



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

613000119 - Seguridad En Sistemas Y Redes

### PLAN DE ESTUDIOS

61AG - Master Universitario En Software De Sistemas Distribuidos Y Empotrados

### CURSO ACADÉMICO Y SEMESTRE

2022/23 - 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.....	7
7. Actividades y criterios de evaluación.....	10
8. Recursos didácticos.....	13
9. Otra información.....	14

## 1. Datos descriptivos

### 1.1. Datos de la asignatura

<b>Nombre de la asignatura</b>	613000119 - Seguridad en Sistemas y Redes
<b>No de créditos</b>	6 ECTS
<b>Carácter</b>	Obligatoria
<b>Curso</b>	Primer curso
<b>Semestre</b>	Segundo semestre
<b>Período de impartición</b>	Febrero-Junio
<b>Idioma de impartición</b>	Castellano
<b>Titulación</b>	61AG - Master Universitario en Software de Sistemas Distribuidos y Empotrados
<b>Centro responsable de la titulación</b>	61 - Escuela Técnica Superior De Ingeniería De Sistemas Informáticos
<b>Curso académico</b>	2022-23

## 2. Profesorado

### 2.1. Profesorado implicado en la docencia

<b>Nombre</b>	<b>Despacho</b>	<b>Correo electrónico</b>	<b>Horario de tutorías *</b>
Borja Bordel Sanchez (Coordinador/a)	4414	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 Inalámbricas

#### 3.2. Otros conocimientos previos recomendados para cursar la asignatura

- Conocimientos de redes en sentido amplio
- Conocimientos de criptografía anivel de usuario

### 4. Competencias y resultados de aprendizaje

---

#### 4.1. Competencias

CE05 - Capacidad para diseñar, desarrollar, gestionar y evaluar mecanismos de garantía de seguridad en el tratamiento y acceso a la información en un sistema de procesamiento local o distribuido.

CE06 - Capacidad para diseñar y evaluar aplicaciones y sistemas basados en computación distribuida y para implantar sistemas operativos y servidores.

CG05 - Gestión de la información.

CG09 - Capacidad de análisis y síntesis.

## 4.2. Resultados del aprendizaje

RA43 - RA112 - Comprende las características de seguridad de un sistema cortafuegos.

RA40 - RA115 - Configura y dimensiona redes privadas virtuales.

RA44 - RA110 - Audita, con criterios de seguridad, redes WIFI.

RA50 - RA117 - Conoce y aplica las técnicas de defensa frente a ataques hacking.

RA42 - RA106 - Genera y crea todas las estructuras de una PKI.

RA48 - RA108 - Comprende los mecanismos de seguridad en redes WIFI.

RA38 - RA118 - Audita redes desde el punto de vista de la defensa y seguridad frente ataques, tanto internos como externos.

RA37 - RA116 - Establece la mejor solución para un diseño de sistemas de túneles para interconectar usuarios o redes.

RA39 - RA114 - Instala y configura adecuadamente sistemas complejos cortafuegos.

RA36 - RA105 - Entiende y aplica los diferentes sistemas de cifrado.

RA46 - RA111 - Comprende, instala y configura mecanismos de seguridad en dispositivos móviles.

RA52 - RA184 - Aplicar técnicas, principios y métodos para identificar información relevante y sintetizarla de manera autónoma, flexible, efectiva y con criterio

RA47 - RA113 - Diseña un sistema de defensa de barrera, incorporando herramientas de detección de intrusos.

RA45 - RA107 - Configura adecuadamente servidores web seguros con soporte de cifrado con el protocolo SSL/TLS.

RA49 - RA178 - RAG5 -Saber buscar la documentación necesaria y la normativa. Elabora la información y la publica adecuadamente

RA51 - RA109 - 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

La asignatura Seguridad en Sistemas y Redes permite adquirir los conocimientos tópicos de la seguridad en redes y sistemas en sentido amplio.

