



UNIVERSIDAD
POLITÉCNICA
DE MADRID

PROCESO DE
COORDINACIÓN DE LAS
ENSEÑANZAS PR/CL/001



E.T.S. de Ingenieros de
Telecomunicacion

ANX-PR/CL/001-01

GUÍA DE APRENDIZAJE

ASIGNATURA

93000824 - Ciberseguridad Y Privacidad: Gestión Y Operación

PLAN DE ESTUDIOS

09AQ - Master Universitario En Ingenieria De Telecomunicacion

CURSO ACADÉMICO Y SEMESTRE

2022/23 - Segundo 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.....	3
6. Cronograma.....	6
7. Actividades y criterios de evaluación.....	8
8. Recursos didácticos.....	11
9. Otra información.....	11

1. Datos descriptivos

1.1. Datos de la asignatura

Nombre de la asignatura	93000824 - Ciberseguridad y Privacidad: Gestión y Operación
No de créditos	6 ECTS
Carácter	Optativa
Curso	Segundo curso
Semestre	Cuarto semestre
Período de impartición	Febrero-Junio
Idioma de impartición	Castellano
Titulación	09AQ - Master Universitario en Ingeniería de Telecomunicacion
Centro responsable de la titulación	09 - Escuela Tecnica Superior De Ingenieros De Telecomunicacion
Curso académico	2022-23

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Enrique Barra Arias	B-323	enrique.barra@upm.es	X - 15:00 - 16:00
Victor Abraham Villagra Gonzalez (Coordinador/a)	B-217	victor.villagra@upm.es	X - 14:00 - 15:00
Jose Maria Del Alamo Ramiro	C-218	jm.delalamo@upm.es	X - 11:00 - 13:00

Xavier Andres Larriva Novo	B-423	xavier.larriva.novo@upm.es	X - 14:00 - 15:00
----------------------------	-------	----------------------------	-------------------

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

3. Conocimientos previos recomendados

3.1. Asignaturas previas que se recomienda haber cursado

El plan de estudios Master Universitario en Ingeniería de Telecomunicación no tiene definidas asignaturas previas recomendadas para esta asignatura.

3.2. Otros conocimientos previos recomendados para cursar la asignatura

- Servicios de Seguridad en Redes, Servicios y Sistemas de Telecomunicación
- Tecnologías de Ciberseguridad

4. Competencias y resultados de aprendizaje

4.1. Competencias

CE6 - Capacidad para modelar, diseñar, implantar, gestionar, operar, administrar y mantener redes, servicios y contenidos.

CE7 - Capacidad para realizar la planificación, toma de decisiones y empaquetamiento de redes, servicios y aplicaciones considerando la calidad de servicio, los costes directos y de operación, el plan de implantación, supervisión, los procedimientos de seguridad, el escalado y el mantenimiento, así como gestionar y asegurar la calidad en el proceso de desarrollo.

4.2. Resultados del aprendizaje

RA205 - Conocer y Diseñar un Centro de Gestión de Ciberincidentes

RA202 - Conocer y comprender los riesgos derivados del procesamiento incorrecto de datos personales

RA200 - Diseñar y desarrollar políticas de seguridad

RA201 - Conocer y aplicar las principales técnicas de ingeniería de privacidad de la información

RA18 - El alumno conoce las arquitecturas correspondientes a los paradigmas de afianzamiento de la seguridad en las redes, aplicaciones y contenidos.

RA199 - Conocer los modelos y estándares de gestión de la seguridad de la información

RA203 - Conocer y comprender la legislación y normativa de aplicación para protección de datos de carácter personal

RA204 - Conocer, comprender y saber aplicar algunos métodos, técnicas y herramientas para el desarrollo de sistemas respetuosos con la privacidad

5. Descripción de la asignatura y temario

5.1. Descripción de la asignatura

Los objetivos de esta asignatura se articulan en tres grandes temas:

- Gestión y Operación de la Seguridad en Corporaciones
- Ingeniería de Privacidad.
- Organización y Gobierno de la Seguridad en Corporaciones

El primer tema trata sobre la problemática de la gestión y monitorización de incidentes de ciberseguridad en una organización, tratando los servicios necesarios a implantar en un Centro de Operaciones de Ciberseguridad (SOC), y los modelos de gestión existentes para estos centros.

