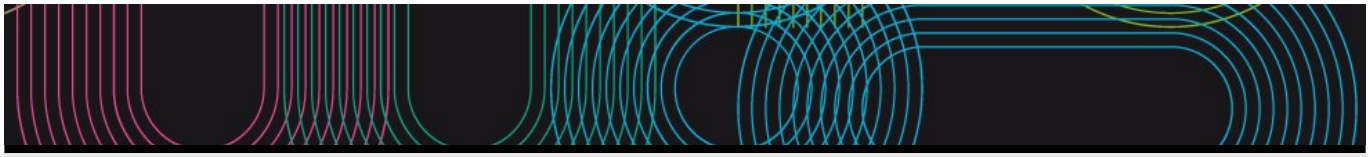

DATOS IDENTIFICATIVOS				
Seguridade en dispositivos móviles				
Materia	Seguridade en dispositivos móviles			
Código	V05M175V11218			
Titulación	Máster Universitario en Ciberseguridade			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	3	OP	1	2c
Lingua de impartición	Castelán Galego Inglés			
Departamento	Dpto. Externo Enxeñaría 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://http://moovi.uvigo.gal			
Descrición xeral	Nesta materia móstrase unha visión xeral da seguridade en dispositivos móbiles con diferentes características. Partindo do estudo da arquitectura destes dispositivos, descubriremos o seu funcionamento interno e cales son as principais ferramentas de seguridade que inclúen, xunto cos riscos e ameazas que sofren. Estudiaremos como atopar, analizar e mitigar as vulnerabilidades que afectan aos dispositivos móbiles, usando ferramentas de análise forense, de desenvolvemento de aplicacións seguras e de xestión de dispositivos en contornos empresariais. A documentación desta materia estará en inglés.			

Resultados de Formación e Aprendizaxe	
Código	
B14	Distinguir os conceptos fundamentais asociados á seguridade nos sistemas operativos móbiles e ao desenvolvemento de aplicacións seguras, así como aos sistemas de xestión de dispositivos móbiles.
C14	Identificar vulnerabilidades en sistemas operativos y aplicaciones propios de los dispositivos móviles, así como realizar un análisis forense y definir la política de seguridad que afecta a las comunicaciones y sistemas móviles de una organización.
D3	Traballa como analista de malware, para protexer as aplicacións, así como analizar a súa seguridade en calquera área de aplicación.
D8	Realizar probas de intrusión en contornas prácticas complexas para identificar vulnerabilidades, así como para realizar ataques en contornas controladas con criterio crítico e ético.
D9	Aplicar métodos de investigación forense para a análise de incidentes ou riscos de ciberseguridade mediante técnicas científicas e analíticas para identificar, preservar, analizar e presentar datos que sexan válidos dentro dun proceso legal.

Resultados previstos na materia	
Resultados previstos na materia	Resultados de Formación e Aprendizaxe
Coñecer os conceptos fundamentais asociados coa seguridade nos sistemas operativos móbiles e desenvolvemento de apps seguras.	B14 C14
Identificar unha app con comportamento malicioso e vulnerabilidades en sistemas operativos e apps	C14 D3

Ser capaz de realizar unha análise forense dun dispositivo móbil	C14 D8 D9
Coñecer os sistemas de xestión dos dispositivos móbiles	B14 C14

Contidos	
Tema	
Introdución: Ameazas e vulnerabilidades que afectan aos dispositivos móbiles	
Arquitecturas de dispositivos móbiles	
Modelos de seguridade de dispositivos móbiles	
Desenvolvemento de aplicacións seguras	Permisos Xestión de paquetes Xestión de usuarios APIs
Seguridade dos datos	
Seguridade dos dispositivos	
Seguridade da rede	
Vulnerabilidades, exploits e aplicacións maliciosas	
Análise forense de sistemas operativos móbiles	
Sistemas de Xestión de Mobilidade Empresarial (EMM)	

Planificación

	Horas na aula	Horas fóra da aula	Horas totais
Lección maxistral	9	9	18
Prácticas con apoio das TIC	12	12	24
Exame de preguntas obxectivas	2	14	16
Resolución de problemas e/ou exercicios	0	5	5
Informe de prácticas, prácticum e prácticas externas	0	12	12

*Os datos que aparecen na táboa de planificación son de carácter orientador, considerando a heteroxeneidade do alumnado.

