Guia docente					
Datos Identificativos					2024/25
Asignatura (*)	Seguridad de Aplicaciones			Código	614530104
Titulación	Máster Universitario en Ciberseguridade				
Descriptores					
Ciclo	Periodo	Curso		Tipo	Créditos
Máster Oficial	1º cuatrimestre	Primero		Obligatoria	5
Idioma	Castellano				
Modalidad docente	Presencial				
Prerrequisitos					
Departamento	Ciencias da Computación e Tecnoloxías da InformaciónComputaciónTecnoloxías da Información e as Comunicacións				
Coordinador/a	Bellas Permuy, Fernando		Correo electrónico	fernando.bellas@udc.es	
Profesorado	Bellas Permuy, Fernando Losada Perez, Jose		Correo electrónico	fernando.bellas@udc.es jose.losada@udc.es	
Web	moovi.uvigo.gal				
Descripción general	Desarrollar aplicaciones seguras no es una tarea trivial. Conocer las vulnerabilidades que habitualmente sufren las aplicaciones, los mecanismos de autenticación, autorización y control de acceso, así como la incorporación de la seguridad al ciclo de vida de desarrollo, es esencial para poder construir y mantener aplicaciones seguras con éxito. En esta materia se estudian de forma práctica todos estos aspectos, con especial énfasis en el desarrollo de aplicaciones y servicios web.				

Competencias / Resultados del título	
Código	Competencias / Resultados del título
A2	CE2 - Conocer en profundidad las técnicas de ciberataque y ciberdefensa
A7	CE7 - Tener capacidad para realizar la auditoría de seguridad de sistemas e instalaciones, el análisis de riesgos derivados de debilidades de ciberseguridad y desarrollar el proceso de certificación de sistemas seguros
A13	CE13 - Tener capacidad de análisis, detección y eliminación de vulnerabilidades, y del malware susceptible de utilizarlas, en sistemas y redes
A24	HD-04 - Prevenir, identificar y corregir las principales vulnerabilidades que sufren las aplicaciones, así como incorporar mecanismos de autenticación, autorización y control de acceso a las aplicaciones
B2	CB2 - 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
B7	CG2 - Resolución de problemas. Tener capacidad de resolver, con los conocimientos adquiridos, problemas específicos del ámbito técnico de la seguridad de la información, las redes y/o los sistemas de comunicaciones
B20	K-04 - Distinguir las principales vulnerabilidades que sufren las aplicaciones, así como los principales mecanismos de autenticación, autorización y control de acceso, con énfasis especial en aplicaciones web y servicios web
C4	CT4 - Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad
C8	C-03 - Trabajar como analista de malware, para proteger aplicaciones, así como analizar su seguridad en cualquier área de aplicación
C19	C-14 - Proyectar, modelar, calcular y diseñar soluciones técnicas y de gestión de seguridad de la información, las redes y/o los sistemas de comunicaciones en todos los ámbitos de aplicación, con criterios éticos de responsabilidad y deontología profesional

Resultados de aprendizaje			
Resultados de aprendizaje	Competencias / Resultados del título		
Conocer las vulnerabilidades que habitualmente sufren las aplicaciones (con especial énfasis en aplicaciones y servicios web) y los mecanismos de prevención.	AP2 AP7 AP13 AP24	BP2 BP7 BP20	CP4 CP8 CP19

Conocer los mecanismos de autenticación, autorización y control de acceso en aplicaciones y servicios.	AP2 AP7 AP13 AP24	BP2 BP7 BP20	CP4 CP8 CP19

Contenidos	
Tema	**Subtema**
Tema 1. Introducción.	1.1 Autenticación, autorización y control de acceso. 1.2 Aplicaciones y servicios con estado. 1.3 Aplicaciones y servicios sin estado. 1.4 Aplicaciones Web tradicionales y SPA.
Tema 2. Vulnerabilidades y mecanismos de prevención en aplicaciones y servicios.	2.1 Marcos de referencia. 2.2 Vulnerabilidades en el tratamiento de los datos de entrada. 2.3 Vulnerabilidades en la autenticación. 2.4 Vulnerabilidades en la gestión de la sesión. 2.5 Exposición de información sensible. 2.6 Vulnerabilidades en el control de acceso. 2.7 Configuración incorrecta. 2.8 Monitorización y log insuficiente. 2.9 Vulnerabilidades en librerías de terceros.
Tema 3. Ciclos de desarrollo de software seguro.	3.1 Seguridad desde la fase de análisis. 3.2 Revisiones de código. 3.3 Herramientas SAST y DAST.
Tema 4. Mecanismos de autenticación, autorización y control de acceso.	4.1 Introducción. 4.2 Autenticación y autorización. 4.2.1 Autenticación en HTTP. 4.2.2 JSON Web Token. 4.2.3 OAuth. 4.2.4 OpenID Connect. 4.2.5 Otros estándares. 4.3 Control de acceso. 4.3.1 Control de acceso basado en roles (RBAC). 4.3.2 Control de acceso basado en atributos (ABAC).

