GUÍA DE APRENDIZAJE

CIBERSEGURIDAD Y PROTECCIÓN DE DATOS

GRADO EN INGENIERIA Y SISTEMAS DE DATOS

CURSO ACADÉMICO	CÓDIGO	CURSO	CRÉDITOS	CARÁCTER	SEMESTRE
2026-27	95000534	4	6 ECTS	OBLIGATORIA	PRIMER SEMESTRE

IDIOMA
ESPAÑOL

CENTRO RESPONSABLE
E.T.S. DE INGENIEROS DE TELECOMUNICACION

DEPARTAMENTO RESPONSABLE
INGENIERÍA DE SISTEMAS TELEMÁTICOS

COORDINADOR/A
XAVIER ANDRES LARRIVA NOVO - xavier.larriva.novo@upm.es

REQUISITOS OBLIGATORIOS

ASIGNATURAS REQUERIDAS

—

CONOCIMIENTOS PREVIOS RECOMENDADOS

ASIGNATURAS RECOMENDADAS

• REDES Y SERVICIOS DE COMUNICACIONES (95000515)
• COMPUTACIÓN EN LA NUBE (95000525)
• PROGRAMACIÓN PARA BIG DATA (95000514)

OTRAS RECOMENDACIONES

No se necesitan otros conocimientos previos distintos a los contenidos en las asignaturas previas que se recomienda

RESULTADOS

RD-1393/2007

Competencias

CB01 Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio

CE21 Que los estudiantes sean capaces de aplicar de manera adecuada la normativa, legislación y regulaciones relativas a los sistemas y servicios específicos de la titulación, así como las especificaciones, estándares y directivas técnicas en función de las características, los requisitos y la funcionalidad que deban implementarse.

CE11 Que los estudiantes sean capaces de diseñar y operar sistemas de almacenamiento y transmisión de datos teniendo en cuenta estrategias y requisitos de seguridad y privacidad, políticas de acceso a los datos, con capacidad de prever ataques y subsanar vulnerabilidades.

CB02 Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio

CE04 Que los estudiantes sean capaces de aplicar los conceptos y tecnologías del ámbito de la ingeniería de la telecomunicación en cualquier sector (eHealth, business intelligence, smart cities, etc.) incorporando aspectos técnicos, de negocio y de gestión.

CE05 Que los estudiantes sean capaces de analizar los requisitos e identificar los riesgos de un proyecto de ingeniería de datos y sistemas en el ámbito de la ingeniería de telecomunicación a partir de la comprensión del ciclo de vida completo del dato.

CG05 Tener la capacidad de concebir y proponer soluciones creativas aplicando los métodos científico y de ingeniería para la definición y resolución de problemas formalizando los objetivos buscados y considerando los recursos disponibles.

CB03 Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética

CG04 Saber identificar y utilizar las herramientas de las Tecnologías de la Información y de las Comunicaciones más adecuadas para plantear y construir soluciones a problemas

CB05	Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía
CG01	Tener capacidad de trabajar en entornos internacionales y multidisciplinares, haciendo uso de la lengua inglesa en forma oral y escrita.
CB04	Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado
CG03	Ser capaz de explicar de forma oral o escrita las soluciones planteadas para la resolución de un problema.

Resultados de aprendizaje

RA104	Comprender las amenazas a la seguridad de las infraestructuras de datos y las metodologías de análisis de riesgos.
RA105	Diseñar y aplicar las técnicas de protección de las infraestructuras de datos.
RA106	Conocer la legislación en materia de protección de datos.

DESCRIPCIÓN

Los objetivos de esta asignatura son:

- Conocer la necesidad de la Ciberseguridad y los componentes y elementos que forman parte de sus competencias.
- Conocer los fundamentos organizativos y legislativos en los que se basan las tecnologías de ciberseguridad y protección de datos.
- Conocer las principales amenazas y vulnerabilidades de los distintos elementos involucrados en la ingeniería de datos, así como sus causas.
- Conocer y ser capaz de diseñar y aplicar las tecnologías y sistemas que conforman una Arquitectura de Seguridad de las TIC, en sus distintas perspectivas, así como los fundamentos de criptografía en los que se basan.
- Conocer y ser capaz de diseñar sistemas de Ingeniería de Privacidad

