ANX-PR/CL/001-01

GUÍA DE APRENDIZAJE

ASIGNATURA

95000051 - Seguridad En Sists Y Redes De Telec.

PLAN DE ESTUDIOS

09TT - Grado En Ingenieria De Tecnologias Y Servicios De Telecomunicacion

CURSO ACADÉMICO Y SEMESTRE

2023/24 - Primer semestre

Índice

Guía de Aprendizaje

1. Datos descriptivos....1
2. Profesorado....1
3. Conocimientos previos recomendados....2
4. Competencias y resultados de aprendizaje....2
5. Descripción de la asignatura y temario....4
6. Cronograma....5
7. Actividades y criterios de evaluación....7
8. Recursos didácticos....10
9. Otra información....10

1. Datos descriptivos

1.1. Datos de la asignatura

Nombre de la asignatura	95000051 - Seguridad en Sists y Redes de Telec.
No de créditos	4.5 ECTS
Carácter	Optativa
Curso	Cuarto curso
Semestre	Séptimo semestre
Período de impartición	Septiembre-Enero
Idioma de impartición	Castellano
Titulación	09TT - Grado en Ingenieria de Tecnologias y Servicios de Telecomunicacion
Centro responsable de la titulación	09 - Escuela Tecnica Superior De Ingenieros De Telecomunicacion
Curso académico	2023-24

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Xavier Andres Larriva Novo	B-423	xavier.larriva.novo@upm.es	X - 14:00 - 15:00
Francisco Faustino Lazaro Anguis	B-217	ff.lazaro@upm.es	X - 11:00 - 12:00
Victor Abraham Villagra Gonzalez	B-217	victor.villagra@upm.es	X - 14:00 - 15:00

Andres Isaac Marin Lopez (Coordinador/a)	B-211	andres.mlopez@upm.es	L - 13:45 - 16:45 Horario flexible, pero confirmar por correo electrónico

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

3. Conocimientos previos recomendados

3.1. Asignaturas previas que se recomienda haber cursado

- Redes De Ordenadores

3.2. Otros conocimientos previos recomendados para cursar la asignatura

El plan de estudios Grado en Ingenieria de Tecnologias y Servicios de Telecomunicacion no tiene definidos otros conocimientos previos para esta asignatura.

4. Competencias y resultados de aprendizaje

4.1. 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

CG11 - Liderazgo de equipos

CG5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía

CG9 - Uso de Tecnologías de la Información y de las Comunicaciones

4.2. Resultados del 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.

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.

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.

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

5. Descripción de la asignatura y temario

5.1. Descripción de la asignatura

Los objetivos de esta asignatura son:

- Conocer los fundamentos organizativos y criptográficos en los que se basan las tecnologías de seguridad.
- Conocer las principales amenazas y vulnerabilidades de los distintos elementos involucrados en las TIC, así como sus causas.
- Conocer y aplicar las tecnologías que conforman una Arquitectura de Seguridad de las TIC, en sus distintas perspectivas.

5.2. Temario de la asignatura

1. Introducción a la Seguridad
2. Amenazas de Internet
3. Criptografía
4. Seguridad en las Comunicaciones
5. Sistemas de Autenticación
6. Arquitecturas de Seguridad
   - 6.1. Identificación
   - 6.2. Protección
   - 6.3. Detección
   - 6.4. Reacción
   - 6.5. Recuperación

