Guía Docente: Ciberseguridad Móvil

DATOS GENERALES	
Facultad	Facultad de Ciencias y Tecnología
Titulación	Máster en Ciberseguridad
Plan de estudios	2018
Materia	Tendencias tecnológicas y Ciberseguridad
Carácter	Obligatorio
Período de impartición	Segundo Trimestre
Curso	Primero
Nivel/Ciclo	Máster
Créditos ECTS	6
Lengua en la que se imparte	Castellano
Prerrequisitos	No se prevén requisitos previos, por tanto los requisitos serán los propios del título.

DATOS DEL PROFESORADO			
Profesor Responsable	Francisco Javier Almeida Martínez	**Correo electrónico**	franciscojavier.almeida@ui1.es
Área		**Facultad**	Facultad de Ciencias y Tecnología
Perfil Profesional 2.0	LinKedin		

CONTEXTUALIZACIÓN Y JUSTIFICACIÓN DE LA ASIGNATURA	
Asignaturas de la materia	• Ciberseguridad Móvil
Contexto y sentido de la asignatura en la titulación y perfil profesional	Esta asignatura se centra en los diferentes mecanismos de seguridad para el desarrollo de aplicaciones móviles tanto en sistemas iOS como Android. El temario incluye un análisis de ambas arquitecturas móviles para estudiar desde la perspectiva del sistema operativo las posibles brechas de seguridad. También se analizan las posibles amezanas, tipos de ataques, etc así como los mecanismos para poder protegerse frente a ellos.

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE Y RESULTADOS DE APRENDIZAJE	
Competencias de la asignatura	• CB7: 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. • CB9: Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación. • CB10: Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo. • CG2: Ser capaz de permanecer eficaz dentro de un medio cambiante, así como a la hora de enfrentarse con nuevas tareas, retos y personas. • CG3: Diseñar y elaborar concisa, clara y razonadamente planes y proyectos de trabajo en el ámbito de la ciberseguridad. • CG5: Ser capaz de proponer soluciones imaginativas y originales así como ser capaz de promover la innovación e identificación de alternativas contrapuestas a los métodos y enfoques tradicionales en el ámbito de la ciberseguridad. • CG7: Ser capaz de integrarse en equipos de trabajo o investigación multidisciplinares de manera eficaz y colaborativa • CE02: Conocer las tendencias actuales en técnicas de ciberataque. • CE07: Comprender, aplicar y evaluar las técnicas de seguridad en el desarrollo y uso de aplicaciones web y en los servicios basados en ellas. • CE10: Conocer los conceptos básicos de los principales procesos y respuestas ante incidentes y su aplicación a casos reales.
Resultados de aprendizaje de la asignatura	• Adquirir las competencias básicas y generales detalladas anteriormente. • Implantar de manera segura las aplicaciones móviles. • Configurar de manera segura sistemas móviles. • Conocer los ciberataques fundamentales a dispositivos móviles y la forma de responder y protegerse.

PROGRAMACION DE CONTENIDOS	

Breve descripción de la asignatura	En esta asignatura se verá, entre otros:
	• Arquitecturas de tecnologías móviles
	  ◦ Wifi y tecnologías inalámbricas.
	  ◦ Vulnerabilidades.
	• Desarrollo seguro de aplicaciones móviles
	  ◦ Modulos de seguridad.
	  ◦ Encriptado.
	• Análisis de riesgos y amenazas en entornos móviles:
	  ◦ Gestión de riesgos.
	  ◦ Ataques de fuerza bruta.
	• Gestión segura de aplicaciones móviles:
	  ◦ Métodos de protección de información.
	  ◦ Procedimientos avanzados de seguridad
	• Seguridad en sistemas operativos móviles:
	  ◦ Control de acceso.
	  ◦ Ramsonware.

