# Cibercrimen

**Curso Académico: ( 2019 / 2020 )** **Fecha de revisión: 21/04/2020 11:24:59**

**Departamento asignado a la asignatura: Departamento de Derecho Penal, Procesal e Historia del Derecho**

**Coordinador/a: OTERO GONZALEZ, MARIA PILAR**

**Tipo: Optativa Créditos ECTS : 3.0**

**Curso : 1 Cuatrimestre : 2**

## REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

Grado en Derecho

- Derecho penal, Parte General y Parte Especial.

## OBJETIVOS

COMPETENCIAS
-Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
-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
-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
-Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
-Redactar informes jurídicos de calidad
-Demostrar que se han asimilado los métodos y principios básicos de la actividad investigadora en el ámbito jurídico procesal penal
-Manejar las fuentes de información jurídica propias de la Justicia Criminal
-Elaborar textos científico-jurídicos y llevar a cabo el análisis de los mismos eficazmente
-Aplicar los conocimientos sobre instituciones penales y procesales en el desempeño de funciones jurídicas
-Comprender los estadios que conducen a la convicción judicial penal y las posibilidades de influencia en ella bajo el principio de presunción de inocencia;
-Informar de la adecuación de métodos de investigación en un ilícito penal y de la suficiencia de las fuentes de prueba y de la adecuación de los medios probatorios en relación con la concreta teoría del caso.
-Discriminar los elementos que conforman cada uno de los principales modelo teóricos de enjuiciamiento penal y su influencia en los ordenamientos jurídico penales contemporáneos;
-Demostrar la asunción de diferentes roles procesales, acusación, defensa y enjuiciamiento y estrategias de argumentación conforme a los mismos
-Comprender los estadios que conducen a la solución de un problema de la Parte General y Especial del Derecho penal vinculado a esta materia y dominen los instrumentos teóricos que tienen a su alcance para conseguir la decisión más precisa o la más favorable a los intereses que defienden
-Aplicar las habilidades de profesiones vinculadas con el ejercicio de la práctica jurídico-penal

METODOLOGÍAS DOCENTES
Detección de riesgos penales en el ámbito de las nuevas tecnologías de la comunicación y la información (TICs).
Reacción jurídica adecuada y adopción de medidas jurídicas ante los riesgos penales detectados en la actividad de las nuevas tecnologías.
Conocerán el estado de la Jurisprudencia de los Tribunales penales europeos para ofrecer soluciones

jurídicas a cuestiones concretas que se puedan plantear en la práctica.
Podrá exponer el complejo panorama de la transnacionalidad de esta delincuencia, cuáles sean sus características y su papel en el ámbito de la criminalidad en su conjunto.
Podrá establecer cuáles son los delitos que de forma principal se asocian a la cibercriminalidad, así como los mecanismos más idóneos de lucha, mediante el Derecho Penal, contra esas organizaciones.
Podrá integrar adecuadamente la regulación nacional sobre cibercriminalidad en el panorama del Derecho Comparado y especialmente en la normativa internacional.

## DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

Cibercrimen: La aparición de esta asignatura se justifica ante el aumento de la criminalidad cometida a través de internet, afectando a bienes jurídicos que van desde el patrimonio y orden socioeconómico, la indemnidad sexual de menores e incapaces, a la intimidad, la propiedad intelectual e industrial, etc. En esta asignatura se estudiarán los fenómenos que afectan a la criminalidad en la red, el impacto de la complejidad de las nuevas formas de tecnología y la protección de datos, y la necesidad de generar respuestas eficaces, como el comiso, la responsabilidad penal de personas jurídicas, y la regulación del secreto bancario para desalentar a la comisión de estos delitos.
CIBERCRIMINALIDAD. RETOS DEL DERECHO PENAL ANTE LAS TICS

I. INTRODUCCIÓN. CONSIDERACIONES POLÍTICO CRIMINALES. DATOS SOBRE CIBERVICTIMIZACIÓN.
1. El Derecho Penal a remolque de las nuevas tecnologías: sociedad de riesgo. Incremento de los delitos de peligro abstracto. Desformalización. Expansión. Perfil pedagógico.
2. Influencia de Internet en el Derecho penal.
3. Lado oscuro del desarrollo: nuevas formas de criminalidad, utilización de las redes informáticas para facilitar la comisión de los delitos convencionales, macrovictimización, problemas de incriminación, problemas de competencia, anonimato: sensación de impunidad. Plataforma de la criminalidad organizada.