6. Cronograma

6.1. Cronograma de la asignatura *

Sem	Actividad en aula	Actividad en laboratorio	Tele-enseñanza	Actividades de evaluación
1	**Introducción** Duración: 01:30 LM: Actividad del tipo Lección Magistral **Amenazas** Duración: 01:30 LM: Actividad del tipo Lección Magistral			
2	**Amenazas** Duración: 03:00 LM: Actividad del tipo Lección Magistral			
3	**Criptografía.** Duración: 03:00 LM: Actividad del tipo Lección Magistral			
4	**Criptografía** Duración: 01:30 LM: Actividad del tipo Lección Magistral	**Prácticas de Criptografía.** Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio		**Evaluación Prácticas Criptografía** TG: Técnica del tipo Trabajo en Grupo Evaluación continua y sólo prueba final No presencial Duración: 00:00
5	**Protección de las comunicaciones** Duración: 01:30 LM: Actividad del tipo Lección Magistral	**Prácticas de Criptografía.** Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio		**Evaluación Prácticas Criptografía II** TG: Técnica del tipo Trabajo en Grupo Evaluación continua y sólo prueba final No presencial Duración: 00:00
6	**Sistemas de Autenticación** Duración: 01:30 LM: Actividad del tipo Lección Magistral **Problemas de TLS** Duración: 01:30 PR: Actividad del tipo Clase de Problemas			
7	**Sistemas AAA** Duración: 01:30 LM: Actividad del tipo Lección Magistral **Problemas de Autenticación** Duración: 01:30 PR: Actividad del tipo Clase de Problemas			**Practica CTF** TG: Técnica del tipo Trabajo en Grupo Evaluación continua y sólo prueba final No presencial Duración: 02:00
8	**Arquitectura de Seguridad** Duración: 03:00 LM: Actividad del tipo Lección Magistral			
9	**Arquitectura de Seguridad** Duración: 03:00 LM: Actividad del tipo Lección Magistral			**Examen Parcial** EX: Técnica del tipo Examen Escrito Evaluación continua Presencial Duración: 01:00

10	**Tema 6: Arquitectura de Seguridad** Duración: 03:00 LM: Actividad del tipo Lección Magistral			
11	**Tema 6: Arquitectura de Seguridad** Duración: 03:00 LM: Actividad del tipo Lección Magistral			
12	**Tema 6: Arquitectura de Seguridad** Duración: 03:00 LM: Actividad del tipo Lección Magistral			
13	**Arquitectura de Seguridad** Duración: 01:30 LM: Actividad del tipo Lección Magistral	**Práctica de Arquitectura de Seguridad** Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio		
14	**Arquitectura de Seguridad** Duración: 01:30 LM: Actividad del tipo Lección Magistral	**Práctica de Arquitectura de Seguridad** Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio		**Practica Arquitecturas Seguridad** TG: Técnica del tipo Trabajo en Grupo Evaluación continua y sólo prueba final No presencial Duración: 03:00 **Actividades en clase (se irán realizando y evaluando presencialmente a lo largo de las distintas semanas del curso)** OT: Otras técnicas evaluativas Evaluación continua y sólo prueba final Presencial Duración: 00:15
15				
16				
17				**Examen Segunda Parte de Asignatura** EX: Técnica del tipo Examen Escrito Evaluación continua y sólo prueba final Presencial Duración: 02:00 **Examen Global Primera Parte** EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Presencial Duración: 01:00

Para el cálculo de los valores totales, se estima que por cada crédito ECTS el alumno dedicará dependiendo del plan de estudios, entre 26 y 27 horas de trabajo presencial y no presencial.

* El cronograma sigue una planificación teórica de la asignatura y puede sufrir modificaciones durante el curso derivadas de la situación creada por la COVID-19.

7. Actividades y criterios de evaluación

7.1. Actividades de evaluación de la asignatura

7.1.1. Evaluación (progresiva)

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
4	Evaluación Prácticas Criptografía	TG: Técnica del tipo Trabajo en Grupo	No Presencial	00:00	2%	/ 10	CE-TL2
5	Evaluación Prácticas Criptografía II	TG: Técnica del tipo Trabajo en Grupo	No Presencial	00:00	2%	/ 10	CE-TL2
7	Practica CTF	TG: Técnica del tipo Trabajo en Grupo	No Presencial	02:00	9%	/ 10	CG9 CE-TL2 CE-TL3 CG5
9	Examen Parcial	EX: Técnica del tipo Examen Escrito	Presencial	01:00	37%	4 / 10	CE-TL2 CE-TL3 CE-TL6 CG5
14	Practica Arquitecturas Seguridad	TG: Técnica del tipo Trabajo en Grupo	No Presencial	03:00	9%	/ 10	CG9 CE-TL2 CE-TL3 CG5
14	Actividades en clase (se irán realizando y evaluando presencialmente a lo largo de las distintas semanas del curso)	OT: Otras técnicas evaluativas	Presencial	00:15	4%	/ 10	CG9 CE-TL2 CE-TL4 CE-TL6
17	Examen Segunda Parte de Asignatura	EX: Técnica del tipo Examen Escrito	Presencial	02:00	37%	3 / 10	CE-TL2 CE-TL4 CE-TL6 CG5