TEMARIO

1. Ciberseguridad y Protección de Datos

1.1. Introducción a la Ciberseguridad

1.2. Componentes de la Ciberseguridad

1.3. Estrategias de Ciberseguridad y Análisis de Riesgos

1.4. Verificación del cumplimiento Legislativo de Protección de Datos

2. Caracterización de Amenazas

2.1. Amenazas Humanas

2.2. Amenazas Tecnológicas

3. Protección de Sistemas, Comunicaciones y Datos

3.1. Criptografía. PKI

3.2. Tecnologías de Control de Acceso a Sistemas y Redes

3.3. Tecnologías de Protección de los Datos y las Comunicaciones

3.4. Seguridad de los datos: securización de BBDD

4. Ingeniería de Privacidad

4.1. Análisis de amenazas de privacidad

4.2. Privacidad desde el diseño y tecnologías de protección de la privacidad

4.3. Anonimato de conjuntos de datos

ACTIVIDADES

Actividad evaluable Actividad formativa

Tema 1

SEMANAS 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 E

PRESENCIALIDAD	DURACIÓN TOTAL	LUGAR	GRUPO
Presencial	09h 20m	Aula (en horario)	Normal

METODOLOGÍA

Lección Magistral

Tema 2

SEMANAS: 1 2 **3** **4** 5 6 7 8 9 10 11 12 13 14 15 E

PRESENCIALIDAD	DURACIÓN TOTAL	LUGAR	GRUPO
Presencial	09h 20m	Aula (en horario)	Normal

METODOLOGÍA
Lección Magistral

Evaluación actividad amenazas

SEMANAS: 1 2 3 **4** 5 6 7 8 9 10 11 12 13 14 15 E

PRESENCIALIDAD	DURACIÓN TOTAL	LUGAR	EVALUACIÓN	PONDERACIÓN	NOTA MÍNIMA
Presencial	00h 00m	Laboratorio	Progresiva	7.5%	3

METODOLOGÍA
Trabajo en Grupo

RESULTADOS EVALUADOS
CB01 CB02 CB03 CB05 CG01 CG03 CG04 CG05

Tema 3

SEMANAS: 1 2 3 4 **5** **6** **7** 8 **9** **10** 11 12 13 14 15 E

PRESENCIALIDAD	DURACIÓN TOTAL	LUGAR	GRUPO
Presencial	23h 20m	Aula (en horario)	Normal

METODOLOGÍA
Lección Magistral

Evaluación Actividad Criptografía

SEMANAS: 1 2 3 4 5 **6** 7 8 9 10 11 12 13 14 15 E

PRESENCIALIDAD	DURACIÓN TOTAL	LUGAR	EVALUACIÓN	PONDERACIÓN	NOTA MÍNIMA
Presencial	00h 00m	Laboratorio	Progresiva	7.5%	3

METODOLOGÍA
Trabajo en Grupo

RESULTADOS EVALUADOS
CB01 CB02 CB03 CB05 CG03 CG04 CG05

Evaluación Actividad Protección Sistemas

SEMANAS: 1 2 3 4 5 6 **7** 8 9 10 11 12 13 14 15 E

PRESENCIALIDAD	DURACIÓN TOTAL	LUGAR	EVALUACIÓN	PONDERACIÓN	NOTA MÍNIMA
Presencial	00h 00m	Laboratorio	Progresiva	10%	3

METODOLOGÍA: Trabajo en Grupo

RESULTADOS EVALUADOS: CE04 CE05 CE11 CB01 CB02 CB03 CB05 CG01 CG03 CG04

Examen Primera Parte de Asignatura

SEMANAS: 1 2 3 4 5 6 7 **8** 9 10 11 12 13 14 15 E

PRESENCIALIDAD	DURACIÓN TOTAL	LUGAR	EVALUACIÓN	PONDERACIÓN	NOTA MÍNIMA
Presencial	02h 00m	Aula de examen	Progresiva	35%	3

METODOLOGÍA: Examen Escrito

RESULTADOS EVALUADOS: CB01 CB02 CB04 CB05 CG01 CG03 CG05

Tema 4

SEMANAS: 1 2 3 4 5 6 7 8 9 10 **11** **12** **13** 14 15 E

PRESENCIALIDAD	DURACIÓN TOTAL	LUGAR	GRUPO
Presencial	14h 00m	Aula (en horario)	Normal

METODOLOGÍA: Lección Magistral

Evaluación Actividad Ing. Privacidad

SEMANAS: 1 2 3 4 5 6 7 8 9 10 11 12 **13** 14 15 E

PRESENCIALIDAD	DURACIÓN TOTAL	LUGAR	EVALUACIÓN	PONDERACIÓN	NOTA MÍNIMA
Presencial	00h 00m	Laboratorio	Progresiva	10%	3

METODOLOGÍA: Trabajo Individual

RESULTADOS EVALUADOS: CE21 CE11 CB01 CB02 CB03 CB04 CB05 CG04

Examen Segunda Parte de Asignatura

SEMANAS: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 **E**

PRESENCIALIDAD	DURACIÓN TOTAL	LUGAR	EVALUACIÓN	PONDERACIÓN	NOTA MÍNIMA
Presencial	02h 00m	Aula de examen	Progresiva, Global	30%	3

