

ANX-PR/CL/001-01
GUÍA DE APRENDIZAJE

ASIGNATURA

Seguridad en sistemas y redes de telecomunicación.

CURSO ACADÉMICO - SEMESTRE

2016-17 - Primer semestre

Datos Descriptivos

Nombre de la Asignatura	Seguridad en sists y redes de telec.
Titulación	09TT - Grado en Ingeniería de Tecnologías y Servicios de Telecomunicación
Centro responsable de la titulación	Escuela Técnica Superior de Ingenieros de Telecomunicación
Semestre/s de impartición	Séptimo semestre
Módulos	Mod tecnol esp telematica
Materias	Tecnología específica telematica
Carácter	Optativa
Código UPM	95000051
Nombre en inglés	Security in telecommunication networks and systems

Datos Generales

Créditos	4.5	Curso	4
Curso Académico	2016-17	Período de impartición	Septiembre-Enero
Idioma de impartición	Castellano	Otros idiomas de impartición	

Requisitos Previos Obligatorios

Asignaturas Previas Requeridas

El plan de estudios Grado en Ingeniería de Tecnologías y Servicios de Telecomunicación no tiene definidas asignaturas previas superadas para esta asignatura.

Otros Requisitos

El plan de estudios Grado en Ingeniería de Tecnologías y Servicios de Telecomunicación no tiene definidos otros requisitos para esta asignatura.

Conocimientos Previos

Asignaturas Previas Recomendadas

Redes de ordenadores

Otros Conocimientos Previos Recomendados

El coordinador de la asignatura no ha definido otros conocimientos previos recomendados.

Competencias

CE-TL2 - 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

CE-TL3 - Capacidad de construir, explotar y gestionar servicios telemáticos utilizando herramientas analíticas de planificación, de dimensionado y de análisis

CE-TL4 - Capacidad de describir, programar, validar y optimizar protocolos e interfaces de comunicación en los diferentes niveles de una arquitectura de redes

CE-TL6 - Capacidad de diseñar arquitecturas de redes y servicios telemáticos

Resultados de Aprendizaje

RA466 - Comprender los distintos mecanismos de seguridad basados en control de acceso: autenticación y defensa perimetral.

RA467 - Comprender y analizar distintos protocolos de seguridad, y cómo se aplican las técnicas criptográficas en las comunicaciones

RA83 - Capacidad de diseñar, desplegar y gestionar arquitecturas de redes y servicios telemáticos, en redes de acceso, troncales y privadas, tanto en entornos fijos como móviles, utilizando herramientas de análisis y dimensionado de red.

RA464 - Conocer el funcionamiento de las amenazas técnicas y humanas a la seguridad de las redes y sistemas de telecomunicación

RA465 - Categorizar adecuadamente los distintos servicios de seguridad para redes y sistemas, en función de los activos que protegen.

RA86 - Capacidad de aplicar a las redes y servicios de telecomunicación los sistemas de gestión de red y de servicios para la configuración, operación, supervisión y tarificación de los mismos.

RA463 - Conocer las principales técnicas criptográficas simétricas y asimétricas y su aplicación a la seguridad de los sistemas y comunicaciones.

RA87 - Capacidad de gestionar la seguridad de las redes y servicios de telecomunicación mediante la aplicación de tunelado, cortafuegos, protocolos de cifrado y autenticación, y mecanismos de protección de contenidos.

RA461 - Capacidad de comprender la necesidad de introducir la seguridad en las redes y sistemas de telecomunicación como parte integral de su diseño y despliegue.

RA632 - Capacidad de entender y aplicar las principales técnicas de programación segura

Profesorado

Profesorado

Nombre	Despacho	e-mail	Tutorías
Villagra Gonzalez, Victor Abraham (Coordinador/a)	B-217	victor.villagra@upm.es	X - 14:00 - 15:00
Mañas Argemi, Jose Antonio	C-219	joseantonio.manas@upm.es	X - 12:00 - 13:00

Nota.- Las horas de tutoría son orientativas y pueden sufrir modificaciones. Se deberá confirmar los horarios de tutorías con el profesorado.

