



UNIVERSIDAD
POLITÉCNICA
DE MADRID

PROCESO DE
COORDINACIÓN DE LAS
ENSEÑANZAS PR/CL/001



E.T.S. de Ingeniería de
Sistemas Informáticos

ANX-PR/CL/001-01

GUÍA DE APRENDIZAJE

ASIGNATURA

615000730 - Seguridad En Sistemas Y Redes

PLAN DE ESTUDIOS

61TI - Grado En Tecnologías Para La Sociedad De La Informacion

CURSO ACADÉMICO Y SEMESTRE

2020/21 - 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.....	9
8. Recursos didácticos.....	11
9. Otra información.....	12

1. Datos descriptivos

1.1. Datos de la asignatura

Nombre de la asignatura	615000730 - Seguridad en Sistemas y Redes
No de créditos	6 ECTS
Carácter	Obligatoria
Curso	Tercero curso
Semestre	Sexto semestre
Período de impartición	Febrero-Junio
Idioma de impartición	Castellano
Titulación	61TI - Grado en Tecnologías para la Sociedad de la Información
Centro responsable de la titulación	61 - Escuela Técnica Superior De Ingeniería De Sistemas Informáticos
Curso académico	2020-21

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Borja Bordel Sanchez (Coordinador/a)	4305	borja.bordel@upm.es	Sin horario. El horario de tutorías se publicará en la web de la ETSISI al comienzo del cuatrimestre

Jesus Sanchez Lopez	1117	jesus.sanchezl@upm.es	Sin horario. El horario de tutorías se publicará en la web de la ETSISI al comienzo del cuatrimestre
---------------------	------	-----------------------	--

* 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 Computadores
- Seguridad De La Informacion

3.2. Otros conocimientos previos recomendados para cursar la asignatura

- Disponer de conocimientos de Redes Avanzadas y Servicios de Internet
- Haber cursado y superado "Redes de Computadores" y "Seguridad de la Información"

4. Competencias y resultados de aprendizaje

4.1. Competencias

CC05 - Conocimiento, administración y mantenimiento de sistemas, servicios y aplicaciones informáticas.

CE07 - Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.

CT02 - Resolución de problemas: Identificar, analizar y definir los elementos significativos que constituyen un problema para resolverlo con criterio y de forma efectiva.

CT04 - Comunicación escrita: Relacionarse eficazmente con otras personas a través de la expresión clara de lo que se piensa, mediante la escritura y los apoyos gráficos.

OB07 - Capacidad para conocer, comprender y aplicar la legislación necesaria durante el desarrollo de la profesión de Ingeniero Técnico en Informática y manejar especificaciones, reglamentos y normas de obligado cumplimiento.

4.2. Resultados del aprendizaje

RA141 - Audita redes desde el punto de vista de la defensa y seguridad frente ataques, tanto internos como externos.

RA136 - Comprende las características de seguridad de un sistema cortafuegos.

RA139 - Establece la mejor solución para un diseño de sistemas de túneles para interconectar usuarios o redes.

RA129 - Entiende y aplica los diferentes sistemas de cifrado.

RA130 - Genera y crea todas las estructuras de una PKI.

RA131 - .Configura adecuadamente servidores web seguros con soporte de cifrado con el protocolo SSL/TLS.

RA132 - Conoce y aplica las medidas de seguridad en un sistema operativo

RA133 - Comprende los mecanismos de seguridad en redes WIFI.

RA138 - Configura y dimensiona redes privadas virtuales

RA140 - .Conoce y aplica las técnicas de defensa frente a ataques hacking.

RA137 - Diseña un sistema de defensa de barrera, incorporando herramientas de detección de intrusos.

RA135 - Conoce debilidades de seguridad en los dispositivos móviles y los asegura.

RA134 - Dimensiona y configura adecuadamente el sistema de seguridad de una red WIFI.

5. Descripción de la asignatura y temario

5.1. Descripción de la asignatura

En la asignatura se estudian los contenidos necesarios para comprender los fundamentos de la seguridad en redes y sistemas en sentido amplio. En el estudio se abarcan todos los aspectos de la seguridad aplicada a las redes imbricando conocimientos de criptografía aplicada con los conocimientos de protección de redes, basados en la esencia de funcionamiento de los protocolos de comunicaciones. En primer lugar se analiza a fondo y se comprenden los métodos de seguridad en redes WIFI, llegando a la posibilidad de indicar la realización de auditorías de estas, desde el punto de vista de la seguridad. Después se estudian los sistemas de protección de barrera como cortafuegos y las topologías de estos, así como el uso y puesta en funcionamiento de redes privadas virtuales. Se analiza la seguridad en sistemas operativos y dispositivos móviles. Al final se hace un barrido extenso en técnicas de haking estableciendo los parámetros que permiten la comprensión de los métodos de ataque a redes y las posibilidades de actuación para su defensa.