Empieza con una introducción a la criptografía aplicada haciendo incidencia en certificados digitales, y PKI's. Después se estudian los protocolos de comunicaciones seguros y sus aplicaciones en las comunicaciones e Internet. En cuanto a la parte clásica de seguridad se estudian los sistemas de protección de barrera, filtros de paquetes, cortafuegos y sus topologías y sistemas de detección y prevención de intrusiones. La interconexión segura de redes queda cubierta con el estudio de las redes privadas virtuales. El hacking y la defensa contra ataques forman la parte final del programa. Es parte importante la seguridad en dispositivos móviles, haciendo fuerte incidencia en la seguridad en redes wifi, en modo infraestructura y adhoc y también en las comunicaciones por bluetooth.

### 5.2. Temario de la asignatura

1. Criptografía Aplicada.
  - 1.1. Funciones Resumen (HASH).
  - 1.2. Sistemas Criptográficos. Criptografía Simétrica y Asimétrica
  - 1.3. Firma electrónica y certificados digitales.
  - 1.4. Cifrado de las comunicaciones. Protocolos SSL y TLS
2. Seguridad en la red y en el acceso.
  - 2.1. Cortafuegos y topologías.
    - 2.1.1. Cortafuegos de filtrado de paquetes.
    - 2.1.2. Otros tipos de cortafuegos
  - 2.2. Sistemas de Detección y Prevención de Intrusiones (IDS/IPS).
  - 2.3. Monitorización y gestión de eventos (SEM/SIM/SIEM).
  - 2.4. Next-generation firewall (NGFW)
  - 2.5. Entorno Linux. Netfilter e iptables.

3. Hacking y prevención de ataques
  - 3.1. Análisis y explotación de vulnerabilidades
  - 3.2. Hacking y prevención de ataques
  - 3.3. Sistemas IDS, IPS y gestión de información
4. Túneles y Redes privadas virtuales
  - 4.1. Concepto de túnel y red privada virtual
  - 4.2. Tipos de túneles
  - 4.3. Túneles a nivel de aplicación
  - 4.4. Túneles a nivel de transporte
  - 4.5. Túneles a nivel de red
  - 4.6. Túneles a nivel de enlace
5. Seguridad en redes Wireless domésticas y corporativas
  - 5.1. Introducción
  - 5.2. Redes domésticas
    - 5.2.1. Mecanismos de seguridad en redes WiFi
    - 5.2.2. Ataques más comunes
    - 5.2.3. Aplicaciones para auditoría
  - 5.3. Redes corporativas
    - 5.3.1. 802.11i
    - 5.3.2. Modo SOHO
    - 5.3.3. Modo Enterprise
6. Seguridad en dispositivos móviles
  - 6.1. Introducción
  - 6.2. Riesgos y vulnerabilidades
  - 6.3. Mecanismos para reforzar la seguridad
  - 6.4. Auditoría y explotación de vulnerabilidades
7. Seguridad en redes Ad Hoc
  - 7.1. Introducción
  - 7.2. Generación y almacenamiento seguro de claves

