# CIBERESPACIO Y DELINCUENCIA INFORMÁTICA

**CURSO:** TERCERO
**SEMESTRE:** PRIMERO
**TIPO:** OBLIGATORIA
**CRÉDITOS:** 3 ECTS
**IDIOMA:** CASTELLLANO
**DOCENTE:** AINA GASSÓ

## OBJETIVOS

Desde hace unos años, con la llegada de internet, el mundo, la sociedad y la forma que tenemos de relacionarnos ha cambiado. Por ello, debemos entender cómo funciona el ciberespacio, qué tipologías delictivas existen en él y cómo prevenirlas. Por tanto, los objetivos de la presente asignatura serán:

- Conocer el contexto virtual conocido como "ciberespacio", cómo funciona y qué características tiene
- Aprender a identificar las diferentes formas de cibercriminalidad y cibervictimización
- Concienciar sobre los riesgo que existen en el ciberespacio y cómo prevenirlos
- Dar herramientas a los alumnos para que sean capaces de identificar y comprender todos los fenómenos de la ciberdelincuencia y su tipificación penal
- Aprender a pensar de forma crítica y conocer la evolución de los diversos fenómenos "ciber"

## COMPETENCIAS

## BÁSICAS Y GENERALES

**G1** - Mostrar actitud positiva y de relación, tanto con profesionales de las diversas facetas de la actividad criminológica como en equipos interdisciplinares y multiculturales.

**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.

**CB5** - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía.

**TRANSVERSALES**

**T1** - Actuar con espíritu y reflexión críticos ante el conocimiento en todas sus dimensiones, mostrando inquietud intelectual, cultural y científica y compromiso hacia el rigor y la calidad en la exigencia profesional.

**T7** - Llegar a ser el actor principal del propio proceso formativo en vistas a una mejora personal y profesional y a la adquisición de una formación integral que permita aprender y convivir en un contexto de diversidad lingüística, con realidades sociales, culturales y económicas diversas.

**ESPECÍFICAS**

**E1** - Evaluar la evolución histórica de las teorías de la criminalidad y de la fenomenología de la delincuencia, valorando los principios y fundamentos de la psicología, la sociología y la criminología, en relación con el delito, el delincuente, la victimización y las respuestas ante el delito y la desviación.

**E4** - Reconocer las diversas formas de delincuencia y criminalidad, comprendiendo su magnitud y las características de los fenómenos relacionados con la criminalidad, a través de estadísticas y otras fuentes de datos.

**E5** - Analizar los principales factores y causas de la aparición de los fenómenos criminales, para el diseño y gestión de proyectos y estrategias innovadoras sobre modelos de intervención social y de prevención estructural e individual.

**E7** - Evaluar los efectos teóricos y empíricos de los programas y las políticas impulsadas para la prevención, protección y actuación frente al delito, distinguiendo la tipología y funciones de los agentes e instituciones públicas implicadas.

**RESULTADOS DE APRENDIZAJE**

**R1** - Reconocer exactamente la normativa vigente en materia de delincuencia informática recogida en el Código Penal español.

**R2** - Utilizar adecuadamente las herramientas necesarias relacionadas con el perfil criminológico del ciberdelincuente.

**R3** - Actuar en las situaciones habituales y las que son propias de la profesión con compromiso y responsabilidad.

**R4** - Realizar procesos de evaluación sobre la propia práctica y la de los demás de forma crítica y responsable.

**R5** - Identificar sus propias necesidades formativas y de organizar su propio aprendizaje con un alto grado de autonomía en todo tipo de contextos (estructurados o no).

**R6** - Reconocer los principales paradigmas criminológicos y manejar los principales tipos y formas de criminalidad.

**CONTENIDOS**

- **Tema 1. Introducción al ciberespacio y a la ciberdelincuencia**
  - 1.1 Introducción
  - 1.2 Características del ciberespacio
  - 1.3 Teorías criminológicas relacionadas con el ciberespacio

- **Tema 2. Cibercriminalidad social**
  - 2.1 Ciberbullying, Ciberstalking y discurso de odio
  - 2.2 Violencia en la pareja a través de las TIC
  - 2.3 Explotación sexual basada en imágenes
  - 2.4 Ciberabuso sexual (online grooming)

- **Tema 3. Otras formas de cibercriminalidad**
  - 3.1 Cibercriminalidad instrumental (ransomware, malware, etc.)
  - 3.2 Cibercrminalidad económica (ciberfraude)
  - 3.3 Cibercriminalidad política (ciberterrorismo)

## SISTEMA DE EVALUACIÓN

Hay un examen (de contenido práctico) que tiene un valor del 40% de la nota final y que hará media con el resto de la evaluación continua a partir del 40 sobre 100. El 60% restante se obtiene de diversas actividades prácticas, tanto individuales como grupales, en las que se evaluará el aprendizaje del estudiante realizado tanto fuera del aula como dentro del aula.

