Guía Docente
Curso Académico 2026/27

Datos Generales

Asignatura: DESARROLLO WEB

Titulación: GRADO EN CIBERSEGURIDAD

Carácter: OBLIGATORIA.

Créditos ECTS: 6 ECTS

Curso: 3º

Distribución temporal: 1º SEMESTRE.

Idioma de impartición: CASTELLANO.

Equipo docente: Dr. Rufino Cabrera rufino.cabrera@euneiz.com

Aula(s): Aula informatizada

Presentación de la asignatura:

Asignatura orientada al diseño, implementación y aseguramiento de aplicaciones web dentro de un marco de desarrollo seguro. Se aprenderá a aplicar buenas prácticas de programación en entornos front-end y back-end, incorporando desde el análisis de requisitos hasta la entrega continua, siempre con foco en la identificación y mitigación de vulnerabilidades.

Datos Específicos

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

Conocimientos y contenidos (C)	C2	Reconocer estructuras y protocolos para implementar soluciones de seguridad a nivel de arquitectura de redes de la ciberseguridad.
	C3	Aplicar los conocimientos de protección de datos y seguridad de la información en distintos niveles.
	C4	Ejecutar técnicas de desarrollo y penetración analizando las mejoras técnicas, soluciones y buenas prácticas.
	C5	Realizar desarrollos seguros y aplicar contramedidas a nivel de código.

[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.

	C13	Analizar la gestión de identidades, cifrado, autenticación, confidencialidad, integridad y disponibilidad de la información.
	C14	Valorar los riesgos que suceda un determinado suceso mediante métodos estadísticos y probabilísticos.
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.
	CO2	Usar diferentes herramientas de ingeniería y ciberseguridad para la resolución de problemas relacionados con los ciberataques.
	CO3	Llevar a cabo distintos procesos de análisis en las diferentes áreas de 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.
	CO8	Analizar y ejecutar test de penetración en sistemas informáticos.
	CO10	Aplicar técnicas y herramientas de desarrollo seguro para la verificación y validación del software.
	CO14	Comprender las vulnerabilidades de las nuevas tecnologías y aportar soluciones de ciberseguridad.
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.
	H3	Ser hábil en la comunicación, tanto por escrito como oralmente, en inglés.
	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*

TEMA 1: Introducción al Desarrollo Web Seguro

- MarkDown.
- OWASP Top 10.
- Web Front-end usando HTML y CSS.
- Web Front-end usando JavaScript (JS).
- Arquitectura Cliente-Servidor.
- Web Back-end basado en Python.
- Web Back-end basado en NGINX/Apache + Python/Node.js.

TEMA 2: Seguridad de sesiones, autenticación y cookies

- Autenticación, sesiones y cookies.
- Autenticación avanzada y tokens.
- Protección contra ataques de fuerza bruta y phishing.

TEMA 3: Fortificación de servidores y diseño inclusivo

- DDoS.
- SSL/TLS.
- HTTPS.

TEMA 4: Integración a entornos reales y proyecto final

- Creación de menús en HTML/CSS/JavaScript.
- Estudio de casos reales y análisis de ataques.
- Auditoría final con checklist de OWASP y pruebas.

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.

[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).

MD5	Aprendizaje cooperativo.
MD6	Tutorías.

Actividades formativas utilizadas en esta asignatura son:

Actividades formativas	Horas previstas	% presencialidad
AF1: Clase teórica.	24	100
AF9: Clase en laboratorio	15	100
AF3: Realización de trabajos (individuales y/o grupales).	11	50
AF3: Tutorías (individuales y/o grupales).	5	50
AF5: Estudio independiente y trabajo autónomo del o la estudiante.	90	0
AF6: Pruebas de evaluación.	12	100
Total	**150**	**--**

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.	10	35
SE6: Evaluación de laboratorios	50	70

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

- Sullivan, B., & Liu, V. (2011). *Web Application Security: A Beginner's Guide*. McGraw-Hill Education.
- Zalewski, M. (2011). *The Tangled Web: A Guide to Securing Modern Web Applications*. No Starch Press.

- Hoffman, A. (2018). *Web Application Security: Exploitation and Countermeasures for Modern Web Applications*. Packt Publishing.

Bibliografía Complementaria

- Stuttard, D., & Pinto, M. (2016). *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws* (2nd ed.). Wiley.
- Grossman, J. (2013). *Pro ASP.NET MVC 5 Security: Securing ASP.NET MVC Applications*. Apress.
- Schroeder, M., & Viega, J. (2011). *Network Security with OpenSSL*. O'Reilly Media.
- Coppolino, L., D'Antonio, S., & Spagnuolo, M. (2016). *Secure Web Application Development: A Security-by-Design Approach*. Springer.

Otros Recursos de Aprendizaje Recomendados[3]

- Coppolino, L., D'Antonio, S., & Spagnuolo, M. (2016). *Secure Web Application Development: A Security-by-Design Approach*. Springer.
- Grimes, R. A. (2017). *Web Security, Privacy & Commerce* (3rd ed.). O'Reilly Media.

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