



GUÍA DOCENTE 2026-2027
CIBERSEGURIDAD Y PROTECCIÓN DE DATOS

1. Denominación de la asignatura:

CIBERSEGURIDAD Y PROTECCIÓN DE DATOS

Titulación

Grado en Tecnologías Digitales para la Empresa

Código

9012

2. Materia o módulo a la que pertenece la asignatura:

Sistemas operativos, sistemas distribuidos y redes

3. Departamento(s) responsable(s) de la asignatura:

Digitalización

4.a Profesor/a que imparte la docencia (Si fuese impartida por más de uno/a incluir todos/as) :

Profesor a contratar

4.b Coordinador/a de la asignatura

Álvaro Herrero Cosío

5. Curso y semestre en el que se imparte la asignatura:

4º - 1er semestre

6. Tipo de la asignatura: (Básica, obligatoria u optativa)

Obligatoria



7. Número de créditos ECTS de la asignatura:

6

8. Competencias // Resultados de aprendizaje

CT1 - Capacidad de análisis y síntesis. CT2 - Capacidad de organización y planificación. CT8 - Aprendizaje y trabajo autónomo. Formación continua y permanente. CT17 - Trabajo en equipo. GC10.1 - Conocer los conceptos principales necesarios para el análisis y gestión de riesgos de los sistemas de información. GC10.2 - Conocer las características de los estándares de gestión de la seguridad de un sistema de información. GC10.3 - Concebir, planificar e implantar políticas y medidas de seguridad informática adecuadas en eficacia y coste. Integrar los conocimientos técnicos de seguridad informática en el plano ético, legal y organizativo. GC10.4 - Ser capaz de realizar tareas técnicas a integrar en un SGSI como pueden ser el control de idoneidad de contraseñas, copias de seguridad, cifrado, uso de anti-malware, auditorías y seguridad física. GC10.5 - Concebir planes de formación para las personas relacionadas con los sistemas de información. GC10.6 - Trabajar eficazmente en grupo para coordinarse en tareas técnicas y organizativas. GC10.7 - Conocer el marco legal que regula el desempeño profesional (RGPD y LOPD, LSSI, Reglamento eIDAS y demás normativa sobre transacciones y firma electrónica).
--

9. Programa de la asignatura

9.1- Objetivos docentes
- Comprender los fundamentos de seguridad en redes y algunos de sus protocolos. - Capacidad para elaborar el pliego de condiciones técnicas de una instalación informática que cumpla los estándares y normativas vigentes. - Conocer los principios y amenazas a la seguridad de los sistemas de información y competencias para diseñar la estrategia y políticas efectivas de seguridad de la información en las organizaciones.



9.2- Unidades docentes (Bloques de contenidos)
Ciberseguridad Introducción Principios de la ciberseguridad; amenazas, ataques y vulnerabilidades; servicios y mecanismos de seguridad Principios de protección de la información Cifrado de la información; tipos de cifrado. Seguridad en la transmisión de la información Protocolos de comunicaciones seguras, redes privadas virtuales, correo electrónico seguro. Gestión y administración de la criptoseguridad sistemas de gestión de la seguridad de la información; análisis y gestión de riesgos; planes de continuidad del negocio.
Protección de datos Aspectos legales de la protección de datos RGPD; autoridades de control; delegado de protección de datos.
9.3- Acceso a la Bibliografía Recomendada desde Leganto
https://leganto.ubu.es/leganto/public/34BUC_UBU/lists?courseCode=9012&auth=SAML

10. Metodología de enseñanza y aprendizaje y su relación con las competencias/resultados de aprendizaje que debe adquirir/alcanzar el/la estudiante:

Metodología	Competencia/resulta do de aprendizaje relacionado	Horas presenciales	Horas de trabajo	Total de horas
Clases teóricas	CT1, CT2, CT8, CT17, GC10.1, GC10.2, GC10.3, GC10.4, GC10.5, GC10.6, GC10.7	24	54	78
Clases prácticas	CT1, CT2, CT8, CT17, GC10.1, GC10.2, GC10.3, GC10.4, GC10.5, GC10.6, GC10.7	24	42	66
Pruebas de evaluación	CT1, CT2, CT8,	6	0	6



	CT17, GC10.1, GC10.2, GC10.3, GC10.4, GC10.5, GC10.6, GC10.7			
Total		54	96	150

11. Sistemas de evaluación:

Para superar la asignatura es necesario obtener una nota mínima de 4 sobre 10 en cada uno de los procedimientos y de 5 sobre 10 en la media ponderada de los mismos. Para la segunda convocatoria, una parte del procedimiento "Seguimiento de la materia" puede no ser recuperable, al consistir en actividades a realizar en el aula. Habiendo superado la asignatura en primera convocatoria, no cabe la opción de presentarse en segunda convocatoria para incrementar las calificaciones.

Procedimiento	Peso primera convocatoria	Peso segunda convocatoria
Prueba final	40 %	40 %
Prácticas de laboratorio	40 %	40 %
Seguimiento de la materia	20 %	20 %
Total	100 %	100 %

Evaluación excepcional:

Para la evaluación excepcional, se aplicarán los siguientes procedimientos, con los correspondientes pesos:

Prueba final (50%)

Prácticas de laboratorio (50%)

Se establecerán las condiciones y plazos para cada curso académico, que serán distintos de la evaluación ordinaria.

12. Idioma en que se imparte:

Español, con algún material en inglés