerequisitos
Conocimientos de redes, aplicaciones web y criptografía básica.
Conocimientos de programación para algunas prácticas y ejercicios de clase.



Competencias - Objetivos

Competencias

GENERALES

CB03	Saber evaluar y seleccionar la teoría científica adecuada y la metodología precisa de sus campos de estudio para formular juicios a partir de información incompleta o limitada incluyendo, cuando sea preciso y pertinente, una reflexión sobre la responsabilidad social o ética ligada a la solución que se proponga en cada caso
CB04	Ser capaces de predecir y controlar la evolución de situaciones complejas mediante el desarrollo de nuevas e innovadoras metodologías de trabajo adaptadas al ámbito científico/investigador, tecnológico o profesional concreto, en general multidisciplinar, en el que se desarrolle su actividad.
CB05	Saber transmitir de un modo claro y sin ambigüedades a un público especializado o no, resultados procedentes de la investigación científica y tecnológica o del ámbito de la innovación más avanzada, así como los fundamentos más relevantes sobre los que se sustentan
CG02	Capacidad para la dirección de obras e instalaciones de sistemas de telecomunicación, cumpliendo la normativa vigente, asegurando la calidad del servicio
CG03	Capacidad para dirigir, planificar y supervisar equipos multidisciplinarios
CG07	Capacidad para la puesta en marcha, dirección y gestión de procesos de fabricación de equipos electrónicos y de telecomunicaciones, con garantía de la seguridad para las personas y bienes, la calidad final de los productos y su homologación
CG09	Capacidad para comprender la responsabilidad ética y la deontología profesional de la actividad de la profesión de Ingeniero de Telecomunicación

ESPECÍFICAS

CGT02	Capacidad para la elaboración, dirección, coordinación, y gestión técnica y económica de proyectos sobre: sistemas, redes, infraestructuras y servicios de telecomunicación, incluyendo la supervisión y coordinación de los proyectos parciales de su obra aneja; infraestructuras comunes de telecomunicación en edificios o núcleos residenciales, incluyendo los proyectos sobre hogar digital; infraestructuras de telecomunicación en transporte y medio ambiente; con sus correspondientes instalaciones de suministro de energía y evaluación de las emisiones electromagnéticas y compatibilidad electromagnética
CTT07	Capacidad para realizar la planificación, toma de decisiones y empaquetamiento de redes, servicios y aplicaciones considerando la calidad de servicio, los costes directos y de operación, el plan de implantación, supervisión, los procedimientos de seguridad, el escalado y el mantenimiento, así como gestionar y asegurar la calidad en el proceso de desarrollo

Resultados de Aprendizaje

RA01	Conocer las tecnologías empleadas para realizar ataques, y medidas para prevenirlas
RA02	Conocer de los sistemas de gestión de la seguridad de la información y como evaluar medidas de protección teniendo en cuenta eficacia y coste



RA03	Conocer las estrategias, políticas y tecnologías de gobierno de la seguridad y saber aplicarlas en el diseño de una política de seguridad.
RA04	Conocer las certificaciones y estándares actuales de la seguridad así como las entidades internacionales de acreditación de la seguridad

BLOQUES TEMÁTICOS Y CONTENIDOS

Contenidos – Bloques Temáticos

- Capítulo 1: Introducción y visión general
- Capítulo 2: Detalles tecnológicos sobre HTTP/HTTPS y los navegadores
- Capítulo 3: Arquitecturas de seguridad y Metodologías de Análisis de la Seguridad
- Capítulo 4: Ataques contra la capa de aplicación, y defensas
- Capítulo 5: Amenazas Persistentes Avanzadas, Vulnerabilidad web habituales, y pruebas de intrusión (pentest)
- Capítulo 6: Ataques contra SSL/HTTPS y defensas
- Capítulo 7: Ataques avanzados de canal lateral (side-channel)
- Capítulo 8: Seguridad en aplicaciones móviles
- Capítulo 9: Sistemas de gestión de la seguridad
- Capítulo 10: Monitorización y Análisis forense
- Capítulo 11: Políticas y gobierno de la seguridad (Planes de Continuidad de Negocio)
- Capítulo 12: Confianza y cumplimiento de la legislación (certificación y estándares)
- Capítulo 13: Conclusiones, Conferencia invitada, Debate sobre actualidad en seguridad

METODOLOGÍA DOCENTE

Aspectos metodológicos generales de la asignatura

Metodología Presencial: Actividades

Clase magistral y presentaciones generales (25 horas presenciales). Exposición de los principales conceptos y procedimientos mediante la explicación por parte del profesor. Incluirá presentaciones dinámicas, pequeños ejemplos prácticos y la participación reglada o espontánea de los estudiantes.

