



UNIVERSIDAD  
POLITÉCNICA  
DE MADRID

PROCESO DE  
COORDINACIÓN DE LAS  
ENSEÑANZAS PR/CL/001



E.T.S. de Ing. de Sistemas  
Informáticos

# ANX-PR/CL/001-01

## GUÍA DE APRENDIZAJE

### ASIGNATURA

613000100 - Seguridad En Aplicaciones Web

### PLAN DE ESTUDIOS

61AF - Master Universitario En Ingeniería Web

### CURSO ACADÉMICO Y SEMESTRE

2025/26 - 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.....	3
6. Cronograma.....	6
7. Actividades y criterios de evaluación.....	8
8. Recursos didácticos.....	12
9. Otra información.....	13

## 1. Datos descriptivos

---

### 1.1. Datos de la asignatura

<b>Nombre de la asignatura</b>	613000100 - Seguridad en Aplicaciones Web
<b>No de créditos</b>	4 ECTS
<b>Carácter</b>	Obligatoria
<b>Curso</b>	Primer curso
<b>Semestre</b>	Primer semestre
<b>Período de impartición</b>	Septiembre-Enero
<b>Idioma de impartición</b>	Castellano
<b>Titulación</b>	61AF - Master Universitario en Ingeniería Web
<b>Centro responsable de la titulación</b>	61 - E.T.S De Ing. De Sistemas Informáticos
<b>Curso académico</b>	2025-26

## 2. Profesorado

---

### 2.1. Profesorado implicado en la docencia

<b>Nombre</b>	<b>Despacho</b>	<b>Correo electrónico</b>	<b>Horario de tutorías</b> *
Juan Alberto De Frutos Velasco (Coordinador/a)	1223	juanalberto.defrutos@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

- Back-end Con Tecnologías De Libre Distribución

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

El plan de estudios Master Universitario en Ingeniería Web no tiene definidos otros conocimientos previos para esta asignatura.

## 4. Competencias y resultados de aprendizaje

---

### 4.1. Competencias

CE01 - Requisar, analizar y diseñar en un desarrollo Web bajo las metodologías vigentes en el entorno profesional.

CE02 - Programar y probar en un desarrollo Web con los lenguajes y técnicas vigentes en el entorno profesional.

CE06 - Incorporar seguridad, calidad, usabilidad y persistencia al desarrollo Web vigentes en el entorno profesional.

CE09 - Respetar los marcos legal, social y económico de los desarrollos vigentes en el entorno profesional.

## 4.2. Resultados del aprendizaje

RA40 - Saber desarrollar software seguro para aplicaciones web usando cualquier plataforma

RA41 - Utilizar herramientas que realicen análisis de vulnerabilidades en las aplicaciones web.

RA36 - Conocer los riesgos de seguridad asociados a las aplicaciones web.

RA39 - Saber identificar vulnerabilidades en las aplicaciones web

RA37 - Configurar un sitio web de forma segura.

RA38 - Utilizar soluciones criptográficas adecuadas para una aplicación web.

## 5. Descripción de la asignatura y temario

---

### 5.1. Descripción de la asignatura

Análisis de riesgos de seguridad asociados a las aplicaciones web: XSS, robos de sesión, SQL injection, etc.

Identificación de vulnerabilidades en aplicaciones web.

Herramientas de análisis de vulnerabilidades en aplicaciones web.

Desarrollo de aplicaciones web seguras.

Empleo de soluciones criptográficas adecuadas.

Configuración segura de sitios web.

## 5.2. Temario de la asignatura

1. Tema 1: Introducción y conceptos previos
2. Tema 2: El protocolo SSL/TLS
  - 2.1. Comunicación segura entre cliente y servidor web
  - 2.2. Autenticación del servidor web con certificado digital
  - 2.3. Cómo obtener un certificado para un servidor web
  - 2.4. Configurar SSL en el servidor web
  - 2.5. Ataques MITM con SSL
  - 2.6. Autenticación de un cliente con certificado digital
  - 2.7. Cómo obtener un certificado digital de cliente
  - 2.8. Configurar SSL para certificados digitales de cliente
3. Tema 3: Cross Site Scripting (XSS)
  - 3.1. XSS Reflejado
  - 3.2. XSS permanente
4. Tema 4: Robo de Sesión
  - 4.1. Sesiones web
  - 4.2. Robo del identificador de sesión
  - 4.3. Ataques de fijación de sesión (Session Fixation)
  - 4.4. Robo del JWT
5. Tema 5: CSRF y ClickJacking
  - 5.1. CSRF (Cross Site Request Forgery)
  - 5.2. ClickJacking
6. Tema 6: SQL Injection
  - 6.1. Concepto de SQL injection
  - 6.2. Medidas para mitigar SQL injection
  - 6.3. SQL injection a través de metadatos del SGDB
  - 6.4. Blind SQL injection
7. Tema 7: Otros temas de seguridad en las aplicaciones web

