Guía Docente
Curso Académico 2026/27

Datos Generales

Asignatura: PROGRAMACIÓN DE DISPOSITIVOS MÓVILES
Titulación: GRADO EN CIBERSEGURIDAD
Carácter: OPTATIVA.
Créditos ECTS: 6 ECTS
Curso: 4º
Distribución temporal: 1º SEMESTRE.
Idioma de impartición: CASTELLANO.
Equipo docente: Carlos Ochoa carlos.ochoa@euneiz.com
Aula(s): Aula informatizada

Presentación de la asignatura:

La asignatura Programación de Dispositivos Móviles introduce al estudiante en el desarrollo de aplicaciones para entornos móviles, abordando los fundamentos de diseño, implementación y despliegue de aplicaciones seguras. Se estudiarán las principales plataformas y herramientas de desarrollo, prestando especial atención a las buenas prácticas de programación, la protección de datos, la gestión segura de permisos y la prevención de vulnerabilidades específicas de dispositivos móviles.

Datos Específicos

Resultados del proceso de formación y aprendizaje (RFA)[1]

Contenidos o conocimientos (C)	C1	Desarrollar habilidades de cálculo para el análisis en los lenguajes de programación.
	C16	Entender el concepto de infraestructura crítica y elementos ciberfísicos para analizar los riesgos específicos que pueden sufrir y desplegar las contramedidas adecuadas para su gestión y teniendo en cuenta la legislación vigente.

[1] La clasificación de los RFA corresponde a la definida en el RD822/2021 y se encuentran definidos en la memoria de verificación del título.

* Extender el contenido utilizando para ello la programación docente. La extensión debe estar en punto intermedio, es decir, ampliar la información en la guía docente pero no llegar a los límites de la programación docente. Se debe incluir el índice de temas a tratar punto por punto (sin desarrollar). Se pueden incluir hasta tres subapartados con ideas claves/subtemas. La extensión máxima será de 2 páginas.

	C17	Conocer los sistemas y las herramientas de los sistemas sanitarios, sus implicaciones y metodologías y herramientas de protección.
Competencias (CO)	CO1	Usar y programar ordenadores, sistemas operativos, redes, bases de datos y el entorno de la nube para su aplicación en la ciberseguridad.
	CO4	Realizar diseños de ingeniería aplicados a la ciberseguridad.
	CO6	Utilizar de forma segura los lenguajes de programación más utilizados para su implementación en situaciones reales.
	CO9	Integrar de forma eficaz soluciones basadas en TI en el entorno del usuario.
	CO10	Aplicar técnicas y herramientas de desarrollo seguro para la verificación y validación del software.
Habilidades y destrezas (H)	H1	Trabajar en grupo transmitiendo conocimientos y habilidades adquiridos.
	H2	Desarrollar habilidades para el análisis, la elaboración y la colaboración en proyectos, partiendo de las necesidades propias del mercado.
	H4	Tomar decisiones en el ámbito profesional, aplicando los conocimientos y técnicas adquiridas a lo largo de la actividad académica.
	H5	Comunicar de forma clara y concisa, a todo tipo de audiencias, conocimientos, ideas, soluciones, datos, etc. en el ámbito del estudio.
	H6	Ser capaz de trabajar con información técnica en inglés, tanto a nivel de consulta como de su elaboración.

Contenido de la Asignatura*

Bloque 1: Arquitectura y "Trasteo" del Dispositivo

- **1.1. Anatomía de un Dispositivo Móvil:** Arquitectura del S.O. (Kernel Linux, capa de abstracción de hardware).
- **1.2. El Modelo de Sandbox (Aislamiento):** Cómo el sistema operativo aísla las aplicaciones para que ninguna pueda robar datos de otra.
- **1.3. Gestión de Permisos:** Permisos en tiempo de instalación vs. tiempo de ejecución. El peligro de los permisos "peligrosos" (Cámara, Ubicación, Almacenamiento).
- **1.4. Práctica de laboratorio:** Configuración del entorno (Android Studio), despliegue en un dispositivo físico/emulador y uso de herramientas de depuración (adb - Android

Debug Bridge) para explorar el sistema de archivos del dispositivo.