7.3. Generadores de números aleatorios basados en lógica digital

7.4. Fuentes de claves erráticas

7.4.1. Sistemas caóticos

7.4.2. Physical Unclonable Functions



## 6. Cronograma

### 6.1. Cronograma de la asignatura \*

Sem	Actividad en aula	Actividad en laboratorio	Tele-enseñanza	Actividades de evaluación
1	<b>Criptografía aplicada.</b> Duración: 03:00 AC: Actividad del tipo Acciones Cooperativas	<b>Resolución de supuestos y actividades prácticas</b> Duración: 03:00 PL: Actividad del tipo Prácticas de Laboratorio		<b>Cuestionario Criptografía Aplicada</b> ET: Técnica del tipo Prueba Telemática Evaluación continua No presencial Duración: 00:30  <b>Entrega proyecto (1) criptografía aplicada</b> TG: Técnica del tipo Trabajo en Grupo Evaluación continua No presencial Duración: 05:00
2	<b>Seguridad en al red y en el acceso.</b> Duración: 03:00 AC: Actividad del tipo Acciones Cooperativas	<b>Resolución de supuestos y actividades prácticas</b> Duración: 03:00 PL: Actividad del tipo Prácticas de Laboratorio		<b>Cuestionario Seguridad en la red y en acceso.</b> ET: Técnica del tipo Prueba Telemática Evaluación continua No presencial Duración: 00:30  <b>Entrega proyecto (2) Seguridad en la Red y el Acceso</b> TG: Técnica del tipo Trabajo en Grupo Evaluación continua No presencial Duración: 05:00
3	<b>Hacking y prevención de ataques.</b> Duración: 03:00 AC: Actividad del tipo Acciones Cooperativas	<b>Resolución de supuestos y actividades prácticas</b> Duración: 03:00 PL: Actividad del tipo Prácticas de Laboratorio		
4	<b>Túneles y redes privadas virtuales.</b> Duración: 03:00 AC: Actividad del tipo Acciones Cooperativas	<b>Resolución de supuestos y actividades prácticas</b> Duración: 03:00 PL: Actividad del tipo Prácticas de Laboratorio		<b>Cuestionario Túneles</b> ET: Técnica del tipo Prueba Telemática Evaluación continua No presencial Duración: 00:30  <b>Entrega proyecto (3): Túneles y VPN</b> TG: Técnica del tipo Trabajo en Grupo Evaluación continua No presencial Duración: 05:00
5	<b>Seguridad en redes Wireless domésticas y corporativas</b> Duración: 03:00 AC: Actividad del tipo Acciones Cooperativas	<b>Resolución de supuestos y actividades prácticas</b> Duración: 03:00 PL: Actividad del tipo Prácticas de Laboratorio		<b>Cuestionario Wireless</b> ET: Técnica del tipo Prueba Telemática Evaluación continua No presencial Duración: 00:30  <b>Entrega proyecto (4) redes Wireless</b> TG: Técnica del tipo Trabajo en Grupo Evaluación continua

				No presencial Duración: 05:00
6	<p><b>Seguridad en dispositivos móviles.</b> <b>Seguridad en redes Ad Hoc</b> Duración: 03:00 AC: Actividad del tipo Acciones Cooperativas</p>	<p><b>Resolución de supuestos y actividades prácticas</b> Duración: 03:00 PL: Actividad del tipo Prácticas de Laboratorio</p>		<p><b>Cuestionario redes ad hoc y móviles</b> ET: Técnica del tipo Prueba Telemática Evaluación continua No presencial Duración: 00:30</p> <p><b>Entrega proyecto (5) redes ad hoc y móviles</b> TG: Técnica del tipo Trabajo en Grupo Evaluación continua No presencial Duración: 05:00</p>
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				<p><b>Entrega proyecto (2) Seguridad en la Red y el Acceso</b> TG: Técnica del tipo Trabajo en Grupo Evaluación sólo prueba final No presencial Duración: 00:30</p> <p><b>Cuestionario Seguridad en la red y en acceso.</b> ET: Técnica del tipo Prueba Telemática Evaluación sólo prueba final No presencial Duración: 00:30</p> <p><b>Entrega proyecto (1) criptografía aplicada</b> TG: Técnica del tipo Trabajo en Grupo Evaluación sólo prueba final No presencial Duración: 00:30</p> <p><b>Entrega proyecto (5) redes ad hoc y móviles</b> TG: Técnica del tipo Trabajo en Grupo Evaluación sólo prueba final No presencial Duración: 00:30</p> <p><b>Cuestionario redes ad hoc y móviles</b> ET: Técnica del tipo Prueba Telemática Evaluación sólo prueba final No presencial Duración: 00:30</p> <p><b>Cuestionario redes ad hoc y móviles</b> ET: Técnica del tipo Prueba Telemática</p>

