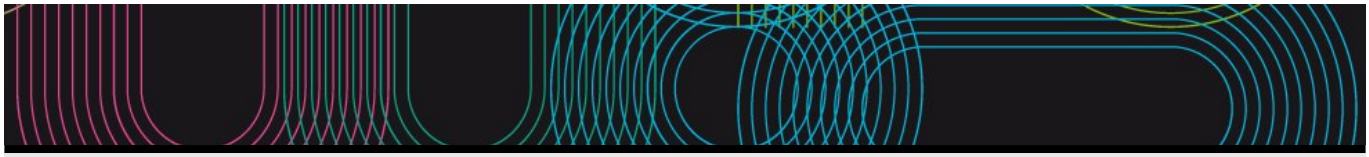

DATOS IDENTIFICATIVOS				
Seguridade en dispositivos móbiles				
Materia	Seguridade en dispositivos móbiles			
Código	V05M175V01206			
Titulación	Máster Universitario en Ciberseguridade			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	3	OP	1	2c
Lingua de impartición	Castelán Galego Inglés			
Departamento				
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://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.			

Competencias	
Código	
A2	Que os estudantes saiban aplicar os coñecementos adquiridos e a súa capacidade de resolución de problemas en contornas novas ou pouco coñecidas dentro de contextos más amplos (ou multidisciplinares) relacionados coa súa área de estudo
A3	Que os estudantes sexan capaces de integrar coñecementos e enfrontarse á complexidade de formar xuízos a partir dunha información que, sendo incompleta ou limitada, inclúa reflexións sobre as responsabilidades sociais e éticas vinculadas á aplicación dos seus coñecementos e xuízos.
A4	Que os estudantes saiban comunicar as súas conclusións ---e os coñecementos e razóns últimas que as sustentan--- a públicos especializados e non especializados de un modo claro e sen ambigüidades
B1	Ter capacidade de análisis e síntesis. Ter capacidade para proxectar, modelar, calcular e diseñar solucións de seguridade da información, as redes e/ou os sistemas de comunicacións en todos os ámbitos de aplicación
B2	Resolución de problemas. Ter capacidade de resolver, cos coñecementos adquiridos, problemas específicos do ámbito técnico da seguridade da información, as redes e/ou os sistemas de comunicacións.
B5	Ter capacidade para aplicar os coñecementos teóricos na práctica, no marco de infraestructuras, equipamientos e aplicacións concretos, e suxeitos a requisitos de funcionamento específicos
C4	Comprender e aplicar os métodos e técnicas de ciberseguridade aplicables ós datos, os equipos informáticos, as redes de comunicacións, as bases de datos, os programas e os servizos de información
C6	Desenvolver e aplicar métodos de investigación forense para o análisis de incidentes ou riscos de ciberseguridade
C9	Ter capacidade para elaborar plans e proxectos de traballo no ámbito da ciberseguridade, claros, concisos e razoados
C15	Ter capacidade de identificar o valor, tanto económico como doutra índole, da información da institución, os seus procesos críticos e o impacto que produciría a interrupción destes; e, tamén, as necesidades internas e externas que permitirán estar preparados ante ataques de seguridade.
D4	Valorar a importancia da seguridade da información no avance socioeconómico da sociedade
D5	Ter capacidade para comunicarse oralmente e por escrito en inglés.

Resultados de aprendizaxe	
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.	A2 B1 C4 C15 D4 D5
Identificar unha app con comportamento malicioso e vulnerabilidades en sistemas operativos e apps	A4 B2 C4 D4 D5
Ser capaz de realizar unha análise forense dun dispositivo móbil	A3 B2 C6 D5
Coñecer os sistemas de xestión dos dispositivos móbiles	A2 B1 B2 B5 C9 D5

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	10	10	20
Exame de preguntas obxectivas	2	14	16
Resolución de problemas e/ou exercicios	0	11	11
Informe de prácticas, prácticum e prácticas externas	0	10	10
*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 CB3, CG1, CE4, CE15 e CT4.
Prácticas con apoio das TIC	Realización por parte do alumnado de prácticas guiadas e supervisadas. Con esta metodoloxía traballaranse as competencias CG2, CG5, CB2, CB4, CE4, CE6 e CE9.

Atención personalizada	
Metodoloxías	**Descrición**

Prácticas con apoio das TIC	Os profesores da materia proporcionarán atención individual e personalizada aos alumnos durante o curso, solucionando as súas dúbidas e preguntas. Así mesmo, os profesores orientarán e guiarán aos alumnos 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, durante o horario establecido para as titorías, ou durante o horario acordado cos alumnos para as 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	Os profesores da materia proporcionarán atención individual e personalizada aos alumnos durante o curso, solucionando as súas dúbidas e preguntas. As dúbidas atenderanse de forma presencial e telemática (durante a propia sesión maxistral, durante o horario establecido para as titorías, ou durante o horario acordado cos alumnos para as 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 bimestre.	50	A3 A4		C4	
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 bimestre, con entregas parciais nas datas indicadas polo profesorado.	20	A2 A4	B1 B2	C4	
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.	30	A4	B5	C4 C6 C9 C15	D4

Outros comentarios sobre a Avaliación

PRIMEIRA OPORTUNIDADE

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

Antes de que finalice a segunda semana do curso, os estudantes deberán indicar ao profesorado da materia o sistema de avaliación elexido. 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.

Sistema de avaliación continua

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

Sistema de avaliación única

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

SEGUNDA OPORTUNIDADE

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 deteción 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, 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

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.

Plan de Continxencias

Descrición

No caso de que a docencia deba levar a caso de maneira totalmente remota, utilizaranse as mesmas metodoloxías e realizaranse as mesmas probas que se desenvolverían de maneira presencial nas aulas e/ou nos laboratorios da Escola, que pasarán a desenvolverse en liña a través do Campus Remoto e Moovi.

No caso de que a avaliación sexa non presencial, o peso das distintas probas de avaliación pasaría a ser o seguinte:

- Exame de preguntas obxectivas: 30 %
- Resolución de problemas e/ou exercicios: 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