



Datos Generales

Asignatura: CRIPTOGRAFÍA

Titulación: GRADO EN CIBERSEGURIDAD

Carácter: OBLIGATORIA.

Créditos ECTS: 6 ECTS

Curso: 2º

Distribución temporal: 2º SEMESTRE.

Idioma de impartición: CASTELLANO.

Equipo docente: Dr. Aitor Gómez Goiri aitor.gomez@euneiz.com

Aula(s): Aula informatizada

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 cifrados en el ámbito de la ciberseguridad. En la parte teórica de la asignatura se fijarán conceptos como los fundamentos matemáticos que facilitan el desarrollo de protocolos y primitivas criptográficas. En la práctica, pondremos en uso librerías que nos permitan aplicar los protocolos más ampliamente usados con seguridad en nuestros desarrollos.

Datos Específicos

Resultados del proceso de formación y aprendizaje (RFA)¹

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

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.

		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, 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*

- **Unidad 1** (teoría): Fundamentos los Códigos Correctores de Errores
 - Introducción a los códigos lineales y su relevancia en la corrección de errores.
 - Definición de la distancia de Hamming y su papel en la detección y corrección de errores.
 - Análisis de códigos perfectos y equivalentes.
- **Unidad 2** (teoría): Estructura y Propiedades de los Códigos Lineales
 - Uso de matrices generadoras y de control para la codificación y decodificación.
 - Propiedades básicas de los códigos lineales.
 - Ejemplos relevantes: Aplicaciones de los códigos de Hamming.
- **Unidad 3** (teoría): Pruebas de Primalidad y Aplicaciones Numéricas
 - Métodos y conceptos para verificar números primos.
 - Test de Fermat y propiedades de los números pseudoprimos.
 - Introducción al test de Miller-Rabin y números pseudoprimos fuertes.
- **Unidad 4** (teoría): Cifrado Clásico y Sistemas Criptográficos de Clave Privada
 - Sistemas de sustitución, afinidad y el método criptográfico de Hill.
 - Introducción al algoritmo DES.
- **Unidad 5** (teoría): Cifrado Moderno y Sistemas Criptográficos de Clave Pública
 - Principios de los sistemas RSA y ElGamal.
 - Aplicaciones del cifrado de clave pública en la seguridad moderna.
- **Unidad 6** (teoría): Protocolos y Herramientas Criptográficas
 - Intercambio de claves mediante el protocolo Diffie-Hellman.
 - Uso de firmas digitales para garantizar autenticidad y no repudio.
- **Unidad 7** (práctica): Cifrado en flujo
 - One-time-passwords (OTP) y sus limitaciones.

Metodologías Docentes y Actividades Formativas²

Metodologías docentes utilizadas en esta asignatura son:

MD1	Método expositivo.
-----	--------------------

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).

MD2	Estudios de caso.
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
AF2: Clase prácticas.	15	100
AF3: Realización de trabajos (individuales y/o grupales).	5	50
AF3: Tutorías (individuales y/o grupales).	5	50
AF5: Estudio independiente y trabajo autónomo del o la estudiante.	89	0
AF6: Pruebas de evaluación.	6	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 continúe 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).



Guía Docente

Curso Académico 2026/27

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 de ciberseguridad

Bibliografía y otros Recursos de Aprendizaje

Bibliografía Básica

- Understanding Cryptography: A Textbook for Students and Practitioners. Christof Paar et al. Springer, 2014



Guía Docente

Curso Académico 2026/27

- 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 Recomendados³

- <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.

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