Guía Docente
Curso Académico 2026/27

Datos Generales

Asignatura: PRÁCTICAS ACADÉMICAS EXTERNAS

Titulación: GRADO EN CIBERSEGURIDAD

Carácter: OPTATIVA.

Créditos ECTS: 6 ECTS

Curso: 4º

Distribución temporal: 2º SEMESTRE.

Idioma de impartición: CASTELLANO.

Equipo docente: Dr. Josué Sallent josue.sallent@euneiz.com

Aula(s): Sede / localización de la entidad donde se realizan las PAE

Presentación de la asignatura:

Las Prácticas académicas externas están configuradas como dos-asignaturas optativas dentro del Grado. Su principal objetivo es la aplicación práctica de los conocimientos adquiridos a lo largo del grado en un entorno empresarial. El objetivo de las prácticas académicas externas es situar al estudiante ante un escenario de aprendizaje profesional para que pueda desarrollar los resultados de formación y aprendizaje adquiridos durante sus estudios en el marco de la realidad empresarial o institucional en el contexto del grado.

Datos Específicos

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

Conocimientos o contenidos (C)	C1	Desarrollar habilidades de cálculo para el análisis en los lenguajes de programación.
	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.

[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.

	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.
	C6	Identificar distintas tipologías de virus informáticos.
	C7	Reconocer técnicas antiforense y su aplicación
	C8	Aplicar bases matemáticas y técnicas de diseño de algoritmos a la criptografía y ciberseguridad.
	C9	Identificar los fundamentos teóricos y arquitecturas de los SSOO.
	C10	Entender las responsabilidades profesionales, éticas y legales a partir de las normas y reglamentos en el ámbito de la ciberseguridad.
	C11	Conocer las diferentes topologías de malware para su posterior análisis y mitigación.
	C12	Conocer la nube, su seguridad y sus aplicaciones.
	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.
	C15	Utilizar la inteligencia artificial como herramienta necesaria para garantizar la seguridad.
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.
	CO5	Aplicar técnicas de prevención, detección y protección de ataques en un sistema informático.

	CO6	Utilizar de forma segura los lenguajes de programación más utilizados para su implementación en situaciones reales.
	CO7	Implementar soluciones criptográficas.
	CO8	Analizar y ejecutar test de penetración en sistemas informáticos.
	CO9	Integrar de forma eficaz soluciones basadas en TI en el entorno del usuario.
	CO10	Aplicar técnicas y herramientas de desarrollo seguro para la verificación y validación del software.
	CO11	Gestionar evidencias de vulnerabilidades.
	CO12	Elaborar análisis forenses.
	CO13	Gestionar auditorías sobre marcos y estándares del mercado.
	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.
	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*

Las prácticas académicas externas se realizarán en una empresa, entidad u organismo de carácter público o privado. Esta experiencia sirve como complemento a la formación del estudiante y permite acercar a los estudiantes al ámbito profesional.

El estudiante contará con un tutor académico y un tutor de prácticas en la empresa, entidad u organismo para su orientación y deberá presentar una memoria final.

Los estudiantes podrán cursar las dos asignaturas , solo una de las dos y/o combinarla con una optativa de las ofertadas en el grado o no cursar prácticas y elegir los créditos entre los ofertados en el grado y que no hayan cursado.

Metodologías Docentes y Actividades Formativas[2]

Metodologías docentes utilizadas en esta asignatura son:

MD4	Aprendizaje basado en proyectos.
MD5	Aprendizaje cooperativo.
MD6	Tutorías.

Actividades formativas utilizadas en esta asignatura son:

Actividades formativas	Horas previstas	% presencialidad
AF7 Prácticas externas	150	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
SE4 Evaluación de las prácticas externas	100	100

El estudiantado posee dos modalidades de evaluación para superar la asignatura:

- Evaluación continua con 2 convocatorias/año: ordinaria y extraordinaria.

[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).

- 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
Hardware y dispositivos específicos (en función de las tareas y la entidad donde se realizan las PAE)
Software específico de ciberseguridad (en función de las tareas y la entidad donde se realizan las PAE)
Laboratorios y espacios adaptados (en función de la entidad donde se realizan las PAE)

Bibliografía y otros Recursos de Aprendizaje

Bibliografía Básica

- Tanenbaum, A. S., & Bos, H. (2013). Fundamentos de arquitectura de computadores (6.ª ed.). Pearson Educación.
- Zacker, C. (2002). Redes: Manual de referencia. McGraw-Hill Interamericana.
- Tanenbaum, A. S., & Bos, H. (2015). Sistemas operativos modernos (4.ª ed.). Pearson Educación.

Bibliografía Complementaria

- Adam Shostack. Threat modeling designing of security.
- Michael Sikorski and Andrew Honig. Practical Malware Analysis.
- Simon Singh. The code book.

Otros Recursos de Aprendizaje Recomendados[3]

- Europass
  https://europass.europa.eu
  Elaboración del CV, portfolio de competencias y preparación para la inserción laboral.
- INCIBE
  https://www.incibe.es
  Recursos técnicos, informes y formación para estudiantes que realizan prácticas en el ámbito de la ciberseguridad.
- Instituto Nacional de Seguridad y Salud en el Trabajo (INSST)
  https://www.insst.es
  Información sobre prevención de riesgos laborales y seguridad en el entorno de trabajo.

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