Contenidos	**Unidad didáctica 1.** Seguridad en dispositivos móviles

- Introducción
- Modelo de seguridad de iOS
- Modelo de seguridad en Android
- Conexión a redes inalámbricas:
  - Redes abiertas
  - Redes cifradas
  - VPNs
  - Bluetooth

Unidad didáctica 2. Módulos de seguridad en dispositivos móviles
- Introducción
- Control de acceso: Touch ID
- Definición de permisos en Android
- API de criptografía en Android
  - Security providers
  - Generación de números aleatorios
  - Funciones hash
  - Criptografía de clave pública
  - Criptografía de clave privada

Unidad didáctica 3. Atacando dispositivos móviles
- Introducción
- Vulnerabilidades en iOS
  - Fuga de datos
  - Corrupción de memoria
- Vulnerabilidades en Android
  - Atacando los componentes de aplicación
  - Acceso al almacenamiento y logs
  - Comunicaciones inseguras

Unidad didáctica 4. Creación de aplicaciones seguras
- Introducción
- Creando aplicaciones seguras en iOS
  - Evitar inyecciones
  - Utilización de protecciones binarias
- Creando applicaciones seguras en Android
  - Mecanismos básicos de seguridad
  - Ingeniería inversa

Unidad didáctica 5. Protección y encriptación de los dispositvos móviles
- Introducción
- Antispyware
- Antivirus
- Antifishing
- Encriptación
- Identificación de aplicaciones dañinas

Unidad didáctica 6. Políticas de seguridad para dispositivos móviles
- Introducción
- Políticas para el acceso físico
- Políticas para respaldo y restauración
- Listas negras
- Configurando políticas de seguridad

METODOLOGÍA	
Actividades formativas	El conjunto de actividades dependerá de la UD que se esté tratando en cada momento. De manera general cada UD puede contar con 1 o dos actividades (individuales o colaborativas). El tipo de actividades será: • **Estudio de Caso de aplicación práctica:** se expondrá al alumno la problemática que estudiará y practicará a lo largo de la unidad didáctica. Se pedirá que piense por sí mismo o de manera colaborativa una solución de programación (o abstracta). Si es de programación, usará las estructuras de programación que actualmente ya sabe, o bien otras que tendrá que buscar por Internet. De este modo se verá totalmente inmerso en el tema y podrá comparar su solución con la aportada posteriormente en la unidad didáctica. • **Foros de Debate:** En cada unidad didáctica se habilitará un foro de discusión/debate. La participación constructiva en ese foro será valorada. Se tendrá en cuenta la calidad de las preguntas y respuestas aportadas a los compañeros. • **Trabajo Colaborativo:** en este caso los alumnos se agruparán en pequeños grupos de trabajo. En una primera fase, cada miembro del equipo de trabajo resolverá individualmente el problema planteado (como una actividad normal). Posteriormente, en una segunda fase, la comparará con las soluciones de sus compañeros y establecerán unas conclusiones sobre esas comparaciones, de forma que unos alumnos puedan aprender de los otros. El alumno buscará por Internet otras posibles soluciones al mismo problema, analizando ventajas e inconvenientes de ambas soluciones (la suya y la encontrada). El alumno no sólo hará esto con su propia solución, sino también con algunas soluciones de sus compañeros. • **Trabajo individual:** en estas actividades los alumnos buscarán las soluciones de manera individual al enunciado propuesto.

EVALUACIÓN	
Sistema evaluativo	*En caso de que la situación sanitaria impida la realización presencial de los exámenes con todas las garantías, la Universidad Isabel I celebrará dichas pruebas en modalidad online. Para la realización de dichos exámenes, la universidad incorporará la herramienta de proctoring a nuestra plataforma tecnopedagógica, con el objetivo de garantizar los procesos de autentificación del alumno, como el control del entorno durante el desarrollo de las pruebas de evaluación. A su vez, la Universidad Isabel I pondrá a disposición del alumnado una Unidad de Exámenes Online específica para ofrecer apoyo técnico durante todo el proceso y así solventar todas las incidencias que se puedan presentar.* El sistema de evaluación se basará en una selección de las pruebas de evaluación más adecuadas para el tipo de competencias que se trabajen. El sistema de calificaciones estará acorde con la legislación vigente *(Real Decreto 1125/2003, de 5 de septiembre, por el que se establece el sistema europeo de créditos y el sistema de calificaciones en las titulaciones universitarias de carácter oficial y de validez en todo el territorio nacional)*. El sistema de evaluación de la Universidad Isabel I queda configurado de la siguiente manera: **Sistema de evaluación convocatoria ordinaria**

Opción 1. Evaluación continua

Los estudiantes que opten por esta vía de evaluación deberán realizar el **seguimiento de la evaluación continua (EC)** y podrán obtener hasta un **60 %** de la calificación final a través de las actividades que se plantean en la evaluación continua.

