Análisis y gestión de riesgos del cibercrimen

1.- Datos de la Asignatura					
Código	306.585	Plan	2025	ECTS	3
Carácter	Obligatoria de especialidad	Curso	1º	Periodicidad	2 semestre
Idioma de impartición asignatura		español			
Área	Ciencia de la Computación e Inteligencia Artificial				
Departamento	Informática y Automática				
Plataforma virtual	Studium https://moodle.usal.es				

1.1.- Datos del profesorado*			
Profesor Coordinador	Pablo Chamoso Santos	Grupo / s	
Departamento	Informática y Automática		
Área	Ciencia de la Computación e Inteligencia Artificial		
Centro	Facultad de Ciencias		
Despacho	F3012		
Horario de tutorías	A convenir con el alumno, solicitado por correo electrónico.		
URL Web	https://produccioncientifica.usal.es/investigadores/57686/detalle		
E-mail	chamoso@usal.es	Teléfono	Ext. 6591

2.- Recomendaciones previas

- Revisar conceptos básicos de ciberseguridad.
- Familiarizarse con herramientas de análisis de vulnerabilidades.

3.- Objetivos de la asignatura

1. Comprender las metodologías y herramientas de análisis de riesgos.
2. Desarrollar competencias en la identificación y clasificación de riesgos.
3. Diseñar e implementar estrategias de mitigación.
4. Fortalecer la toma de decisiones bajo incertidumbre.
5. Mejorar las habilidades de comunicación técnica.
6. Fomentar el aprendizaje autónomo y práctico.

4.- Competencias a adquirir / Resultados de aprendizaje

Resultados de aprendizaje

4.1: Conocimientos:

C1. Defender las bases conceptuales de la ciberdelincuencia, ciberamenazas y la seguridad informática

C2. Examinar el funcionamiento de las tecnologías disruptivas utilizadas por delincuentes y por profesionales que actúan ante la cibercriminalidad, así como los principios básicos de ciberespacio

C4. Evaluar las herramientas técnicas y legales necesarias para analizar y hacer frente a diferentes riesgos, ciberamenazas y ciberdelitos.

C9. E2 Comparar conocimientos específicos para elaborar estudios e informes criminológicos en

el ámbito de la ciberdelincuencia y profundizar en las teorías criminológicas que explican el delito en el ciberespacio, así como otros factores relacionados con el proceso penal.

4.2: Habilidades:

H1. Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales

H3. Practicar con pericia la búsqueda de legislación y jurisprudencia a través de diferentes técnicas que puedan favorecer la investigación, la prueba y la intervención ante ciberdelitos.

H5. Aplicar con dominio la normativa nacional e internacional que regula la ciberdelincuencia, así como su persecución, investigación y represión en casos concretos.

H6. Concluir las cuestiones jurídicas más relevantes implicadas en un conjunto complejo de hechos relacionados con casos de cibercriminalidad.

H10. E2 Desarrollar estrategias de prevención e intervención ante ciberataques u otro tipo de ciberdelitos, razonando y argumentando la propuesta con un enfoque interdisciplinar y teniendo en cuenta las particularidades de las víctimas para que la propuesta responda a las necesidades de éstas.

4.3: Competencias:

K1. Discriminar los tipos de ciberdelito, comprendiendo los nuevos espacios virtuales y, en atención a ellos, aplicar la normativa vigente y las resoluciones jurisprudenciales vinculantes en cada caso en cuestión

K3. Analizar pormenorizadamente cada ciberdelito, incluyendo perfiles diferenciados de víctimas y agresores en el uso de la tecnología cibernética

K5. En casos de cibercriminalidad, redactar textos legales para los diferentes momentos procesales y desde el punto de vistas de diferentes profesiones implicadas, y que estos textos sean comprensibles tanto para un público especialista como para un público profano

K6. Discriminar las funciones de cada una de las autoridades y profesionales que intervienen en casos de ciberdelincuencia, identificando los requisitos formales que van ligados a todas ellas para poder poner en práctica las mismas

Especialidad en aspectos jurídicos de la cibercriminalidad:

K10. E2 Determinar, tras su evaluación, el tratamiento individualizado de las víctimas de un cibercrimen, así como planes de prevención para hacer frente a los riesgos derivados de este tipo de criminalidad en diferentes sectores de la población

5.- Contenidos (temario)

Teóricos:

1. Fundamentos de la gestión de riesgos en ciberseguridad.
2. Metodologías de análisis de riesgos y modelado de amenazas.
3. Evaluación de riesgos: matrices de riesgo y análisis cualitativo/cuantiativo.
4. Gestión de incidentes de ciberseguridad: respuesta, mitigación y recuperación.
5. Comunicación de estrategias de gestión de riesgos y consideraciones éticas.