5.2. Temario de la asignatura

1. Criptografía aplicada. Certificados y estructura PKI. Protocolos SSL, TLS.

- 1.1. Funciones HASH. Funciones HMAC.
- 1.2. Criptografía básica. Simétrica. Asimétrica.
- 1.3. Certificados digitales. Tipos. Formatos.
- 1.4. Autoridades de Certificación. Firma digital.
- 1.5. Cifrado de las comunicaciones. Protocolos de cifrado.
- 1.6. TLS y SSL en Internet. Aplicación para el web.
- 1.7. Autenticación del Servidor. Autenticación del Cliente.

2. Seguridad en la red y el acceso. Cortafuegos y topologías.

- 2.1. Filtros de paquetes de datos.
- 2.2. Filtros de aplicación. Proxys. Filtros de kernel.
- 2.3. Ejemplos de proxys, ejemplos de filtros de red: iptables
- 2.4. Cortafuegos. Topologías de cortafuegos.
- 2.5. Dual homed host. Screened host. Screened subnet. Backbone.
- 2.6. Sistemas de detección de intrusos. IDS'S.

- 2.7. Sistemas de protección de intrusos. IPS'S.
- 3. Seguridad y ataques informáticos
 - 3.1. Seguridad y ataques informáticos
 - 3.2. Hacking y prevención de ataques
 - 3.3. Análisis y explotación de vulnerabilidades
- 4. Seguridad en Sistemas Operativos
 - 4.1. Seguridad externa. Seguridad física
 - 4.2. Seguridad basada en hardware
 - 4.3. Núcleos de seguridad y seguridad mediante configuración
 - 4.4. Amenazas generales y casos actuales
 - 4.5. Algunas aplicaciones útiles
- 5. Seguridad en dispositivos móviles
 - 5.1. Introducción
 - 5.2. Riesgos y vulnerabilidades
 - 5.3. Mecanismos para reforzar la seguridad
 - 5.4. Auditoría y explotación de vulnerabilidades
- 6. Seguridad en redes wireless: Wi-Fi
 - 6.1. Introducción
 - 6.2. Mecanismos de seguridad en redes WiFi
 - 6.3. Ataques más comunes
 - 6.4. Aplicaciones para auditoría
- 7. Túneles y Redes privadas virtuales
 - 7.1. Concepto de túnel y red privada virtual
 - 7.2. Tipos de túneles
 - 7.3. Túneles a nivel de aplicación
 - 7.4. Túneles a nivel de transporte
 - 7.5. Túneles a nivel de red
 - 7.6. Túneles a nivel de enlace

6. Cronograma

6.1. Cronograma de la asignatura *

Sem	Actividad presencial en aula	Actividad presencial en laboratorio	Tele-enseñanza	Actividades de evaluación
1		Clase de prácticas. Exposición de conceptos teóricos y/o casos prácticos Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	Clase de prácticas. Exposición de conceptos teóricos y/o casos prácticos Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	
2		Clase de prácticas. Exposición de conceptos teóricos y/o casos prácticos Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	Clase de prácticas. Exposición de conceptos teóricos y/o casos prácticos Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	Realización de Cuestionario Criptografía aplicada ET: Técnica del tipo Prueba Telemática Evaluación continua No presencial Duración: 01:00 Realización de prácticas. Criptografía aplicada TG: Técnica del tipo Trabajo en Grupo Evaluación continua No presencial Duración: 10:00
3		Clase de prácticas. Exposición de conceptos teóricos y/o casos prácticos Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	Clase de prácticas. Exposición de conceptos teóricos y/o casos prácticos Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	
4		Clase de prácticas. Exposición de conceptos teóricos y/o casos prácticos Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	Clase de prácticas. Exposición de conceptos teóricos y/o casos prácticos Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	Realización de Cuestionarios Cortafuegos ET: Técnica del tipo Prueba Telemática Evaluación continua No presencial Duración: 01:00 Realización de prácticas. Cortafuegos TG: Técnica del tipo Trabajo en Grupo Evaluación continua No presencial Duración: 10:00
5		Clase de prácticas. Exposición de conceptos teóricos y/o casos prácticos Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	Clase de prácticas. Exposición de conceptos teóricos y/o casos prácticos Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	
6		Clase de prácticas. Exposición de conceptos teóricos y/o casos prácticos Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	Clase de prácticas. Exposición de conceptos teóricos y/o casos prácticos Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	

7		Clase de prácticas. Exposición de conceptos teóricos y/o casos prácticos Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	Clase de prácticas. Exposición de conceptos teóricos y/o casos prácticos Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	
8		Clase de prácticas. Realización de proyecto práctico Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	Clase de prácticas. Realización de proyecto práctico Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	
9		Clase de prácticas. Realización de proyecto práctico Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	Clase de prácticas. Realización de proyecto práctico Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	
10		Clase de prácticas. Realización de proyecto práctico Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	Clase de prácticas. Realización de proyecto práctico Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	
11		Clase de prácticas. Realización de proyecto práctico Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	Clase de prácticas. Realización de proyecto práctico Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	
12		Clase de prácticas. Realización de proyecto práctico Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	Clase de prácticas. Realización de proyecto práctico Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	
13		Clase de prácticas. Realización de proyecto práctico Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	Clase de prácticas. Realización de proyecto práctico Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	
14		Clase de prácticas. Realización de proyecto práctico Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	Clase de prácticas. Realización de proyecto práctico Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	
15		Clase de prácticas. Realización de proyecto práctico Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	Clase de prácticas. Realización de proyecto práctico Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	Proyecto final TG: Técnica del tipo Trabajo en Grupo Evaluación continua No presencial Duración: 30:00 Realización de Ejercicios sobre Hacking, reversing, binary exploitation ET: Técnica del tipo Prueba Telemática Evaluación continua No presencial Duración: 12:00
16				