7.1.2. Prueba evaluación global

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas

4	Evaluación Prácticas Criptografía	TG: Técnica del tipo Trabajo en Grupo	No Presencial	00:00	2%	/ 10	CE-TL2
5	Evaluación Prácticas Criptografía II	TG: Técnica del tipo Trabajo en Grupo	No Presencial	00:00	2%	/ 10	CE-TL2
7	Practica CTF	TG: Técnica del tipo Trabajo en Grupo	No Presencial	02:00	9%	/ 10	CG9 CE-TL2 CE-TL3 CG5
14	Practica Arquitecturas Seguridad	TG: Técnica del tipo Trabajo en Grupo	No Presencial	03:00	9%	/ 10	CG9 CE-TL2 CE-TL3 CG5
14	Actividades en clase (se irán realizando y evaluando presencialmente a lo largo de las distintas semanas del curso)	OT: Otras técnicas evaluativas	Presencial	00:15	4%	/ 10	CG9 CE-TL2 CE-TL4 CE-TL6
17	Examen Segunda Parte de Asignatura	EX: Técnica del tipo Examen Escrito	Presencial	02:00	37%	3 / 10	CE-TL2 CE-TL4 CE-TL6 CG5
17	Examen Global Primera Parte	EX: Técnica del tipo Examen Escrito	Presencial	01:00	37%	3 / 10	CE-TL2 CE-TL3 CE-TL4 CE-TL6 CG5

7.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
Examen Final Extraordinario	EX: Técnica del tipo Examen Escrito	Presencial	04:00	80%	3 / 10	CG9 CE-TL2 CE-TL3 CE-TL4 CE-TL6 CG5
Entrega Trabajos Extraordinaria	TI: Técnica del tipo Trabajo Individual	Presencial	00:00	20%	3 / 10	CG9 CE-TL2 CE-TL3 CE-TL4 CE-TL6 CG5

7.2. Criterios de evaluación

La evaluación de la asignatura se realizará de forma progresiva, de acuerdo con los siguientes pesos para los distintos bloques evaluables:

Bloque	Peso en convocatoria ordinaria (%)	Peso en convocatoria extraordinaria (%)
1. Prácticas Criptografía (I)	2	2
2. Prácticas Criptografía (II)	2	2
3. Prácticas CTF	9	8
4. Prácticas Arquitectura de Seguridad	9	8
5. Actividades en clase: problemas, tests, wooclaps, etc.	4	0
6. Examen Parcial Parte 1 E1	37	40
7. Examen Parcial Parte 2 E2	37	40

Los cuatro bloques de prácticas (1, 2, 3 y 4) son bloques liberatorios independientes. Cada uno se liberará individualmente hasta la convocatoria extraordinaria del mismo curso, siempre que la nota sea al menos de 4 puntos sobre 10.

E1 y E2 constituyen bloques liberatorios hasta la convocatoria extraordinaria, siempre que la nota sea al menos de 4 puntos sobre 10.

La evaluación extraordinaria constará de:

- Examen Parcial Parte 1 E1 (40%)
- Examen Parcial Parte 2 E2 (40%)

La convocatoria extraordinaria se ofrecerá exclusivamente los alumnos que hayan suspendido, que tendrán que volvera a evaluar aquellas prácticas y realizar aquellos exámenes parciales cuya nota en la ordinaria fuese inferior a 4. Será posible volver a realizar los examenes parciales con nota superior a 4, avisando por correo electrónico una semana antes del examen. Si se repite un bloque liberatorio, en la evaluación se utilizará la nota más favorable.

En la evaluación extraordinaria en todos los bloques de la asignatura se exige una nota mínima de 3 sobre 10. Las notas inferiores se evaluarán con 0%.

8. Recursos didácticos

8.1. Recursos didácticos de la asignatura

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

9. Otra información

9.1. Otra información sobre la asignatura

La asignatura se relaciona con los ODS 4 y 9:

Subobjetivo 4.4: Aumentar considerablemente el número de jóvenes y adultos que tienen las competencias profesionales y técnicas necesarias para acceder al empleo y al emprendimiento.

Subobjetivo 9.1: Desarrollar infraestructuras fiables, sostenibles, resilientes y de calidad.