Bloque 2: Desarrollo de Apps y Almacenamiento Seguro

- **2.1. Componentes básicos de una App:** Actividades (UI) y Ciclo de vida.
- **2.2. Intercambio de datos e Intents:** Cómo se comunican las apps entre sí y los riesgos de los *Intents* maliciosos o expuestos.
- **2.3. El peligro del almacenamiento local:** Inseguridad en *SharedPreferences* y bases de datos locales (SQLite). Por qué nunca se deben dejar contraseñas o tokens en texto plano.
- **2.4. Criptografía en Móviles:** Uso del *Android Keystore* para guardar claves criptográficas respaldadas por hardware.
- **2.5. Práctica de laboratorio:** Crear una app de notas o gestión de usuarios que cifre la información localmente de extremo a extremo.

Bloque 3: Comunicaciones en Red y APIs Seguras

- **3.1. Conectividad y consumo de APIs REST:** Buenas prácticas en el transporte de datos (HTTPS/TLS).
- **3.2. Fugas de datos en tránsito:** Ataques Man-in-the-Middle (MitM). Cómo interceptar el tráfico de una app usando proxies de interceptación (ej. *Burp Suite* o *OWASP ZAP*).
- **3.3. Certificado Pinning (Network Security Config):** Configurar la app para que solo confíe en el servidor legítimo, evitando la interceptación de datos.
- **3.4. Práctica de laboratorio:** Interceptar el tráfico de su propia aplicación, ver cómo se exponen los datos y luego implementar medidas de configuración de red seguras para bloquear el ataque.

Bloque 4: Ingeniería Inversa y Bastionado de Apps

- **4.1. Ingeniería Inversa básica:** Descompilar una aplicación propia (fichero APK) usando herramientas como *JADX* o *Apktool*. Ver cómo el código fuente original queda expuesto.
- **4.2. Ingeniería Social y Malware Móvil:** Cómo se empaqueta el malware (repackaging) sustituyendo código legítimo.
- **4.3. Ofuscación de código:** Configuración de *ProGuard / R8* para dificultar la lectura del código descompilado.
- **4.4. Técnicas de Anti-Tampering:** Conceptos básicos de detección de Root, emuladores y verificación de firma de la app.
- **4.5. Práctica de laboratorio/Proyecto:** Descompilar la app de un compañero para intentar extraer una "clave secreta" oculta en el código (búsqueda de *secrets* cableados) y corregirla aplicando ofuscación.

Metodologías Docentes y Actividades Formativas[2]

Metodologías docentes utilizadas en esta asignatura son:

MD1	Método expositivo.
MD2	Estudios de caso.
MD3	Aprendizaje basado en problemas.
MD4	Aprendizaje basado en proyectos.
MD5	Aprendizaje cooperativo.
MD6	Tutorías.

Actividades formativas utilizadas en esta asignatura son:

Actividades formativas	Horas previstas	% presencialidad
AF1: Clase teórica.	18	100
AF2: Clase prácticas.	5	100
AF3: Realización de trabajos (individuales y/o grupales).	17	50
AF3: Tutorías (individuales y/o grupales).	2	50
AF5: Estudio independiente y trabajo autónomo del o la estudiante.	96	0
AF6: Pruebas de evaluación.	2	40
AF9: Clase en laboratorio	10	100
Total	**150**	**--**

[2] Se deberán extraer de la memoria verificada del título las metodologías docentes, actividades formativas y sistemas de evaluación. (1 ECTS = 25 horas de trabajo del estudiante).

Evaluación: Sistemas y Criterios de Evaluación

Las semanas de evaluación están definidas en el calendario académico publicado en la web de la universidad; la concreción de las fechas se realizará una vez que la docencia haya comenzado.

Sistemas de evaluación utilizados en esta asignatura son:

Denominación	Pond. Mín	Pond. Máx
SE1 Evaluación de la asistencia y participación del o la estudiante.	0	5
SE2 Evaluación de trabajos.	5	15
SE3 Pruebas de evaluación y/o exámenes	50	70
SE6: Evaluación de laboratorios	10	30

El estudiantado posee dos modalidades de evaluación para superar la asignatura:

- Evaluación continua con 2 convocatorias/año: ordinaria y extraordinaria.
- Evaluación única con 2 convocatorias/año.

En la Universidad Euneiz la evaluación continua (media ponderada de las diferentes actividades evaluables de la asignatura definidas por el profesorado) es la evaluación primordial; pero Euneiz permite al estudiantado acogerse a la evaluación única.

