ANX-PR/CL/001-01

GUÍA DE APRENDIZAJE

ASIGNATURA

595020231 - Seguridad En Redes Y Servicios

PLAN DE ESTUDIOS

59EC - Grado En Ingenieria Electronica De Comunicaciones

CURSO ACADÉMICO Y SEMESTRE

2022/23 - Segundo semestre

Índice

Guía de Aprendizaje

1. Datos descriptivos

1.1. Datos de la asignatura

Nombre de la asignatura	595020231 - Seguridad en Redes y Servicios
No de créditos	6 ECTS
Carácter	Optativa
Curso	Tercero curso
Semestre	Sexto semestre
Período de impartición	Febrero-Junio
Idioma de impartición	Castellano
Titulación	59EC - Grado en Ingenieria Electronica de Comunicaciones
Centro responsable de la titulación	59 - Escuela Tecnica Superior De Ingenieria Y Sistemas De Telecomunicacion
Curso académico	2022-23

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Pedro Castillejo Parrilla	A4401	pedro.castillejo@upm.es	Sin horario.
Esther Gago Garcia	A4419	esther.gago@upm.es	Sin horario.
Maria Luisa Martin Ruiz (Coordinador/a)	A4406	marialuisa.martinr@upm.es	Sin horario.

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

2.2. Personal investigador en formación o similar

Nombre	Correo electrónico	Profesor responsable
Diez Muñoz, Fernando	fernando.diez.munoz@upm.es	Martin Ruiz, Maria Luisa

3. Requisitos previos obligatorios

3.1. Asignaturas previas requeridas para cursar la asignatura

- Programacion II

- Redes de Ordenadores

- Redes y Servicios de Telecomunicacion

3.2. Otros requisitos previos para cursar la asignatura

El plan de estudios Grado En Ingenieria Electronica De Comunicaciones no tiene definidos requisitos para esta asignatura.

4. Competencias y resultados de aprendizaje

4.1. Competencias

CE TL01 - Capacidad de 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 servicios telemáticos.

CE TL02 - 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 TL05 - Capacidad de seguir el progreso tecnológico de transmisión, conmutación y proceso para mejorar las

redes y servicios Telemáticos.

CG 02 - Capacidad de búsqueda y selección de información, de razonamiento crítico y de elaboración y defensa de argumentos dentro del área.

CG 05 - Capacidad de trabajo en equipo y en entornos multidisciplinares.

4.2. Resultados del aprendizaje

RA466 - Establecer las funcionalidades avanzadas de la certificación X509

RA474 - Diseñar y definir la solución más óptima para un sistema telemático específico que satisfaga sus requisitos de seguridad

RA467 - Describir los elementos, estructura y capacidades de los tokens criptográficos

RA472 - Describir los mecanismos de seguridad más empleados para la protección de redes y sistemas a nivel de transporte

RA473 - Describir los mecanismos de seguridad más empleados en servicios telemáticos tradicionales como correo electrónico y servicio Web

RA471 - Describir los mecanismos de seguridad más empleados para la protección de redes y sistemas a nivel de red

RA470 - Definir los protocolos de actuación para una gestión eficiente de la seguridad de las redes y sus sistemas conforme a la normalización y recomendaciones vigentes

RA460 - Describir los servicios básicos de seguridad en las Redes Telemáticas

RA462 - Describir los algoritmos más comúnmente empleados en criptosistemas de clave secreta y de clave pública

RA463 - Establecer una comparativa entre criptosistemas de clave pública y de clave simétrica

RA465 - Describir los elementos, estructura y capacidades de las infraestructuras de distribución de claves

5. Descripción de la asignatura y temario

5.1. Descripción de la asignatura

Seguridad en Redes y Servicios es una asignatura perteneciente a la materia denominada "Redes, Sistemas y Servicios Telemáticos" que se imparte como asignatura troncal dentro del plan de estudios de la titulación de Grado en Ingeniería Telemática de la UPM y como optativa para el resto de las titulaciones.

El objetivo principal de esta asignatura es que el alumno adquiera una amplia visión de las soluciones que pueden aplicarse para la securización de sistemas de información. Para ello, se presentan los sistemas de criptografía simétrica y asimétrica, con énfasis especial en las posibilidades que ofrece la firma electrónica como elemento de autenticación. Asimismo, se presentan las soluciones más comunes para securizar distintos servicios telemáticos y la normativa de seguridad que afecta a los servicios ofrecidos a través de la Administración y el comercio electrónico.

Para poder ser cursada con aprovechamiento es necesario haber adquirido con anterioridad competencias que corresponden a asignaturas que la preceden en el plan de estudios. En concreto, los conocimientos previos necesarios para cursar esta asignatura son haber aprobado las asignaturas Redes y Servicios de Telecomunicación, Redes de Ordenadores y Programación II.