El segundo tema trata sobre la ingeniería de la privacidad, en el que se pretende que el alumno conozca y comprenda los riesgos derivados del procesamiento incorrecto de datos personales, la legislación y normativa de aplicación para protección de datos de carácter personal y sepa aplicar algunos métodos, técnicas y herramientas

para el desarrollo de sistemas respetuosos con la privacidad

El tercer tema tiene como objetivo que el alumno se adentre en la implantación de una política de seguridad en una organización, siendo capaz de realizar una planificación y diseño de la misma, a nivel de estrategia corporativa, y su análisis de riesgos. Se verán las distintas aproximaciones al análisis y gestión de riesgos, con casos de estudio que permitan el diseño de distintos análisis de riesgos de determinadas organizaciones. Se capacitará al alumno para conocer los conceptos, estándares, normativa, regulación y buenas prácticas de uso más extendido en la gestión de la seguridad de la información: ISO 27001, Esquema Nacional de Seguridad (ENS), etc.

La asignatura incluirá trabajos personales de los alumnos de casos de estudio de situaciones muy cercanas a casos reales en dichos temas.

5.2. Temario de la asignatura

1. Gestión y Operación de la Ciberseguridad
 - 1.1. Diseño de un Centro de Operación de Ciberseguridad
 - 1.2. Servicios de un Centro de Operación de Ciberseguridad
2. Ingeniería de la Privacidad
 - 2.1. Introducción a la Privacidad y Conceptos Básicos
 - 2.2. Perspectiva Social e Individual de la Ingeniería de la Privacidad
 - 2.3. Legislación para Protección de Datos Personales
 - 2.4. Evaluación y Gestión de Riesgos: evaluación del impacto para la privacidad
 - 2.5. Técnicas y Herramientas Básicas de Ingeniería de la Privacidad
3. Dirección y Gobierno de la Ciberseguridad
 - 3.1. Diseño de Estrategias Corporativas de Ciberseguridad
 - 3.2. Gestión de Riesgos.
 - 3.3. Sistemas de Gestión de la Seguridad de la Información

3.4. Gestión de la Continuidad del Negocio

6. Cronograma

6.1. Cronograma de la asignatura *

Sem	Actividad en aula	Actividad en laboratorio	Tele-enseñanza	Actividades de evaluación
1	Introducción a la Asignatura Duración: 01:00 LM: Actividad del tipo Lección Magistral Tema 1: Gestión y Operación de la Ciberseguridad Duración: 03:00 LM: Actividad del tipo Lección Magistral			
2	Tema 1: Gestión y Operación de la Ciberseguridad Duración: 04:00 LM: Actividad del tipo Lección Magistral			
3	Tema 1: Gestión y Operación de la Ciberseguridad Duración: 04:00 LM: Actividad del tipo Lección Magistral			
4	Tema 1: Gestión y Operación de la Ciberseguridad Duración: 02:00 LM: Actividad del tipo Lección Magistral	Prácticas de Laboratorio Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
5				Presentación de Trabajos TG: Técnica del tipo Trabajo en Grupo Evaluación continua Presencial Duración: 02:00 Examen Final EX: Técnica del tipo Examen Escrito Evaluación continua Presencial Duración: 02:00
6	Tema 3: Ingeniería de la Privacidad Duración: 04:00 LM: Actividad del tipo Lección Magistral			
7	Tema 3: Ingeniería de la Privacidad Duración: 04:00 LM: Actividad del tipo Lección Magistral			
8	Tema 3: Ingeniería de la Privacidad Duración: 04:00 LM: Actividad del tipo Lección Magistral			
9	Tema 3: Ingeniería de la Privacidad Duración: 02:00 LM: Actividad del tipo Lección Magistral	Prácticas de Laboratorio Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		

10				Presentación de Trabajos TG: Técnica del tipo Trabajo en Grupo Evaluación continua Presencial Duración: 02:00 Examen Final EX: Técnica del tipo Examen Escrito Evaluación continua Presencial Duración: 02:00
11	Tema 3: Dirección y Gobierno de la Coberseguridad Duración: 04:00 LM: Actividad del tipo Lección Magistral			
12	Tema 3: Dirección y Gobierno de la Coberseguridad Duración: 04:00 LM: Actividad del tipo Lección Magistral			
13	Tema 3: Dirección y Gobierno de la Coberseguridad Duración: 04:00 LM: Actividad del tipo Lección Magistral			
14	Tema 3: Dirección y Gobierno de la Coberseguridad Duración: 02:00 LM: Actividad del tipo Lección Magistral	Prácticas de Laboratorio Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
15				Presentación de Trabajos TG: Técnica del tipo Trabajo en Grupo Evaluación continua Presencial Duración: 02:00 Examen Final EX: Técnica del tipo Examen Escrito Evaluación continua Presencial Duración: 02:00
16				
17				Examen Final EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Presencial Duración: 02:00 Presentacion de Trabajos TG: Técnica del tipo Trabajo en Grupo Evaluación sólo prueba final Presencial Duración: 04:00

