



UNIVERSIDAD
POLITÉCNICA
DE MADRID

PROCESO DE
COORDINACIÓN DE LAS
ENSEÑANZAS PR/CL/001



E.T.S. de Ingenieros de
Telecomunicacion

ANX-PR/CL/001-01

GUÍA DE APRENDIZAJE

ASIGNATURA

93001009 - Seguridad en el Desarrollo Software

PLAN DE ESTUDIOS

09AW - Master Universitario En Ciberseguridad

CURSO ACADÉMICO Y SEMESTRE

2019/20 - Segundo semestre

Índice

Guía de Aprendizaje

1. Datos descriptivos.....	1
2. Profesorado.....	1
3. Competencias y resultados de aprendizaje.....	2
4. Descripción de la asignatura y temario.....	3
5. Cronograma.....	4
6. Actividades y criterios de evaluación.....	6
7. Recursos didácticos.....	8

1. Datos descriptivos

1.1. Datos de la asignatura

Nombre de la asignatura	93001009 - Seguridad en el Desarrollo Software
No de créditos	3 ECTS
Carácter	Obligatoria
Curso	Primer curso
Semestre	Segundo semestre
Período de impartición	Febrero-Junio
Idioma de impartición	Castellano
Titulación	09AW - Master Universitario En Ciberseguridad
Centro responsable de la titulación	09 - Escuela Tecnica Superior de Ingenieros de Telecomunicacion
Curso académico	2019-20

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Juan Alberto De Frutos Velasco (Coordinador/a)	1223 (ETSISI)	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.

2.3. Profesorado externo

Nombre	Correo electrónico	Centro de procedencia
Socorro Bernardos Galindo	sbernardos@fi.upm.es	ETSIIInf (UPM)

3. Competencias y resultados de aprendizaje

3.1. Competencias

CE06 - Capacidad de aplicar las principales metodologías y técnicas de seguridad en el desarrollo del software y sistemas informáticos

CG02 - Dotar al alumno del conocimiento de los distintos tipos de amenazas que pueden afectar a una organización y sus consecuencias en diferentes escenarios sociales, económicos e industriales y dotarle de la capacidad de aplicar las técnicas de análisis y gestión de todo tipo de riesgos para definir e implantar las salvaguardas necesarias para mitigar o eliminar sus impactos hacer resiliente a la organización

CT12 - Aprendizaje autónomo, adaptación a nuevas situaciones y motivación por el desarrollo profesional permanente

CT14 - Motivación por la calidad

3.2. Resultados del aprendizaje

RA14 - Conocer las técnicas de ciberataques para explotar las vulnerabilidades en el software

RA13 - Analizar las vulnerabilidades que puedan existir en una aplicación software. Así como saber programar para evitar dichas vulnerabilidades

4. Descripción de la asignatura y temario

4.1. Descripción de la asignatura

- Presentación de las vulnerabilidades más relevantes asociadas al desarrollo software en diferentes lenguajes y plataformas: C, C++, Java, aplicaciones web, aplicaciones móviles.
- Explotación de las vulnerabilidades.
- Análisis de los motivos por los que se producen dichas vulnerabilidades.
- Medidas para mitigar los riesgos asociados a estas vulnerabilidades.
- Modelos de desarrollo seguro.

4.2. Temario de la asignatura

1. Programación segura en las aplicaciones web
 - 1.1. Introducción. Conceptos Previos
 - 1.2. Cross Site Scripting. XSS
 - 1.3. Robos de sesión
 - 1.4. SQL injection
 - 1.5. Otros temas de seguridad web
 - 1.6. Análisis de vulnerabilidades web
2. Violaciones de memoria
 - 2.1. Buffer Overflow
3. Programación segura en Java
4. Programación segura en las aplicaciones móviles
 - 4.1. OWASP top 10 para móviles
5. Modelos de desarrollo software seguro

5. Cronograma

5.1. Cronograma de la asignatura *

Sem	Actividad presencial en aula	Actividad presencial en laboratorio	Otra actividad presencial	Actividades de evaluación
1	Tema 1. Apartado 1.1: Introducción. Conceptos Previos. Duración: 01:30 LM: Actividad del tipo Lección Magistral Tema 1. Apartado 1.2: Cross Site Scripting Duración: 01:30 LM: Actividad del tipo Lección Magistral Tema 1. Apartado 1.3: Robos de sesión Duración: 02:00 LM: Actividad del tipo Lección Magistral Tema 1. Apartado 1.4: SQL injection Duración: 01:00 LM: Actividad del tipo Lección Magistral	Laboratorio de Cross Site Scripting Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio Laboratorio de robos de sesión Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		Asistencia a clases OT: Otras técnicas evaluativas Evaluación continua Duración: 00:00
2	Tema 1. Apartado 1.5: Otras vulnerabilidades web Duración: 02:00 LM: Actividad del tipo Lección Magistral Tema 2: Violaciones de memoria Duración: 01:30 LM: Actividad del tipo Lección Magistral Tema 3: Programación segura en Java. Duración: 01:00 LM: Actividad del tipo Lección Magistral	Laboratorio SQL injection. Duración: 01:40 PL: Actividad del tipo Prácticas de Laboratorio Laboratorio otras vulnerabilidades web Duración: 01:00 PL: Actividad del tipo Prácticas de Laboratorio Laboratorio análisis de vulnerabilidades web Duración: 01:00 PL: Actividad del tipo Prácticas de Laboratorio Laboratorio Violaciones de memoria Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio		Test Tema 1 (Programación segura en aplicaciones web) EX: Técnica del tipo Examen Escrito Evaluación continua Duración: 00:20 Asistencia a clases OT: Otras técnicas evaluativas Evaluación continua Duración: 00:00
3	Tema 3: Programación segura en Java. Duración: 01:00 LM: Actividad del tipo Lección Magistral Tema 4: Programación segura en aplicaciones móviles Duración: 02:00 LM: Actividad del tipo Lección Magistral Tema 5: Modelos de desarrollo software seguro. Duración: 03:40 LM: Actividad del tipo Lección Magistral	Laboratorio programación segura en Java Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio Laboratorio programación segura en aplicaciones móviles Duración: 01:00 PL: Actividad del tipo Prácticas de Laboratorio		Test temas 2,3,4 y 5 EX: Técnica del tipo Examen Escrito Evaluación continua Duración: 00:20 Asistencia a clases OT: Otras técnicas evaluativas Evaluación continua Duración: 00:00

