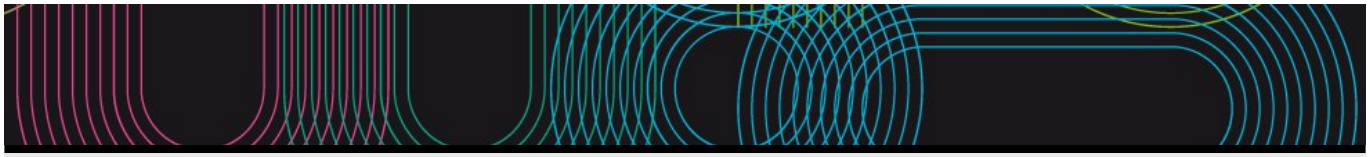

DATOS IDENTIFICATIVOS				
Seguridad en dispositivos móviles				
Asignatura	Seguridad en dispositivos móviles			
Código	V05M175V01206			
Titulacion	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	3	OP	1	2c
Lengua Impartición	Castellano Gallego Inglés			
Departamento	Dpto. Externo Ingeniería telemática			
Coordinador/a	López Bravo, Cristina			
Profesorado	Fernández Caramés, Tiago Manuel López Bravo, Cristina Rivas López, Jose Luis			
Correo-e	clbravo@det.uvigo.es			
Web	http://faitic.uvigo.es			
Descripción general	En esta asignatura se muestra una visión general de la seguridad en dispositivos móviles con diferentes características. Partiendo del estudio de la arquitectura de estos dispositivos, descubriremos su funcionamiento interno y cuáles son las principales herramientas de seguridad que incluyen, junto con los riesgos y amenazas que sufren. Estudiaremos cómo encontrar, analizar y mitigar las vulnerabilidades que afectan a los dispositivos móviles, usando herramientas de análisis forense, de desarrollo de aplicaciones seguras y de gestión de dispositivos en entornos empresariales. La documentación de esta materia estará en inglés.			

Competencias	
Código	
A2	Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
A3	Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formar juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.
A4	Que los estudiantes sepan comunicar sus conclusiones ---y los conocimientos y razones últimas que las sustentan--- a públicos especializados y no especializados de un modo claro y sin ambigüedades
B1	Tener capacidad de análisis y síntesis. Tener capacidad para proyectar, modelar, calcular y diseñar soluciones de seguridad de la información, las redes y/o los sistemas de comunicaciones en todos los ámbitos de aplicación
B2	Resolución de problemas. Tener capacidad de resolver, con los conocimientos adquiridos, problemas específicos del ámbito técnico de la seguridad de la información, las redes y/o los sistemas de comunicaciones.
B5	Tener capacidad para aplicar los conocimientos teóricos en la práctica, en el marco de infraestructuras, equipamientos y aplicaciones concretos, y sujetos a requisitos de funcionamiento específicos
C4	Comprender y aplicar los métodos y técnicas de ciberseguridad aplicables a los datos, los equipos informáticos, las redes de comunicaciones, las bases de datos, los programas y los servicios de información
C6	Desarrollar y aplicar métodos de investigación forense para el análisis de incidentes o riesgos de ciberseguridad
C9	Tener capacidad para elaborar planes y proyectos de trabajo en el ámbito de la ciberseguridad, claros, concisos y razonados
C15	Tener capacidad de identificar el valor, tanto económico como de otra índole, de la información de la institución, sus procesos críticos y el impacto que produciría la interrupción de estos; y, también, las necesidades internas y externas que permitirán estar preparados ante ataques de seguridad.
D4	Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad

D5 Tener capacidad para comunicarse oralmente y por escrito en inglés.

