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

2022/23 - Segundo semestre

Índice

Guía de Aprendizaje

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	2022-23

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	ETSIInf (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. CSRF y ClickJacking
   1.5. SQL injection
   1.6. Otros temas de seguridad web
   1.7. Herramientas de análisis de vulnerabilidades web
2. Programación segura en Java
3. Programación segura en las aplicaciones móviles
   3.1. OWASP top 10 para móviles
4. Violaciones de memoria
   4.1. Buffer Overflow
5. Modelos de desarrollo software seguro

5. Cronograma

5.1. Cronograma de la asignatura *

Sem	Actividad en aula	Actividad en laboratorio	Tele-enseñanza	Actividades de evaluación
1		**Tema 1. Apartado 1.1: Introducción. Conceptos Previos.** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio **Tema 1. Apartado 1.2: Cross Site Scripting** Duración: 03:30 PL: Actividad del tipo Prácticas de Laboratorio **Tema 1. Apartado 1.3: Robos de sesión** Duración: 03:30 PL: Actividad del tipo Prácticas de Laboratorio **Tema 1. Apartado 1.4: SQL injection** Duración: 01:00 PL: Actividad del tipo Prácticas de Laboratorio		**Práctica 1. Programación segura web: XSS y Robo de sesión** TI: Técnica del tipo Trabajo Individual Evaluación continua y sólo prueba final No presencial Duración: 14:00
2		**Tema 1. Apartado 1.4: SQL injection** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio **Tema 1. Apartado 1.5: Otros temas de seguridad web** Duración: 03:00 PL: Actividad del tipo Prácticas de Laboratorio **Tema 1. Apartado 1.6: Análisis de vulnerabilidades** Duración: 01:40 PL: Actividad del tipo Prácticas de Laboratorio **Tema 2: Programación segura en Java.** Duración: 03:00 PL: Actividad del tipo Prácticas de Laboratorio		**Práctica 2. Programación segura web: SQL injection, Path traversal y Pentesting web** TI: Técnica del tipo Trabajo Individual Evaluación continua y sólo prueba final No presencial Duración: 21:00 **Test Tema 1 (Programación segura en aplicaciones web)** EX: Técnica del tipo Examen Escrito Evaluación continua Presencial Duración: 00:20
3		**Tema 3: Programación segura en aplicaciones móviles** Duración: 03:00 PL: Actividad del tipo Prácticas de Laboratorio **Tema 4: Violaciones de memoria** Duración: 03:40 PL: Actividad del tipo Prácticas de		**Práctica 3. Violaciones de Memoria** TI: Técnica del tipo Trabajo Individual Evaluación continua y sólo prueba final No presencial Duración: 11:00 **Test temas 2,3,4 y 5** EX: Técnica del tipo Examen Escrito Evaluación continua y sólo prueba final

		Laboratorio **Tema 5: Modelos de desarrollo software seguro.** Duración: 03:00 PL: Actividad del tipo Prácticas de Laboratorio		Presencial Duración: 00:20 **Recuperación Test tema 1** EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final No presencial Duración: 00:20
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				

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.

6. Actividades y criterios de evaluación

6.1. Actividades de evaluación de la asignatura

6.1.1. Evaluación (progresiva)

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
1	Práctica 1. Programación segura web: XSS y Robo de sesión	TI: Técnica del tipo Trabajo Individual	No Presencial	14:00	22%	3 / 10	CT14 CG02 CE06 CT12
2	Práctica 2. Programación segura web: SQL injection, Path traversal y Pentesting web	TI: Técnica del tipo Trabajo Individual	No Presencial	21:00	32%	3 / 10	CT12 CT14 CG02 CE06
2	Test Tema 1 (Programación segura en aplicaciones web)	EX: Técnica del tipo Examen Escrito	Presencial	00:20	15%	/ 10	CE06 CG02
3	Práctica 3. Violaciones de Memoria	TI: Técnica del tipo Trabajo Individual	No Presencial	11:00	16%	3 / 10	CE06 CT12 CT14 CG02
3	Test temas 2,3,4 y 5	EX: Técnica del tipo Examen Escrito	Presencial	00:20	15%	/ 10	CE06 CG02

