1. DATOS BÁSICOS

Asignatura	M2. Delitos informáticos y ciberdelincuencia
Titulación	Máster Universitario en Derecho Penal Económico
Escuela/ Facultad	Ciencias Sociales y de la Comunicación
Curso	Primero
ECTS	6 ECTS
Carácter	Obligatorio
Idioma/s	Castellano
Modalidad	A distancia
Semestre	Primer semestre
Curso académico	2024/2025
Docente coordinador	Jesús Villamor Blanco

2. PRESENTACIÓN

El presente módulo pretende ser un acercamiento global y riguroso a los delitos socioeconómicos cometidos por medios informáticos, identificando las principales modalidades delictivas cometidos en el ciberespacio (tanto delitos previstos específicamente para su comisión en red, como delitos que, a pesar de no estar previstos para su comisión informática, tienen una alta incidencia en este campo, como son las falsedades documentales o el blanqueo de capitales), y los específicos criterios para la determinación de la autoría y participación en estos. Se realiza un acercamiento a las diferentes formas en las que se cometen los delitos mencionados y la prevención de los mismos.

Se realiza un acercamiento a los aspectos criminológicos de esta forma de delincuencia, con especial atención a los nexos de unión entre la ciberdelincuencia y la delincuencia organizada.

Finalmente, se estudiará la legislación y resoluciones internacionales sobre la ciberdelincuencia, y su ámbito de aplicación en España.

3. COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

Competencias básicas:

- CB3. Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.
- CB4. Que los estudiantes sepan comunicar sus conclusiones –y los conocimientos y razones últimas que las sustentan- a públicos especializados y no especializados de un modo claro y sin ambigüedades.

Competencias transversales:

- CT3. Competencia digital. Utilizar las tecnologías de la información y de la comunicación para la búsqueda y análisis de datos, la investigación, la comunicación y el aprendizaje.

- CT4. Liderazgo influyente. Influir en otros para guiarles y dirigirles hacía unos objetivos y metas concretos, tomando en consideración sus puntos de vista, especialmente en situaciones derivadas de entornos volátiles, inciertos, complejos y ambiguos (VUCA) del mundo actual.
- CT6. Análisis crítico. Integrar el análisis con el pensamiento crítico en un proceso de evaluación de distintas ideas o posibilidades y su potencial de error, basándose en evidencias y datos objetivos que lleven a una toma de decisiones eficaz y válida.

Competencias específicas:

- CE1. Analizar y desglosar cada uno de los delitos de naturaleza económica, así como las categorías e instituciones jurídico penales relacionadas con los mismos.
- CE3. Descomponer y ordenar los elementos esenciales, objetivos y subjetivos, de los tipos penales de contenido económico.
- CE7. Descubrir y combinar elementos de naturaleza jurídica distinta a la penal en los delitos de contenido económico.

Resultados de aprendizaje:

- RA1. Analizar la legislación vigente en el ámbito de los delitos informáticos.
- RA2. Identificar los elementos básicos de los delitos informáticos y su incidencia económica.
- RA3. Diferenciar cada uno de los tipos penales de delitos informáticos y de ciberdelincuencia.
- RA4. Argumentar la fenomenología y etiología de los delitos informáticos y de ciberdelincuencia.
- RA5. Explicar los diversos métodos utilizados por la ciberdelincuencia para realizar delitos de naturaleza económica.
- RA6. Diseñar sistemas de prevención de ciberdelitos.

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
CB3-CT6-CE1	**RA1.** Analizar la legislación vigente en el ámbito de los delitos informáticos.
CB4-CT3-CE3	**RA2.** Identificar los elementos básicos de los delitos informáticos y su incidencia económica.
CB4-CT4-CE1	**RA3.** Diferenciar cada uno de los tipos penales de delitos informáticos y de ciberdelincuencia.
CB3-CT3-CE7	**RA 4.** Argumentar la fenomenología y etiología de los delitos informáticos y de ciberdelincuencia.
CB3-CT6-CE3	**RA5.** Explicar los diversos métodos utilizados por la ciberdelincuencia para realizar delitos de naturaleza económica.
CB4-CT4-CE7	**RA6.** Diseñar sistemas de prevención de ciberdelitos.

4. CONTENIDOS

El Módulo de la materia está organizada en seis unidades de aprendizaje, las cuales, a su vez, están divididas en temas (cuatro o cinco temas dependiendo de las unidades):

Módulo 2.

Unidad 1.- Delitos socioeconómicos en red
Tema 1.- Delito de estafa informática
Tema 2.- Delito de blanqueo de capitales
Tema 3.- Delito de receptación de servicios de telecomunicaciones

Unidad 2.- Delitos socioeconómicos en red
Tema 1.- Delito de descubrimiento y revelación de secretos
Tema 2.- Delito de descubrimiento y revelación de secretos de empresa
Tema 3.- Delito de difusión de información engañosa sobre empresas

Unidad 3.- Delitos de daños, propiedad intelectual, y falsedad documental
Tema 1.- Delito de daños
Tema 2.- Delito de propiedad intelectual
Tema 3.- Delito de falsedad documental