Además, deberán realizar un **examen final presencial (EX)** que supondrá el **40 %** restante. Esta prueba tiene una parte dedicada al control de la identidad de los estudiantes que consiste en la verificación del trabajo realizado durante la evaluación continua y otra parte en la que realizan diferentes pruebas teórico-prácticas para evaluar las competencias previstas en cada asignatura.

Para la aplicación de los porcentajes correspondientes, el estudiante debe haber obtenido una nota mínima de un 4 en cada una de las partes de las que consta el sistema de evaluación continua.

Se considerará que el estudiante supera la asignatura en la convocatoria ordinaria por el sistema de evaluación continua, siempre y cuando al aplicar los porcentajes correspondientes se alcance una calificación mínima de un 5.

Opción 2. Prueba de evaluación de competencias

Los estudiantes que opten por esta vía de evaluación deberán realizar una **prueba de evaluación de competencias (PEC)** y un **examen final presencial (EX)**.

La **PEC** se propone como una prueba que el docente plantea con el objetivo de evaluar en qué medida el estudiante adquiere las competencias definidas en su asignatura. Dicha prueba podrá ser de diversa tipología, ajustándose a las características de la asignatura y garantizando la evaluación de los resultados de aprendizaje definidos. Esta prueba supone el 50 % de la calificación final.

El **examen final presencial**, supondrá el **50 %** de la calificación final. Esta prueba tiene una parte dedicada al control de la identidad de los estudiantes que consiste en la verificación del seguimiento de las actividades formativas desarrolladas en el aula virtual y otra parte en la que realizan diferentes pruebas teórico-prácticas para evaluar las competencias previstas en cada asignatura.

Al igual que con el sistema de evaluación anterior, para la aplicación de los porcentajes correspondientes el estudiante debe haber obtenido una puntuación mínima de un 4 en cada una de las partes de las que consta la opción de prueba de evaluación de competencias.

Se considerará que el estudiante supera la asignatura en la convocatoria ordinaria por el sistema de la prueba de evaluación de competencias siempre y cuando al aplicar los porcentajes correspondientes se alcance una calificación mínima de un 5.

Sistema de evaluación convocatoria extraordinaria

Todos los estudiantes, independientemente de la opción seleccionada, que no superen las pruebas evaluativas en la convocatoria ordinaria tendrán derecho a una convocatoria extraordinaria.

La convocatoria extraordinaria completa consistirá en la realización de una **prueba de evaluación de competencias** que supondrá el **50 %** de la calificación final y un **examen final presencial** cuya calificación será el **50 %** de la calificación final.

Para la aplicación de los porcentajes correspondientes, el estudiante debe haber obtenido una nota mínima de un 4 en cada una de las partes de las que consta el sistema de

	evaluación de la convocatoria extraordinaria. Los estudiantes que hayan suspendido todas las pruebas evaluativas en convocatoria ordinaria (evaluación continua o prueba de evaluación de competencias y examen final) o no se hayan presentado deberán realizar la convocatoria extraordinaria completa, como se recoge en el párrafo anterior. En caso de que hayan alcanzado una puntuación mínima de un 4 en alguna de las pruebas evaluativas de la convocatoria ordinaria (evaluación continua o prueba de evaluación de competencias y examen final), se considerará su calificación para la convocatoria extraordinaria, debiendo el estudiante presentarse a la prueba que no haya alcanzado dicha puntuación o que no haya realizado. En el caso de que el alumno obtenga una puntuación que oscile entre el 4 y el 4,9 en las dos partes de que se compone la convocatoria ordinaria (EC o PEC y examen), solo se considerará para la convocatoria extraordinaria la nota obtenida en la evaluación continua o prueba de evaluación de competencias ordinaria (en función del sistema de evaluación elegido), debiendo el alumno realizar el examen extraordinario para poder superar la asignatura. Al igual que en la convocatoria ordinaria, se entenderá que el alumno ha superado la materia en convocatoria extraordinaria si, aplicando los porcentajes correspondientes, se alcanza una calificación mínima de un 5.

