



UNIVERSIDAD
POLITÉCNICA
DE MADRID

PROCESO DE
COORDINACIÓN DE LAS
ENSEÑANZAS PR/CL/001



E.T.S. de Ingeniería y Sistemas
de Telecomunicación

ANX-PR/CL/001-01

GUÍA DE APRENDIZAJE

ASIGNATURA

595000534 - Ciberseguridad Y Protección De Datos

PLAN DE ESTUDIOS

59ID - Grado En Ingeniería Y Sistemas De Datos

CURSO ACADÉMICO Y SEMESTRE

2023/24 - Primer semestre

Índice

Guía de Aprendizaje

| | |
|--|----|
| 1. Datos descriptivos..... | 1 |
| 2. Profesorado..... | 1 |
| 3. Conocimientos previos recomendados..... | 2 |
| 4. Competencias y resultados de aprendizaje..... | 2 |
| 5. Descripción de la asignatura y temario..... | 4 |
| 6. Cronograma..... | 6 |
| 7. Actividades y criterios de evaluación..... | 8 |
| 8. Recursos didácticos..... | 11 |

1. Datos descriptivos

1.1. Datos de la asignatura

| | |
|--|--|
| Nombre de la asignatura | 595000534 - Ciberseguridad y Protección de Datos |
| No de créditos | 6 ECTS |
| Carácter | Obligatoria |
| Curso | Cuarto curso |
| Semestre | Séptimo semestre |
| Período de impartición | Septiembre-Enero |
| Idioma de impartición | Castellano |
| Titulación | 59ID - Grado en Ingeniería y Sistemas de Datos |
| Centro responsable de la titulación | 59 - Escuela Técnica Superior De Ingeniería Y Sistemas De Telecomunicación |
| Curso académico | 2023-24 |

2. Profesorado

2.1. Profesorado implicado en la docencia

| Nombre | Despacho | Correo electrónico | Horario de tutorías * |
|--|-----------------|---------------------------|---------------------------------|
| Ivan Pau De La Cruz (Coordinador/a) | | ivan.pau@upm.es | - - |

* Las horas de tutoría son orientativas y pueden sufrir modificaciones. Se deberá confirmar los horarios de tutorías con el profesorado.

2.3. Profesorado externo

| Nombre | Correo electrónico | Centro de procedencia |
|-------------------|--------------------|-----------------------|
| Mario Vega Barbas | mario.vega@upm.es | Despacho A4404 |

3. Conocimientos previos recomendados

3.1. Asignaturas previas que se recomienda haber cursado

- Redes Y Servicios De Comunicaciones
- Computación En La Nube
- Programación Para Big Data

3.2. Otros conocimientos previos recomendados para cursar la asignatura

El plan de estudios Grado en Ingeniería y Sistemas de Datos no tiene definidos otros conocimientos previos para esta asignatura.

4. Competencias y resultados de aprendizaje

4.1. 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

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

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

CB04 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto

especializado como no especializado

CB05 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía

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.

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.

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.

CG01 - Tener capacidad de trabajar en entornos internacionales y multidisciplinares, haciendo uso de la lengua inglesa en forma oral y escrita.

CG03 - Ser capaz de explicar de forma oral o escrita las soluciones planteadas para la resolución de un problema.

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

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.

4.2. Resultados del aprendizaje

RA105 - Diseñar y aplicar las técnicas de protección de las infraestructuras de datos.

RA104 - Comprender las amenazas a la seguridad de las infraestructuras de datos y las metodologías de análisis de riesgos.

RA106 - Conocer la legislación en materia de protección de datos.

