1. DATOS BÁSICOS

Asignatura	Gestión de riesgos tecnológicos
Titulación	Criminología
Escuela/ Facultad	Facultad de Ciencias Jurídicas, Educación y Humanidades
Curso	Cuarto
ECTS	6
Carácter	Obligatoria
Idioma/s	Castellano
Modalidad	Presencial/Online
Semestre	S7/S8
Curso académico	2025/2026
Docente coordinador	David Temprano de Miguel
Docente	David Temprano de Miguel; Aitor Romeo Echeverría

2. PRESENTACIÓN

La asignatura Gestión de Riesgos Tecnológicos es una asignatura optativa dentro del Grado de Criminología impartida durante el cuarto curso, con un valor de seis créditos ECTS, al igual que el resto de las materias optativas de la titulación.

Esta materia pretende aportar conocimientos para la comprensión de los conceptos de ciberseguridad, así como los distintos tipos de actividad delictiva que pueden desarrollarse en la red, junto con sus características, fines, objetivos, estructura, financiación, tipología y relaciones, y mecanismos legales, jurídicos, estatales y europeos en la dirección y gestión de los diversos servicios de ciberseguridad.

El alumno manejará también conceptos relacionados con la evolución de la tecnología aplicada al ámbito de la seguridad y de la criminalidad, así como a nuevos mecanismos de comunicación, propaganda, activismo social o terrorismo

3. COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

Conocimientos:

- CON01. Relacionar los elementos básicos procedentes de disciplinas íntimamente relacionadas con la Criminología, como la Psicología el Derecho Penal o la Sociología.
- CON03. Reconocer los principales sistemas de seguridad aplicables a la protección de instalaciones y personas.
- CON04. Reconocer la principal legislación aplicable a la seguridad privada y pública nacional.

Habilidades:

- HAB04. Integrar el marco normativo, doctrinal y jurisprudencial de las relaciones jurídicas públicas y privadas relacionadas con el fenómeno criminológico estudiado.
- HAB05. Utilizar las tecnologías de la información y de la comunicación para la búsqueda y análisis de datos, la investigación, la comunicación y el aprendizaje.

Competencias:

- CP04. Realizar planes de intervención eficaces que permitan solucionar problemáticas criminológicas concretas.
- CP06. *Trabajar en equipo para alcanzar la resolución de los problemas criminológicos y/o victimológicos planteados.*
- CP09. Manejar y utilizar con eficacia y soltura las nuevas tecnologías para acceder a archivos y datos criminológicos, fuentes de consulta, repositorios y bases de datos jurídicas.

Resultados de aprendizaje:

Conocimientos específicos de la materia:

- Describir correctamente la tipología de la ciberdelincuencia.
- Reconocer los conceptos básicos relacionados con la gestión del cibercrimen.
- Describir la legislación aplicable a la seguridad en la red y a la protección de datos y del comercio electrónico.

Habilidades específicas de la materia:

- Analizar la evolución del cibercrimen en la sociedad actual.
- Examinar las estrategias de control y enfrentamiento del cibercrimen.
- Planificar, desde un plano teórico, planes de contingencia ante ciberataques a estructuras críticas.

En la tabla inferior se muestra la relación entre las competencias que se desarrollan en la asignatura y los resultados de aprendizaje que se persiguen:

Competencias	Resultados de aprendizaje
CON01, CON04, HAB04, CP09	• Describir correctamente la tipología de la ciberdelincuencia.
CON03, CON04, HAB04,CP09	• Reconocer los conceptos básicos relacionados con la gestión del cibercrimen.
CON01, CON03, CON04, HAB04	• Describir la legislación aplicable a la seguridad en la red y a la protección de datos y del comercio electrónico.
CON01, HAB04, CP06, CP09	• Analizar la evolución del cibercrimen en la sociedad actual.
CON03, CON04, HAB05, CP04, CP06	• Examinar las estrategias de control y enfrentamiento del cibercrimen.
CON01, CON03, CON04, HAB04, CP04, CP06	• Planificar, desde un plano teórico, planes de contingencia ante ciberataques a estructuras críticas.

4. CONTENIDOS

- Seguridad de sistemas, redes e Internet.
- Protección de datos.
- Auditoría y análisis de riesgos de sistemas de información.
- Seguridad en el comercio electrónico.

5. METODOLOGÍAS DE ENSEÑANZA-APRENDIZAJE

A continuación, se indican los tipos de metodologías de enseñanza-aprendizaje que se aplicarán:

Clase magistral.
Aprendizaje cooperativo.
Aprendizaje basado en problemas.