- 7.1. Validación de los datos no fiables
  - 7.2. Parameter Tampering
  - 7.3. Proteger información sensible
  - 7.4. Ataques de Path Traversal
  - 7.5. Ataques de File Inclusion
  - 7.6. Referencias directas inseguras a objetos
  - 7.7. Carga de ficheros en el servidor (Upload)
  - 7.8. Inyecciones de código del sistema operativo.
8. Tema 8: Herramientas de análisis de vulnerabilidades en aplicaciones web
- 8.1. SAST (Static Analysis Security Testing)
  - 8.2. DAST (Dynamic Analysis Security Testing)
    - 8.2.1. Escaneo pasivo
    - 8.2.2. Escaneo activo
  - 8.3. DevSecOps

## 6. Cronograma

### 6.1. Cronograma de la asignatura \*

Sem	Actividad tipo 1	Actividad tipo 2	Tele-enseñanza	Actividades de evaluación
1	<p><b>Tema 1: Conceptos Previos</b> Duración: 02:00 LM: Actividad del tipo Lección Magistral</p> <p><b>Tema 2: El protocolo SSL/TLS</b> Duración: 05:00 LM: Actividad del tipo Lección Magistral</p> <p><b>Tema 3: Cross Site Scripting</b> Duración: 03:00 LM: Actividad del tipo Lección Magistral</p>	<p><b>Tema 1: Conceptos Previos</b> Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio</p> <p><b>Tema 2: El protocolo SSL/TLS</b> Duración: 05:00 PL: Actividad del tipo Prácticas de Laboratorio</p> <p><b>Tema 3: Cross Site Scripting</b> Duración: 03:00 PL: Actividad del tipo Prácticas de Laboratorio</p>	<p><b>Tema 1. Estudio individual del material aportado por el profesor</b> Duración: 00:00 AIV: Aula invertida</p> <p><b>Tema 2. Estudio individual del material aportado por el profesor</b> Duración: 00:00 AIV: Aula invertida</p> <p><b>Tema 3. Estudio individual del material aportado por el profesor</b> Duración: 00:00 AIV: Aula invertida</p>	<p><b>Asistencia y participación en el aula (RA36, RA37, RA38, RA39, RA40, RA41)</b> OT: Otras técnicas evaluativas Evaluación Progresiva y Global Presencial Duración: 00:00</p> <p><b>Práctica 1: SSL/TLS, XSS y Robos de Sesión (RA36, RA37, RA38, RA39, RA40)</b> TI: Técnica del tipo Trabajo Individual Evaluación Progresiva y Global No presencial Duración: 22:00</p>
2	<p><b>Tema 4: Robo de sesión</b> Duración: 02:00 LM: Actividad del tipo Lección Magistral</p> <p><b>Tema 5: CSRF y ClickJacking</b> Duración: 02:00 LM: Actividad del tipo Lección Magistral</p> <p><b>Tema 6 : SQL injection</b> Duración: 02:00 LM: Actividad del tipo Lección Magistral</p> <p><b>Tema 7: Otros temas de seguridad en las aplicaciones web</b> Duración: 02:40 LM: Actividad del tipo Lección Magistral</p> <p><b>Examen de test</b> Duración: 00:20 OT: Otras actividades formativas / Evaluación</p>	<p><b>Tema 4: Robo de sesión</b> Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio</p> <p><b>Tema 5: CSRF y ClickJacking</b> Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio</p> <p><b>Tema 6 : SQL injection</b> Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio</p> <p><b>Tema 7: Otros temas de seguridad en las aplicaciones web</b> Duración: 03:00 PL: Actividad del tipo Prácticas de Laboratorio</p> <p><b>Tema 8: Herramientas de análisis de vulnerabilidades en aplicaciones web</b> Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio</p>	<p><b>Tema 4. Estudio individual del material aportado por el profesor</b> Duración: 00:00 AIV: Aula invertida</p> <p><b>Tema 5. Estudio individual del material aportado por el profesor</b> Duración: 00:00 AIV: Aula invertida</p> <p><b>Tema 6. Estudio individual del material aportado por el profesor</b> Duración: 00:00 AIV: Aula invertida</p> <p><b>Tema 7. Estudio individual del material aportado por el profesor</b> Duración: 00:00 AIV: Aula invertida</p>	<p><b>Asistencia y participación en el aula (RA36, RA37, RA38, RA39, RA40, RA41)</b> OT: Otras técnicas evaluativas Evaluación Progresiva y Global Presencial Duración: 00:00</p> <p><b>Práctica 2: SQL injection, Path traversal y herramientas DAST (RA36, RA39, RA40, R41)</b> TI: Técnica del tipo Trabajo Individual Evaluación Progresiva y Global No presencial Duración: 18:00</p> <p><b>Examen de Test (RA36, RA37, RA38, RA39, RA40, RA41)</b> EX: Técnica del tipo Examen Escrito Evaluación Progresiva Presencial Duración: 00:20</p>
3				
4				
5				

6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				Examen de Test. Recuperación (RA36, RA37, RA38, RA39, RA40, RA41) EX: Técnica del tipo Examen Escrito Evaluación Global Presencial Duración: 00:20

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.

