



| Guía Docente          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                    |                                              |          |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|----------------------------------------------|----------|
| Datos Identificativos |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                    |                                              | 2023/24  |
| Asignatura (*)        | Seguridade de Aplicacións                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Código             | 614530104                                    |          |
| Titulación            | Máster Universitario en Ciberseguridade                                                                                                                                                                                                                                                                                                                                                                                                                                              |                    |                                              |          |
| Descritores           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                    |                                              |          |
| Ciclo                 | Período                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Curso              | Tipo                                         | Créditos |
| Mestrado Oficial      | 1º cuatrimestre                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Primeiro           | Obrigatoria                                  | 5        |
| Idioma                | Castelán                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                    |                                              |          |
| Modalidade docente    | Presencial                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                    |                                              |          |
| Prerrequisitos        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                    |                                              |          |
| Departamento          | Ciencias da Computación e Tecnoloxías da InformaciónComputaciónTecnoloxías da Información e as Comunicacions                                                                                                                                                                                                                                                                                                                                                                         |                    |                                              |          |
| Coordinación          | Bellas Permuy, Fernando                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Correo electrónico | fernando.bellas@udc.es                       |          |
| Profesorado           | Bellas Permuy, Fernando<br>Losada Perez, Jose                                                                                                                                                                                                                                                                                                                                                                                                                                        | Correo electrónico | fernando.bellas@udc.es<br>jose.losada@udc.es |          |
| Web                   | moovi.uvigo.gal                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                    |                                              |          |
| 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. Nesta materia estúdanse de forma práctica todos estes aspectos, con especial énfase no desenvolvemento de aplicacións e servizos web. |                    |                                              |          |

| Competencias do título |                                                                                                                                                                                                                                                                   |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Código                 | Competencias do título                                                                                                                                                                                                                                            |
| A2                     | CE2 - Coñecer en profundidade as técnicas de ciberataque e ciberdefensa                                                                                                                                                                                           |
| A7                     | CE7 - Ter capacidade para realizar a auditoría de seguridade de sistemas e instalacións, o análisis de riscos derivados de debilidades de ciberseguridade e desenvolver o proceso de certificación de sistemas seguros                                            |
| A13                    | CE13 - Ter capacidade de análisis, detección e eliminación de vulnerabilidades, e do malware susceptible de utilizalas, en sistemas e 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 os estudantes saiban aplicar os coñecementos adquiridos e a súa capacidade de resolución de problemas en contornas novas ou pouco coñecidas dentro de contextos máis amplos (ou multidisciplinares) relacionados coa súa área de estudo                 |
| B7                     | CG2 - Resolución de problemas. Ter capacidade de resolver, cos coñecementos adquiridos, problemas específicos do ámbito técnico da seguridade da información, as redes e/ou os sistemas de comunicacións                                                          |
| 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 a importancia da seguridade da información no avance socioeconómico da sociedade                                                                                                                                                                    |
| 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 da aprendizaxe                                                                                                                                   |  |                        |      |      |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------|--|------------------------|------|------|
| Resultados de aprendizaxe                                                                                                                                   |  | Competencias 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                    | BP2  | CP4  |
|                                                                                                                                                             |  | AP7                    | BP7  | CP8  |
|                                                                                                                                                             |  | AP13                   | BP20 | CP19 |
|                                                                                                                                                             |  | AP24                   |      |      |



|                                                                                                     |      |      |      |
|-----------------------------------------------------------------------------------------------------|------|------|------|
| Coñecer os mecanismos de autenticación, autorización e control de acceso en aplicacións e servizos. | AP2  | BP2  | CP4  |
|                                                                                                     | AP7  | BP7  | CP8  |
|                                                                                                     | AP13 | BP20 | CP19 |
|                                                                                                     | AP24 |      |      |