Prácticos:

1. Herramientas para el análisis de vulnerabilidades y simulación de ataques cibernéticos.
2. Taller de análisis de riesgos y modelado de amenazas.

6.- Metodologías docentes

La asignatura “Análisis y Gestión de Riesgos del Cibercrimen” combina teoría y práctica, priorizando el aprendizaje activo. Las sesiones magistrales ofrecerán los fundamentos teóricos sobre cibercriminalidad y gestión de riesgos. Las prácticas permitirán aplicar estos conocimientos en ejercicios y simulaciones usando herramientas especializadas. Además, los estudiantes presentarán sus trabajos en exposiciones y debates, fomentando la comunicación y reflexión

crítica, permitiendo entender cómo abordar el mayor número de ejemplos posible.

6.1.- Distribución de metodologías docentes

		Horas dirigidas por el profesor		Horas de trabajo autónomo	HORAS TOTALES
		Horas presenciales.	Horas no presenciales.		
Sesiones magistrales		9		10	19
Prácticas	- En aula	7		10	17
	- En el laboratorio				
	- En aula de informática				
	- De campo				
	- Otras (detallar)				
Seminarios					
Exposiciones y debates		8		15	23
Tutorías		4			4
Actividades de seguimiento online					
Preparación de trabajos					
Otras actividades (detallar)					
Exámenes		2		10	12
TOTAL		**30**		**45**	**75**

7.- Recursos, bibliografía, referencias electrónicas o de otro tipo

Rausand, M. (2013). Risk assessment: theory, methods, and applications (Vol. 115). John Wiley & Sons.
Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. Business Horizons, 64(5), 659-671.
Reuvid, J. (Ed.). (2018). Managing cybersecurity risk: Cases studies and solutions. Legend Press Ltd.

8.- Evaluación

8.1: Criterios de evaluación:

Los criterios de evaluación estarán enfocados en la comprobación de la adquisición de las competencias y resultados de aprendizaje de la asignatura. Estos criterios serán los siguientes:

1. Dominio de los conceptos teóricos.
2. Capacidad de aplicar metodologías de análisis de riesgos.
3. Competencia práctica en la gestión de incidentes.
4. Habilidades de comunicación.
5. Pensamiento crítico y toma de decisiones.

8.2: Sistemas de evaluación:

Parte teórica (50%) examen tipo test.
Parte práctica (50%) trabajo realizado (calidad, dificultad, materiales entregados y presentación).

8.3: Consideraciones generales y recomendaciones para la evaluación y la recuperación:

Se requerirá aprobar cada una de las dos partes para poder superar la asignatura.
De cara a la segunda convocatoria, se guardará la nota de la parte aprobada en caso de haberla.
El suspenso en la parte práctica implicará rehacerla por completo de cara a la recuperación.
El examen en la parte teórica podría ser a desarrollar en la recuperación.

9.- Organización docente semanal

Complete este apartado si es preciso

MODELO ÚNICO de guía docente de asignaturas de Grado y Máster Universitario
Curso 2025-2026

Aspectos legales de la ciberdelincuencia

1.- Datos de la Asignatura					
Código	306.570	Plan	2025	ECTS	6
Carácter	Obligatoria de especialidad	Curso	1º	Periodicidad	1º Semestre
Idioma de impartición asignatura		español			
Área	Derecho Constitucional, Derecho Administrativo y Derecho Procesal				
Departamento	Derecho Administrativo, Financiero y Procesal y Derecho Público General				
Plataforma virtual	Studium https://moodle.usal.es				