## 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	Asistencia y participación en el aula (RA36, RA37, RA38, RA39, RA40, RA41)	OT: Otras técnicas evaluativas	Presencial	00:00	5%	5 / 10	CE02 CE06 CE09 CE01
1	Práctica 1: SSL/TLS, XSS y Robos de Sesión (RA36, RA37, RA38, RA39, RA40)	TI: Técnica del tipo Trabajo Individual	No Presencial	22:00	40%	3 / 10	CE01 CE02 CE06 CE09
2	Asistencia y participación en el aula (RA36, RA37, RA38, RA39, RA40, RA41)	OT: Otras técnicas evaluativas	Presencial	00:00	5%	5 / 10	CE01 CE02 CE06 CE09
2	Práctica 2: SQL injection, Path traversal y herramientas DAST (RA36, RA39, RA40, R41)	TI: Técnica del tipo Trabajo Individual	No Presencial	18:00	35%	3 / 10	CE01 CE02 CE06 CE09
2	Examen de Test (RA36, RA37, RA38, RA39, RA40, RA41)	EX: Técnica del tipo Examen Escrito	Presencial	00:20	15%	3 / 10	CE01 CE02 CE06 CE09

#### 7.1.2. Prueba evaluación global

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
1	Asistencia y participación en el aula (RA36, RA37, RA38, RA39, RA40, RA41)	OT: Otras técnicas evaluativas	Presencial	00:00	5%	5 / 10	CE02 CE06 CE09 CE01
1	Práctica 1: SSL/TLS, XSS y Robos de Sesión (RA36, RA37, RA38, RA39, RA40)	TI: Técnica del tipo Trabajo Individual	No Presencial	22:00	40%	3 / 10	CE01 CE02 CE06 CE09

2	Asistencia y participación en el aula (RA36, RA37, RA38, RA39, RA40, RA41)	OT: Otras técnicas evaluativas	Presencial	00:00	5%	5 / 10	CE01 CE02 CE06 CE09
2	Práctica 2: SQL injection, Path traversal y herramientas DAST (RA36, RA39, RA40, R41)	TI: Técnica del tipo Trabajo Individual	No Presencial	18:00	35%	3 / 10	CE01 CE02 CE06 CE09
17	Examen de Test. Recuperación (RA36, RA37, RA38, RA39, RA40, RA41)	EX: Técnica del tipo Examen Escrito	Presencial	00:20	15%	3 / 10	CE01 CE02 CE06 CE09

### 7.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
Exámen final escrito (RA36, RA37, RA38, RA39, RA40, RA41)	EX: Técnica del tipo Examen Escrito	Presencial	01:30	25%	3 / 10	CE01 CE02 CE06 CE09
Práctica 1: SSL/TLS, XSS y Robos de sesión (RA36, RA37, RA38, RA39, RA40)	TI: Técnica del tipo Trabajo Individual	Presencial	30:00	40%	3 / 10	CE01 CE02 CE06 CE09
Práctica 2: SQL injection, Path traversal y herramientas DAST (RA36, RA39, RA40, RA41)	TI: Técnica del tipo Trabajo Individual	Presencial	28:00	35%	3 / 10	CE01 CE02 CE06 CE09

## 7.2. Criterios de evaluación

De acuerdo con la normativa reguladora de evaluación del aprendizaje en las titulaciones oficiales de grado y máster universitario de la Universidad Politécnica de Madrid, aprobada por Consejo de Gobierno en su sesión del 26 de mayo de 2022, el sistema de evaluación que contribuye a favorecer el aprendizaje del estudiante y el logro de los resultados de aprendizaje y la adquisición de las competencias correspondientes es el sistema de evaluación progresiva.

### SISTEMA DE EVALUACIÓN PROGRESIVA (CONVOCATORIA ORDINARIA)

La calificación de la asignatura se obtendrá tomando consideración las siguientes actividades de evaluación:

- Asistencia y participación en el aula (APA)
- Práctica 1 (Pr1)
- Práctica 2 (Pr2)
- Examen de test (Test)

La calificación final se obtiene de la siguiente fórmula:

$$\text{Nota final} = 0,1 \text{ APA} + 0,4 \text{ Pr1} * 0,35 \text{ Pr2} + 0,15 \text{ Test}$$

Además de obtener una nota final mayor o igual que 5.0, para superar la asignatura se deberán cumplir los siguientes requisitos:

- Obtener al menos un 4 en la calificación de cada una de las prácticas y un 3.5 en el examen de tipo test:  
Pr1  $\geq$  4.0, Pr2  $\geq$  4.0 y Test  $\geq$  3.5.