6.1.2. Prueba evaluación global

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
1	Práctica 1. Programación segura web: XSS y Robo de sesión	TI: Técnica del tipo Trabajo Individual	No Presencial	14:00	22%	3 / 10	CT14 CG02 CE06 CT12
2	Práctica 2. Programación segura web: SQL injection, Path traversal y Pentesting web	TI: Técnica del tipo Trabajo Individual	No Presencial	21:00	32%	3 / 10	CT12 CT14 CG02 CE06

3	Práctica 3. Violaciones de Memoria	TI: Técnica del tipo Trabajo Individual	No Presencial	11:00	16%	3 / 10	CE06 CT12 CT14 CG02
3	Test temas 2,3,4 y 5	EX: Técnica del tipo Examen Escrito	Presencial	00:20	15%	/ 10	CE06 CG02
3	Recuperación Test tema 1	EX: Técnica del tipo Examen Escrito	No Presencial	00:20	15%	/ 10	CE06 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	30%	3 / 10	CE06 CG02
Practica 1. Programación segura web: XSS y Robo de sesión	TI: Técnica del tipo Trabajo Individual	Presencial	14:00	22%	3 / 10	CE06 CT12 CT14 CG02
Práctica 2. Programacións segura web: SQL injection, Path traversal y Pentesting web	TI: Técnica del tipo Trabajo Individual	Presencial	21:00	32%	3 / 10	CE06 CT12 CT14 CG02
Práctica 3. Violaciones de memoria	TI: Técnica del tipo Trabajo Individual	Presencial	11:00	16%	3 / 10	CE06 CT12 CT14 CG02

6.2. Criterios de evaluación

CONVOCATORIA ORDINARIA

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

- Examen de tipo test del tema 1 (Test1)**.**
- Examen de tipo test de los temas (Test2).
- Práctica 1 (Pr1).
- Práctica 2 (Pr2).
- Práctica 3 (Pr3).

La calificación final de la asignatura se obtiene según la siguiente fórmula:

Nota Final = 0,15 Test1 + 0,15 Test 2 + 0,22 Pr1 + 0,32 Pr2 + 0,16 Pr3

Para superar la asignatura, además de obtener una nota final mayor o igual que 5.0, se deben cumplir los siguientes requisitos:

- Obtener al menos un 3.0 en la calificación de cada una de las prácticas: Pr1 >= 3.0, Pr2 >= 3.0 y Pr3 >= 3.0.
- Obtener al menos un 3.0 en la nota media de los dos exámenes de tipo test: (Test1 + Test2) / 2 >= 3.0

Sistema de evaluación progresiva

La única actividad que puede considerarse en el sistema de evaluación progresiva es Test1, ya que se realiza dentro del período de docencia.

Sistema de evaluación global

Los alumnos que hubieran obtenido una calificación inferior a 5.0 en la actividad Test1 en la evaluación progresiva, podrán recuperarla mediante otro examen al finalizar el periodo de docencia de la asignatura.

La actividad de evaluación Test2 se considera como de evaluación global, ya que se realiza al finalizar el periodo de docencia de la asignatura. Por lo tanto, no puede recuperarse.

Las actividades de prácticas Pr1, Pr2 y Pr3 se consideran también como de evaluación global, ya que se entregan una vez finalizado el periodo de docencia de la asignatura. Por tanto, no pueden recuperarse.

CONVOCATORIA EXTRAORDINARIA:

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

- Examen de evaluación final escrito (Ex)
- Práctica 1 (Pr1)
- Práctica 2 (Pr2)
- Práctica 3 (Pr3)

La calificación final de la asignatura se obtiene según la siguiente fórmula:

Nota Final = 0,3 Ex + 0,22 Pr1 + 0,32 Pr2 + 0,16 Pr3

Para superar la asignatura, además de obtener una nota final mayor o igual que 5.0, se deben cumplir los siguientes requisitos:

- Obtener al menos un 3.0 en la calificación de cada una de las prácticas: Pr1 >= 3.0, Pr2 >= 3.0 y Pr3 >= 3.0.
- Obtener al menos un 3.0 en el examen final: Ex >= 3.0

7. Recursos didácticos

7.1. Recursos didácticos de la asignatura

Nombre	Tipo	Observaciones
https://moodle.upm.es	Recursos web	Plataforma moodle dela 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 libe, 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