COMILLAS
UNIVERSIDAD PONTIFICIA
ICAI ICADE CIHS

GUÍA DOCENTE
2018 - 2019

FICHA TÉCNICA DE LA ASIGNATURA

Datos de la asignatura	
NombreCompleto	Seguridad en sistemas de comunicación
Código	DTC-TEL-612
Título	Máster Universitario en Ingeniería de Telecomunicación
Impartido en	Máster Universitario en Ingeniería de Telecomunicación [Segundo Curso] Máster Universitario en Ingeniería de Telecomunicación y Mást. Univ. en Administración de Empresas [Segundo Curso] Máster Universitario en Ingeniería de Telecomunicación + Máster Big Data.Tecnología y Anal. Avanzada [Segundo Curso]
Nivel	Postgrado Oficial Master
Cuatrimestre	Semestral
Créditos	4,5
Carácter	Obligatoria
Departamento / Área	Departamento de Telemática y Computación
Responsable	Rafael Palacios Hielscher
Horario	Mañana y Tarde
Horario de tutorías	Pedir hora a los profesores

Datos del profesorado	
Profesor	
Nombre	Ángel Prado Montes
Departamento / Área	Departamento de Telemática y Computación
Correo electrónico	aprado@comillas.edu
Profesor	
Nombre	Rafael Palacios Hielscher
Departamento / Área	Departamento de Telemática y Computación
Despacho	Alberto Aguilera 25 [Dirección]
Correo electrónico	Rafael.Palacios@iit.comillas.edu

DATOS ESPECÍFICOS DE LA ASIGNATURA

Contextualización de la asignatura

Prerrequisitos

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 multidisciplinares.
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	
RA1	Conocer las tecnologías de los sistemas de gestión de la seguridad de la información
RA2	Conocer las estrategias, políticas y tecnologías de gobierno de la seguridad y saber aplicarlas en el diseño de una política segura de comunicaciones.
RA3	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

1.1 Ciberseguridad en 2015

1.2 Brechas de seguridad destacables

1.3 Cómo es el día del personal de seguridad

Capítulo 2: Detalles tecnológicos aobre http, https y de los navegadores

2.1 Anatomía de Internet

2.2 Peticiones y respuestas en HTTP

2.3 Sesiones y cookies

2.4 Características de seguridad del navegador. HTTPS

2.5 Políticas de origen común

2.6 Codificación de entidad y JavaScript

2.7 Características nuevas de HTML5

2.8 Peticiones entre dominios (cross-domain)

2.9 Mensajes POST y almacenamiento local

2.10 Privacidad en el navegador. Identificación del navegador (Fingerprinting). Modo privado

Capítulo 3: Modelo de amenaza y pruebas de penetración

3.1 Modelado de vectores de ataque

3.2 Amenazas y estrategias de defensa

3.3 Revisión de código y análisis de tráfico

3.4 Ciclo de vida de desarrollo seguro

3.5 El modelo STRIDE

Capítulo 4: Vulnerabilidad web habituales

4.1 OWASP top 10

4.2 Cross-Site Scripting (XSS)

4.3 Cross-Site Remote Forgery (CSRF)

4.4 Ataques de XML external entity

4.5 Robo de clicks (Clickjacking)

4.6 Redirecciones abiertas

4.7 Inyección SQL

4.8 Inyección SQL ciega

4.9 Denegación de servicio

4.10 Ataques Mutation XSS (mXSS)

4.11 Ejecución de origen común

Capítulo 5: Ataques contra la capa de aplicación

5.1 Referencias inseguras a objetos

5.2 Configuraciones inseguras

5.3 Autenticación vulnerable

5.4 Gestión de sesión vulnerable

5.5 Autorización vulnerable

5.6 Ataques RTL (Right to Left)

5.7 Ataques con CAPTCHA

5.8 Aprovechamiento de los Metadatos públicos

5.9 Contraseñas débiles

5.10 Redirección de DNS

Capítulo 6: Ataques contra SSL

6.1 SSL stripping

6.2 Mezcla de contenidos HTTPS y HTTP

6.3 Cómo evitar la seguridad de transporte HSTS

6.4 BREACH

6.5 LUCKY 13

6.6 RC4 biases

6.7 POODLE

6.8 Heartbleed

Capítulo 7: Ataques avanzados de canal lateral (side-channel)