El examen es obligatorio y se debe obtener una calificación a partir del 40 sobre 100 para poder hacer la media.

Las actividades prácticas no se pueden recuperar. El examen se puede recuperar. Para la calificación final, se tendrá especialmente en cuenta la participación del estudiante en las actividades de clase, con un valor máximo del 10% de la nota final.

| SISTEMA DE EVALUACÓN | VALOR |
|---|---|
| Trabajo 1 (Análisis criminológico de un ciberdelito – Grupal) | 15,00% |
| Trabajo 2 (Análisis preventivo de un ciberdelito - Grupal) | 20,00% |
| Actividad (caso práctico - Individual) | 10,00% |
| Exposición trabajo 2 (Grupal) | 15,00% |
| Examen | 40,00% |

Es obligatorio asistir, como mínimo, al 80% de las horas lectivas. Las faltas sólo serán eliminadas en el caso de que están debidamente justificadas. Si el alumno no asiste, como mínimo, al 80% de las clases no se le evaluará por evaluación continua.

En el siguiente cuadro se muestra la dedicación aproximada que debe realizar el alumno para poder superar las actividades propuestas:

| Actividad | Evaluación | Competencias y RA | Condicionante | Dedicación |
|---|---|---|---|---|
| Trabajo 1 | 15,00% | Competencias: CB2, T1, E1, E4<br>Resultados de aprendizaje: R1, R2, R6, XX | No recuperable<br>Grupal<br>Obligatoria | 9 horas |

| | | | | |
|---|---|---|---|---|
| Trabajo 2 | 20,00% | Competencias: G1, T2, E5, E7<br>Resultados de aprendizaje: R1, R2, R6 | No recuperable<br>Grupal<br>Obligatoria | 12 horas |
| Actividad | 10,00% | Competencias: T1, E1, E7<br>Resultados de aprendizaje: R2, , R3, R4 | No recuperable<br>Individual<br>Voluntaria | 3 horas |
| Exposición trabajo 2 | 15,00% | Competencias: CB2, T7, E4, E7, R3, R4, R5 | No recuperable<br>Grupal | 6h |
| Examen | 40,00% | Competencias: CB5, E1, E4<br>Resultados de aprendizaje: R1, R2, R5, R6 | Recuperable<br>Individual<br>Obligatorio | 20 horas |
| **Horas de clase** | | | | 30 horas |
| **Horas dedicación** | | | | 50 horas |
| **TOTAL HORAS** | | | | **80 horas** |

**METODOLOGÍA**

La asignatura utiliza criterios de evaluación continua y combina los conocimientos teóricos con su puesta en práctica. A lo largo de las sesiones de clase, el profesor expondrá contenidos del programa mediante el uso de diferentes metodologías de aprendizaje, además de efectuar actividades formativas en grupo para complementar y poner en práctica los conocimientos adquiridos. Asimismo, los alumnos deberán realizar actividades individuales durante las horas de trabajo personal.

Los alumnos deberán realizar dos trabajos, una actividad práctica fuera del aula y una exposición oral del segundo trabajo, que serán objeto de evaluación. Asimismo, se evaluará el trabajo realizado dentro del aula en las sesiones dedicadas a la resolución en grupo de las actividades propuestas.

Por último, se recomienda al alumno que dedique cada semana, unas horas de trabajo personal a esta asignatura para poder ir consolidando los conocimientos adquiridos en cada uno de los temas. Este trabajo personal consistirá en realizar un repaso de los aspectos teóricos tratados en clase y complementarlos con la bibliografía básica.

**BIBLIOGRAFÍA RECOMENDADA**

Agustina, J. R., Montiel, I., Gámez-Guadix, M. (2020). *Cibercriminología y victimización online*. Madrid: Editorial Síntesis.

Holt, T.J., Bossler, A.M.; Seigfried-Spellar, K.C. (2015). "Cybercrime and criminological theories". In Cybercrime and Digital Forensics. An Introduction. Routledge: London and New York, pp. 282-314.

Miró, F. (2011). La oportunidad criminal en el ciberespacio. aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. http://criminet.ugr.es/recpc/13/recpc13-07.pdf

Miró Llinares, F. (2012). El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. *Madrid, Marcial Pons*.

Miró, F. (2016). Taxonomía de la comunicación violenta y el discurso del odio en Internet. IDP. Revista de Internet, Derecho y Política, 22.

Teruelo, J. G. F. (2007). *Cibercrimen: los delitos cometidos a través de Internet: estafas, distribución de pornografía infantil, atentados contra la propiedad intelectual, daños informáticos, delitos contra la intimidad y otros delitos en la Red*. CCC-Constitutio Criminalis Carolina.

Weimann, Gabriel (2015): Terrorism in Cyberspace: The Next Generation, Woodrow Wilson Center Press with Columbia University Press.