						<p>Evaluación sólo prueba final No presencial Duración: 00:30</p> <p><b>Entrega proyecto (4) redes Wireless</b> TG: Técnica del tipo Trabajo en Grupo Evaluación sólo prueba final No presencial Duración: 00:30</p> <p><b>Cuestionario Wireless</b> ET: Técnica del tipo Prueba Telemática Evaluación sólo prueba final No presencial Duración: 00:30</p> <p><b>Entrega proyecto (3): Túneles y VPN</b> TG: Técnica del tipo Trabajo en Grupo Evaluación sólo prueba final No presencial Duración: 00:30</p> <p><b>Cuestionario Túneles</b> ET: Técnica del tipo Prueba Telemática Evaluación sólo prueba final No presencial Duración: 00:30</p>
--	--	--	--	--	--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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
1	Cuestionario Criptografía Aplicada	ET: Técnica del tipo Prueba Telemática	No Presencial	00:30	5%	0 / 10	CG05
1	Entrega proyecto (1) criptografía aplicada	TG: Técnica del tipo Trabajo en Grupo	No Presencial	05:00	15%	0 / 10	CE05 CG05 CG09 CE06
2	Cuestionario Seguridad en la red y en acceso.	ET: Técnica del tipo Prueba Telemática	No Presencial	00:30	5%	0 / 10	CG05 CG09
2	Entrega proyecto (2) Seguridad en la Red y el Acceso	TG: Técnica del tipo Trabajo en Grupo	No Presencial	05:00	15%	0 / 10	CG05 CG09 CE06 CE05
4	Cuestionario Túneles	ET: Técnica del tipo Prueba Telemática	No Presencial	00:30	5%	0 / 10	CG05 CG09
4	Entrega proyecto (3): Túneles y VPN	TG: Técnica del tipo Trabajo en Grupo	No Presencial	05:00	15%	0 / 10	CE05 CG05 CG09 CE06
5	Cuestionario Wireless	ET: Técnica del tipo Prueba Telemática	No Presencial	00:30	5%	0 / 10	CG05 CG09
5	Entrega proyecto (4) redes Wireless	TG: Técnica del tipo Trabajo en Grupo	No Presencial	05:00	15%	0 / 10	CG09 CE05 CG05 CE06

6	Cuestionario redes ad hoc y móviles	ET: Técnica del tipo Prueba Telemática	No Presencial	00:30	5%	0 / 10	CE05 CG09
6	Entrega proyecto (5) redes ad hoc y móviles	TG: Técnica del tipo Trabajo en Grupo	No Presencial	05:00	15%	0 / 10	CE05 CG05 CG09 CE06

### 7.1.2. Prueba evaluación global

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
17	Cuestionario redes ad hoc y móviles	ET: Técnica del tipo Prueba Telemática	No Presencial	00:30	5%	0 / 10	CE05 CG05 CG09 CE06
17	Cuestionario redes ad hoc y móviles	ET: Técnica del tipo Prueba Telemática	No Presencial	00:30	5%	0 / 10	CE05 CG05 CG09 CE06
17	Entrega proyecto (1) criptografía aplicada	TG: Técnica del tipo Trabajo en Grupo	No Presencial	00:30	15%	0 / 10	CG09 CE06 CE05 CG05
17	Cuestionario Seguridad en la red y en acceso.	ET: Técnica del tipo Prueba Telemática	No Presencial	00:30	5%	0 / 10	CE05 CG05 CG09 CE06
17	Entrega proyecto (5) redes ad hoc y móviles	TG: Técnica del tipo Trabajo en Grupo	No Presencial	00:30	15%	0 / 10	
17	Entrega proyecto (2) Seguridad en la Red y el Acceso	TG: Técnica del tipo Trabajo en Grupo	No Presencial	00:30	15%	0 / 10	CE05 CG05 CG09 CE06
17	Entrega proyecto (4) redes Wireless	TG: Técnica del tipo Trabajo en Grupo	No Presencial	00:30	15%	0 / 10	CE05 CG05 CG09 CE06
17	Cuestionario Wireless	ET: Técnica del tipo Prueba Telemática	No Presencial	00:30	5%	0 / 10	CE05 CG05 CG09 CE06
17	Entrega proyecto (3): Túneles y VPN	TG: Técnica del tipo Trabajo en Grupo	No Presencial	00:30	15%	0 / 10	CE05 CG05 CG09 CE06