1.1.- Datos del profesorado*			
Profesor Coordinador	Fernando Martín Diz	Grupo / s	Único
Departamento	Derecho Administrativo, Financiero y Procesal		
Área	Derecho Procesal		
Centro	Facultad de Derecho		
Despacho	269		
Horario de tutorías	Previa petición al correo electrónico: fmdiz@usal.es		
URL Web	*https://produccioncientifica.usal.es/investigadores/56336/detalle*		
E-mail	fmdiz@usal.es	Teléfono	Ext. 1698
Profesor Coordinador	Mª Inmaculada Sánchez Barrios	Grupo / s	Único
Departamento	Derecho Administrativo, Financiero y Procesal		
Área	Derecho Procesal		
Centro	Facultad de Derecho		
Despacho	287		
Horario de tutorías	Previa petición al correo electrónico: misaba@usal.es		
URL Web	María Inmaculada Sánchez Barrios - Universidad de Salamanca		
E-mail	misaba@usal.es	Teléfono	Ext. 6942
Profesor Coordinador	Daniel Terrón Santos	Grupo / s	Único
Departamento	Derecho Administrativo, Financiero y Procesal		
Área	Derecho Administrativo		
Centro	Facultad de Derecho		
Despacho	255		

Horario de tutorías	Previa petición por correo electrónico datersa@usal.es		
URL Web			
E-mail	datersa@usal.es	Teléfono	Ext. 1645
Profesor Coordinador	Sergio Martín Guardado	Grupo/s	Único
Departamento	Derecho Público General		
Área	Derecho Constitucional		
Centro	Facultad de Derecho		
Despacho	256		
Horario de tutorías	Previa petición por correo electrónico martinguardado@usal.es		
URL Web	*https://produccioncientifica.usal.es/investigadores/148275/detalle*		
E-mail	Martinguardado@usal.es	Teléfono	Ext. 1645

*Replique esta tabla por cada profesor/a que imparte la asignatura

2.- Recomendaciones previas

- Haber cursado el Grado en derecho o en criminología
- Seguir los materiales aportados por el profesorado

3.- Objetivos de la asignatura

1. **Analizar el marco constitucional aplicable a la cibercriminalidad**, identificando los derechos fundamentales que pueden verse afectados por los delitos informáticos (como la intimidad, libertad de expresión o protección de datos), así como los límites y garantías del Estado en su persecución.
2. **Comprender los procedimientos procesales específicos en la investigación y enjuiciamiento de delitos cibernéticos**, incluyendo la obtención de pruebas digitales, las medidas cautelares tecnológicas y la cooperación internacional en materia penal.
3. **Estudiar la normativa administrativa y de ciberseguridad vigente**, evaluando el papel de las autoridades competentes en la prevención de ataques informáticos, la protección de infraestructuras críticas y la aplicación de sanciones administrativas en caso de incumplimiento de las obligaciones legales en entornos digitales.

4.- Competencias a adquirir / Resultados de aprendizaje

Resultados de aprendizaje

4.1: Conocimientos:

C1. Defender las bases conceptuales de la ciberdelincuencia, ciberamenazas y la seguridad informática

C4. Evaluar las herramientas técnicas y legales necesarias para analizar y hacer frente a diferentes riesgos, ciberamenazas y ciberdelitos.

C5. Interpretar la normativa nacional e internacional que regula la ciberdelincuencia, así como las funciones de autoridades y profesionales en el marco de detección, prevención, actuación e intervención en casos de ciberdelincuencia.

C6. Discriminar, por un lado, las particularidades de las personas víctimas de las actividades ilícitas que llevan a cabo los criminales utilizando tecnologías de la información y las comunicaciones; y, por otro, las necesidades de intervención que se derivan tras estos delitos.

C7. Contrastar la jurisprudencia estatal y supranacional en materia de ciberdelincuencia e investigación tecnológica

4.2: Habilidades:

H1. Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales

H2. Identificar el funcionamiento técnico de las ciberamenazas y ciberdelitos, en relación con las herramientas técnicas y legales disponibles para su cese y represión.

H3. Practicar con pericia la búsqueda de legislación y jurisprudencia a través de diferentes técnicas que puedan favorecer la investigación, la prueba y la intervención ante ciberdelitos.