## SISTEMA DE EVALUACIÓN GLOBAL (CONVOCATORIA ORDINARIA)

- En el día fijado para el examen final de la asignatura todos los alumnos podrán volver a realizar el test de la asignatura, independientemente de la nota que hubieran obtenido en el test de evaluación progresiva (semana 2). La nota que se considerará para la actividad del Test será siempre la mayor que obtenga el alumno.
- Las actividades práctica1 y practica2 se consideran como no recuperables en la evaluación global debido a que no hay tiempo para poder recuperarlas. Esta asignatura es la última en impartirse en el primer semestre, por lo que las fechas de entrega de las prácticas en evaluación progresiva son muy próximas al examen final de la convocatoria ordinaria.
- La actividad APA (asistencia y participación en clase) tampoco puede ser recuperable.

En definitiva, la calificación de la asignatura en evaluación global se obtiene igual que en evaluación progresiva, pero teniendo en cuenta el examen de test realizado en la recuperación.

- Nota final =  $0,1 \text{ APA} + 0,4 \text{ Pr1} + 0,35 \text{ Pr2} + 0,15 \text{ Test}$  (nota mayor)

Ademas de obtener una nota final mayor o igual que 5.0, para superar la asignatura se deberán cumplir los siguientes requisitos:

- Obtener al menos un 4 en la calificación de cada una de las prácticas y un 3.5 en el test:  $\text{Pr1} \geq 4.0$ ,  $\text{Pr2} \geq 4.0$  y  $\text{Test} \geq 3.5$ .

## CONVOCATORIA EXTRAORDINARIA:

La calificación de la asignatura se obtendrá tomando consideración las siguientes actividades de evaluación:

- Práctica 1 (Pr1)
- Práctica 2 (Pr2)
- Examen final escrito (Ex)

Nota final = 0,4 Pr1 + 0,35 Pr2 + 0,25 Ex.

Además de obtener una nota final mayor o igual que 5.0, para superar la asignatura se deberán cumplir los siguientes requisitos:

- Obtener al menos un 4 en la calificación de cada una de las prácticas y un 3.5 en el examen final escrito:  
Pr1  $\geq$  4.0, Pr2  $\geq$  4.0 y Ex  $\geq$  3.5.

## 8. Recursos didácticos

---

### 8.1. Recursos didácticos de la asignatura

Nombre	Tipo	Observaciones
<a href="https://moodle.upm.es">https://moodle.upm.es</a>	Recursos web	Plataforma Moodle de la UPM en donde se dispone de todos los recursos utilizados en clase.
<a href="http://www.owasp.org">http://www.owasp.org</a>	Recursos web	Comunidad abierta y libre, enfocada a facilitar a las organizaciones a desarrollar, adquirir y mantener aplicaciones más seguras.
Web Application Security, Bryan Sullivan, Vincent Luiw, Mc Graw Hill, 2012	Bibliografía	Fundamentos sobre la programación web segura
Pro PHP Security, 2nd Edition, Chris Snider, Thomas Myer, Michale Southwell, Apress, 2010	Bibliografía	Programación web segura con PHP

Essential PHP Security, Chris Shiflett, O'Really, 2005	Bibliografía	Programación web segura con PHP
Bulletproof SSL/TLS and PKI, Ivan Ristic, 2022	Bibliografía	Protocolo TLS/SSL
Iron-Clad Java: Bulding Secure Web Applications	Bibliografía	Programación web segura con Java

## 9. Otra información

---

### 9.1. Otra información sobre la asignatura

El Máster Universitario en Ingeniería Web se ofrece en dos modalidades de impartición diferentes:

Modalidad Presencial\*, con presencialidad de lunes a jueves, en horario de mañana

Modalidad Semipresencial, con presencialidad en viernes tarde y sábados mañana.

\* por decisión de la Junta de Escuela del 14/03/2022, a partir del curso 2022-2023 el máster sólo se ofrecerá en modalidad semipresencial.

En ambos casos las actividades formativas llevadas a cabo y las metodologías docentes empleadas permiten evaluar los resultados de aprendizaje descritos en la memoria del programa. La oferta de estas dos modalidades se asienta en tres componentes básicos: las clases presenciales, las tutorías (presenciales, por correo electrónico, foros, chats, videoconferencia, etc.) y los recursos tecnológicos (plataforma virtual Moodle) . Para garantizar la adquisición de las competencias definidas en la memoria del título, se emplea un sistema de evaluación común e independiente de la modalidad de enseñanza cursada.