Personal Investigador en Formación o Similar

Nombre	e-mail	Profesor Responsable
Holgado Ortiz, Maria Del Pilar	mariadelpilar.holgado@upm.es	Villagra Gonzalez, Víctor Abraham

Descripción de la Asignatura

Los objetivos de esta asignatura son:

- Conocer y aplicar las tecnologías que proporcionan seguridad a los sistemas y redes de telecomunicación
- Conocer los fundamentos organizativos y criptográficos en los que se basan las tecnologías de seguridad y su aplicación a la programación y desarrollo de software seguro.

Temario

1. Introducción a la Seguridad
2. Criptografía
3. Firma Electrónica
4. Programación Segura
5. Amenazas de Internet
6. Servicios de Control de Acceso
7. Servicios de Protección de la Comunicación

Cronograma

Horas totales: 71 horas

Horas presenciales: 56 horas (47.9%)

Peso total de actividades de evaluación continua:
100%

Peso total de actividades de evaluación sólo prueba final:
100%

Semana	Actividad Presencial en Aula	Actividad Presencial en Laboratorio	Otra Actividad Presencial	Actividades Evaluación
Semana 1	Tema 1: Introducción y Motivación. Tema 2: Criptografía Duración: 03:00 LM: Actividad del tipo Lección Magistral			
Semana 2	Tema 2: Criptografía Duración: 03:00 LM: Actividad del tipo Lección Magistral			
Semana 3	Tema 2. Criptografía. Tema 3: Firma Digital Duración: 03:00 LM: Actividad del tipo Lección Magistral			Entrega del Trabajo Duración: 03:00 TI: Técnica del tipo Trabajo Individual Evaluación continua Actividad no presencial
Semana 4	Tema 3. Firma Digital Duración: 03:00 LM: Actividad del tipo Lección Magistral			
Semana 5	Tema 4: Programación Segura. Duración: 03:00 LM: Actividad del tipo Lección Magistral			Entrega del Trabajo Duración: 03:00 PI: Técnica del tipo Presentación Individual Evaluación continua Actividad no presencial
Semana 6	Tema 4: Programación Segura. Duración: 03:00 LM: Actividad del tipo Lección Magistral			
Semana 7	Trabajo de Programación Segura Duración: 02:00 PR: Actividad del tipo Clase de Problemas Conferencia Duración: 01:00 OT: Otras actividades formativas			Entrega del Trabajo Duración: 03:00 TG: Técnica del tipo Trabajo en Grupo Evaluación continua Actividad no presencial
Semana 8	Tema 5: Amenazas de Internet Duración: 03:00 LM: Actividad del tipo Lección Magistral			Examen Parcial Duración: 01:00 EX: Técnica del tipo Examen Escrito Evaluación continua Actividad presencial
Semana 9	Tema 6: Sistemas de Control de Acceso Duración: 03:00 LM: Actividad del tipo Lección Magistral			

Semana 10	Tema 6: Sistemas de Control de Acceso Duración: 03:00 LM: Actividad del tipo Lección Magistral			
Semana 11	Tema 6: Sistemas de Control de Acceso Duración: 03:00 LM: Actividad del tipo Lección Magistral			
Semana 12	Tema 8: Servicios de Protección de Comunicaciones Duración: 03:00 LM: Actividad del tipo Lección Magistral			
Semana 13	Tema 8: Servicios de Protección de Comunicaciones Duración: 03:00 LM: Actividad del tipo Lección Magistral	Practica de Explotacion de Vulnerabilidades Duración: 04:00 PL: Actividad del tipo Prácticas de Laboratorio		
Semana 14	Conferencia Duración: 01:00 OT: Otras actividades formativas	Práctica de Configuración de Cortafuegos Duración: 06:00 PL: Actividad del tipo Prácticas de Laboratorio		Evaluación Prácticas de Laboratorio Duración: 06:00 EP: Técnica del tipo Examen de Prácticas Evaluación continua Actividad no presencial
Semana 15			Visita a un Centro de Operación de Seguridad empresarial. (3h) Duración: 03:00 OT: Otras actividades formativas	
Semana 16				
Semana 17				Examen Segunda Parte de Asignatura Duración: 02:00 EX: Técnica del tipo Examen Escrito Evaluación continua Actividad presencial Examen Final Duración: 03:00 EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Actividad presencial

Nota.- El cronograma sigue una planificación teórica de la asignatura que puede sufrir modificaciones durante el curso.

Nota 2.- Para poder calcular correctamente la dedicación de un alumno, la duración de las actividades que se repiten en el tiempo (por ejemplo, subgrupos de prácticas") únicamente se indican la primera vez que se definen.

