Guía Docente				
Datos Identificativos				2020/21
Asignatura (*)	Seguridade de Aplicacións		Código	614530005
Titulación				
Descriptores				
Ciclo	Período	Curso	Tipo	Créditos
Mestrado Oficial	1º cuadrimestre	Primeiro	Obrigatoria	6
Idioma	Castelán			
Modalidade docente	Presencial			
Prerrequisitos				
Departamento	Ciencias da Computación e Tecnoloxías da InformaciónComputaciónTecnoloxías da Información e as Comunicacións			
Coordinación	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	faitic.uvigo.es			
Descrición xeral	Desenvolver aplicacións seguras non é unha tarefa trivial. Coñecer as vulnerabilidades que habitualmente sofren as aplicacións, os mecanismos de autenticación, autorización e control de acceso, así como a incorporación da seguridade ó ciclo de vida de desenrolo, é esencial para poder construír e manter aplicacións seguras con éxito. En esta materia estúdanse de forma práctica todos estes aspectos, con especial énfase no desenvolvemento de aplicacións e servizos web.			

Plan de continxencia	1. Modificacións nos contidos Sen cambios. 2. Metodoloxías * Metodoloxías docentes que se manteñen - Sesión maxistral. Se algunha/algún estudante non pode asistir en persoa ás clases de teoría, ben por confinamento parcial ou por problemas de aforo, usarase o sistema de videoconferencia integrado cos sistemas de docencia online síncrona das universidades. En caso de que ocorra unha situación de confinamento que impida impartir as clases de teoría en persoa, impartiranse de maneira síncrona no horario oficial mediante os sistemas de docencia online síncrona das universidades e quedarán gravadas e accesibles. - Prácticas a través de TIC. De maneira xeral, empregarse a mesma solución que para as sesións maxistrais. Se as clases de laboratorio se teñen que impartir mediante os sistemas de docencia online das universidades, só quedarán gravadas as explicacións xerais do laboratorio, dado que é o único que ten sentido gravar. Polo demais, no hai cambios nos contidos das prácticas, dado que se fan no ordenador persoal da/do estudante, usando software dispoñible publicamente. - Proba de resposta múltiple. Se non é posible realizala en persoa, farase unha proba online. * Metodoloxías docentes que se modifican Ningunha. 3. Mecanismos de atención personalizada ao alumnado - Moodle. Tódolos recursos docentes (diapositivas, exemplos, enunciado da práctica, anuncios, etc.) estarán dispoñibles a través de Moodle. Se é preciso impartir as clases de teoría ou explicacións xerais de laboratorio online, os vídeos quedarán accesibles dende Moodle. - Sistemas de docencia online das universidades. Se é preciso usaranse para impartir as clases de teoría e laboratorio como se indica anteriormente. As titorías atenderanse preferentemente por estes mesmos medios. - Correo electrónico. Para atender a calquera consulta. 4. Modificacións na avaliación Sen cambios. *Observacións de avaliación: Sen cambios. 5. Modificacións da bibliografía ou webgrafía Non é necesario realizar ningunha modificación. Tódolos recursos bibliográficos son sitios web públicos.

Competencias / Resultados do título

Código	Competencias / Resultados do título

Resultados da aprendizaxe			
Resultados de aprendizaxe	Competencias / Resultados do título		
Coñecer as vulnerabilidades que habitualmente sofren as aplicacións (con especial énfase en aplicacións e servizos web) e os seus mecanismos de prevención.	AP2 AP7 AP13	BP2 BP7	CP4
Coñecer os mecanismos de autenticación, autorización e control de acceso en aplicacións e servizos.	AP2 AP7 AP13	BP2 BP7	CP4

