

Curso Académico: (2023 / 2024)

Fecha de revisión: 28-04-2023

Departamento asignado a la asignatura: Departamento de Informática

Coordinador/a: PERIS LOPEZ, PEDRO

Tipo: Optativa Créditos ECTS : 6.0

Curso : 4 Cuatrimestre :

REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

Criptografía y Seguridad Informática (3º curso / 1 cuatrimestre).

Redes de Ordenadores (3º curso / 1 cuatrimestre).

Ingeniería de la ciberseguridad aplicada a la Ingeniería de Computadores / a los sistemas de información (3º curso / 2 cuatrimestre).

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

1. Introducción a la seguridad de la computación móvil.
2. Vulnerabilidades de la infraestructura móvil.
 - a. Vulnerabilidades
 - b. Técnicas de mitigación
3. Vulnerabilidades de las comunicaciones móviles.
 - a. Vulnerabilidades
 - b. Técnicas de mitigación
4. Vulnerabilidades de los dispositivos móviles.
 - a. Vulnerabilidades
 - b. Técnicas de mitigación
5. Vulnerabilidades de las plataformas móviles
 - a. Vulnerabilidades
 - b. Técnicas de mitigación
6. Vulnerabilidades de las aplicaciones móviles.
 - a. Vulnerabilidades
 - b. Técnicas de mitigación

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

AF1. CLASES TEÓRICO-PRÁCTICAS. 1,5 ECTS con total presencialidad. En ellas se presentarán los conocimientos que deben adquirir los alumnos. Estos recibirán las notas de clase y tendrán textos básicos de referencia para facilitar el seguimiento de las clases y el desarrollo del trabajo posterior. Se resolverán ejercicios, prácticas problemas por parte del alumno y se realizarán talleres y pruebas de evaluación para adquirir las capacidades necesarias.

AF2. TUTORÍAS. 0,25 ECTS con total presencialidad. Asistencia individualizada (tutorías individuales) o en grupo (tutorías colectivas) a los estudiantes por parte del profesor.

AF3. TRABAJO INDIVIDUAL O EN GRUPO DEL ESTUDIANTE 3,75 ECTS con 0% presencialidad.

AF8: TALLERES Y LABORATORIOS. 0,25 ECTS con total presencialidad

AF9: EXAMEN FINAL. 0,25 ECTS con total presencialidad. En el que se valorarán de forma global los conocimientos, destrezas y capacidades adquiridas a lo largo del curso.

MD1: CLASE TEÓRICA. El profesor realizará presentaciones en clase, con ayudas informáticas y audiovisuales, en las que se desarrollarán los principales conceptos del curso. También se proporcionará material y bibliografía adicional para complementar el aprendizaje del alumno.

MD2: CASOS PRÁCTICOS. Los alumnos deberán resolver casos prácticos, problemas, etc. planteados por el profesor tanto de forma individual como en grupo.

MD3: TUTORÍAS. Asistencia individualizada (tutorías individuales) o en grupo (tutorías colectivas) a los estudiantes por parte del profesor.
MD6: PRÁCTICAS DE LABORATORIO. Docencia aplicada/experimental a talleres y laboratorios bajo la supervisión de un tutor.

SISTEMA DE EVALUACIÓN

SE1: EXAMEN FINAL. En el que se valorarán de forma global los conocimientos, destrezas y capacidades adquiridas a lo largo del curso.

SE2: EVALUACIÓN CONTINUA. En ella se valorarán los trabajos, presentaciones, actuación en debates, exposiciones en clase, ejercicios, prácticas y trabajo en los talleres a lo largo del curso

Peso porcentual del Examen Final:	30
Peso porcentual del resto de la evaluación:	70

BIBLIOGRAFÍA BÁSICA

- Androulidakis, I. Mobile Phone Security and Forensics: A Practical Approach, Springer, 2012
- Bergman, N., Stanfield, M., Rouse, J., Scambray, J., et al. Hacking Exposed Mobile: Security Secrets & Solutions., McGraw Hill Osbourne Media: New York, NY, 2013
- Buttyan, L. and Hubaux, J. Security and Cooperation in Wireless Networks: Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing, Cambridge University Press, 2007

BIBLIOGRAFÍA COMPLEMENTARIA

- Jeff Six Application Security for the Android Platform, O'Really Media, Inc, 2011
- Johnny Cache, Joshua Wright, Vincent Liu. Hacking wireless exposed: wireless security secrets and solutions., McGraw-Hill, 2010
- Pragati Ogal Rai Android Application Security Essentials, Packt Publishing, 2013

RECURSOS ELECTRÓNICOS BÁSICOS

- Apple Inc. . iOS security guide: https://manuals.info.apple.com/MANUALS/1000/MA1902/en_US/apple-platform-security-guide.pdf
- Google Inc. . Android security for developers: <https://developer.android.com/topic/security>