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

| Planificación              |                                      |                   |                                           |              |
|----------------------------|--------------------------------------|-------------------|-------------------------------------------|--------------|
| Metodoloxías / probas      | Competencias                         | Horas presenciais | Horas non presenciais / traballo autónomo | Horas totais |
| Sesión maxistral           | A2 A7 A13 A24 B2 B7<br>B20 C4 C8 C19 | 24                | 24                                        | 48           |
| Prácticas a través de TIC  | A2 A7 A13 A24 B2 B7<br>B20 C4 C8 C19 | 18                | 47                                        | 65           |
| Proba de resposta múltiple | A2 A7 A13 A24 B2 B7<br>B20 C4 C8 C19 | 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 profesorado 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 | <p>Titorías e consultas vía correo electrónico ou Teams para dúbidas específicas.</p> <p>Horarios de titorías:</p> <ul style="list-style-type: none"> <li>- Profesorado UDC: <a href="https://www.udc.es/gl/centros_departamentos_servizos/centros/titorias/?codigo=614">https://www.udc.es/gl/centros_departamentos_servizos/centros/titorias/?codigo=614</a>.</li> <li>- Profesorado UVIGO: <a href="https://moovi.uvigo.gal/user/profile.php?id=11662">https://moovi.uvigo.gal/user/profile.php?id=11662</a>.</li> </ul> <p>Presenza do profesor/a no laboratorio para axudar ó alumno/a no desenvolvemento da práctica.</p> |

### Avaliación

| Metodoloxías               | Competencias                      | Descrición                                                                                                        | Cualificación |
|----------------------------|-----------------------------------|-------------------------------------------------------------------------------------------------------------------|---------------|
| Prácticas a través de TIC  | A2 A7 A13 A24 B2 B7 B20 C4 C8 C19 | A entrega das dúas prácticas é obrigatoria.                                                                       | 60            |
| Proba de resposta múltiple | A2 A7 A13 A24 B2 B7 B20 C4 C8 C19 | Realizarase un exame tipo test, cuxo obxectivo é comprobar que a/o estudante asimilou os conceptos correctamente. | 40            |

### Observacións avaliación

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Para aprobar a materia é preciso obter:</p> <p>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: <math>0,40 * \text{práctica1} + 0,20 * \text{práctica2} + 0,40 * \text{exame}</math>. As notas das prácticas e a do exame tipo test consérvanse da primeira oportunidade á segunda oportunidade (extraordinaria en UVIGO).</p> |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Fontes de información

|                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Bibliografía básica</b>         | <p>Open Web Application Security Project (OWASP), <a href="https://www.owasp.org">https://www.owasp.org</a>. Common Weakness Enumeration (CWE), <a href="https://cwe.mitre.org">https://cwe.mitre.org</a>. Common Vulnerabilities and Exposures (CVE), <a href="https://cve.mitre.org">https://cve.mitre.org</a>. National Vulnerability Database (NVD), <a href="https://nvd.nist.gov">https://nvd.nist.gov</a>. Common Attack Pattern Enumeration and Classification (CAPEC), <a href="https://capec.mitre.org">https://capec.mitre.org</a>. JSON Web Token (JWT), <a href="https://jwt.io">https://jwt.io</a>. OAuth, <a href="https://oauth.net">https://oauth.net</a>. OpenID Connect, <a href="http://openid.net/connect/">http://openid.net/connect/</a>. Open Web Application Security Project (OWASP), <a href="https://www.owasp.org">https://www.owasp.org</a>. Common Weakness Enumeration (CWE), <a href="https://cwe.mitre.org">https://cwe.mitre.org</a>. Common Vulnerabilities and Exposures (CVE), <a href="https://cve.mitre.org">https://cve.mitre.org</a>. National Vulnerability Database (NVD), <a href="https://nvd.nist.gov">https://nvd.nist.gov</a>. Common Attack Pattern Enumeration and Classification (CAPEC), <a href="https://capec.mitre.org">https://capec.mitre.org</a>. JSON Web Token (JWT), <a href="https://jwt.io">https://jwt.io</a>. OAuth, <a href="https://oauth.net">https://oauth.net</a>. OpenID Connect, <a href="http://openid.net/connect/">http://openid.net/connect/</a>.</p> |
| <b>Bibliografía complementaria</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |



| 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