Guía Docente: Desarrollo de aplicaciones móviles seguras

DATOS GENERALES	
Facultad	Facultad de Ciencias y Tecnología
Titulación	Máster en Tecnologías Móviles
Plan de estudios	2020
Materia	Seguridad en dispositivos móviles
Carácter	Optativo
Período de impartición	Segundo Trimestre
Curso	Primero
Nivel/Ciclo	Máster
Créditos ECTS	6
Lengua en la que se imparte	Castellano
Prerrequisitos	Conocimiento de Android e iOS.

DATOS DEL PROFESORADO			
Profesor Responsable	Iván Luis Rodriguez Robles	**Correo electrónico**	ivanluis.rodriguez@ui1.es
Área		**Facultad**	Facultad de Ciencias y Tecnología
Perfil Profesional 2.0	Curriculum Ivan L. Rodriguez Robles		

CONTEXTUALIZACIÓN Y JUSTIFICACIÓN DE LA ASIGNATURA	
Asignaturas de la materia	• Comunicación segura con dispositivos remotos y periféricos • Desarrollo de aplicaciones móviles seguras
Contexto y sentido de la asignatura en la titulación y perfil profesional	La gran mayoría de la población mundial posee un móvil conectado a internet. Los móviles almacenan información personal y confidencial, y las operaciones que realizan, por ejemplo uso de banca, hacen que cada día sea más importante la seguridad en estos y en el desarrollo de sus de aplicaciones con el objetivo de evitar los efectos secundarios de los ataques de los cibercriminales. Hoy los móviles tienen todo tipo de dispositivos hardware: GPS, cámara, tecnologías inalámbricas (GSM, UMTS, Wifi, Bluetooth, NFC), sensores huella, sensores de movimiento. Debido a todas estas prestaciones los sistemas operativos son grandes, y complejos, incrementando así las vulnerabilidades a las que se exponen los usuarios. El cibercrimen está continuamente innovando sus ataques, esto hace obligatorio que las aplicaciones estén siempre actualizadas en términos de seguridad y así prevenir futuros desastres.

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE Y RESULTADOS DE APRENDIZAJE	
Competencias de la asignatura	**BA?SICAS Y GENERALES** • CG01 - Conocer los usos de productos tecnológicos de distintos colectivos sociales y ser capaz de encontrar nuevas necesidades. • CG02 - Ser capaz de proponer soluciones imaginativas y originales así como de promover la innovación e identificación de alternativas en el desarrollo de aplicaciones móviles. • CG04 - Conocer las particularidades y necesidades relacionadas con la accesibilidad a los dispositivos, sistemas operativos y aplicaciones móviles. • 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 • CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular 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 • CB9 - 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 • 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. **ESPECÍFICAS** • CES01 - Comprender, aplicar y evaluar las técnicas de seguridad informática en dispositivos móviles. • CES02 - Conocer, aplicar y evaluar las técnicas de seguridad en el desarrollo y uso de aplicaciones móviles y en los servicios basados en ellas. • CES03 - Conocer, definir y evaluar las vulnerabilidades de los sistemas informáticos y de telecomunicaciones.
Resultados de aprendizaje de la asignatura	• Saber aplicar métodos de seguridad en aplicaciones móviles. • Conocer las principales amenazas de seguridad en dispositivos móviles. • Conocer los principales frameworks de seguridad en dispositivos móviles.

PROGRAMACION DE CONTENIDOS	
Breve descripción de la asignatura	**Criptografía simétrica** • Cifrados de flujo • Cifrados de bloque **Criptografía asimétrica** • Firma digital • Certificados x509 **Validación de certificados en dispositivos móviles** • Bouncy castle Android

	• Bouncy castle iOS **Utilización de dispositivos biométricos** • Lector de huellas • FaceID

Contenidos	• **Unidad didáctica 1. Introducción a la seguridad en aplicaciones móviles android.**
	  ◦ Arquitectura de Seguridad Android.
	  ◦ Prácticas esenciales de seguridad en Android.
	  ◦ Almacenamiento seguro.
	  ◦ Claves.
	  ◦ Security JetPack.
	• **Unidad didáctica 2. Keystore y Criptografía simétrica.**
	  ◦ Funciones del Keystore
	  ▪ Autorizaciones de uso de claves.
	  ▪ Módulo de seguridad HW.
	  ▪ Prevención.
	  ▪ Proveedores de clave.
	  ▪ Generación de claves.
	  ▪ Importar claves encriptadas de forma segura.
	  ▪ Autenticación para el uso de claves.
	  ◦ Criptografía
	  ▪ Algoritmos
	  ▪ El Cifrador simétrico:
	  • Cifrador de bloque.
	  • Cifrador de flujo.
	• **Unidad didáctica 3. Criptografía asimétrica y Dispositivos biométricos en Android.**
	  ◦ Criptografía asimétrica
	  ◦ Firma digital.
	  ◦ Certificado x509.

