UNAM

UNIVERSIDAD DEL ATLÁNTICO MEDIO

Guía Docente

Ciberdelincuencia

Grado en Derecho

MODALIDAD PRESENCIAL

Curso Académico 2024-2025

Índice

RESUMEN

Centro	Universidad del Atlántico Medio
Titulación	Derecho
Asignatura	Ciberdelincuencia
Materia	Elementos de Intensificación para el Estudio del Derecho de las TIC
Carácter	Formación Optativa
Curso	4º
Semestre	1
Créditos ECTS	6
Lengua de impartición	Castellano
Curso académico	2024-2025

DATOS DEL PROFESORADO

Responsable de Asignatura	Haga clic o pulse aquí para escribir texto.
Correo Electrónico	@pdi.atlanticomedio.es
Tutorías	El horario de tutorías será el siguiente: • Lunes de 9:00 a 11:00 • Viernes de 15:00 a 17:00 El alumnado deberá solicitar la tutoría previamente a través del Campus Virtual o a través del correo electrónico.

REQUISITOS PREVIOS

Sin requisitos previos.

RESULTADOS DEL APRENDIZAJE

Conocimientos o contenidos:

- 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.
- Adquisición de conceptos vinculados a la sensibilidad hacia la diversidad y compromiso étnico.
- Capacidad de tener conciencia crítica sobre las realidades sociales y las corrientes de pensamiento.
- 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.

Habilidades o destrezas:

- 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.
- Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado.
- Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía.
- Capacidad de trabajo en equipo y en entornos diversos y multiculturales.
- Capacidad para dominar las competencias digitales.

Competencias:

- 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.
- Capacidad para la resolución de problemas y toma de decisiones.

CONTENIDOS DE LA ASIGNATURA

- Introducción a la ciberdelincuencia. Características de la ciberdelincuencia y del ciberdelincuente. Ciberdelincuencia organizada. Respuestas ante el ciberdelito.
- 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.
- Tipos delictivos (II). Daños informáticos. Propiedad intelectual.
- Tipos delictivos (III). Difusión de contenidos ilícitos. Otros ciberdelitos.
- Denuncias sobre ciberdelitos. Salvaguarda de evidencias digitales.
- 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

CRONOGRAMA ORIENTATIVO DE LA ASIGNATURA

Unidad 1.
Semanas 1-2

Unidad 2.
Semanas 3-4

Unidad 3.
Semanas 5-6-7

Unidad 4.
Semanas 8-9-10-11

Unidad 5.
Semanas 12-13

Unidad 6.
Semanas 14-15-16

Nota: La distribución expuesta tiene un carácter general y orientativo, ajustándose a las características y circunstancias de cada curso académico y grupo clase.

METODOLOGÍA
Exposición/lección magistral
Aprendizaje cooperativo
Aprendizaje constructivo y práctico
Aprendizaje autónomo
Estudio dirigido
Estudio de caso

ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS
Clases Magistrales Participativas	**42**
Trabajo en grupo	**13,5**
Resolución de problemas o supuestos prácticos	**9**
Trabajo autónomo	**76,5**
Tutorías	**3**
Estudio de casos	**6**

Las actividades formativas tienen un porcentaje de presencialidad del 100% a excepción del TrabajoAutónomo del Alumno.

EVALUACIÓN

CRITERIOS DE EVALUACIÓN	PORCENTAJE CALIFICACIÓN FINAL
Examen teórico y/práctico	50%
Evaluación de trabajos	50%

- Examen final teórico-práctico que consistirá en preguntas de desarrollo y/o tipo test; y resolución de casos prácticos: 50% de la nota final.
- Resolución de pruebas intermedias y de los ejercicios propuestos en la asignatura: 50% de la nota final.

Sistemas de evaluación

El sistema de calificaciones (R.D. 1125/2003, de 5 de septiembre) será:
0 – 4,9 Suspenso (SS)
5,0 – 6,9 Aprobado (AP)
7,0 – 8,9 Notable (NT)
9,0 – 10 Sobresaliente (SB)

La mención de "matrícula de honor" podrá ser otorgada a alumnos que hayan obtenido una calificación igual o superior a 9,0. Se podrá conceder una matrícula por cada 20 alumnos o fracción.

Criterios de Calificación

Se aplicará el sistema de evaluación continua, donde se valorará de forma integral los resultados obtenidos por el estudiante, mediante los criterios de evaluación indicados, siempre que, el alumno haya asistido, como mínimo, **al 80% de las clases.**

Para aprobar el examen es necesario superar tanto la parte teórica como la parte práctica. Se entenderá superada cada parte cuando se obtenga una puntuación mínima de 5 puntos sobre 10.

Será necesario aprobar con un 5 los dos bloques de sistemas de evaluación de forma independiente; es decir, la evaluación de examen y la evaluación de trabajo, con el fin de que haga media y obtener la calificación final de la asignatura.

En el caso de que los alumnos asistan a clase en un porcentaje inferior al 80%, el alumno no podrá presentarse a la convocatoria ordinaria.

Si el alumno no se presenta al examen en convocatoria oficial, figurará como "No Presentado" en actas.

Si el alumno no aprueba el examen de la asignatura, en actas aparecerá el porcentaje correspondiente a la calificación obtenida en la prueba.

Los alumnos podrán examinarse en convocatoria extraordinaria atendiendo al mismo sistema de evaluación de la convocatoria ordinaria.

BIBLIOGRAFÍA

Básica

- Fernández Bermejo, D. y Martínez Atienza, G. *Ciberseguridad, ciberespacio y ciberdelincuencia* (última edición). Aranzadi.
- Tejerina Rodríguez, O. *Aspectos jurídicos de la ciberseguridad* (última edición). Ra-Ma.

Complementaria

- Canals Ametller, D. *Ciberseguridad. Un nuevo reto para el Estado y los Gobiernos Locales* (última edición). Wolters Kluwer.
- Delgado Martín, J. *Investigación tecnológica y prueba digital en todas las jurisdicciones* (última edición). Wolters Kluwer.
- Giutiérrez Mayo, E. *Delitos informáticos. Paso a paso. Análisis detallado de las conductas delictivas más comunes en el entorno informático* (última edición). Colex.
- López Gorostidi, J. *Ciberdelincuencia: proporcionalidad y bienes jurídicos protegidos* (última edición). Comares.
- Pérez Bes, F. (coord.). *Memento Experto: Ciberseguridad* (última edición). Francis Lefebvre.
- Velasco Núñez, E. *Delitos tecnológicos. Cuestiones penales y procesales* (última edición). Wolters Kluwer.

Recursos web

- Base de Datos Tirant Lo Blanch.
- Biblioteca digital:
    - E-Libro.
    - Scopus.