II. MARCO JURÍDICO INTERNACIONAL DE REFERENCIA.

III. BIENES JURÍDICOS AFECTADOS POR LA CIBERDELINCUENCIA.
Intimidad, honor, libertad, libertad e indemnidad sexual, patrimonio, propiedad intelectual, seguridad exterior e interior del Estado. Especial referencia a la protección penal de la intimidad y del patrimonio en relación con la delincuencia en el ciberespacio.

IV. TECNOLOGÍAS DE LA COMUNICACIÓN. LA PROTECCIÓN DE DATOS Y LOS RIESGOS ANTE LAS TECNOLOGÍAS DE LA COMUNICACIÓN.
1. Evolución de la intimidad: Teoría de las esferas. Privacy e impacto de nuevas tecnologías: derecho activo de control vinculado a la autodeterminación. Expansión redes telefonía. Sociedad postindustrial: moderno secreto profesional. El derecho al anonimato. El derecho al olvido.
2. Crisis de lo público. Invocación de autorregulaciones.
3. Tipificación del control clandestino auditivo y visual, control ilícito de señales de comunicación: interceptación de señales, de conversaciones, vulneración password.
4. Supuestos especiales: Videocámaras en espacios públicos. Escuchas clandestinas. Cámaras ocultas y grabaciones en las que el interlocutor participa. Difusión inconsentida de vídeos íntimos. Requisitos de las escuchas autorizadas judicialmente: análisis jurisprudencial.
5. Protección de datos: el habeas data informática.

V. LA CIBERDELINCUENCIA COMO PLATAFORMA PARA LA CRIMINALIDAD ORGANIZADA.
1. Crimen organizado y sociología criminal: concepto y características. Tipologías. Estructura organizativa. Corrupción, globalización, sofisticación. Relación Estado-crimen organizado.
2. Justificación de la respuesta penal específica ante el crimen organizado. Fundamento. Bien jurídico protegido. Incentivos de la colaboración con la justicia.
3. Técnica legislativa penal. Tipos penales. Problemas concursales.
4. Respuesta basada en que el delito ¿no resulte provechoso¿: el comiso, el blanqueo de capitales, organismos internacionales autónomos de control de las finanzas. Los paraísos fiscales y las jurisdicciones con secreto bancario.

VI. TECNOLOGÍAS DE LA INFORMACIÓN. CONDUCTAS DELICTIVAS.
1. Delitos cuyo único medio de comisión es la Red: hacking, sabotaje informático (cracking). Especial referencia a la denegación de Servicios (Denial of Service).
2. Infracciones tradicionales que utilizan las redes telemáticas como instrumento: los fraudes en internet (phising), tratamiento del spoofing, el espionaje (Spyware), atentados a la propiedad

intelectual e industrial (Linking, Inlining, Metatags, keywords), ataques a bienes personalísimos realizados a través de internet acompañados o no de TICs: ciberbullying, child grooming, Sexting.
3. Ataques por el contenido transmitido: pornografía infantil, ciberterrorismo.

VII. ATRIBUCIÓN DE RESPONSABILIDAD PENAL A LAS PERSONAS FÍSICAS Y JURÍDICAS POR PUBLICACIÓN DE CONTENIDOS DELICTIVOS (PROVEEDORES DE CONTENIDOS, PROVEEDORES DE SERVICIOS).

VIII. PERSEGUIBILIDAD. PROBLEMAS DE COMPETENCIA.

## ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

Exposición del material teórico, seminarios con conferenciantes/expertos invitados, y análisis de casos prácticos.