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	Presentación de Trabajos	TG: Técnica del tipo Trabajo en Grupo	Presencial	02:00	13%	4 / 10	CE6 CE7
5	Examen Final	EX: Técnica del tipo Examen Escrito	Presencial	02:00	20%	4 / 10	CE6 CE7
10	Presentación de Trabajos	TG: Técnica del tipo Trabajo en Grupo	Presencial	02:00	13%	4 / 10	CE6 CE7
10	Examen Final	EX: Técnica del tipo Examen Escrito	Presencial	02:00	20%	4 / 10	CE6 CE7
15	Presentación de Trabajos	TG: Técnica del tipo Trabajo en Grupo	Presencial	02:00	14%	4 / 10	CE6 CE7
15	Examen Final	EX: Técnica del tipo Examen Escrito	Presencial	02:00	20%	4 / 10	CE6 CE7

7.1.2. Prueba evaluación global

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
17	Examen Final	EX: Técnica del tipo Examen Escrito	Presencial	02:00	60%	4 / 10	CE6 CE7

17	Presentacion de Trabajos	TG: Técnica del tipo Trabajo en Grupo	Presencial	04:00	40%	4 / 10	CE6 CE7
----	--------------------------	---------------------------------------	------------	-------	-----	--------	------------

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	02:00	60%	4 / 10	CE6 CE7
Presentacion de Trabajos	TI: Técnica del tipo Trabajo Individual	Presencial	04:00	40%	4 / 10	CE6 CE7

7.2. Criterios de evaluación

La evaluación comprobará si los estudiantes han adquirido las competencias de la asignatura. Por tanto, la evaluación mediante prueba final usará los mismos tipos de técnicas evaluativas que se usan en la evaluación continua (EX, ET, TG, etc.), y se realizarán en las fechas y horas de evaluación final aprobadas por la Junta de Escuela para el presente curso y semestre..

La evaluación principal se basa en evaluación progresiva consistente en:

Parte 1: Operación de Ciberseguridad

- Prácticas Operación de Ciberseguridad (13%)
- Examen Parcial P1: Operación en Ciberseguridad (20%)

Parte 2:: Ingeniería de Privacidad

- Prácticas Ingeniería de Privacidad (13%)
- Examen parcial P2: Ingeniería de Privacidad (20%)

Parte 3:: Dirección y Organización de la Ciberseguridad

- Prácticas Dirección y Organización de la Ciberseguridad (13%)
- Examen Parcial P3: Dirección y Organización de la Ciberseguridad (20%) (Coincidente con la evaluación global)

Las pruebas de prácticas de las tres partes son bloque liberatorios que permitirán liberarlos en la convocatoria extraordinaria del mismo curso. Las materia de la parte 1 y 2 serán evaluadas mediante exámenes parciales P1 y P2. En caso de obtener menos de 4 puntos o desear subir nota, el alumno deberá presentarse a la recuperación en la evaluación global, renunciando a la nota del primer parcial.

La evaluación global constará de:

- Examen Parcial P1: Operación en Ciberseguridad (20%)
- Examen parcial P2: Ingeniería de Privacidad (20%)
- Examen Parcial P3: Dirección y Organización de la Ciberseguridad (20%)

La evaluación en la convocatoria extraordinaria se realizará exclusivamente a través del sistema de prueba final (60%) y entrega de prácticas (40%)

En todas las partes de la asignatura se exige una nota mínima de 4 sobre 10.

8. Recursos didácticos

8.1. Recursos didácticos de la asignatura

Nombre	Tipo	Observaciones
Moodle	Recursos web	Servidor Moodle de la Asignatura
Equipamiento	Equipamiento	Aula, Laboratorio, Sala de Trabajo en Grupo
Referencias	Bibliografía	Bibliografía

9. Otra información

9.1. Otra información sobre la asignatura

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.