ANX-PR/CL/001-01

GUÍA DE APRENDIZAJE

ASIGNATURA

595000231 - Seguridad en redes y servicios

PLAN DE ESTUDIOS

59TL - Grado En Ingenieria Telematica

CURSO ACADÉMICO Y SEMESTRE

2018/19 - Segundo 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....6
7. Actividades y criterios de evaluación....8
8. Recursos didácticos....10

1. Datos descriptivos

1.1. Datos de la asignatura

Nombre de la asignatura	595000231 - Seguridad en redes y servicios
No de créditos	6 ECTS
Carácter	Obligatoria
Curso	Tercero curso
Semestre	Sexto semestre
Período de impartición	Febrero-Junio
Idioma de impartición	Castellano
Titulación	59TL - Grado en ingenieria telematica
Centro en el que se imparte	59 - Escuela Tecnica Superior de Ingenieria y Sistemas de Telecomunicacion
Curso académico	2018-19

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Maria Luisa Martin Ruiz	A4406	marialuisa.martinr@upm.es	Sin horario.
Ivan Pau De La Cruz (Coordinador/a)	A4404	ivan.pau@upm.es	Sin horario.
Esther Gago Garcia	A4419	esther.gago@upm.es	Sin horario.

* 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

- Programacion II

- Redes de ordenadores

- Redes y servicios de telecomunicacion

3.2. Otros conocimientos previos recomendados para cursar la asignatura

El plan de estudios Grado en Ingenieria Telematica no tiene definidos otros conocimientos previos 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

RA421 - Describir los elementos, estructura y capacidades de los tokens criptográficos

RA414 - Describir los servicios básicos de seguridad en las Redes Telemáticas

RA428 - Diseñar y definir la solución más óptima para un sistema telemático específico que satisfaga sus requisitos de seguridad

RA417 - Establecer una comparativa entre criptosistemas de clave pública y de clave simétrica

RA909 - Establecer las funcionalidades avanzadas de la certificación x.509

RA419 - Describir los elementos, estructura y capacidades de las infraestructuras de distribución de claves

RA427 - Describir los mecanismos de seguridad más empleados en servicios telemáticos tradicionales como correo electrónico y servicio Web

RA912 - 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

RA426 - Describir los mecanismos de seguridad más empleados para la protección de redes y sistemas a nivel de transporte

RA425 - Describir los mecanismos de seguridad más empleados para la protección de redes y sistemas a nivel de red

RA913 - Describir los algoritmos más conmúnmente empleados en criptosistemas de clave secreta y de clave pública

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 en redes de área local

3.2. Seguridad a nivel de red

3.3. Seguridad a nivel de transporte

4. Seguridad en aplicaciones telemáticas

4.1. Dinero electrónico

4.2. Comercio electrónico

4.3. Correo electrónico

4.4. Aplicaciones web

5. Práctica 1: Programación de aplicaciones protegidas criptográficamente

6. Práctica 2: Desarrollo de una Autoridad de Certificación

7. Práctica 3: Cortafuegos

6. Cronograma

6.1. Cronograma de la asignatura *

Sem	Actividad presencial en aula	Actividad presencial en laboratorio	Otra actividad presencial	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 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** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Práctica 2** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
9	**Tema 3** Duración: 02:00 LM: Actividad del tipo Lección Magistral			**Evaluación Práctica 2** ET: Técnica del tipo Prueba Telemática Evaluación continua Duración: 02:00
10	**Tema 3** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Práctica 3** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		

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 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: 01:00 LM: Actividad del tipo Lección Magistral	**Práctica 3** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
14	**Tema 4** Duración: 02:00 LM: Actividad del tipo Lección Magistral			
15				
16				**Evaluación Práctica 3** EP: Técnica del tipo Examen de Prácticas Evaluación continua Duración: 01:00
17				**Prueba evaluación continua** EX: Técnica del tipo Examen Escrito Evaluación continua Duración: 02:00 **Prueba final** EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Duración: 04:00

Las horas de actividades formativas no presenciales son aquellas que el estudiante debe dedicar al estudio o al trabajo personal.

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.

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	15%	0 / 10	CE TL02
9	Evaluación Práctica 2	ET: Técnica del tipo Prueba Telemática	Presencial	02:00	15%	0 / 10	CE TL01 CE TL02
16	Evaluación Práctica 3	EP: Técnica del tipo Examen de Prácticas	Presencial	01:00	20%	0 / 10	CE TL02 CG 02 CG 05
17	Prueba evaluación continua	EX: Técnica del tipo Examen Escrito	Presencial	02:00	50%	0 / 10	CE TL01 CE TL02 CE TL05

7.1.2. Evaluación sólo prueba final

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
17	Prueba final	EX: Técnica del tipo Examen Escrito	Presencial	04:00	100%	0 / 10	CE TL01 CE TL02 CE TL05 CG 02 CG 05

7.1.3. Evaluación convocatoria extraordinaria

No se ha definido la evaluación extraordinaria.

7.2. Criterios de evaluación

La asignatura se calificará sobre un total de 10 puntos. Para aprobarla se debe alcanzar una puntuación global de al menos 5 puntos.

Evaluación continua

El sistema de evaluación continua será el que se aplique en general a todos los estudiantes de la asignatura.

Evaluación a través de "solo prueba final"

El alumno que desee seguir el sistema de evaluación mediante sólo prueba final deberá comunicarlo por escrito, rellenando y presentando en la secretaría del Departamento la instancia que a tal efecto se habilite. El plazo de presentación de dicha instancia se cerrará tres semanas después del comienzo de la asignatura.

Una vez elegido el itinerario de "sólo prueba final" no es posible el cambio de itinerario por parte del alumno, excepto por causa sobrevenida y de fuerza mayor.

La evaluación mediante "solo prueba final" incluirá una prueba de evaluación para cada una las prácticas propuestas durante el curso, con un peso del 50% y una parte teórica coincidente con la prueba de evaluación continúa del resto de los alumnos, con un peso del 50%.

Examen extraordinario (examen de julio)

Los alumnos que habiendo seguido el itinerario de "evaluación continua" no hayan superado la asignatura tendrán opción de ser evaluados únicamente de aquellas partes de la asignatura que no hayan superado (**Teoría**, **Práctica 1**, **Práctica 2** y **Práctica 3)**, siendo obligatorio realizar el examen de todas las partes no superadas.

Los alumnos que habiendo cursado el itinerario de "solo prueba final" no hayan superado la asignatura tendrán opción de ser evaluados únicamente de aquellas partes de la asignatura que no hayan superado (**Teoría**, **Práctica 1**, **Práctica 2** y **Práctica 3)**, siendo obligatorio realizar el examen de todas las partes no superadas.

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
Norma 3	Bibliografía	Ley 34/2002. Ley de Servicios de la Sociedad de la Información y Comercio Electrónico
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