5.2. Temario de la asignatura

1. Planteamientos generales sobre la seguridad de las redes y los servicios
    1.1. Problemática de seguridad: amenazas y ataques
    1.2. Servicios y mecanismos de seguridad
    1.3. Criptosistemas de secreto perfecto
    1.4. Criptosistemas de clave secreta
    1.5. Criptosistemas de clave pública
    1.6. Tokens criptográficos
2. Infraestructuras de seguridad
    2.1. Modelos de establecimiento de confianza: modelos basados en TTP y modelos de confianza directa
    2.2. Arquitecturas basadas en TTP
        2.2.1. Infraestructuras de clave pública: PKI (CA, Autoridad de Registro, Autoridad de Sello de Tiempo,

PMI)

2.2.2. Infraestructuras de clave secreta (Kerberos)

2.3. Modelos de confianza directa (PGP)

3. Seguridad en el bloque de transporte

3.1. Seguridad a nivel de red

3.2. Seguridad a nivel de transporte

4. Seguridad en aplicaciones telemáticas

4.1. Dinero electrónico

4.2. Seguridad en Redes Wifi

5. Práctica 1: Programación de aplicaciones protegidas criptográficamente

6. Práctica 2: Desarrollo de una Autoridad de Certificación

7. Práctica 3: OpenSSL y Cortafuegos

6. Cronograma

6.1. Cronograma de la asignatura *

Sem	Actividad presencial en aula	Actividad presencial en laboratorio	Tele-enseñanza	Actividades de evaluación
1	**Tema 1** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Presentación entorno prácticas laboratorio** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
2	**Tema 1** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Práctica 1** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
3	**Tema 1** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Práctica 1** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
4	**Tema 2** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Práctica 1** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
5	**Tema 2** Duración: 02:00 LM: Actividad del tipo Lección Magistral			**Evaluación Práctica 1** EP: Técnica del tipo Examen de Prácticas Evaluación continua Presencial Duración: 02:00
6	**Tema 2** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Práctica 2** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
7	**Tema 2** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Práctica 2** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
8	**Tema 2/Tema 3** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Práctica 2** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
9				
10	**Tema 3** Duración: 02:00 LM: Actividad del tipo Lección Magistral			**Evaluación Práctica 2** ET: Técnica del tipo Prueba Telemática Evaluación continua Presencial Duración: 02:00
11	**Tema 3** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Práctica 3** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		

12	**Tema 3/Tema 4** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Práctica 3** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
13	**Tema 4** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Práctica 3** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
14				
15	**Tema 4** Duración: 01:00 LM: Actividad del tipo Lección Magistral			**Evaluación Práctica 3** EP: Técnica del tipo Examen de Prácticas Evaluación continua Presencial Duración: 01:00
16				
17				**Prueba evaluación continua** EX: Técnica del tipo Examen Escrito Evaluación continua Presencial Duración: 02:00

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 continua

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
5	Evaluación Práctica 1	EP: Técnica del tipo Examen de Prácticas	Presencial	02:00	10%	0 / 10	CE TL02
10	Evaluación Práctica 2	ET: Técnica del tipo Prueba Telemática	Presencial	02:00	15%	0 / 10	CE TL01 CE TL02
15	Evaluación Práctica 3	EP: Técnica del tipo Examen de Prácticas	Presencial	01:00	15%	0 / 10	CE TL02 CG 02 CG 05
17	Prueba evaluación continua	EX: Técnica del tipo Examen Escrito	Presencial	02:00	60%	0 / 10	CE TL05 CE TL01 CE TL02

7.1.2. Evaluación sólo prueba final

No se ha definido la evaluacion sólo por prueba final.

7.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
Examen escrito contenidos del curso	EX: Técnica del tipo Examen Escrito	Presencial	03:00	100%	0 / 10	CE TL05 CE TL01 CE TL02 CG 02 CG 05

7.2. Criterios de evaluación

En la convocatoria ordinaria, la evaluación constará de dos partes

- Examen escrito final sobre los contenidos del curso (con un peso del 60%).

- Tres exámenes, uno sobre cada práctica de laboratorio (con un peso del 10%, 15% y 15%):

  - Las prácticas serán evaluadas mediante exámenes orales en los laboratorios o alternativamente mediante exámenes escritos sobre los aspectos tratados en las prácticas.
  - Para evaluarse de cada una de las prácticas es imprescindible haber entregado la memoria correspondiente.

Asimismo, la evaluación en la convocatoria extraordinaria se realizará a través de un examen escrito con preguntas sobre los contenidos del curso.

8. Recursos didácticos

8.1. Recursos didácticos de la asignatura

Nombre	Tipo	Observaciones
Libro 1	Bibliografía	Carracedo, J. Seguridad en Redes Telemáticas. Mc Graw Hill. 2004
Libro 2	Bibliografía	Stallings, William Network security essentials : applications and standards Pearson Prentice Hall, 2007
Red temática CRIPTORED	Recursos web	Red Temática CRIPTORED: Criptografía y seguridad de la información www.criptored.upm.es
Intypedia	Recursos web	Enciclopedia visual de la seguridad de la información www.intypedia.com

Libro 3	Bibliografía	Stalling, William & Brown, Lawrie. Computer Security. Principles and Practice. Third Edition. Pearson. 2015. Chapter 24. Wireless Network Security. 733-765.