Planificación				
Metodologías / pruebas	**Competencias / Resultados**	**Horas lectivas (presenciales y virtuales)**	**Horas trabajo autónomo**	**Horas totales**
Sesión magistral	A2 A7 A13 A24 B2 B7 B20 C4 C8 C19	24	24	48
Prácticas a través de TIC	A2 A7 A13 A24 B2 B7 B20 C4 C8 C19	18	47	65
Prueba de respuesta múltiple	A2 A7 A13 A24 B2 B7 B20 C4 C8 C19	2	8	10
Atención personalizada		2	0	2
(*)Los datos que aparecen en la tabla de planificación són de carácter orientativo, considerando la heterogeneidad de los alumnos				

Metodologías	
Metodologías	**Descripción**

Sesión magistral	Clases impartidas por el profesorado mediante la proyección de diapositivas. Las clases tienen un enfoque totalmente práctico, explicando los conceptos teóricos mediante el uso de ejemplos sencillos y casos de estudio. Las diapositivas están disponibles a través de la plataforma de docencia de la universidad.
Prácticas a través de TIC	Para experimentar con los conceptos estudiados en la asignatura, la/el estudiante realizará dos prácticas. La primera estará centrada en el análisis de vulnerabilidades de una aplicación web. La/El estudiante partirá del código fuente de una aplicación web y tendrá que detectar las vulnerabilidades, explotarlas y corregirlas. La segunda práctica estará centrada en los mecanismos de autenticación, autorización y control de acceso. La/El estudiante partirá del código fuente de una aplicación, que consta de una interfaz de usuario y un servicio, y tendrá que encargarse de implementar los aspectos de autenticación, autorización y control de acceso, siguiendo distintas estrategias.
Prueba de respuesta múltiple	Se realizará un examen de tipo test, cuyo objetivo es comprobar que la/el estudiante ha asimilado los conceptos correctamente. El examen tipo test se compone de un conjunto de preguntas con varias respuestas posibles, de las que sólo una es correcta. Las preguntas no contestadas no puntúan y las contestadas erróneamente puntúan negativamente.

Atención personalizada	
Metodologías	**Descripción**
Prácticas a través de TIC	Tutorías y consultas vía correo electrónico o Teams para dudas específicas. Horarios de tutorías: - Profesorado UDC: https://www.udc.es/gl/centros_departamentos_servizos/centros/titorias/?codigo=614. - Profesorado UVIGO: https://moovi.uvigo.gal/user/profile.php?id=11662. Presencia del profesor/a en el laboratorio para ayudar al alumno/a en el desarrollo de la práctica.

Evaluación			
Metodologías	**Competencias / Resultados**	**Descripción**	**Calificación**
Prácticas a través de TIC	A2 A7 A13 A24 B2 B7 B20 C4 C8 C19	La entrega de las dos prácticas es obligatoria.	60
Prueba de respuesta múltiple	A2 A7 A13 A24 B2 B7 B20 C4 C8 C19	Se realizará un examen de tipo test, cuyo objetivo es comprobar que la/el estudiante ha asimilado los conceptos correctamente.	40

Observaciones evaluación
Para aprobar la asignatura es preciso obtener: Un mínimo de 4 puntos (sobre 10) en la evaluación de cada práctica. Un mínimo de 4 puntos (sobre 10) en el examen tipo test. Un mínimo de 5 puntos (sobre 10) en la nota final, que se calcula como: 0,60 * (0,70 * práctica1 + 0,30 * práctica2) + 0,40 * examen. Las notas de las prácticas y la del examen tipo test se conservan de la primera oportunidad a la segunda oportunidad (extraordinaria en UVIGO).

Fuentes de información	
Básica	Open Web Application Security Project (OWASP), https://www.owasp.org.Common Weakness Enumeration (CWE), https://cwe.mitre.org.Common Vulnerabilities and Exposures (CVE), https://cve.mitre.org.National Vulnerability Database (NVD), https://nvd.nist.gov.Common Attack Pattern Enumeration and Classification (CAPEC), https://capec.mitre.org.JSON Web Token (JWT), https://jwt.io.OAuth, https://oauth.net.OpenID Connect, http://openid.net/connect/.Open Web Application Security Project (OWASP), https://www.owasp.org.Common Weakness Enumeration (CWE), https://cwe.mitre.org.Common Vulnerabilities and Exposures (CVE), https://cve.mitre.org.National Vulnerability Database (NVD), https://nvd.nist.gov.Common Attack Pattern Enumeration and Classification (CAPEC), https://capec.mitre.org.JSON Web Token (JWT), https://jwt.io.OAuth, https://oauth.net.OpenID Connect, http://openid.net/connect/.
Complementária	

Recomendaciones
Asignaturas que se recomienda haber cursado previamente
Asignaturas que se recomienda cursar simultáneamente
Asignaturas que continúan el temario
Otros comentarios

(*) La Guía Docente es el documento donde se visualiza la propuesta académica de la UDC. Este documento es público y no se puede modificar, salvo cosas excepcionales bajo la revisión del órgano competente de acuerdo a la normativa vigente que establece el proceso de elaboración de guías