5. Descripción de la asignatura y temario

5.1. Descripción de la asignatura

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

5.2. Temario de la asignatura

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 provenientes de usuarios
 - 2.2. Amenazas tecnológicas
3. Protección de Sistemas, Comunicaciones y Datos
 - 3.1. Criptografía e Infraestructuras de Clave Pública
 - 3.2. Tecnologías de control de acceso a sistemas y redes
 - 3.3. Tecnologías de protección de datos y las comunicaciones
 - 3.4. Seguridad de los datos: securización de bases de datos
4. Ingeniería de privacidad
 - 4.1. Análisis de amenazas a la privacidad
 - 4.2. Privacidad desde el diseño y tecnologías de protección a la privacidad
 - 4.3. Anonimato de conjuntos de datos

6. Cronograma

6.1. Cronograma de la asignatura *

| Sem | Actividad en aula | Actividad en laboratorio | Tele-enseñanza | Actividades de evaluación |
|-----|--|---|----------------|---|
| 1 | Tema 1 Duración: 04:00 LM: Actividad del tipo Lección Magistral | | | |
| 2 | Tema 1 Duración: 03:00 LM: Actividad del tipo Lección Magistral Tema 2 Duración: 01:00 LM: Actividad del tipo Lección Magistral | | | |
| 3 | Tema 2 Duración: 04:00 LM: Actividad del tipo Lección Magistral | | | |
| 4 | Tema 2 Duración: 02:00 LM: Actividad del tipo Lección Magistral | Actividad Amenazas Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio | | |
| 5 | Tema 3 Duración: 03:30 LM: Actividad del tipo Lección Magistral | | | Evaluación actividad amenazas ET: Técnica del tipo Prueba Telemática Evaluación continua Presencial Duración: 00:30 |
| 6 | Tema 3 Duración: 04:00 LM: Actividad del tipo Lección Magistral | | | |
| 7 | Tema 3 Duración: 02:00 LM: Actividad del tipo Lección Magistral | Actividad criptografía Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio | | |
| 8 | Tema 3 Duración: 02:00 LM: Actividad del tipo Lección Magistral | Actividad criptografía Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio | | |
| 9 | Tema 3 Duración: 03:30 LM: Actividad del tipo Lección Magistral | | | Evaluación actividad criptografía ET: Técnica del tipo Prueba Telemática Evaluación continua Presencial Duración: 00:30 |
| 10 | Tema 3 Duración: 02:00 LM: Actividad del tipo Lección Magistral | Actividad Protección de Sistemas Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio | | Examen Primer Bloque de la Asignatura EX: Técnica del tipo Examen Escrito Evaluación continua Presencial Duración: 02:00 |

| | | | | |
|----|--|---|--|---|
| 11 | Tema 4 Duración: 02:00 LM: Actividad del tipo Lección Magistral | Actividad Protección de Sistemas Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio | | |
| 12 | Tema 4 Duración: 03:30 LM: Actividad del tipo Lección Magistral | | | Evaluación actividad Protección de Sistemas ET: Técnica del tipo Prueba Telemática Evaluación continua Presencial Duración: 00:30 |
| 13 | Tema 4 Duración: 02:00 LM: Actividad del tipo Lección Magistral | Actividad Ingeniería de Privacidad Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio | | |
| 14 | Tema 4 Duración: 02:00 LM: Actividad del tipo Lección Magistral | Actividad Ingeniería de Privacidad Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio | | |
| 15 | | | | |
| 16 | | | | |
| 17 | | | | Evaluación actividad de ingeniería de privacidad ET: Técnica del tipo Prueba Telemática Evaluación continua y sólo prueba final Presencial Duración: 00:30 Examen Segundo Bloque de la Asignatura EX: Técnica del tipo Examen Escrito Evaluación continua y sólo prueba final Presencial Duración: 02:00 Examen Global EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Presencial Duración: 02:00 |

Para el cálculo de los valores totales, se estima que por cada crédito ECTS el alumno dedicará dependiendo del plan de estudios, entre 26 y 27 horas de trabajo presencial y no presencial.

* El cronograma sigue una planificación teórica de la asignatura y puede sufrir modificaciones durante el curso derivadas de la situación creada por la COVID-19.