## SISTEMA DE EVALUACIÓN

| | |
|---|---|
| **Peso porcentual del Examen/Prueba Final:** | 100 |
| **Peso porcentual del resto de la evaluación:** | 0 |

CONVOCATORIA ORDINARIA

El sistema de calificación del presente módulo está basado en una prueba final al término del módulo que tendrá un valor del 100% de la asignatura

La asistencia a las clases y actividades que componen el módulo es obligatoria.

La ausencia injustificada del alumno superior a un 10% de las sesiones de cada una de las materias (Investigación o prueba) puede llevar aparejada la no calificación en dicha materia y la necesidad de cursar de nuevo la materia concreta y, en el caso de superar el 20% de las sesiones del módulo, la necesidad de repetir íntegramente el módulo.

CONVOCATORIA EXTRAORDINARIA

En la convocatoria extraordinaria el examen consistirá en un caso

## BIBLIOGRAFÍA BÁSICA


- ALVAREZ VIZCAYA, M.: ¿Consideraciones político criminales sobre la delincuencia informática: el papel del Derecho penal en la red¿, Internet y Derecho penal. Cuadernos de Derecho Judicial, Madrid,, 2001, pp.255-280.

- FARALDO CABANA, P. : Las nuevas tecnolgías en los delitos contra el patrimonio y el orden socioeconómico, , Tirant lo Blanch, Valencia,, 2009

- GÓMEZ MARTÍN, V. ¿Sabotaje informático, top manta, importaciones paralelas y fraude de inversiones¿ , Revista Jurídica de Catalunya, vol. 110, nº 4, 2011, pp. 1017 y ss.

- HERNÁNDEZ DÍAZ, L.: , ¿El delito informático¿ , en Eguzkilore. , nº 23, , 2009, pp. 227 y ss.

- LOYÈRE, G. de la ¿Flujos transfronterizos y globalización: ¿cómo proteger la intimidad en un mundo global? El papel de las autoridades de protección de datos en materia de transferencias internacionales de datos¿ , en Revista de la Agencia de Protección de Datos de la Comunidad de Madrid, nº 20,, : 2006.

- MIRÓ LLINARES, F. ¿Derecho penal y libre competencia en internet¿ , , en Cuadernos de Política Criminal, nº 94, 2008, pp 110 y ss.

- MIRÓ LLINARES, F.: ¿La protección penal de los derechos de explotación exclusiva sobre el software¿ , en Revista Penal, nº 13,, 2004, pp. 85 y ss.

- OTERO GONZÁLEZ, P.: ¿Delitos contra la intimidad, derecho a la propia imagen, inviolabilidad del domicilio de personas jurídicas y establelecimientos abiertos al público¿ , en Memento Práctico : Penal Económico y de la Empresa, Madrid: Francis Lefebvre, 2011-12, pp.337 y ss.

BIBLIOGRAFÍA COMPLEMENTARIA

- -MORÓN LERMA, Esther, Internet y Derecho penal: hacking y otras conductas ilícitas en la red, , Pamplona: Aranzadi,, 1999

- MIRÓ LLINARES, F.: , ¿Delitos Informáticos¿, en ORTIZ DE URBINA GIMENO, Í.(DIR.):Memento Derecho Penal Económico y de la Empresa, Francis Lefebvre, Madrid,, 2011.

- MORALES GARCÍA, Óscar, "Criterios de atribución de responsabilidad penal a los prestadores de servicios e intermediarios de la Sociedad de la Información",, en Revista de Derecho y Proceso Penal, nº 5, Aranzadi,, 2001

- MORÓN LERMA, Esther, ¿Daños informáticos: art. 264¿, en Consideraciones a propósito del Proyecto de Ley de 2009 de modificación del Código Penal (Directores: FJ Álvarez García; JL González Cussac), , Valencia: Tirant lo Blanch, 2010

- SANCHÍS CRESPO, C. (dir.): Fraude electrónico: entidades financieras y usuarios de banca. Problemas y soluciones,, Aranzadi/Thomson Reuters, Cizur Menor, , 2011.

- VELASCO NUÑEZ, E.: ¿Estafa informática y banda organizada¿, en La ley penal, nº 49, , 2008.