Resultados de aprendizaje	
Resultados previstos en la materia	Resultados de Formación y Aprendizaje
Conocer los conceptos fundamentales asociados con la seguridad en los sistemas operativos móviles y el desarrollo de apps seguras.	A2 B1 C4 C15 D4 D5
Identificar una app con comportamiento malicioso y vulnerabilidades en sistemas operativos y apps	A4 B2 C4 D4 D5
Ser capaz de realizar un análisis forense de un dispositivo móvil	A3 B2 C6 D5
Conocer los sistemas gestión de dispositivos móviles	A2 B1 B2 B5 C9 D5

Contenidos	
Tema	
Introducción: Amenazas y vulnerabilidades que afectan a los dispositivos móviles	
Arquitecturas de dispositivos móviles	
Modelos de seguridad de dispositivos móviles	
Desarrollo de aplicaciones seguras	Permisos Gestión de paquetes Gestión de usuarios APIs
Seguridad de los datos	
Seguridad de los dispositivos	
Seguridad de la red	
Vulnerabilidades, exploits y aplicaciones maliciosas	
Análisis forense de sistemas operativos móviles	
Sistemas para la gestión de la movilidad empresarial (EMM)	

Planificación			
	Horas en clase	Horas fuera de clase	Horas totales
Lección magistral	9	9	18
Prácticas con apoyo de las TIC	10	10	20
Examen de preguntas objetivas	2	14	16
Resolución de problemas y/o ejercicios	0	11	11
Informe de prácticas, prácticum y prácticas externas	0	10	10
*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado			

Metodologías	
	Descripción
Lección magistral	Exposición, por parte del profesorado, de los principales contenidos teóricos relacionados con la seguridad en dispositivos móviles. Con esta metodología se contribuirá a la adquisición de las competencias CB3, CG1, CE4, CE15, CT4 y CT5.
Prácticas con apoyo de las TIC	Realización por parte del alumnado de prácticas guiadas y supervisadas. Con esta metodología se trabajarán las competencias CG2, CG5, CB2, CB4, CE4, CE6, CE9 y CT5.

Atención personalizada

Metodologías	Descripción
Prácticas con apoyo de las TIC	Los profesores de la materia proporcionarán atención individual y personalizada los alumnos durante el curso, solucionando sus dudas y preguntas. Así mismo, los profesores orientarán y guiarán a los alumnos durante la realización de las tareas que tienen asignadas en las prácticas con apoyo de las TIC. Las dudas se atenderán de forma presencial o telemática (durante las propias prácticas, durante el horario establecido para las tutorías o durante el horario acordado con los alumnos para tutorías). El horario de tutorías se fijará al inicio del curso y se publicará en la página web de la asignatura. Fuera de este horarió, será necesario reservar las tutorías mediante cita previa.
Lección magistral	Los profesores de la materia proporcionarán atención individual y personalizada a los alumnos durante el curso, solucionando sus dudas y preguntas. Las dudas se atenderán de forma presencial o telemática (durante la propia sesión magistral, durante el horario establecido para las tutorías o durante el horario acordado con los alumnos para tutorías). El horario de tutorías se fijará al inicio del curso, y se publicará en la web de la asignatura. Fuera de este horario, será necesario reservar las tutorías mediante cita previa.

Evaluación

	Descripción	Calificación	Resultados de Formación y Aprendizaje
Examen de preguntas objetivas	Examen de preguntas cortas sobre los contenidos teóricos y prácticos revisados a lo largo del curso, tanto en las sesiones magistrales como en las prácticas de laboratorio. Este examen se realizará al final del bimestre.	50	A3 A4 C4
Resolución de problemas y/o ejercicios	Resolución de problemas en los que se haga uso de los conocimientos adquiridos tanto en las sesiones de teoría como de prácticas. Esta prueba se realizará a lo largo del bimestre, con entregas parciales en las fechas indicadas por el profesorado.	20	A2 A4 B1 B2 C4
Informe de prácticas, prácticum y prácticas externas	El alumnado completará de forma individual cuestionarios y/o informes de prácticas donde se mostrará la correcta realización y comprensión de las prácticas.	30	A4 B5 C4 C6 C9 C15 D4

Otros comentarios sobre la Evaluación

PRIMERA OPORTUNIDAD

Siguiendo las directrices propias de la titulación se ofertará a quienes cursen esta materia dos sistemas de evaluación: evaluación continua y evaluación única.

Antes de que finalice la segunda semana del curso, los estudiantes deberán indicar al profesorado de la asignatura el sistema de evaluación elegido. Quienes opten por el sistema de evaluación continua no podrán ser calificados como "no presentados" si realizan una entrega o prueba de evaluación con posterioridad a la comunicación de su decisión.

Sistema de evaluación continua

La calificación global de la asignatura será igual a la media aritmética ponderada de las pruebas indicadas previamente. Para superar la asignatura la calificación global debe ser mayor o igual que cinco.