Metodoloxía docente

	Descrición
Lección maxistral	Exposición, por parte do profesorado, dos principais contidos teóricos relacionados coa seguridade en dispositivos móbiles. Con esta metodoloxía contribuirase á adquisición das competencias B14 e C14.
Prácticas con apoio das TIC	Realización por parte do alumnado de prácticas guiadas e supervisadas. Con esta metodoloxía traballaranse as competencias C14, D3, D8 e D9.

Atención personalizada

Metodoloxías	**Descrición**
Prácticas con apoio das TIC	O conxunto de profesores da materia proporcionará atención individual e personalizada aos alumnos e alumnas durante o curso, solucionando as súas dúbidas e preguntas. Así mesmo, o profesorado orientará e guiará ao alumnado durante a realización das tarefas que teñen asignadas nas prácticas con apoio das TIC. As dúbidas atenderanse de forma presencial ou telemática (durante as propias prácticas, ou durante o horario de titorías). O horario de titorías establecerase ao inicio do curso e publicarase na páxina web da materia. Fora dese horario, será preciso reservar as titorías mediante cita previa.
Lección maxistral	O conxunto de profesores da materia proporcionará atención individual e personalizada aos alumnos e alumnas durante o curso, solucionando as súas dúbidas e preguntas. As dúbidas atenderanse de forma presencial e telemática (durante a propia sesión maxistral, ou durante o horario de titorías). O horario de titorías establecerase ao inicio do curso e publicarase na páxina web da materia. Fora dese horario, será preciso reservar as titorías mediante cita previa.

Avaliación

	Descrición	Cualificación	Resultados de Formación e Aprendizaxe

Exame de preguntas obxectivas	Exame de preguntas cortas sobre os contidos teóricos e prácticos revisados ao longo do curso, tanto nas sesións maxistrais, como nas prácticas de laboratorio. Este exame realizarase ao finalizar o cuadrimestre.	40
Resolución de problemas e/ou exercicios	Resolución de problemas nos que se faga uso dos coñecementos adquiridos tanto nas sesións de teoría como de prácticas. Esta proba realizarase ao longo do cuadrimestre, con entregas parciais nas datas indicadas polo profesorado.	25
Informe de prácticas, prácticum e prácticas externas	O alumnado completará de forma individual cuestionarios e/ou informes de prácticas onde mostrarán a correcta realización e comprensión das prácticas.	35

Outros comentarios sobre a Avaliación

OPORTUNIDADE ORDINARIA

Seguindo as directrices propias da titulación ofertaranse a quen curse esta materia dous sistemas de avaliación: avaliación continua e avaliación global.

Antes de que finalice a cuarta semana do curso, os e as estudantes deberán indicar ao profesorado da materia o sistema de avaliación elixido. Quen opte polo sistema de avaliación continua non poderá ser cualificado como "non presentado" se realiza unha entrega ou proba de avaliación con posterioridade á comunicación da súa decisión.

Avaliación continua

A cualificación final da materia será igual á media aritmética ponderada das probas indicadas previamente. Para superar a materia a cualificación final debe ser maior ou igual que cinco.

Avaliación global

A cualificación final da materia será igual á media aritmética ponderada das probas indicadas previamente. Neste caso, a proba de resolución de problemas farase nunha única proba ao finalizar o cuadrimestre. Para superar a materia, a cualificación final debe ser maior ou igual que cinco.

OPORTUNIDADE EXTRAORDINARIA

A avaliación consistirá en realizar un exame de preguntas obxectivas, un exame de resolución de problemas e entregar os informes de prácticas de todas as prácticas realizadas ao longo do curso.

OUTROS COMENTARIOS

As puntuacións obtidas solo son válidas para o curso académico en vigor.

O uso de calquera material durante a realización dos exames e probas de avaliación deberá ser autorizado explicitamente polo profesorado da materia.

No caso de detección de plaxio nalgún dos traballos/probas realizadas, a cualificación final da materia será de suspenso (0) e os profesores comunicarán o asunto á dirección da escola para que tome as medidas que considere oportunas.

Bibliografía. Fontes 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, Jonh Wiley & Sons, 2014

Charles Miller, **iOS hacker's handbook**, 1, Jonh Wiley & Sons, 2013

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

Recomendacións

Outros comentarios

Recoméndase ter coñecementos básicos sobre o S.O. Linux e coñecementos de programación en Java. Así mesmo, se ben non é imprescindible, recoméndase ter coñecementos de programación de dispositivos móbiles Android.