17	Cuestionario Túneles	ET: Técnica del tipo Prueba Telemática	No Presencial	00:30	5%	0 / 10	CE05 CG05 CG09 CE06
----	----------------------	----------------------------------------	---------------	-------	----	--------	------------------------------

### 7.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
Convocatoria extraordinaria	EX: Técnica del tipo Examen Escrito	Presencial	02:00	100%	5 / 10	CE05 CG05 CG09 CE06

## 7.2. Criterios de evaluación

Para superar la asignatura el alumno deberá obtener una calificación igual o superior a 5.0 puntos por la realización de las diferentes actividades de evaluación y en las condiciones indicadas en el apartado anterior.

En la evaluación PROGRESIVA, las distintas entregas del proyecto de evaluación se harán de manera escalonada. Para aquellos alumnos que no superen estas pruebas se dispondrá de una prueba de evaluación global en la Semana 17 consistente en la entrega del mismo proyecto (en una memoria y entrega únicas), y que supondrá el 100% de la calificación de la asignatura.

En convocatoria Extraordinaria se aplicarán estos mismos criterios.

### ATENCIÓN A LOS DIFERENTES PERFILES DE ACCESO

En función de su perfil de acceso, los alumnos podrán optar por distintas modalidades para la realización del proyecto. La primera modalidad trabajará los contenidos desde una perspectiva clásica, mientras que aquellos alumnos con un nivel formativo inferior en el área de redes podrán optar por una actividad de revisión tecnológica, investigación o despliegue de un sistema de demostración de acuerdo a un esquema guiado y previamente definido por el profesor. El profesorado, a la vista del nivel formativo de los alumnos, podrá ofrecerles esta alternativa en los casos que considere oportunos.

## 8. Recursos didácticos

### 8.1. Recursos didácticos de la asignatura

Nombre	Tipo	Observaciones
Bibliografía	Bibliografía	Colección de diapositivas realizadas por el profesor para cada tema.
Recursos web	Recursos web	Plataforma moodle de la asignatura
Equipamiento	Equipamiento	Software de libre distribución aplicable al contenido de la asignatura: Dsistribución Kali Linux.Distribución pfSense.
Aula	Otros	Aula equipada con ordenador proyector de video y pizarra.
Laboratorio	Equipamiento	Laboratorio con ordenadores con software adecuado para la realización de las prácticas. Plataforma PKI. Plataforma servidora RADIUS. Routes WIFI.
Articulos1	Bibliografía	Artículos de la revista haking9, especificados en el moodle de la asignatura.
Artículos2	Bibliografía	FAQ'S de criptografía Especificacion TLS Tutorial de manejo de OpenSSL
Norma IEEE802.11i	Bibliografía	Norma IEEE802.11i
Página web de netfilter	Bibliografía	Descripción del funcionamiento del netfilter de linux
Documentación IPSec	Bibliografía	Página wen IPSec, especificación de la norma.
Página web de OpenVPN	Bibliografía	Página web de OpenVPN.
Herramientas hacking	Bibliografía	Página de dsniff Página de knockd Herramientas DOS Lista de fuzzers  

## 9. Otra información

---

### 9.1. Otra información sobre la asignatura

#### ATENCIÓN A LOS DIFERENTES PERFILES DE ACCESO

Para aquellos alumnos que, por su perfil de acceso al máster, así lo precisen, se dispondrá de un "Tema 0" impartido en formato "Flipped Classroom". El objetivo es apoyar a aquellos alumnos que así lo precisen en formación básica de redes de computadores. Los materiales incluirán vídeos y lecturas que les permitan garantizar el adecuado seguimiento de la asignatura.