



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

**93001011 - Gestión De Riesgos Y Operaciones En Ciberseguridad**

### PLAN DE ESTUDIOS

09AW - Master Universitario En Ciberseguridad

### 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.....	3
5. Descripción de la asignatura y temario.....	4
6. Cronograma.....	6
7. Actividades y criterios de evaluación.....	8
8. Recursos didácticos.....	11
9. Otra información.....	12

## 1. Datos descriptivos

---

### 1.1. Datos de la asignatura

<b>Nombre de la asignatura</b>	93001011 - Gestión de Riesgos y Operaciones en Ciberseguridad
<b>No de créditos</b>	6 ECTS
<b>Carácter</b>	Obligatoria
<b>Curso</b>	Primer curso
<b>Semestre</b>	Segundo semestre
<b>Período de impartición</b>	Febrero-Junio
<b>Idioma de impartición</b>	Castellano
<b>Titulación</b>	09AW - Master Universitario en Ciberseguridad
<b>Centro responsable de la titulación</b>	09 - Escuela Tecnica Superior De Ingenieros De Telecomunicacion
<b>Curso académico</b>	2022-23

## 2. Profesorado

---

### 2.1. Profesorado implicado en la docencia

<b>Nombre</b>	<b>Despacho</b>	<b>Correo electrónico</b>	<b>Horario de tutorías *</b>
Xavier Andres Larriva Novo	B-423	xavier.larriva.novo@upm.es	Sin horario.
Victor Abraham Villagra Gonzalez (Coordinador/a)	B-217	victor.villagra@upm.es	X - 14:00 - 15:00
Joaquin Luciano Salvachua Rodriguez	C-220	joaquin.salvachua@upm.es	X - 14:00 - 15:00

Gabriel Huecas Fernandez-Toribio	C-219	gabriel.huecas@upm.es	X - 14:00 - 15:00
Enrique Barra Arias	B-323	enrique.barra@upm.es	X - 15:00 - 16:00

\* 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

- Ciberseguridad: Contexto Y Amenazas
- Protección De La Información
- Protección De Sistemas Y Servicios
- Servicios De Control De Acceso
- Servicios De Seguridad En Red
- Auditoría Técnica De Seguridad

#### 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

CB07 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio

CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo

CE03 - Capacidad para realizar un análisis y evaluación de los riesgos de una organización, con un enfoque de gestión de riesgos enmarcado en un Sistema de Gestión de Seguridad de la Información

CE07 - - Capacidad para diseñar un centro de gestión y operación de ciberseguridad, con la combinación adecuada de servicios preventivos, de detección y de respuesta a incidentes

CG01 - Proporcionar al alumno los conceptos y tecnologías utilizadas en la implantación de la Ciberseguridad en una organización, dotándole de la capacidad para definir estrategias, políticas y normas para la seguridad corporativa

CG05 - Dotar al alumno de la capacidad de estar al día de los desarrollos más recientes que tengan que ver con la ciberseguridad, así como de contribuir con ideas contrastadas al desarrollo técnico de lo aprendido y a nuevas áreas en las que sea de aplicación la ciberseguridad, con posibilidad de participar en actividades directivas de nivel medio de gerencia

CT10 - Resolución de problemas

CT11 - Razonamiento crítico

CT12 - Aprendizaje autónomo, adaptación a nuevas situaciones y motivación por el desarrollo profesional permanente

## 4.2. Resultados del aprendizaje

RA17 - Conocer los componentes de un riesgo, y saber aplicar las metodologías para la realización de un análisis de riesgos

RA18 - Conocer los distintos componentes organizativos y tecnológicos de un Centro de Gestión de Ciberseguridad, y ser capaz de realizar su diseño

## 5. Descripción de la asignatura y temario

---

### 5.1. Descripción de la asignatura

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

- Análisis y Gestión de Riesgos de Ciberseguridad
- Gestión y Operación de la Seguridad en Corporaciones

El primer tema tiene como objetivo que el alumno conozca la problemática asociada a 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.

El segundo 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,. En este tema se tratará de forma especial las tecnologías y modelos de Big Data y Machine Learning aplicados a la gestión de incidentes en ciberseguridad.

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. Analisis y Gestión de Riesgos
2. Gestión y Operación de la Ciberseguridad
  - 2.1. Diseño de un Centro de Operación de Ciberseguridad
  - 2.2. Servicios de un Centro de Operación de Ciberseguridad
  - 2.3. Técnicas de Machine Learning y Big Data en Ciberseguridad

## 6. Cronograma

### 6.1. Cronograma de la asignatura \*

Sem	Actividad en aula	Actividad en laboratorio	Tele-enseñanza	Actividades de evaluación
1				
2				
3				
4	<p><b>Clases Teóricas de Análisis y Gestión de Riesgos</b> Duración: 04:00 LM: Actividad del tipo Lección Magistral</p> <p><b>Clases Teóricas de Gestión de Operaciones en Ciberseguridad</b> Duración: 04:00 LM: Actividad del tipo Lección Magistral</p>			
5	<p><b>Clases Teóricas de Análisis y Gestión de Riesgos</b> Duración: 04:00 LM: Actividad del tipo Lección Magistral</p> <p><b>Clases Teóricas de Gestión de Operaciones en Ciberseguridad</b> Duración: 04:00 LM: Actividad del tipo Lección Magistral</p>			
6	<p><b>Clases Teóricas de Análisis y Gestión de Riesgos</b> Duración: 04:00 LM: Actividad del tipo Lección Magistral</p> <p><b>Clases Teóricas de Gestión de Operaciones en Ciberseguridad</b> Duración: 04:00 LM: Actividad del tipo Lección Magistral</p>			
7	<p><b>Clases Teóricas de Análisis y Gestión de Riesgos</b> Duración: 04:00 LM: Actividad del tipo Lección Magistral</p> <p><b>Clases Teóricas de Gestión de Operaciones en Ciberseguridad</b> Duración: 04:00 LM: Actividad del tipo Lección Magistral</p>			
8	<p><b>Clases Teóricas de Análisis y Gestión de Riesgos</b> Duración: 04:00 LM: Actividad del tipo Lección Magistral</p> <p><b>Clases Teóricas de Gestión de Operaciones en Ciberseguridad</b> Duración: 04:00 LM: Actividad del tipo Lección Magistral</p>			