4				<p>Práctica 1. Programación segura web: XSS y Robos de sesión</p> <p>Ti: Técnica del tipo Trabajo Individual Evaluación continua Duración: 12:00</p>
5				<p>Práctica 2. Programación segura web: SQL injection, path traversal y análisis de vulnerabilidades</p> <p>Ti: Técnica del tipo Trabajo Individual Evaluación continua Duración: 10:00</p> <p>Práctica 3.</p> <p>Ti: Técnica del tipo Trabajo Individual Evaluación continua Duración: 06:00</p>
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				<p>Exámen evaluación final</p> <p>EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Duración: 02:00</p> <p>Práctica Final</p> <p>Ti: Técnica del tipo Trabajo Individual Evaluación sólo prueba final Duración: 28:00</p>
17				

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.

6. Actividades y criterios de evaluación

6.1. Actividades de evaluación de la asignatura

6.1.1. Evaluación continua

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
1	Asistencia a clases	OT: Otras técnicas evaluativas	Presencial	00:00	1.67%	5 / 10	
2	Test Tema 1 (Programación segura en aplicaciones web)	EX: Técnica del tipo Examen Escrito	Presencial	00:20	15%	/ 10	CE06 CG02
2	Asistencia a clases	OT: Otras técnicas evaluativas	Presencial	00:00	1.67%	5 / 10	
3	Test temas 2,3,4 y 5	EX: Técnica del tipo Examen Escrito	Presencial	00:20	15%	/ 10	CE06 CG02
3	Asistencia a clases	OT: Otras técnicas evaluativas	Presencial	00:00	1.66%	5 / 10	
4	Práctica 1. Programación segura web: XSS y Robos de sesión	TI: Técnica del tipo Trabajo Individual	No Presencial	12:00	25%	3 / 10	CE06 CT12 CT14 CG02
5	Práctica 2. Programación segura web: SQL injection, path traversal y análisis de vulnerabilidades	TI: Técnica del tipo Trabajo Individual	No Presencial	10:00	25%	3 / 10	CE06 CT12 CT14 CG02
5	Práctica 3.	TI: Técnica del tipo Trabajo Individual	No Presencial	06:00	15%	3 / 10	CT14 CG02 CE06 CT12

6.1.2. Evaluación sólo prueba final

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
-----	-------------	-----------	------	----------	-----------------	-------------	------------------------

16	Exámen evaluación final	EX: Técnica del tipo Examen Escrito	Presencial	02:00	40%	3 / 10	CE06 CG02
16	Práctica Final	TI: Técnica del tipo Trabajo Individual	No Presencial	28:00	60%	3 / 10	CE06 CT12 CT14 CG02

6.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
Examen evaluación final	EX: Técnica del tipo Examen Escrito	Presencial	02:00	40%	3 / 10	CE06 CG02
Práctica Final	TI: Técnica del tipo Trabajo Individual	Presencial	28:00	60%	3 / 10	CE06 CT12 CT14 CG02

6.2. Criterios de evaluación

En la convocatoria ordinaria se contemplan dos mecanismos de evaluación diferenciados y excluyentes:

- Evaluación continua. La calificación de la asignatura se obtendrá tomando en consideración los pesos de las diferentes actividades de evaluación expuestos en el apartado anterior. Para superar la asignatura se deberán cumplir los siguientes requisitos:

- Obtener al menos 5.0 en la suma ponderada de las calificaciones.
- Haber asistido al menos al 50% de las clases.
- Obtener al menos un 3.0 en la calificación de cada una de las prácticas.
- Obtener al menos un 3.0 en la nota media de los tests: $(\text{Test 1} + \text{Test 2}) / 2 \geq 3.0$.

- Evaluación sólo mediante prueba final (para aquellos alumnos que opten a ella). La calificación final de la asignatura tendrá en cuenta una práctica final y un examen escrito, con un 60% y un 40% de peso en la nota, respectivamente. La práctica integrará los contenidos de las tres prácticas que se han propuesto durante el curso, y habrá de obtenerse al menos un 30% de la nota total. De forma similar, en el examen escrito habrá de obtenerse

al menos un 30% de la nota.

En la **convocatoria extraordinaria** se seguirán los mismos criterios de evaluación que en la convocatoria ordinaria por prueba final.

7. Recursos didácticos

7.1. Recursos didácticos de la asignatura

Nombre	Tipo	Observaciones
https://moodle.upm.es	Recursos web	Plataforma moodle de la UPM en donde se ponen a disposición de los alumnos los recursos utilizados en la asignatura.
The CERT Oracle Secure Coding Standard for Java, Fred Long, Dhruv Mohindra, Robert C. Seacord, Dean F. Sutherland, David Svoboda, Addison Wesley, 2012	Bibliografía	Técnicas de programación segura en Java
https://www.owasp.org	Recursos web	Comunidad abierta y libre, enfocada a facilitar a las organizaciones desarrollar, adquirir y mantener aplicaciones más seguras.
Web Application Security, Bryan Sullivan, Vincent Liu, 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