Seguridad en dispositivos móviles

Curso Académico: (2021 / 2022) **Fecha de revisión: 27/08/2021 09:18:32**

Departamento asignado a la asignatura:

Coordinador/a: PERIS LOPEZ, PEDRO

Tipo: Obligatoria Créditos ECTS : 6.0

Curso : 4 Cuatrimestre : 2

REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

Criptografia 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)

OBJETIVOS

CG2 - Ser capaz de generar nuevas ideas (creatividad) y de anticipar nuevas situaciones y de adaptarse a Trabajar en equipo y relacionarse con otros, pero al mismo tiempo tener capacidad de trabajar de forma autónoma.
CGB4 - Conocimientos básicos sobre el uso y programación de los ordenadores, sistemas operativos, bases de datos y programas informáticos con aplicación en ingeniería.
CGB5 - Conocimiento de la estructura, organización, funcionamiento e interconexión de los sistemas informáticos, los fundamentos de su programación, y su aplicación para la resolución de problemas propios de la ingeniería.
CG9 - Utilizar de forma eficiente medios TIC para redactar informes técnicos y memorias de proyectos y trabajos sobre Informática, así como presentaciones de calidad.
CGO3 - Capacidad para diseñar, desarrollar, evaluar y asegurar la accesibilidad, ergonomía, usabilidad y seguridad de los sistemas, servicios y aplicaciones informáticas, así como de la información que gestionan.
CGO6 - Capacidad para concebir y desarrollar sistemas o arquitecturas informáticas centralizadas o distribuidas integrando hardware, software y redes de acuerdo con los conocimientos adquiridos.
CGO8 - Conocimiento de las materias básicas y tecnologías, que capaciten para el aprendizaje y desarrollo de nuevos métodos y tecnologías, así como las que les doten de una gran versatilidad para adaptarse a nuevas situaciones.
CGO9 - Capacidad para resolver problemas con iniciativa, toma de decisiones, autonomía y creatividad. Capacidad para saber comunicar y transmitir los conocimientos, habilidades y destrezas de la profesión de Ingeniero Técnico en Informática.
CB3 - Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética
CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía
CECRI10 - Conocimiento de las características, funcionalidades y estructura de los Sistemas Operativos y diseñar e implementar aplicaciones basadas en sus servicios.
CECRI11 - Conocimiento y aplicación de las características, funcionalidades y estructura de los Sistemas Distribuidos, las Redes de Computadores e Internet y diseñar e implementar aplicaciones basadas en ellas.
CECRI18 - Conocimiento de la normativa y la regulación de la informática en los ámbitos nacional, europeo e internacional.

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

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

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.

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