BIBLIOGRAFÍA Y OTROS RECURSOS	
Bibliografía básica	• Campagna, R., Iyer, S., Krishnan, A., & Books24x7, I. (2011). *Mobile device security for dummies* (1. Aufl. ed.). Chichester;Hoboken, N.J;: Wiley. Este libro pretende proporcionar compresión sobre los principios básicos de seguridad en dispositivos móviles así como conocer las principales formas de minimizar sus riesgos. • Chell, D. (2015). *The mobile application hacker's handbook* (1st ed.). Indianapolis, IN: Wiley. Este libro se centra en conocer las principales vulnerabilidades de los sistemas móviles. Se pretende estudiar la seguridad de los sistemas móviles mediante los ataques a los que están expuestos. Para intentar minimizar los daños ocasionados por estos ataques, se plantean medidas de seguridad para defenderse ante ellos.
BibliografÍa complementaria	• Ogal Rai, P., & ebrary, I. (2013). *Android application security essentials* (1st ed.). Birmingham: Packt Publishing. • Doherty, J. (2016;2015;). *Wireless and mobile device security* (1st ed.). Burlington, MA: Jones & Bartlett Learning. • Viega, J., & Michael, B. (2010). Mobile device security. *IEEE Security & Privacy, 8*(2), 11. doi:10.1109/MSP.2010.76 • Hewitt, B., Dolezel, D., & McLeod, J., Alexander. (2017). Mobile device security: Perspectives of future healthcare workers. *Perspectives in Health Information Management, 14*(Winter), 1c. • Shukla, S. (2017). Editorial: Security of mobile devices. *ACM Transactions on Embedded Computing Systems (TECS), 16*(4), 1-2. doi:10.1145/3129534 • Thompson, N., McGill, T. J., & Wang, X. (2017). "security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security, 70*, 376. doi:10.1016/j.cose.2017.07.003

- Wessel, S., Huber, M., Stumpf, F., & Eckert, C. (2015). Improving mobile device security with operating system-level virtualization. *Computers & Security, 52*, 207-220. doi:10.1016/j.cose.2015.02.005
- CHIN, A. G., ETUDO, U., HARRIS, M. A., Augusta University Cyber Institute, & Department of Information Systems, School of Business, Virginia Commonwealth University. (2016). On mobile device security practices and training efficacy: An empirical study. *Informatics in Education - an International Journal, 15*(2), 235-252. doi:10.15388/infedu.2016.12
- Kim, D., Chung, K., & Hong, K. (2010). Person authentication using face, teeth and voice modalities for mobile device security. *IEEE Transactions on Consumer Electronics, 56*(4), 2678-2685. doi:10.1109/TCE.2010.5681156
- A. Harris, M., & P. Patten, K. (2014). Mobile device security considerations for small- and medium-sized enterprise business mobility. *Information Management & Computer Security, 22*(1), 97-114. doi:10.1108/IMCS-03-2013-0019

Otros recursos

- Video (Seguridad informática por Chema Alonso):
  - https://www.youtube.com/watch?v=-B3jzIW7hks
- Video ("Thinking about Security" de Chema Alonso):
  - https://www.youtube.com/watch?v=Rxs9meo9vwQ
- Vídeo (Conferencia completa Seguridad informática por Chema Alonso):
  - https://www.youtube.com/watch?v=XgEdDMzj_tA
- Vídeo (Principios de la seguridad de la información aplicables a la privacidad):
  - https://www.youtube.com/watch?v=__hng-WgkYE
- Vídeo(Curso Hacking - Tipos de Ataques):
  - https://www.youtube.com/watch?v=wC6lZfv8IRY
- Vídeo(Android vs IOS Security (The Cyber Underground)):
  - https://www.youtube.com/watch?v=TMPYlwOkdTo
- Video (How secure are our cell phones from being hacked? Are iPhones more secure or Androids?):
  - https://www.youtube.com/watch?v=0A4u7nn7Uho
- Video (Tu iPhone es tan (in)seguro como tu Windows)
  - https://www.youtube.com/watch?v=DbqkBAjId_U