7. Actividades y criterios de evaluación

7.1. Actividades de evaluación de la asignatura

7.1.1. Evaluación (progresiva)

| Sem. | Descripción | Modalidad | Tipo | Duración | Peso en la nota | Nota mínima | Competencias evaluadas |
|------|--|--|------------|----------|-----------------|-------------|--|
| 5 | Evaluación actividad amenazas | ET: Técnica del tipo Prueba Telemática | Presencial | 00:30 | 5% | 3.5 / 10 | CB05 CG03 CG05 CB01 CB02 CB03 CG04 CG01 |
| 9 | Evaluación actividad criptografía | ET: Técnica del tipo Prueba Telemática | Presencial | 00:30 | 10% | 3.5 / 10 | CG04 CB05 CG03 CG05 CB01 CB02 CB03 |
| 10 | Examen Primer Bloque de la Asignatura | EX: Técnica del tipo Examen Escrito | Presencial | 02:00 | 35% | 3.5 / 10 | |
| 12 | Evaluación actividad Protección de Sistemas | ET: Técnica del tipo Prueba Telemática | Presencial | 00:30 | 10% | 3.5 / 10 | CE04 CE21 CG04 CG01 CB05 CG03 CG05 CE11 CB01 CB02 CB03 |
| 17 | Evaluación actividad de ingeniería de privacidad | ET: Técnica del tipo Prueba Telemática | Presencial | 00:30 | 10% | 3.5 / 10 | CG04 CE11 CB01 CB02 CB03 CE21 CB04 |

| | | | | | | | |
|----|--|-------------------------------------|------------|-------|-----|----------|--|
| 17 | Examen Segundo Bloque de la Asignatura | EX: Técnica del tipo Examen Escrito | Presencial | 02:00 | 30% | 3.5 / 10 | CE04 CE05 CB04 CG01 CB05 CG03 CB01 |
|----|--|-------------------------------------|------------|-------|-----|----------|--|

7.1.2. Prueba evaluación global

| Sem | Descripción | Modalidad | Tipo | Duración | Peso en la nota | Nota mínima | Competencias evaluadas |
|-----|--|--|------------|----------|-----------------|-------------|--|
| 17 | Evaluación actividad de ingeniería de privacidad | ET: Técnica del tipo Prueba Telemática | Presencial | 00:30 | 10% | 3.5 / 10 | CG04 CE11 CB01 CB02 CB03 CE21 CB04 |
| 17 | Examen Segundo Bloque de la Asignatura | EX: Técnica del tipo Examen Escrito | Presencial | 02:00 | 30% | 3.5 / 10 | CE04 CE05 CB04 CG01 CB05 CG03 CB01 |
| 17 | Examen Global | EX: Técnica del tipo Examen Escrito | Presencial | 02:00 | 60% | 5 / 10 | CE04 CE05 CB05 CG03 CB01 CB02 CB03 |

7.1.3. Evaluación convocatoria extraordinaria

| Descripción | Modalidad | Tipo | Duración | Peso en la nota | Nota mínima | Competencias evaluadas |
|-----------------------------|-------------------------------------|------------|----------|-----------------|-------------|--|
| Examen Final Extraordinario | EX: Técnica del tipo Examen Escrito | Presencial | 03:30 | 100% | 5 / 10 | CE04 CE21 CE05 CB04 CG04 CG01 CB05 CG03 CG05 |

La evaluación extraordinaria se basará en un examen final con la misma estructura que el examen final de la evaluación ordinaria. Se compondrá de las evaluaciones de los seis bloques definidos, existiendo las mismas restricciones que en el periodo ordinario.

8. Recursos didácticos

8.1. Recursos didácticos de la asignatura

| Nombre | Tipo | Observaciones |
|---------------------------------|--------------|---------------|
| Espacio Moodle de la Asignatura | Recursos web | |