METODOLOGÍA
Examen Escrito

RESULTADOS EVALUADOS
CE04 CE05 CB01 CB04 CB05 CG01 CG03 CG04

Examen Global Primera Parte de Asignatura

SEMANAS: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 **E**

PRESENCIALIDAD	DURACIÓN TOTAL	LUGAR	EVALUACIÓN	PONDERACIÓN	NOTA MÍNIMA
Presencial	02h 00m	Aula de examen	Global	35%	3

METODOLOGÍA
Examen Escrito

RESULTADOS EVALUADOS
CE04 CE05 CB01 CB02 CB03 CB05 CG03

Evaluación Actividad Amenazas

SEMANAS: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 **E**

PRESENCIALIDAD	DURACIÓN TOTAL	LUGAR	EVALUACIÓN	PONDERACIÓN	NOTA MÍNIMA
Presencial	00h 00m	Aula de examen	Global	7.5%	3

METODOLOGÍA
Examen Escrito Examen oral Examen de Prácticas Otras técnicas

RESULTADOS EVALUADOS
CB01 CB02 CB03 CB05 CG03 CG04 CG05

Evaluación Actividad Criptografía

SEMANAS: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 **E**

PRESENCIALIDAD	DURACIÓN TOTAL	LUGAR	EVALUACIÓN	PONDERACIÓN	NOTA MÍNIMA
Presencial	00h 00m	Aula de examen	Global	7.5%	3

METODOLOGÍA
Examen Escrito Examen oral Otras técnicas Examen de Prácticas

RESULTADOS EVALUADOS
CB01 CB02 CB03 CB05 CG03 CG04 CG05

Evaluación Actividad Protección de Sistemas

SEMANAS: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 E

PRESENCIALIDAD	DURACIÓN TOTAL	LUGAR	EVALUACIÓN	PONDERACIÓN	NOTA MÍNIMA
Presencial	00h 00m	Aula de examen	Global	10%	3

METODOLOGÍA
Examen Escrito | Examen de Prácticas | Examen oral | Otras técnicas

RESULTADOS EVALUADOS
CE04 | CE05 | CE11 | CB01 | CB02 | CB03 | CB05 | CG01 | CG03 | CG04

Evaluación Actividad Ing. Privacidad

SEMANAS: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 E

PRESENCIALIDAD	DURACIÓN TOTAL	LUGAR	EVALUACIÓN	PONDERACIÓN	NOTA MÍNIMA
Presencial	00h 00m	Aula de examen	Global	10%	3

METODOLOGÍA
Examen Escrito | Examen oral | Otras técnicas | Examen de Prácticas

RESULTADOS EVALUADOS
CE21 | CE11 | CB01 | CB02 | CB03 | CB04 | CB05 | CG04

Examen Final Extraordinario

SEMANAS: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 E

PRESENCIALIDAD	DURACIÓN TOTAL	LUGAR	EVALUACIÓN	PONDERACIÓN	NOTA MÍNIMA
Presencial	03h 00m	Aula de examen	Extraordinaria	65%	3

METODOLOGÍA
Examen Escrito

RESULTADOS EVALUADOS
CE21 | CE04 | CE05 | CE11 | CB01 | CB02 | CB03 | CB04 | CB05 | CG01 | CG03 | CG04 | CG05

Evaluación Actividades Extraordinaria

SEMANAS: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 E

PRESENCIALIDAD	DURACIÓN TOTAL	LUGAR	EVALUACIÓN	PONDERACIÓN	NOTA MÍNIMA
Presencial	01h 00m	Aula de examen	Extraordinaria	35%	3

METODOLOGÍA
Examen Escrito | Examen de Prácticas | Examen oral | Otras técnicas

RESULTADOS EVALUADOS
CE21 | CE04 | CE05 | CE11 | CB01 | CB02 | CB03 | CB04 | CB05 | CG01 | CG03 | CG04 | CG05

PLANIFICACIÓN SEMANAL

Actividad evaluable | Actividad formativa | • Semana con actividad | E Período de exámenes

Actividad	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	E
Tema 1	•	•														
Tema 2			•	•												
Evaluación actividad amenazas				•												
Tema 3					•	•	•		•	•						
Evaluación Actividad Criptografía						•										
Evaluación Actividad Protección Sistemas							•									
Examen Primera Parte de Asignatura								•								
Tema 4											•	•	•			
Evaluación Actividad Ing. Privacidad													•			
Examen Segunda Parte de Asignatura																•
Examen Global Primera Parte de Asignatura																•
Evaluación Actividad Amenazas																•
Evaluación Actividad Criptografía																•
Evaluación Actividad Protección de Sistemas																•
Evaluación Actividad Ing. Privacidad																•
Examen Final Extraordinario																•
Evaluación Actividades Extraordinaria																•

CRITERIOS DE EVALUACIÓN

Criterios Generales

La evaluación de la asignatura se realiza de forma progresiva. La calificación combina **65 % de teoría** (exámenes) y **35 % de práctica** (actividades de evaluación), con la misma ponderación en las tres convocatorias.

