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

2023/24 - Segundo semestre

Índice

Guía de Aprendizaje

1. Datos descriptivos

1.1. Datos de la asignatura

Nombre de la asignatura	93001011 - Gestión de Riesgos y Operaciones en Ciberseguridad
No de créditos	6 ECTS
Carácter	Obligatoria
Curso	Primer curso
Semestre	Segundo semestre
Período de impartición	Febrero-Junio
Idioma de impartición	Castellano
Titulación	09AW - Master Universitario en Ciberseguridad
Centro responsable de la titulación	09 - Escuela Tecnica Superior De Ingenieros De Telecomunicacion
Curso académico	2023-24

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
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
Andres Isaac Marin Lopez	B-211	andres.mlopez@upm.es	Sin horario. Concertar cita por correo electrónico

* 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 riegos. Se verán las distinas 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	**Clases Teóricas de Análisis y Gestión de Riesgos** Duración: 04:00 LM: Actividad del tipo Lección Magistral **Clases Teóricas de Gestión de Operaciones en Ciberseguridad** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
5	**Clases Teóricas de Análisis y Gestión de Riesgos** Duración: 04:00 LM: Actividad del tipo Lección Magistral **Clases Teóricas de Gestión de Operaciones en Ciberseguridad** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
6	**Clases Teóricas de Análisis y Gestión de Riesgos** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Clases Teóricas de Gestión de Operaciones en Ciberseguridad** Duración: 04:00 LM: Actividad del tipo Lección Magistral	**Practica de Laboratorio de Analisis de Riesgos** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
7	**Clases Teóricas de Análisis y Gestión de Riesgos** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Clases Teóricas de Gestión de Operaciones en Ciberseguridad** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Practica de Laboratorio de Analisis de Riesgos** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio **Practica de Laboratorio de Configuracion de SIEM** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
8	**Clases Teóricas de Gestión de Operaciones en Ciberseguridad** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Practica de Laboratorio de Configuracion de SIEM** Duración: 04:00 PL: Actividad del tipo Prácticas de Laboratorio **Practica de Laboratorio de Analisis de Riesgos**		

		Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
9	**Clases Teóricas de Gestión de Operaciones en Ciberseguridad** Duración: 04:00 LM: Actividad del tipo Lección Magistral	**Practica de Laboratorio de Configuracion de SIEM** Duración: 04:00 PL: Actividad del tipo Prácticas de Laboratorio		
10	**Clases Teóricas de técnicas ML aplicadas a la Operación de Ciberseguridad** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Practica de Laboratorio de Aplicación de Técnicas ML a la Operación de Ciberseguridad** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio **Practica de Laboratorio de Configuracion de SIEM** Duración: 04:00 PL: Actividad del tipo Prácticas de Laboratorio		
11		**Practica de Laboratorio de Aplicación de Técnicas ML a la Operación de Ciberseguridad** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
12				**Evaluación de Trabajos de Gestión de Operaciones** TG: Técnica del tipo Trabajo en Grupo Evaluación continua y sólo prueba final No presencial Duración: 00:00 **Examen Final** EX: Técnica del tipo Examen Escrito Evaluación continua y sólo prueba final Presencial Duración: 02:00 **Evaluación de Trabajos de Análisis de Riesgos** TG: Técnica del tipo Trabajo en Grupo Evaluación continua y sólo prueba final No presencial Duración: 00:00 **Evaluación de Trabajos de Machine Learning** TG: Técnica del tipo Trabajo en Grupo Evaluación continua y sólo prueba final No presencial Duración: 00:00
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	No Presencial	00:00	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	00:00	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	00:00	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	No Presencial	00:00	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	00:00	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	00:00	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
Evaluacion de Trabajos de Gestion de Operaciones	TI: Técnica del tipo Trabajo Individual	Presencial	00:00	25%	4 / 10	CB07 CT10 CG01 CT11 CT12 CG05 CB10 CE07
Evaluacion de Trabajos de Analisis de Riesgos	TI: Técnica del tipo Trabajo Individual	Presencial	02:00	20%	4 / 10	CG01 CB07 CT10 CT11 CT12 CG05 CE03

						CB10
Evaluacion 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)

Las materias (examen y prácticas) de la parte 1 y 2 serán evaluadas en evaluación progresiva mediante un examen y entrega de prácticas y trabajos coincidente con la evaluación global .

Las pruebas de prácticas y exámenes de la cada partes son bloques liberatorios que permitirán liberarlos en la convocatoria extraordinaria del mismo curso. Los alumnos que quiera volver a presentarse de nuevo habiéndolos liberado deberá avisar con 14 días de antelación al coordinador de la asignatura.

La evaluación en la convocatoria extraordinaria se realizará exclusivamente a través del sistema de examen final (50%) y entrega de prácticas (50%) de las dos partes para los bloques no liberados previamente.

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

Cualquier evaluación o entrega realizada podrá requerir una evaluación oral complementaria por parte del profesor para validar que se ha realizado por el alumno sin ayuda de sistemas de IA.

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.