Contidos	
Temas	Subtemas
Tema 1. Introdución.	1.1 Autenticación, autorización e control de acceso. 1.2 Aplicacións e servizos con estado. 1.3 Aplicacións e servizos sen estado. 1.4 Aplicacións Web tradicionais e SPA.
Tema 2. Vulnerabilidades e mecanismos de prevención en aplicacións e servizos.	2.1 Marcos de referencia. 2.2 Vulnerabilidades no tratamento dos datos de entrada. 2.3 Vulnerabilidades na autenticación. 2.4 Vulnerabilidades na xestión da sesión. 2.5 Exposición de información sensible. 2.6 Vulnerabilidades no control de acceso. 2.7 Configuración incorrecta. 2.8 Monitorización e log insuficiente. 2.9 Vulnerabilidades en librerías de terceiros.
Tema 3. Ciclos de desenvolvemento de software seguro.	3.1 Seguridade dende a fase de análise. 3.2 Revisións de código. 3.3 Ferramentas SAST e DAST.
Tema 4. Mecanismos de autenticación, autorización e control de acceso.	4.1 Introdución. 4.2 Autenticación e autorización. 4.2.1 Autenticación en HTTP. 4.2.2 JSON Web Token. 4.2.3 OAuth2. 4.2.4 OpenID Connect. 4.2.5 Outros estándares. 4.3 Control de acceso. 4.3.1 Control de acceso baseado en roles (RBAC). 4.3.2 Control de acceso baseado en atributos (ABAC).

Planificación				
Metodoloxías / probas	Competencias / Resultados	Horas lectivas (presenciais e virtuais)	Horas traballo autónomo	Horas totais
Sesión maxistral	A2 A7 A13 B2 B7 C4	22.5	22.5	45
Prácticas a través de TIC	A2 A7 A13 B2 B7 C4	19.5	73.5	93
Proba de resposta múltiple	A2 A7 A13 B2 B7 C4	2	8	10
Atención personalizada		2	0	2
*Os datos que aparecen na táboa de planificación son de carácter orientativo, considerando a heteroxeneidade do alumnado				

Metodoloxías	
Metodoloxías	**Descrición**
Sesión maxistral	Clases impartidas polo profesor mediante a proxección de diapositivas. As clases teñen un enfoque totalmente práctico, explicando os conceptos teóricos mediante o uso de exemplos sinxelos e casos de estudo. As diapositivas están dispoñibles a través da plataforma de docencia da universidade.
Prácticas a través de TIC	Para experimentar cos conceptos estudados na materia, a/o estudante realizará dúas prácticas. A primeira estará centrada no análise de vulnerabilidades dunha aplicación web. A/O estudante partirá do código fonte dunha aplicación web e terá que detectar as vulnerabilidades, explotalas e corrixilas. A segunda práctica estará centrada nos mecanismos de autenticación, autorización e control de acceso. A/O estudante partirá do código fonte dunha aplicación, que consta dunha interface de usuario e un servizo, e terá que encargarse de implementar os aspectos de autenticación, autorización e control de acceso, seguindo distintas estratexias.
Proba de resposta múltiple	Realizarase un exame de tipo test, cuxo obxectivo é comprobar que a/o estudante asimilou os conceptos correctamente. O exame tipo test componse dun conxunto de preguntas con varias respostas posibles, das que só unha delas é correcta. As preguntas non contestadas non puntúan e as contestadas erroneamente puntúan negativamente.

Atención personalizada	
Metodoloxías	**Descrición**
Prácticas a través de TIC	Faranse varias sesións para axudar ó estudante no desenrolo da práctica.

Avaliación			
Metodoloxías	**Competencias / Resultados**	**Descrición**	**Cualificación**
Prácticas a través de TIC	A2 A7 A13 B2 B7 C4	A entrega das dúas prácticas é obrigatoria.	60
Proba de resposta múltiple	A2 A7 A13 B2 B7 C4	Realizarase un exame tipo test, cuxo obxectivo é comprobar que a/o estudante asimilou os conceptos correctamente.	40

Observacións avaliación
Para aprobar a materia é preciso obter: Un mínimo de 4 puntos (sobre 10) na avaliación de cada práctica.Un mínimo de 4 puntos (sobre 10) no exame tipo test.Un mínimo de 5 puntos (sobre 10) na nota final, que se calcula como: 0,60 * (0,70 * práctica1 + 0,30 * práctica2) + 0,40 * exame.As notas das prácticas e a do exame tipo test consérvanse da primeira oportunidade á segunda.

Fontes de información	
Bibliografía 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 2.0, https://oauth.net/2/.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 2.0, https://oauth.net/2/.OpenID Connect, http://openid.net/connect/.
Bibliografía complementaria	

Recomendacións
Materias que se recomenda ter cursado previamente

Materias que se recomenda cursar simultaneamente
Materias que continúan o temario
Observacións

(*)A Guía docente é o documento onde se visualiza a proposta académica da UDC. Este documento é público e non se pode modificar, salvo casos excepcionais baixo a revisión do órgano competente dacordo coa normativa vixente que establece o proceso de elaboración de guías