9	<b>Clases Teóricas de Análisis y Gestión de Riesgos</b> Duración: 02:00 LM: Actividad del tipo Lección Magistral	<b>Practica de Laboratorio de Configuración de SIEM</b> Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
10	<b>Clases Teóricas de técnicas ML aplicadas a la Operación de Ciberseguridad</b> Duración: 04:00 LM: Actividad del tipo Lección Magistral	<b>Practica de Laboratorio de Configuración de SIEM</b> Duración: 04:00 PL: Actividad del tipo Prácticas de Laboratorio		
11		<b>Practica de Laboratorio de Configuración de SIEM</b> Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio  <b>Practica de Laboratorio de Aplicación de Técnicas ML a la Operación de Ciberseguridad</b> Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
12		<b>Practica de Laboratorio de Aplicación de Técnicas ML a la Operación de Ciberseguridad</b> Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		<b>Evaluación de Trabajos de Gestión de Operaciones</b> TG: Técnica del tipo Trabajo en Grupo Evaluación continua y sólo prueba final Presencial Duración: 01:00  <b>Examen Final</b> EX: Técnica del tipo Examen Escrito Evaluación continua y sólo prueba final Presencial Duración: 02:00  <b>Evaluación de Trabajos de Análisis de Riesgos</b> TG: Técnica del tipo Trabajo en Grupo Evaluación continua y sólo prueba final No presencial Duración: 02:00  <b>Evaluación de Trabajos de Machine Learning</b> TG: Técnica del tipo Trabajo en Grupo Evaluación continua y sólo prueba final No presencial Duración: 02:00
13				
14				
15				
16				
17				

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
12	Evaluación de Trabajos de Gestión de Operaciones	TG: Técnica del tipo Trabajo en Grupo	Presencial	01:00	25%	4 / 10	CG01 CB07 CT10 CT11 CT12 CG05 CB10 CE07
12	Examen Final	EX: Técnica del tipo Examen Escrito	Presencial	02:00	50%	4 / 10	CG01 CB07 CE03 CE07
12	Evaluación de Trabajos de Análisis de Riesgos	TG: Técnica del tipo Trabajo en Grupo	No Presencial	02:00	20%	4 / 10	CG01 CB07 CT10 CT11 CT12 CG05 CE03 CB10
12	Evaluación de Trabajos de Machine Learning	TG: Técnica del tipo Trabajo en Grupo	No Presencial	02:00	5%	4 / 10	CG01 CB07 CT10 CT11 CT12 CG05 CB10 CE07

#### 7.1.2. Prueba evaluación global

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
12	Evaluación de Trabajos de Gestión de Operaciones	TG: Técnica del tipo Trabajo en Grupo	Presencial	01:00	25%	4 / 10	CG01 CB07 CT10 CT11 CT12 CG05 CB10

							CE07
12	Examen Final	EX: Técnica del tipo Examen Escrito	Presencial	02:00	50%	4 / 10	CG01 CB07 CE03 CE07
12	Evaluación de Trabajos de Análisis de Riesgos	TG: Técnica del tipo Trabajo en Grupo	No Presencial	02:00	20%	4 / 10	CG01 CB07 CT10 CT11 CT12 CG05 CE03 CB10
12	Evaluación de Trabajos de Machine Learning	TG: Técnica del tipo Trabajo en Grupo	No Presencial	02:00	5%	4 / 10	CG01 CB07 CT10 CT11 CT12 CG05 CB10 CE07

### 7.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
Examen Final	EX: Técnica del tipo Examen Escrito	Presencial	02:00	50%	4 / 10	CG01 CB07 CE03 CE07
Evaluación de Trabajos de Gestión de Operaciones	TI: Técnica del tipo Trabajo Individual	Presencial	02:00	25%	4 / 10	CB07 CT10 CG01 CT11 CT12 CG05 CB10 CE07
Evaluación de Trabajos de Análisis de Riesgos	TI: Técnica del tipo Trabajo Individual	Presencial	02:00	20%	4 / 10	CG01 CB07 CT10 CT11 CT12 CG05 CE03

						CB10
Evaluación de Trabajos de Machine Learning	TI: Técnica del tipo Trabajo Individual	Presencial	02:00	5%	4 / 10	CG01 CB07 CT10 CT11 CT12 CG05 CB10 CE07

## 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 (20%)
- Prácticas Machine Learning (5%)
- Examen Operación de Ciberseguridad (25%) (coincidente con la evaluación global)

### Parte 2:

- Trabajos Análisis y Gestión de Riesgos (20%)

- Examen Análisis y Gestión de Riesgo (25%) (coincidente con la evaluación global)

Todas las pruebas son bloque liberatorios que permitirán liberarlos en la convocatoria extraordinaria del mismo curso. Es necesario obtener 4 puntos en cada una de las pruebas para poder liberarlo.

La evaluación global constará de:

- Examen Operación de Ciberseguridad (25%)
- Examen Análisis y Gestión de Riesgo (25%)
- Entregas de prácticas de la asignatura (50%)

La evaluación en la convocatoria extraordinaria se realizará exclusivamente a través del sistema de examen final (50%) y entrega de prácticas (50%)

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.