H4. Evaluar la viabilidad de diferentes herramientas y medidas de investigación en atención al tipo de delictivo presentado, las autoridades involucradas y el momento procesal del caso**.**

H6. Concluir las cuestiones jurídicas más relevantes implicadas en un conjunto complejo de hechos relacionados con casos de cibercriminalidad.

4.3: Competencias:

K1. Discriminar los tipos de ciberdelito, comprendiendo los nuevos espacios virtuales y, en atención a ellos, aplicar la normativa vigente y las resoluciones jurisprudenciales vinculantes en cada caso en cuestión

K3. Analizar pormenorizadamente cada ciberdelito, incluyendo perfiles diferenciados de víctimas y agresores en el uso de la tecnología cibernética

K5. En casos de cibercriminalidad, redactar textos legales para los diferentes momentos procesales y desde el punto de vistas de diferentes profesiones implicadas, y que estos textos sean comprensibles tanto para un público especialista como para un público profano

K6. Discriminar las funciones de cada una de las autoridades y profesionales que intervienen en casos de ciberdelincuencia, identificando los requisitos formales que van ligados a todas ellas para poder poner en práctica las mismas

Especialidad en aspectos jurídicos de la cibercriminalidad:

K7. E1 Seleccionar los conocimientos específicos y cualidades más idóneos necesarios para garantizar y salvaguardar los derechos y principios jurídicos que favorezcan la intervención eficaz de diferentes autoridades en casos de ciberdelincuencia nacional e internacional.

5.- Contenidos (temario)

PARTE CONSTITUCIONAL

Tema sobre Conceptos Generales en el Derecho
del Ciberespacio
OBJETIVO: buscar un uso seguro y un desarrollo de los derechos y libertades fundamentales seguro dentro del ciberespacio debe partir de una visión integradora del ordenamiento jurídico en la esfera digital
CONTENIDO:
- Digitalización de la vida social y efectividad de los derechos fundamentales en el ciberespacio
- Desregulación del ciberespacio: ciber-libertarismo vs. ciber-regulación.
- Libertad informática y seguridad en el ciberespacio.
- Transformación digital de la función estatal de la protección de la seguridad pública.
- El fenómeno de la cibercriminalidad y el Estado de Derecho: la tipicidad y la criminalidad moderna.

Tema sobre la Determinación de la Ley Penal aplicable en el Ciberespacio
OBJETIVO: mostrar la dificultad de asegurar la vigencia de los derechos fundamentales a través de la función preventiva y reactiva del Derecho Penal, debido al nuevo escenario que supone la cibercriminalidad.
CONTENIDO:
- Delitos a distancia y criminalidad transnacional

- Principio de territorialidad (art. 23.1 LOPJ) vs. Principios de extraterritorialidad: personalidad activa, personalidad pasiva, protección de intereses nacionales, justicia universal (protección de intereses internacionales o de interés para la comunidad internacional) y justicia supletoria.
- Teoría de la acción, Teoría del resultado y Teoría de la Unidad o Ubicuidad.
- Convenio contra la Delincuencia Organizada Transnacional
- Convenio sobre Cibercriminalidad del Consejo de Europa
- Decisión Marco del Consejo de la Unión Europea, de 25 de febrero 2005, relativa a los ataques contra los sistemas de información y Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, que la sustituye.

Tema sobre Estado de Derecho, protección del ciberespacio y represión del ciberdelito
- Ius puniendi del Estado y represión del ciberdelito.
- Fuentes del Derecho en el Ciberespacio
- Tutela judicial efectiva y legalidad penal en el ámbito de la cibercriminalidad.
- Técnicas para la represión del ciberdelito: Leyes penales especiales, Tipificación de nuevas figuras delictivas en el Código Penal y Elaboración de normas internacionales.
- El ciberespacio como bien digno de protección jurídica
- Especificidad de los bienes jurídicos protegidos

PARTE PROCESAL

Tema .- Aspectos Procesales de la Ciberdelincuencia (I)
1.- Determinación y delimitación de la jurisdicción española en materia de ciberdelincuencia
2.- Aspectos orgánicos: juzgados, fiscalía especializada, unidades especializadas de los Cuerpos y Fuerzas de Seguridad del Estado. Cooperación judicial y policial internacional.