Actividades de Evaluación

Semana	Descripción	Duración	Tipo evaluación	Técnica evaluativa	Presencial	Peso	Nota mínima	Competencias evaluadas
3	Entrega del Trabajo	03:00	Evaluación continua	TI: Técnica del tipo Trabajo Individual	No	3%	3.5 / 10	CE-TL2
5	Entrega del Trabajo	03:00	Evaluación continua	PI: Técnica del tipo Presentación Individual	No	3%	3.5 / 10	CE-TL2, CE-TL6
7	Entrega del Trabajo	03:00	Evaluación continua	TG: Técnica del tipo Trabajo en Grupo	No	4%	3.5 / 10	CE-TL3
8	Examen Parcial	01:00	Evaluación continua	EX: Técnica del tipo Examen Escrito	Sí	40%	3.5 / 10	CE-TL2, CE-TL3, CE-TL6
14	Evaluación Prácticas de Laboratorio	06:00	Evaluación continua	EP: Técnica del tipo Examen de Prácticas	No	10%	3.5 / 10	CE-TL4, CE-TL2
17	Examen Segunda Parte de Asignatura	02:00	Evaluación continua	EX: Técnica del tipo Examen Escrito	Sí	40%	3.5 / 10	CE-TL4, CE-TL2, CE-TL6
17	Examen Final	03:00	Evaluación sólo prueba final	EX: Técnica del tipo Examen Escrito	Sí	100%	5 / 10	CE-TL4, CE-TL2, CE-TL3, CE-TL6

Criterios de Evaluación

Los alumnos que deseen ser evaluados en convocatoria ordinaria mediante una única prueba final deben expresarlo mediante escrito formalizado en el registro de la ETSI Telecomunicación y dirigido al Director del Departamento no más tarde del 30 de septiembre. La presentación de este escrito supondrá la renuncia automática a la evaluación continua.

CONVOCATORIA ORDINARIA: MODALIDAD EVALUACIÓN CONTINUA

La asignatura se aprobará cuando se obtenga una calificación mayor o igual a 5 puntos sobre un total de 10. La nota final se obtendrá mediante la suma de las calificaciones correspondientes a las diferentes actividades de evaluación, con los siguientes pesos:

- P1: Prueba parcial Bloque 1: 40%
- P2: Prueba parcial Bloque 2: 40%
- E1: Realización y entrega de trabajos (Bloque 1): 10%
- E2: Realización y entrega de prácticas de laboratorio (Bloque 2): 10%

En todos ellos se exige una nota mínima de 3,5 sobre 10.

La materia del bloque 1 será evaluada mediante un examen parcial P1. En caso de obtener menos de 4 puntos o desear subir nota, el alumno deberá presentarse a la recuperación en la convocatoria oficial de examen, renunciando a la nota del primer parcial. Las actividades de realización y entrega de trabajos y prácticas de laboratorio (E1 y E2) solo serán evaluables si se han realizado todas las actividades propuestas en cada una de ellas. En caso de inasistencia o no entrega de alguno de los componentes de cada actividad, se considerará que el alumno no se ha presentado y no podrá seguir la evaluación continua, debiendo optar por evaluación única

CONVOCATORIA ORDINARIA: EVALUACIÓN MEDIANTE UNA ÚNICA PRUEBA FINAL

El 100% de la calificación de los alumnos que presenten el escrito arriba referido se otorgará en función de una única prueba final.

CONVOCATORIA EXTRAORDINARIA



CAMPUS
DE EXCELENCIA
INTERNACIONAL

UNIVERSIDAD POLITÉCNICA DE MADRID

Escuela Técnica Superior de Ingenieros de Telecomunicación

PROCESO DE COORDINACIÓN DE LAS ENSEÑANZAS

ANX-PR/CL/001-01: GUÍA DE APRENDIZAJE



Código PR/CL/001

La evaluación de la asignatura en su convocatoria extraordinaria se realizará mediante una única prueba final, con independencia de la opción elegida en la convocatoria ordinaria.

Recursos Didácticos

Descripción	Tipo	Observaciones
Moodle	Recursos web	Servidor Moodle de la Asignatura
Equipamiento	Equipamiento	Aula, Laboratorio, Sala de Trabajo en Grupo
Referencias	Bibliografía	Bibliografía