Unidad 4.- Delitos de daños, propiedad intelectual, y falsedad documental
Tema 1.- El INCIBE
Tema 2.- Ransomwere
Tema 3.- Ciberespionaje y ciberacoso
Tema 4.- Suplantacion de identidad
Tema 5.- Incidentes malware
Tema 6.- Protocolos de compliance con relación a los ciberdelitos

Unidad 5.- Etiología y fenomenología criminal
Tema 1.- Cibercriminología
Tema 2.- Perfil del delincuente y de la víctima
Tema 3.- Ciberdelincuencia y delincuencia organizada
Tema 4.- Ciberdelincuencia y proceso penal

Unidad 6.- Aspectos internacionales
Tema 1.- Convenios internacionales
Tema 2.- La conferencia de Interpol y Europol sobre ciberdelincuencia
Tema 3.- La UNDOC
Tema 4.- Problemas de jurisdicción. Ciberdelitos en el tiempo y en el espacio

5. METODOLOGÍAS DE ENSEÑANZA-APRENDIZAJE

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

- Clase Magistral.
- Método del caso.
- Aprendizaje basado en problemas.
- Aprendizaje inverso.

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 online:

Actividad formativa	Número de horas
Clases magistrales	10
Clases virtuales	20
Análisis de casos	10
Resolución de problemas	10
Elaboración de informes y escritos	12
Investigaciones y proyectos	10
Estudios de contenidos y documentación complementaria	50
Foro virtual	8
Tutoría virtual	18
Pruebas presenciales de conocimientos	2
TOTAL	**150**

7. EVALUACIÓN

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

Modalidad online:

Sistema de evaluación	Peso
Pruebas presenciales de conocimiento	60%
Informes y escritos	10%
Caso/Problema	10%
Investigaciones y proyectos	10%

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 4,0 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 extraordinaria 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 4,0 en la prueba final, para que la misma pueda hacer media con el resto de las 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:

Actividades evaluables	Fecha
Actividad 1. Casos de tipificación	Semana 16-17
Actividad 2. Cuestionario unidad 3	Semana 16-17
Actividad 3. Dictamen jurídico unidad 4	Semana 20-21
Actividad 4. Cuestionario unidad 6	Semana 20-21
Actividad 5. Prueba final presencial	Semana 30

Este cronograma podrá sufrir modificaciones por razones logísticas de las actividades, así como por su número y contenido. Cualquier modificación será notificada al estudiante en tiempo y forma.

9. BIBLIOGRAFÍA

A continuación, se indica bibliografía recomendada (ediciones más actualizadas):

Devia González, E.A. (2017) “Delito informático: Estafa informática del artículo 248-2 del Código Penal”, Universidad de Sevilla, Tesis en espacio abierto disponible en <https://dialnet-unirioja.es>
Galán Muñoz, A. (2005) “El fraude y la estafa mediante sistemas informáticos. Análisis del artículo 248.2 C.P.”, Valencia, Editorial Tirant Lo Blanch
Gutiérrez Mayo, E. (2021) “Delitos informáticos paso a paso. Análisis detallado de las conductas delictivas más comunes en el entorno informático”, A Coruña, Editorial Colex
Serrano Ferrer, M.P. (2021) “Derecho penal y nuevas tecnologías”, Navarra, Thomson Reuters Aranzadi
CASABIANCA ZULETA, P (2016). Las intervenciones telefónicas en el sistema penal. Bosch: Barcelona
Circular de la Fiscalía General del Estado 1/2013, sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas, https://www.boe.es/buscar/doc.php?coleccion=fiscalia&id=FIS-C-2013-00001
Circular 2/2019, de 6 de marzo, de la Fiscalía General del Estado, sobre interceptación de comunicaciones telefónicas y telemáticas. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-4241
LAFONT NICUESA, L. (2022). El agente policial encubierto. Valencia: Tirant lo Blanch

10. UNIDAD DE ATENCIÓN A LA DIVERSIDAD

Estudiantes con necesidades específicas de apoyo educativo:

Las adaptaciones o ajustes curriculares para estudiantes con necesidades específicas de apoyo educativo, a fin de garantizar la equidad de oportunidades, serán pautadas por la Unidad de Atención a la Diversidad (UAD).

Será requisito imprescindible la emisión de un informe de adaptaciones/ajustes curriculares por parte de dicha Unidad, por lo que los estudiantes con necesidades específicas de apoyo educativo deberán contactar a través de: unidad.diversidad@universidadeuropea.es al comienzo de cada semestre.

11. ENCUESTAS DE SATISFACCIÓN

¡Tú 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.

12. REGLAMENTO DE USO DE IA

El estudiante debe ser el autor o autora de sus trabajos/actividades.

El uso de herramientas de Inteligencia Artificial (IA) debe ser autorizado por el docente en cada trabajo/actividad, indicando de qué manera está permitido su uso. El docente informará previamente en qué situaciones se podrá usar herramientas de IA para mejorar la ortografía, gramática y edición en general. El estudiante es responsable de precisar la información dada por la herramienta y declarar debidamente el uso de cualquier herramienta de IA, en función de las directrices que marque el docente. La decisión final sobre la autoría del trabajo y la idoneidad del uso reportado de una herramienta de IA recae en el docente y en los responsables de la titulación.