Sistema de evaluación única

La calificación global de la asignatura será igual a la media aritmética ponderada de las tareas indicadas previamante. En este caso, la prueba de resolución de problemas se hará en un única prueba al finalizar el bimestre. Para superar la asignatura la calificación global debe ser mayor o igual que cinco.

SEGUNDA OPORTUNIDAD

La evaluación consistirá en realizar un examen de preguntas objetivas, un examen de resolución de problemas y entregar los informes de prácticas de todas las prácticas realizadas a lo largo del curso.

OTROS COMENTARIOS

Las puntuaciones obtenidas solo son válidas para el curso académico en vigor.

El uso de cualquier material durante la realización de los exámenes y pruebas de evaluación tendrá que ser autorizado explícitamente por el profesorado de la asignatura.

En caso de detección de plagio en alguno de los trabajos/pruebas realizadas la calificación final de la asignatura será de suspenso (0) y los profesores comunicarán a la dirección de la escuela el asunto para que tome las medidas que considere oportunas.

Fuentes de información

Bibliografía Básica

Dominic Chell, **The mobile application hacker´s handbook**, 1, Jonh Wiley & Sons, 2015

Bibliografía Complementaria

Joshua Drake, **Android hacker's handbook**, 1, John Wiley & Sons, 2014

Charles Miller, **iOS hacker's handbook**, 1, John Wiley & Sons, 2012

Abhishek Dubey, Anmol Misra, **Android security: attacks and defenses**, 1, CRC Press, 2013

David Thiel, **iOS application security: the definitive guide for hackers and developers**, 1, No Starch Press, 2016

Nikolay Elenkov, **Android security internals: an in-depth guide to Android's security architecture**, 1, No Starch Press, 2015

Andrew Hoog, **iPhone and iOS forensics: investigation, analysis, and mobile security for Apple iPhone, iPad, and iOS devices**, 1, Syngress/Elsevier, 2011

Andrew Hoog, **iPhone and iOS forensics: investigation, analysis, and mobile security for Apple iPhone, iPad, and iOS devices**, 1, Syngress/Elsevier, 2011

Recomendaciones

Otros comentarios

Se recomienda tener conocimientos básicos sobre el S.O. Linux y conocimientos de programación en Java. Así mismo, si bien no es imprescindible, se recomienda tener conocimientos de programación de dispositivos móviles Android.

Plan de Contingencias

Descripción

En caso de que la docencia sea exclusivamente no presencial, se usarán las mismas metodologías y se realizarán las mismas pruebas que se llevaban a cabo de modo presencial en las aulas y/o laboratorios de la Escuela, que pasarán a desarrollarse en línea a través de Campus Remoto y Faitic.

En caso de que la evaluación sea no presencial, el peso de las distintas pruebas de evaluación pasaría a ser el siguiente:

- Examen de preguntas objetivas: 30 %
- Resolución de problemas y/o ejercicios: 30 %
- Informes de prácticas: 40 %

BIBLIOGRAFÍA COMPLEMENTARIA

- Platform Architecture - Android Developers: https://developer.android.com/guide/platform/ - Android Secure: https://source.android.com/security
- Android Enterprise: https://www.android.com/enterprise/
- Mobile Threat Catalogue - NIST: https://pages.nist.gov/mobile-threat-catalogue/
- OWASP Mobile Security Project: https://www.owasp.org/index.php/OWASP_Mobile_Security_Project
- ENISA: Smartphone Secure Development Guidelines: https://www.enisa.europa.eu/publications/smartphone-secure-development-guidelines-2016
- Guía de Seguridad de las TIC CCN-STIC 453E. SEGURIDAD DE DISPOSITIVOS MÓVILES: ANDROID 9.x. Centro Criptográfico Nacional. NIPO: 083-19-015-2: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/400-guias-generales/3588-ccnstic-453g-guia-practica-de-seguridad-en-dispositvos-moviles-android-9/file.html
- Guía de seguridad de las TIC (CCN-STIC-457): Gestión de dispositivos móviles: https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-accesopublico-ccn-stic/14-ccn-stic-457-herramienta-de-gestion-dedispositivos-moviles-mdm/file.html