



| Guía Docente | | | | |
|-----------------------|--|--------------------|--|----------|
| Datos Identificativos | | | | 2018/19 |
| Asignatura (*) | Seguridade de Aplicacións | Código | 614530005 | |
| Titulación | | | | |
| Descritores | | | | |
| Ciclo | Período | Curso | Tipo | Créditos |
| Mestrado Oficial | 1º cuatrimestre | Primeiro | Obrigatoria | 6 |
| Idioma | Castelán | | | |
| Modalidade docente | Presencial | | | |
| Prerrequisitos | | | | |
| Departamento | ComputaciónTecnoloxías 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 | moodle.udc.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. | | | |

| 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 y control de acceso en aplicacións y servizos. | AP2 AP7 AP13 | BP2 BP7 | CP4 |

| Contidos | |
|--|---|
| Temas | Subtemas |
| Tema 1. Introducción. | 1.1 Autenticación, autorización e control de acceso. 1.2 Servizos con estado e sen estado. 1.3 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 Monitorización e log insuficiente. 2.8 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. | <p>4.1 Introducción.</p> <p>4.2 Autenticación e autorización.</p> <p>4.2.1 Autenticación en HTTP.</p> <p>4.2.2 JSON Web Token.</p> <p>4.2.3 OAuth2.</p> <p>4.2.4 OpenID Connect.</p> <p>4.2.5 Outros estándares.</p> <p>4.3 Control de acceso.</p> <p>4.3.1 Control de acceso baseado en roles (RBAC).</p> <p>4.3.2 Control de acceso baseado en atributos (ABAC).</p> |
|--|--|

| Planificación | | | | |
|----------------------------|---------------------------|---|-------------------------|--------------|
| Metodoloxías / probas | Competencias / Resultados | Horas lectivas (presenciais e virtuais) | Horas traballo autónomo | Horas totais |
| Sesión maxistral | A2 A7 A13 B7 B2 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 transparencias. As clases teñen un enfoque totalmente práctico, explicando os conceptos teóricos mediante o uso de exemplos sinxelos e casos de estudo. As transparencias están dispoñibles a través da plataforma de docencia da universidade. |
| Prácticas a través de TIC | Para experimentar cos conceptos estudados na materia, o alumno realizará dúas prácticas. A primeira estará centrada no análise de vulnerabilidades dunha aplicación web. O alumno partirá do código fonte de unha aplicación web e terá que detectar as vulnerabilidades, explotalas e corríxilas. A segunda práctica estará centrada nos mecanismos de autenticación, autorización e control de acceso. O alumno 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 o alumno 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 o alumno 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: $0,60 * (0,70 * \text{práctica1} + 0,30 * \text{práctica2}) + 0,40 * \text{exame}$. Cada práctica avalíase durante unha clase de laboratorio. 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