UNIVERSIDAD DEL ATLÁNTICO MEDIO

GUÍA DOCENTE

CIBERDELINCUENCIA

GRADO EN DERECHO

MODALIDAD VIRTUAL

CURSO ACADÉMICO 2023-2024

ÍNDICE

RESUMEN

Centro	Facultad de Ciencias Sociales y Jurídicas		
Titulación	Grado en Derecho		
Asignatura	Ciberdelincuencia	**Código**	F1C1G07035
Materia	Elementos de Intensificación para el Estudio del Derecho de las TIC (virtual)		
Carácter	Optativa		
Curso	4º		
Semestre	1º		
Créditos ECTS	6		
Lengua de impartición	Castellano		
Curso académico	2023-2024		

DATOS DEL PROFESORADO

Responsable de Asignatura	
Correo electrónico	@pdi.atlanticomedio.es
Teléfono	828.019.019
Tutorías	Consultar horario de tutorías en el campus virtual. El horario de atención al estudiante se publicará al inicio de curso en el Campus Virtual. En caso de incompatibilidad con las franjas horarias establecidas pueden ponerse en contacto a través del *mail* para concertar una tutoría fuera de este horario. Se ruega que se solicite la tutoría a través del Campus Virtual o a través del correo electrónico.

REQUISITOS PREVIOS

Sin requisitos previos.

COMPETENCIAS

Competencias básicas:

CB1

Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio.

CB2

Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio.

CB3

Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética.

CB4

Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado.

CB5

Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía.

Competencias transversales:

CT1

Capacidad para la resolución de problemas y toma de decisiones

CT2

Capacidad de trabajo en equipo y en entornos diversos y multiculturales

CT3

Adquisición de conceptos vinculados a la sensibilidad hacia la diversidad y compromiso étnico.

CT4

Capacidad de tener conciencia crítica sobre las realidades sociales y las corrientes de pensamiento.

CT5

Capacidad para dominar las competencias digitales.

Competencias específicas:

CE12

Conocimiento de las Instituciones y del Derecho Penal y capacidad de pronunciamiento, con una argumentación jurídica oral y escrita convincente sobre una cuestión relativa al Derecho Penal.

RESULTADOS DE APRENDIZAJE

Cuando el estudiante supere esta asignatura será capaz de:

- Comprender el lenguaje jurídico y el marco conceptual en materia de delitos cometidos a mediando la Red.
- Analizar supuestos de ciberdelincuencia.
- Aplicar normativa, argumentaciones y razonamientos jurídicos en materia de ciberdelitos.

CONTENIDOS DE LA ASIGNATURA

1. Introducción a la ciberdelincuencia. Características de la ciberdelincuencia y del ciberdelincuente. Ciberdelincuencia organizada. Respuestas ante el ciberdelito.
2. Tipos delictivos (I). Fraudes en la red. Estafas en banca electrónica. Phishing. Fraude en medios de pago físico. Otros tipos de fraude en la red.
3. Tipos delictivos (II). Daños informáticos. Propiedad intelectual.
4. Tipos delictivos (III). Difusión de contenidos ilícitos. Otros ciberdelitos.
5. Denuncias sobre ciberdelitos. Salvaguarda de evidencias digitales.
6. ISO/IEC 27037:2012.

Estos contenidos se desarrollarán por medio del siguiente programa:

1. Introducción a la ciberdelincuencia.

    1.1 - Características de la ciberdelincuencia y del ciberdelincuente.

    1.2 - Ciberdelincuencia organizada.

    1.3 - Respuestas ante el ciberdelito.

2. Tipos delictivos (I): Fraudes en la red. Estafas en banca electrónica. Phishing. Fraude en medios de pago físico. Otros tipos de fraude en la red.

    2.1 – Fraudes en la red.

    2.2 – Estafas en banca electrónica.

    2.3 – Phishing.

    2.4 – Fraude en medios de pago físico.

    2.5 – Otros tipos de fraude en la red.

3. Tipos delictivos (II). Daños informáticos. Propiedad intelectual.

    3.1 – Responsabilidad penal en materia de daños informáticos.

    3.2 – Delitos informáticos contra la propiedad intelectual.

4. Tipos delictivos (III). Difusión de contenidos ilícitos. Blanqueo de capitales. Otros ciberdelitos.

    4.1 – Responsabilidad penal por difusión de contenidos ilícitos.

    4.2 – Blanqueo informático de capitales.

    4.3 - Otros ciberdelitos.