CB03, CB04, CG02, CG03, CG07, CG09, CTT07

Prácticas de laboratorio (20 horas presenciales). Cada alumno realizará de forma aislada o en grupo una serie de prácticas de laboratorio regladas. Las prácticas de laboratorio finalizarán con la redacción de un informe de laboratorio o la inclusión de las distintas experiencias en un cuaderno de laboratorio.

CB05, CGT02

Metodología No presencial: Actividades

Estudio individual del material (40 horas no presenciales). Actividad realizada individualmente por el estudiante cuando analiza, busca e interioriza la información que aporta la materia y que será discutida con sus compañeros y el profesor en clases posteriores.

CB03, CG07, CG09, CTT07, CGT02



Resolución de problemas prácticos a resolver fuera del horario de clase por parte del alumno (20 horas no presenciales). El alumno debe utilizar e interiorizar los conocimientos aportados en la materia. La corrección a la clase se realizará por parte de alguno de los alumnos o el profesor según los casos. La corrección individualizada de cada ejercicio la realizará el propio alumno u otro compañero según los casos (método de intercambio).

CB03, CB04, CB05, CG02, CG03, CG07, CG09, CTT07, CGT02

Trabajos de carácter práctico individual o en grupo (30 horas no presenciales). Actividades de aprendizaje que se realizarán de forma individual fuera del horario lectivo, que requerirán algún tipo de investigación o la lectura de distintos textos.

CB03, CB04, CG09, CTT07

RESUMEN HORAS DE TRABAJO DEL ALUMNO

HORAS PRESENCIALES		
Clase magistral y presentaciones generales	Prácticas de laboratorio	
25.00	20.00	
HORAS NO PRESENCIALES		
Estudio y resolución de problemas prácticos a resolver fuera del horario de clase por parte del alumno	Estudio individual del material	Trabajos de carácter práctico individual y de grupo
20.00	40.00	30.00
CRÉDITOS ECTS: 4,5 (135,00 horas)		

EVALUACIÓN Y CRITERIOS DE CALIFICACIÓN

Actividades de evaluación	Criterios de evaluación	Peso
Examen Final (50%) Pruebas intermedias (20%)	<ul style="list-style-type: none"> Comprensión de conceptos. Aplicación de conceptos a la resolución de problemas prácticos. Tener en cuenta todos los aspectos críticos de seguridad. 	70
Prácticas: Trabajos de carácter práctico individual o en grupo. Participación activa en clase	<ul style="list-style-type: none"> Comprensión de conceptos. Aplicación de conceptos a la resolución de problemas prácticos. Tener en cuenta todos los aspectos críticos de seguridad. 	30

Calificaciones

Convocatoria Ordinaria

La calificación en la convocatoria ordinaria de la asignatura se obtendrá como:

- Un 70% la calificación de los exámenes.
 - 50% de la nota final en la asignatura



- 20% de la nota será la de pruebas intermedias.
- Un 30% será la nota de trabajos prácticos y participación en clase

No hay nota mínima en el examen final de la asignatura.

Convocatoria Extraordinaria

- Un 80% la nota del examen de la convocatoria extraordinaria.
- Un 20% la nota de trabajos de carácter práctico individual.

PLAN DE TRABAJO Y CRONOGRAMA

Actividades	Fecha de realización	Fecha de entrega
Prácticas de laboratorio y elaborar informe	Después de las clases prácticas	
Lectura y estudio de contenidos teóricos	Después de las clases teóricas	
Preparación de pruebas a realizar en tiempo de clase	Durante varios días antes de la clase	
Preparación del examen final	Durante varios días antes del examen	

BIBLIOGRAFÍA Y RECURSOS

Bibliografía Básica

- John Vacca, *Managing Information Security*. 2nd edition. Ed. Syngress. (2014).
- Michael Zalewski, *The Tangled Web. A guide to securing modern web applications*. Ed. No Starch Press (2012).

Bibliografía Complementaria

Colección de artículos que se actualizan en Moodle de la asignatura.

En cumplimiento de la normativa vigente en materia de **protección de datos de carácter personal**, le informamos y recordamos que puede consultar los aspectos relativos a privacidad y protección de datos [que ha aceptado en su matrícula](#) entrando en esta web y pulsando "descargar"

<https://servicios.upcomillas.es/sedelectronica/inicio.aspx?csv=02E4557CAA66F4A81663AD10CED66792>