17				Examen final EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final 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
2	Realización de Cuestionario Criptografía aplicada	ET: Técnica del tipo Prueba Telemática	No Presencial	01:00	3.5%	0 / 10	CT02 CC05
2	Realización de prácticas. Criptografía aplicada	TG: Técnica del tipo Trabajo en Grupo	No Presencial	10:00	21.5%	0 / 10	CT04 CC05 OB07
4	Realización de Cuestionarios Cortafuegos	ET: Técnica del tipo Prueba Telemática	No Presencial	01:00	3.5%	0 / 10	CT02 CE07
4	Realización de prácticas. Cortafuegos	TG: Técnica del tipo Trabajo en Grupo	No Presencial	10:00	21.5%	0 / 10	
15	Proyecto final	TG: Técnica del tipo Trabajo en Grupo	No Presencial	30:00	35%	0 / 10	CT02 CC05 OB07 CT04 CE07
15	Realización de Ejercicios sobre Hacking, reversing, binary exploitation	ET: Técnica del tipo Prueba Telemática	No Presencial	12:00	15%	0 / 10	CT02 CC05 CE07

7.1.2. Evaluación sólo prueba final

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
17	Examen final	EX: Técnica del tipo Examen Escrito	Presencial	02:00	100%	5 / 10	CT02 CC05 OB07 CT04 CE07

7.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
Examen final	EX: Técnica del tipo Examen Escrito	Presencial	02:00	100%	5 / 10	CT02 CC05 OB07 CT04 CE07

7.2. Criterios de evaluación

EVALUACIÓN CONTINUA:

La evaluación continua se realiza de tal manera que cada actividad, test, práctica, examen parcial o trabajo en grupo tiene un peso en la evaluación indicado por el cronograma de la tabla anterior. Se aprobará la asignatura si la media pondera al final del curso supera o iguala el valor 5.0. No se consideran restricciones adicionales.

EVALUACIÓN mediante SOLO EXAMEN FINAL:

Los alumnos que deseen ser evaluados SOLO mediante examen final y no seguir la evaluación continua, deberán solicitarlo en tiempo y forma al inicio del semestre.

Los alumnos que decidan optar por la opción de sólo examen final deberán comunicarlo antes de la realización de la primera práctica mediante el procedimiento disponible en Moodle.

El examen final consistirá en una prueba escrita sobre los contenidos teóricos y prácticos de la asignatura. Esta prueba se calificará sobre 10 puntos siendo necesario obtener una nota igual o superior a 5.

En el caso de optar en evaluación ordinaria por el procedimiento de "solo prueba final", será condición indispensable para poder presentarse al examen entregar TODAS las prácticas previstas en el cronograma. Dichas prácticas serán calificadas como APTO/NO APTO, dando permitiendo (si APTO) presentarse al examen.

EVALUACIÓN CONVOCATORIA EXTRAORDINARIA:

La evaluación en convocatoria extraordinaria será igual que la EVALUACIÓN mediante SOLO PRUEBA FINAL

8. Recursos didácticos

8.1. Recursos didácticos de la asignatura

Nombre	Tipo	Observaciones
Colección de diapositivas para cada tema	Otros	Diapositivas desarrollando el tema que se está impartiendo.
Enlaces web	Recursos web	Enlaces web a páginas con documentación aplicables a cada parte de los contenidos
Plataforma moodle	Recursos web	Plataforma moodle de apoyo a la docencia:
Aula equipadas con ordenador proyector de video y pizarra.	Equipamiento	Proyector de video para seguir las explicaciones y demostraciones en directo.
Laboratorio de prácticas	Equipamiento	Laboratorio con 12 ordenadores con software adecuado para la realización de las prácticas.
Routers WIFI	Equipamiento	12 Routers WIFI y portátiles para la realización de las prácticas. Servidor RADIUS, configurado al efecto.

9. Otra información

9.1. Otra información sobre la asignatura

En previsión de posibles recidivas de la epidemia de COVID, la presente guía contempla la impartición de la asignatura en formato bimodal: todas las actividades formativas planificadas inicialmente como actividades presenciales, en caso de ser necesario pasarán a desarrollarse a través de plataformas online.

Será de uso preferente en esta asignatura la plataforma Collaborate, aunque podrán utilizarse otras si su mayor utilidad lo justifica.