- Validación de certificados Bouncy Castle Android.
- Identidad de Usuario y sus datos
  - Introducción
  - Utilización de dispositivos biométricos
    - Proceso de autenticación
- Buenas prácticas de seguridad en Android.

- **Unidad didáctica 4. Introducción a la seguridad en aplicaciones móviles iOS.**
  - Capas de seguridad en iOS.
  - Swift y la seguridad.
  - Prácticas esenciales de seguridad en las aplicaciones móviles iOS.
  - Prácticas seguras en el almacenamiento.
  - Administración de claves iOS.
    - Estructura de claves iOS.
    - Administración claves en iOS.
- **Unidad didáctica 5. Criptografía iOS.**
  - Introducción.
  - Security Framework iOS.
  - Apple CryptoKit.
  - Cifrado con Swift.
- **Unidad didáctica 6. Criptografía iOS.**
  - Firma digital.
  - Certificados.
  - Identidad de Usuario y sus datos.
    - Introducción.
    - Utilización de dispositivos biométricos.
      - Proceso de autenticación.
  - Buenas prácticas de seguridad en iOS.

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 pedirá al alumno 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 al menos dos unidades 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. • **Cuestionarios evaluables**: en estas actividades los alumnos responderán de forma individual una serie de preguntas relacionadas con el temario dado hasta ese momento.

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	Nikolay Elenkov. (2014). Android security Internals - An In-Depth Guide to android's security architecture. San Francisco, CA 94103: No Starch Press, Inc • Android Security Internals de Android Nikolay Elenkov nos muestra la arquitectura de seguridad de Android buceando en la implementación de los principales componentes y la seguridad, como Binder IPC, permisos, proveedores criptográficos y administración de dispositivos. David Thiel. (2015). iOS Application Security: The Definitive Guide for Hackers and Developers. San Francisco, CA 94103: No Starch Press, Inc • David Thiel muestra los malos hábitos de codificación en iOS para evitar serios problemas de seguridad, y muestra cómo solucionarlos. En este libro se aprenderá: ◦ El modelo de seguridad de iOS y los límites de sus protecciones integradas. ◦ Cómo evitar que los datos confidenciales puedan filtrarse. ◦ Cómo implementar el cifrado con Keychain y la API de protección de datos entre otros.
Bibliografía complementaria	Charles S. Edge. (2015). Learning iOS Security. Birmingham, UK: Packt Publishing Ltd. Eric Butow. (2018). Pro iOS Security and Forensics. Enterprise iPhone and iPad Safety. Jackson, California, USA: Apress; Edición: 1st ed. Jeff Six. (2012). Application Security for the Android Platform: Processes, Permissions, and Other Safeguards. Sebastopol, CA: O'Reilly Media, Inc. Joshua J. Drake, Pau Oliva Fora, Zach Lanier, Collin Mulliner, Stephen A. Ridley, Georg Wicherski. (2014). AndroidTM Hacker's Handbook. Indianapolis, IN: John Wiley & Sons, Inc.
Otros recursos	Android: • Best practices: https://developer.android.com/topic/security/best-practices • Secure Data: https://developer.android.com/topic/security/data • Criptography: https://developer.android.com/guide/topics/security/cryptography • Keystore: https://developer.android.com/training/articles/keystore • BouncyCastle Android: http://www.bouncycastle.org/wiki/display/JA1/X.509+Public+Key+Certificate+and+Certification+Request+Generation iOS • Segiridad en las plataformas apple: https://support.apple.com/es-es/guide/security/welcome/web • Security Framework: https://developer.apple.com/documentation/security • Apple Criptokit: https://developer.apple.com/documentation/cryptokit • Cripto swift: https://github.com/apple/swift-crypto Bouncy Castle: • https://www.bouncycastle.org/