



Guía Docente

Curso Académico 2024/25

Datos Generales

Asignatura: CRIPTOGRAFÍA

Titulación: GRADO EN CIBERSEGURIDAD

Carácter: OBLIGATORIA

Créditos ECTS: 6 ECTS

Curso: 2º

Distribución temporal: semestre, año, etc.: 2º SEMESTRE

Idioma de impartición: CASTELLANO

Equipo docente: Iratxe González iratxe.gonzalez@euneiz.com

Presentación de la asignatura:

Asignatura para conocer y afianzar todos los conceptos relacionados con la criptografía en el marco de la ciberseguridad que serán de gran importancia de cara a aplicar e implementar los conocimientos en diferentes entornos encriptados en el ámbito de la ciberseguridad.

Datos Específicos

Resultados del proceso de formación y aprendizaje (RFA)

Contenidos o conocimientos (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.
	C6	Identificar distintas tipologías de virus informáticos.
	C7	Reconocer técnicas antiforenses y su aplicación.
	C8	Aplicar bases matemáticas y técnicas de diseño de algoritmos a la criptografía y ciberseguridad.
	C11	Conocer las diferentes topologías de malware para su posterior análisis y mitigación.
	C13	Analizar la gestión de identidades, cifrado, autenticación,



Guía Docente

Curso Académico 2024/25

		confidencialidad, integridad y disponibilidad de la información.
	C14	Valorar los riesgos que suceda un determinado suceso mediante métodos estadísticos y probabilísticos.
Competencias (CO)	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.
	CO5	Aplicar técnicas de prevención, detección y protección de ataques en un sistema informático.
	CO7	Implementar soluciones criptográficas.
	CO11	Gestionar evidencias de vulnerabilidades.
	CO12	Elaborar análisis forenses.
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*

1. Criptología, Criptografía y Criptoanálisis.
2. Historia de criptología clásica y criptología moderna.
3. Criptosistemas de clave pública y clave privada.
4. Técnicas básicas: cifrado-descifrado y firma.
5. Criptología de clave privada y de clave pública.
6. Bases matemáticas de la criptografía.

(*El contenido desarrollado está disponible en la Programación Docente de la asignatura publicada en el Campus Virtual de la Universidad)



Guía Docente

Curso Académico 2024/25

Metodologías Docentes y Actividades Formativas

Metodologías docentes utilizadas en esta asignatura son:

MD1	Método expositivo
MD2	Estudio de casos
MD3	Aprendizaje basado en problemas
MD4	Aprendizaje basado en proyectos
MD5	Aprendizaje cooperativo
MD6	Tutorías

Actividades formativas utilizadas en esta asignatura son:

Actividades formativas	Horas previstas	% presencialidad
AF1: Clase teórica	22,5	100
AF9: Clase en laboratorio	15	100
AF3: Realización de trabajos (individuales y/o grupales)	12,5	50
AF4: Tutorías (individuales y/o grupales)	5	50



Guía Docente

Curso Académico 2024/25

AF5: Estudio independiente y trabajo autónomo del estudiante	89	0
AF6: Pruebas de evaluación	6	100
Total	150	

Evaluación: Sistemas y Criterios de Evaluación

Sistemas de evaluación utilizados en esta asignatura son:

Denominación	Pond. mín.	Pond. Máx
SE1 Evaluación de la asistencia y participación del estudiante	0	5
SE2 Evaluación de trabajos	10	35
SE3 Pruebas de evaluación y/o exámenes	50	70

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

- Evaluación continua con 2 convocatorias/año: ordinaria y extraordinaria.
- Evaluación única con una convocatoria/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 estudiante acogerse a la evaluación única (examen único).
- No se permite el cambio del sistema de evaluación escogido por el estudiante a lo largo del curso.
- El estudiante que desee acogerse a la 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 del curso.
- Si el estudiante no asiste un 80% a las clases presenciales no podrá presentarse a la



Guía Docente

Curso Académico 2024/25

convocatoria ordinaria y pasará automáticamente a convocatoria extraordinaria.

- Las faltas de asistencia deben justificarse al profesor responsable de la asignatura.
- De manera excepcional, el docente responsable de la asignatura podrá valorar con otros criterios adicionales como la participación, la actitud, el grado de desempeño y aprovechamiento del estudiante, etc. la posibilidad de permitir que el estudiante continúe en la convocatoria ordinaria, siempre que su asistencia mínima se encuentre por encima del 70%.
- El 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 que hayan obtenido una calificación igual o superior a 9.0. Su número no podrá exceder del cinco por ciento de los alumnos matriculados en una materia en el correspondiente curso académico, salvo que el número de alumnos matriculados sea inferior a 20, en cuyo caso se podrá conceder una sola «Matrícula de Honor»
- Será considerado no presentado (NP) el estudiante matriculado que no realice ninguna actividad evaluativa.
- Toda actividad evaluativa escrita (trabajos, exámenes...) considerará las faltas ortográficas 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 para analizar las posibles fuentes de plagio y evaluar si están justificadas.
 - Cualquier trabajo con un índice de similitud superior al 30% no será evaluado.



Guía Docente

Curso Académico 2024/25

Bibliografía y otros Recursos de Aprendizaje

Bibliografía Básica

- Understanding Cryptography: A Textbook for Students and Practitioners. Christof Paar et al. Springer, 2014
- Manual básico de criptología. Introducción a la ciencia del secreto. Luis Hernandez Encinas. Pinolia, 2023.
- Criptografía. Técnicas de desarrollo para profesionales. Ariel Maiorano. RA-MA S.A. Editorial y Publicaciones, 2010.

Bibliografía Complementaria

- Aplicaciones criptográficas. Segunda edición. Jorge Ramió.
- Técnicas criptográficas de protección de datos. Amparo Fuster, Dolores de la Guía, Luis Hernández Encinas, Fausto Montoya y Jaime Muñoz
- Criptografía y seguridad en computadores. Manuel J. Lucena López.

Otros Recursos de Aprendizaje Recomendados

- <https://www.udemy.com/course/cursodecriptografia>
- Paredes, G. G. (2006). Introducción a la criptografía.
- Marrero Travieso, Y. (2003). La Criptografía como elemento de la seguridad informática. *Acimed*, 11(6), 0-0.