7.1 BEAST

7.2 Ataques por hora y caché

7.3 Ataques haciendo uso de Unicode

7.4 Inspección de contenido y políglotas

7.5 Rosetta Flash

7.6 SMB relay

7.7 Estimar la localización (geoinference)

Capítulo 8: Seguridad en aplicaciones móviles

8.1 El modelo de las sandbox

8.2 Visión global de la seguridad en Android

8.3 Visión global de la seguridad en iOS

8.4 Gestión de dispositivos móviles (Mobile Device Management MDM)

8.5 Comprobación de aplicaciones móviles

8.6 Pinning de certificados

Capítulo 9: Sistemas de gestión de la seguridad

9.1 Estándares de gestión

9.2 Políticas de seguridad

9.3 Controles de seguridad

9.4 Acceso a la red

9.5 Gestión de identidades

9.6 Valoración del riesgo. Criterios técnicos y económicos

Capítulo 10: Mejora continua. Sistemas de vigilancia y análisis forense

10.1 Sistemas de prevención y de detección de intrusiones

10.2 Cortafuegos de red

10.3 Análisis forense

10.4 Detección de anomalías

10.5 Respuesta a incidencias

10.6 Gestión de crisis

10.7 Amenazas Persistentes Avanzadas (APT)

Capítulo 11: Políticas y gobierno de la seguridad

11.1 Integridad del negocio

11.2 Gestión de la privacidad

11.3 Prevención del fraude

11.4 Gestión de las amenazas y vulnerabilidades

11.5 Planes de continuidad de negocio

11.6 Políticas de seguridad de la información empresarial

Capítulo 12: Confianza y cumplimiento de la legislación

12.1 Introducción a la certificación y los estándares

12.2 PCI DSS , FISMA, GLBA, SOX, ISO 27001 and HIPAA

12.3 Ley de protección de datos de España (LOPD)

12.4 Iniciativas comunes de seguridad en la Unión Europea

12.5 Residencia de los datos y cuestiones de privacidad de la información

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
Resolución en clase de problemas prácticos(5 horas presenciales). Resolución de unos primeros problemas para situar al alumno en contexto. La resolución correrá a cargo del profesor y los alumnos de forma cooperativa.	CB05
Resolución grupal de problemas(5 horas presenciales). El profesor planteará pequeños problemas que los alumnos resolverán en pequeños grupos en clase y cuya solución discutirán con el resto de grupos.	CB05, CTT07
Prácticas de laboratorio(10 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(45 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, 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).	CB05, CGT02
Trabajos de carácter práctico individual o en grupo(25 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.	CB05, CGT02

RESUMEN HORAS DE TRABAJO DEL ALUMNO

HORAS PRESENCIALES			
Clase magistral y presentaciones generales	Resolución en clase de problemas prácticos	Prácticas de laboratorio	Resolución grupal de problemas
25,00	5,00	10,00	5,00
HORAS NO PRESENCIALES			
Trabajos de carácter práctico individual	Estudio y resolución de problemas prácticos fuera del horario de clase por parte del alumno	Estudio individual del material	
25,00	20,00	45,00	
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%)	• Comprensión de conceptos. • Aplicación de conceptos a la resolución de problemas prácticos. • Tener en cuenta todos los aspectos críticos de seguridad. • Presentación y comunicación escrita.	70 %
Prácticas: Trabajos de carácter práctico individual.	• Comprensión de conceptos. • Aplicación de conceptos a la resolución de problemas prácticos. • Tener en cuenta todos los aspectos críticos de seguridad.	30 %

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 cases 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.2ndedition 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.