Son bloques liberatorios e independientes las cuatro actividades de evaluación (amenazas 7,5 %, criptografía 7,5 %, protección de sistemas 10 % e ingeniería de privacidad 10 %) y los dos exámenes de teoría (1ª parte 35 %, 2ª parte 30 %). Cada bloque superado conserva su nota hasta la convocatoria extraordinaria del mismo curso sin necesidad de repetirlo.

En cualquier convocatoria, cada bloque debe alcanzar una nota mínima de **3 sobre 10** para computar; las notas inferiores se calificarán con 0 %. Para superar la asignatura se exige una media ponderada de al menos **5 sobre 10**, respetando ese mínimo en todos los bloques.

Los trabajos y entregas deberán ser originales. El uso no autorizado o no declarado de herramientas de inteligencia artificial generativa, así como la copia o el plagio total o parcial, podrá conllevar la realización de una **evaluación adicional individual** (por ejemplo, defensa oral) para verificar la autoría y el dominio de los contenidos, identificando las posibles medidas disciplinarias que correspondan según la normativa de la UPM.

Criterios de Evaluación en Convocatoria Ordinaria. Evaluación progresiva

Criterios de evaluación

Consta de las cuatro actividades de evaluación y dos exámenes parciales de teoría.

Las cuatro actividades prácticas (35 % en conjunto) se realizan a lo largo del curso. Cada actividad y cada parcial son liberatorios de forma independiente conforme a los criterios generales.

Actividades

- Evaluación actividad amenazas (7.5%)
- Evaluación Actividad Criptografía (7.5%)
- Evaluación Actividad Protección Sistemas (10%)

- Examen Primera Parte de Asignatura (35%)
- Evaluación Actividad Ing. Privacidad (10%)
- Examen Segunda Parte de Asignatura (30%)

Criterios de Evaluación en Convocatoria Ordinaria. Prueba global

Criterios de evaluación

Consta de las cuatro actividades de evaluación y Examen, que se compone de **dos partes**:

- *Examen Global Primera Parte* , 35 %.
- *Examen Segunda Parte* , 30 %; correspondiente con el Parcial 2 de la evaluación progresiva.

Las cuatro actividades de evaluación de esta modalidad podrán evaluarse mediante **examen escrito, examen oral, examen de prácticas (laboratorio) u otras técnicas**, según determine el profesorado.

Quien en la evaluación progresiva haya superado el Parcial 1 realiza únicamente la segunda parte; quien no lo haya superado, o curse la modalidad global, realiza ambas partes. De este modo, "examen global" y "segundo parcial" no son pruebas distintas, sino partes del mismo examen de enero.

Actividades

- Examen Segunda Parte de Asignatura (30%)
- Examen Global Primera Parte de Asignatura (35%)
- Evaluación Actividad Amenazas (7.5%)
- Evaluación Actividad Criptografía (7.5%)
- Evaluación Actividad Protección de Sistemas (10%)
- Evaluación Actividad Ing. Privacidad (10%)

Criterios de Evaluación en Convocatoria Extraordinaria

Criterios de evaluación

Se ofrece exclusivamente al alumnado que no haya superado la asignatura en la convocatoria ordinaria. Consta de dos evaluaciones, divididos internamente por temas:

- *Examen Final Extraordinario* (teoría), 65 %.
- *Evaluación de Actividades*, 35 %.

El estudiante se evalúa únicamente de los bloques no superados (nota inferior a 3) y podrá repetir voluntariamente bloques ya superados para mejorar nota, avisando por correo electrónico con al menos una semana de antelación; en todos los casos se conserva la nota más favorable. Se mantienen la nota mínima de 3 sobre 10 por bloque.

Tanto la parte teórica como la evaluación de Actividades podría evaluarse mediante **examen escrito, examen oral, examen de prácticas (laboratorio) u otras técnicas**..

Actividades

- Examen Final Extraordinario (65%)
- Evaluación Actividades Extraordinaria (35%)

RECURSOS

Web

Moodle
Servidor Moodle de la Asignatura

Equipamiento

Equipamiento
Aula, Laboratorio, Sala de Trabajo en Grupo

Bibliografía

Referencias
Bibliografía

OBJETIVOS DE DESARROLLO SOSTENIBLE

Educación de calidad

Industria, innovación e infraestructura

OTRA INFORMACIÓN

La asignatura se relaciona con los ODS 4 y 9:

Subobjetivo 4.4: Aumentar considerablemente el número de jóvenes y adultos que tienen las competencias profesionales y técnicas necesarias para acceder al empleo y al emprendimiento.

Subobjetivo 9.1: Desarrollar infraestructuras fiables, sostenibles, resilientes y de calidad.