6. ACTIVIDADES FORMATIVAS

A continuación, se identifican los tipos de actividades formativas que se realizarán y la dedicación en horas del estudiante a cada una de ellas:

Modalidad presencial:

Actividad formativa	Número de horas
Clases magistrales	10
Clases de aplicación práctica	20
Resolución de problemas	30
Elaboración de informes y escritos	15
Exposiciones orales de trabajos	5
Trabajo autónomo	60
Debates y coloquios	8
Pruebas de evaluación presenciales	2
	150

Modalidad virtual:

Actividad formativa	Número de horas
Clases magistrales	10
Clases virtuales síncronas	20

Resolución de problemas	30
Elaboración de informes y escritos	15
Exposiciones orales de trabajos síncronos	5
Estudio de contenidos y documentación complementaria (Trabajo Autónomo)	60
Foro virtual	8
Pruebas de evaluación virtuales	2
	150

7. EVALUACIÓN

A continuación, se relacionan los sistemas de evaluación, así como su peso sobre la calificación total de la asignatura:

Modalidad presencial:

Sistema de evaluación	Peso
Pruebas de evaluación presenciales	60%
Informes y escritos	25%
Caso/problema	15%

Modalidad virtual:

Sistema de evaluación	Peso
Pruebas de evaluación presenciales	60%
Informes y escritos	25%
Caso/problema	15%

En el Campus Virtual, cuando accedas a la asignatura, podrás consultar en detalle las actividades de evaluación que debes realizar, así como las fechas de entrega y los procedimientos de evaluación de cada una de ellas.

7.1. Convocatoria ordinaria

Para superar la asignatura en convocatoria ordinaria deberás obtener una calificación mayor o igual que 5,0 sobre 10,0 en la calificación final (media ponderada) de la asignatura.

En todo caso, será necesario que obtengas una calificación mayor o igual que 5,0 en la prueba final, para que la misma pueda hacer media con el resto de las actividades.

7.2. Convocatoria extraordinaria

Para superar la asignatura en convocatoria ordinaria deberás obtener una calificación mayor o igual que 5,0 sobre 10,0 en la calificación final (media ponderada) de la asignatura.

En todo caso, será necesario que obtengas una calificación mayor o igual que 5,0 en la prueba final, para que la misma pueda hacer media con el resto de actividades.

Se deben entregar las actividades no superadas en convocatoria ordinaria, tras haber recibido las correcciones correspondientes a las mismas por parte del docente, o bien aquellas que no fueron entregadas.

8. CRONOGRAMA

En este apartado se indica el cronograma con fechas de entrega de actividades evaluables de la asignatura:

Modalidad presencial:

Actividades evaluables	Fecha
Actividad 1	A concretar por el profesor
Actividad 2	A concretar por el profesor
Prueba de evaluación	A concretar por el profesor

Modalidad online:

Actividades evaluables	Fecha
Actividad 1	23 mazo 2026
Actividad 2	27 mayo 2026
Prueba de evaluación	A concretar

Este cronograma podrá sufrir modificaciones por razones logísticas de las actividades. Cualquier modificación será notificada al estudiante en tiempo y forma.

9. BIBLIOGRAFÍA

- Miró Llinares F. (2012), *El cibercrimen. Fenomenología y criminología de la delincuencia en el*
- *ciberespacio.* Ed: Marcial Pons.
- Bartlett, J. (2015) *The Dark Net*, Windmill Books, London.
- Brooks, C. J., Grow, C., Craig, P. y Short, D. (2018). *Cybersecurity Essentials*. Sybex.

- Crowell, W., Cole, E. (2011), *Physical and Logical security convergence*. Syngress.
- Davis, N. (2000), An information based revolution in military affairs. Ed: In Athena's camp:
- preparing for conflict in the Information Age. RAND Co: Santa Monica.
- NATO Cybersecurity Framework Manual.
- Tikk, E., y Kerttunen, M. (2020). *Routdlege Handbook of International Cybersecurity*. Routledge.

10. UNIDAD DE ORIENTACIÓN EDUCATIVA Y DIVERSIDAD

Desde la Unidad de Orientación Educativa y Diversidad (ODI) ofrecemos acompañamiento a nuestros estudiantes a lo largo de su vida universitaria para ayudarles a alcanzar sus logros académicos. Otros de los pilares de nuestra actuación son la inclusión del estudiante con necesidades específicas de apoyo educativo, la accesibilidad universal en los distintos campus de la universidad y la equiparación de oportunidades.

Desde esta Unidad se ofrece a los estudiantes:

1. Acompañamiento y seguimiento mediante la realización de asesorías y planes personalizados a estudiantes que necesitan mejorar su rendimiento académico.
2. En materia de atención a la diversidad, se realizan ajustes curriculares no significativos, es decir, a nivel de metodología y evaluación, en aquellos alumnos con necesidades específicas de apoyo educativo persiguiendo con ello una equidad de oportunidades para todos los estudiantes.
3. Ofrecemos a los estudiantes diferentes recursos formativos extracurriculares para desarrollar diversas competencias que les enriquecerán en su desarrollo personal y profesional.
4. Orientación vocacional mediante la dotación de herramientas y asesorías a estudiantes con dudas vocacionales o que creen que se han equivocado en la elección de la titulación.

Los estudiantes que necesiten apoyo educativo pueden escribirnos a:
orientacioneducativa@universidadeuropea.es

11. ENCUESTAS DE SATISFACCIÓN

¡Tu opinión importa!

La Universidad Europea te anima a participar en las encuestas de satisfacción para detectar puntos fuertes y áreas de mejora sobre el profesorado, la titulación y el proceso de enseñanza-aprendizaje.

Las encuestas estarán disponibles en el espacio de encuestas de tu campus virtual o a través de tu correo electrónico.

Tu valoración es necesaria para mejorar la calidad de la titulación.

Muchas gracias por tu participación.