No se permite el cambio de modalidad de evaluación (de continua a única) escogido por el estudiante a lo largo del curso.

El/la estudiante que desee acogerse a la modalidad de evaluación única deberá solicitarlo por escrito formal que lo justifique dirigido al profesorado responsable de la asignatura y a la Coordinación del título en las dos primeras semanas del inicio de la misma.

Si el/la estudiante no asiste un 80% a las clases presenciales, pasará directamente a la convocatoria extraordinaria de la evaluación única.

De manera excepcional, el/la docente responsable de la asignatura podrá valorar con otros criterios adicionales como la participación, la actitud, el grado de desempeño y aprovechamiento del o la estudiante, etc., la posibilidad de permitir que el/la estudiante continue en la convocatoria ordinaria, siempre que su asistencia mínima se encuentre por encima del 70%.

Las faltas de asistencia deben justificarse al profesor/a responsable de la asignatura con un plazo máximo de 1 semana. El justificante oficial deberá ser presentado al profesor/a responsable mediante un correo electrónico.

El/la estudiante irá a la evaluación extraordinaria ÚNICAMENTE con las partes suspendidas.

El sistema de calificación de la asignatura sigue lo establecido en el RD 1125/2003 y los resultados obtenidos se calificarán siguiendo la escala numérica de 0 a 10, con expresión de un decimal.

- 0-4,9: Suspenso (SS).
- 5,0-6,9: Aprobado (AP).
- 7,0-8,9: Notable (NT).
- 9,0-10: Sobresaliente (SB).

La mención de «Matrícula de Honor» podrá ser otorgada a alumnos/as que hayan obtenido una calificación igual o superior a 9,0. Su número no podrá exceder del cinco por ciento de los/las alumnos/as matriculados en una materia en el correspondiente curso académico, salvo que el número de alumnos/as matriculados sea inferior a 20, en cuyo caso se podrá conceder una sola «Matrícula de Honor».

Será considerado no presentado (NP) el estudiantado matriculado que no realice ninguna actividad evaluativa.

Toda actividad evaluativa escrita (trabajos, exámenes...) considerará las faltas ortotipográficas en la calificación final.

El plagio está prohibido, tanto en los trabajos, como en los exámenes, en caso de detectarse la calificación será suspenso. Los trabajos entregados a través del campus virtual serán objeto de análisis por la herramienta Turnitin:

- Los informes con un índice de similitud entre el 20% y el 30% serán revisados por el profesor/a para analizar las posibles fuentes de plagio y evaluar si están justificadas.
- Cualquier trabajo con un índice de similitud superior al 30%, una vez realizado el análisis del o la docente, no será evaluado.

Recursos materiales e infraestructuras necesarias

Tipo de recurso material y/o infraestructura
Material docente (apuntes, presentaciones, guías, tareas…)

Recursos audiovisuales
Material específico de la asignatura
Aula informatizada
Laboratorio Ciberseguridad

Bibliografía y otros Recursos de Aprendizaje

Bibliografía Básica

- Elenkov, N. (2014). Android security internals: An in-depth guide to Android's security architecture. No Starch Press.
- Phillips, B., Stewart, C., Marsicano, K., & Gardner, B. (2022). Android programming: The Big Nerd Ranch guide (5.ª ed.). Big Nerd Ranch Guides
- Tanenbaum, A. S., & Bos, H. (2015). Sistemas operativos modernos (4.ª ed.). Pearson Educación.

Bibliografía Complementaria

- Burns, J. (2022). Android Studio Koala Essentials: Kotlin Edition. Payload Media.
- Darcey, L., & Conder, S. (2020). Android Wireless Application Development Volume I: Android Essentials (5th ed.). Addison-Wesley Professional.
- Jemerov, D., & Isakova, S. (2021). Kotlin in Action (2nd ed.). Manning Publications.
- Osmani, A. (2023). Learning Progressive Web Apps. O'Reilly Media.

Otros Recursos de Aprendizaje Recomendados[3]

- Android Developers.
- Kotlin Documentation.
- Google Codelabs.
- Firebase Documentation.

[3] Entre otros recursos de aprendizaje pueden incluirse páginas web, software, materia audiovisual, etc.