5. Denuncias sobre ciberdelitos. Salvaguarda de evidencias digitales. La prueba pericial forense electrónica.

    5.1 – Consideraciones generales

    5.2 - Aspectos a tener en cuenta sobre las evidencias digitales

    5.3 - La adquisición de la prueba

6. ISO/IEC 27037:2012.

    6.1 – Consideraciones generales

    6.2 – Principios rectores de la prueba digital

    6.3 – Sujetos de la recopilación digital de prueba

    6.4 – Objeto de la recopilación digital de prueba

    6.5 – Procedimiento y foro de la recopilación digital de prueba

6.6 – La prueba digital: perspectivas de futuro

METODOLOGÍA

- Exposición / lección magistral
- Aprendizaje constructivo y práctico
- Aprendizaje autónomo
- Estudio dirigido

ACTIVIDADES FORMATIVAS

Elaboración de informes y/o dictámenes	40,6 horas
Clases magistrales participativas	35,2 horas
Resolución de problemas o supuestos prácticos	20,2 horas
Trabajo autónomo	73 horas
Tutorías	1,4 horas

EVALUACIÓN

	% CALIFICACIÓN FINAL
Examen (teórico y/o práctico)	50 %
Evaluación de trabajos	50%

Sistemas de evaluación

A) <u>Sistema de evaluación de la convocatoria ordinaria</u>

Se aplicará el sistema de evaluación continua por asignatura donde se valorará de forma integral los resultados obtenidos por el estudiante mediante los procedimientos de evaluación indicados.

La evaluación es el reconocimiento del nivel de competencia adquirido por el estudiante y se expresa en calificaciones numéricas, de acuerdo con lo establecido en la legislación vigente.

1. **Evaluación de los conocimientos teórico-prácticos (50% de la nota final):**

   Se valorará mediante la realización de un examen final obligatorio y presencial que adoptará la forma de preguntas de desarrollo y, en su caso, de test. Constará de una parte teórica y de una parte práctica. Esta prueba comprenderá preguntas para valorar las competencias previstas en la asignatura y otra parte dedicada a la verificación del trabajo realizado en la evaluación continua (evaluación de trabajos).

2. **Evaluación de trabajos (50% de la nota final):**

   Se valorará mediante la entrega de trabajos y actividades que se propongan a lo largo del curso a través del campus virtual para la comprobación de la adquisición por parte del estudiante de las competencias descritas en esta guía docente.

B) **Sistema de evaluación de la convocatoria extraordinaria**

En convocatoria extraordinaria se evaluará a través del mismo sistema de evaluación que en la convocatoria ordinaria.

C) Si se hubiera superado en convocatoria ordinaria el examen final o la evaluación de los trabajos, se mantendrá la nota para la convocatoria extraordinaria. Por tanto, el alumno tendrá que realizar las pruebas que tenga pendiente de aprobación, mediante nuevos trabajos o la presentación al examen de esta convocatoria. Las calificaciones solo se guardarán para las convocatorias asociadas a la presente guía docente.

Criterios de calificación

El criterio de calificación general consiste en que cada tarea se valora con una calificación de 0 a 10. Para realizar la aplicación de los porcentajes correspondientes, será necesario obtener al menos 4 puntos en cada una de las partes. Además, para superar la asignatura es necesario obtener una calificación mínima final de 5, como resultado de la media aritmética de los sistemas de evaluación previstos.

1. **Evaluación de los conocimientos teórico-prácticos**

a) Los conocimientos teóricos se evaluarán mediante un examen con un mínimo de tres preguntas de desarrollo medio y un test de 20 preguntas.

Las preguntas de desarrollo se valorarán en su conjunto con un máximo de 2,5 puntos del examen final. Las preguntas tipo test del examen final también se valorarán en su conjunto con un máximo de 2,5 puntos.

b) Los conocimientos prácticos se evaluarán mediante la realización de dos casos prácticos del tipo de los realizados a lo largo del curso.

Cada caso práctico se valorará con un máximo de 2,5 puntos del examen final.

Para superar el examen habrá de superarse tanto la parte teórica como la parte práctica, alcanzando una nota mínima de 2,5 puntos en cada una de ellas.

2. Evaluación de los trabajos

Se valorará mediante la entrega de al menos dos trabajos individuales de entrega obligatoria.

BIBLIOGRAFÍA

- **Básica:**
  - Fernández Bermejo, Daniel y Martínez Atienza, Gorgonio. *Ciberseguridad, ciberespacio y ciberdelincuencia*. Aranzadi, 2018.
  - Tejerina Rodríguez, Ofelia. *Aspectos jurídicos de la ciberseguridad*. Ra-Ma, 2020.
- **Recursos web:**
  - *Base de Datos Tirant Lo Blanch.*
  - Biblioteca digital:
    - E-Libro.
    - Scopus.