Tema.- Aspectos Procesales de la Ciberdelincuencia (II)
1.- Normativa internacional sobre aspectos procesales de la ciberdelincuencia
2.- Normativa española sobre aspectos procesales de la ciberdelincuencia

PARTE DERECHO ADMINISTRATIVO – CIBERDELINCUENCIA
Tema.- Ciberdelincuencia y ciberseguridad: aspectos normativos
1.-Legislación sobre ciberseguridad: las Directivas NIS I y II.
2.-La transversalidad de la ciberseguridad como garantía de lucha contra el cibercrimen.
3.-Esquema nacional de seguridad.
4.-Gobernanza de la ciberseguridad frente al cibercrimen.
5.-IA ¿riesgo de suma 0?

6.- Metodologías docentes

Clases magistrales teórico-prácticas, seminarios especializados, comentarios jurisprudenciales y debate en el aula para fomentar el espíritu crítico.

6.1.- Distribución de metodologías docentes

		Horas dirigidas por el profesor		Horas de trabajo autónomo	HORAS TOTALES
		Horas presenciales.	Horas no presenciales.		
Sesiones magistrales		24		20	44
Prácticas	- En aula	12		40	52

	- En el laboratorio				
	- En aula de informática				
	- De campo				
	- Otras (detallar)				
Seminarios					
Exposiciones y debates		12		10	22
Tutorías		2		5	7
Actividades de seguimiento online		10		15	25
Preparación de trabajos					
Otras actividades (detallar)					
Exámenes					
TOTAL		**60**		**90**	**150**

7.- Recursos, bibliografía, referencias electrónicas o de otro tipo

BALAGUER CALLEJÓN, Francisco. LA CONSTITUCIÓN DEL ALGORITMO. Fundación Manuel Giménez Abad, 2022.

AAVV. (MÍNGUEZ ROSIQUE, Mariana y GALLEGO ARRIBAS, David; Coords.). CIBERCRIMEN: TENDENCIAS Y DESAFIOS ACTUALES. Boletín Oficial del Estado, 2025.

PÉREZ ARISA, Jacinto. CIBERCRIMINALIDAD: HACIA LA NUEVA REALIDAD -VIRTUAL- DEL DERECHO PENAL. Revista Internacional de Doctrina y Jurisprudencia, vol. 26, 2021.

PRESNO LINERA, Miguel Ángel. DERECHOS FUNDAMENTALES E INTELIGENCIA ARTIFICAIAL EN EL ESTADO SOCIAL, DEMOCRÁTICO Y DIGITAL DE DERECHO. En AA.VV. Constitucionalismo: diálogos intergeneracionales entre España e Italia. Vol. 2, 2025.

GOLUMBIA, David. Ciberlibertarismo: Los fundamentos extremistas de la 'libertad digital'. Prometeica, n. 10, 2015

8.- Evaluación

8.1: Criterios de evaluación:

8.2: Sistemas de evaluación:

- Sobre la parte de Derecho Constitucional, se tendrá en cuenta la participación en clase (30% de la nota) así como la elaboración y defensa de un trabajo (70%).
- Sobre el módulo relativo a Aspectos Procesales de la Ciberdelincuencia (I):
  Asistencia y participación en clase (30%)
  Realización de un trabajo de investigación final y exposición del mismo (70% de la calificación)
- Sobre el módulo relativo a Aspectos Procesales de la Ciberdelincuencia (II):
  Asistencia y participación en clase (30%)
  Realización de un trabajo de investigación final y exposición del mismo (70% de la calificación)
  Sobre el módulo Ciberdelincuencia y ciberseguridad: aspectos normativos, se tendrá en cuenta la participación en clase (30% de la nota) así como la elaboración y defensa de un trabajo (70%).

  Los aspectos de la convocatoria extraordinaria se explicarán al inicio del curso

8.3: Consideraciones generales y recomendaciones para la evaluación y la recuperación:

9.- Organización docente semanal

Aspectos probatorios de la cibercriminalidad

1.- Datos de la Asignatura					
Código	306.578	Plan	2025	ECTS	6
Carácter	Obligatoria de especialidad	Curso	1º	Periodicidad	2º Semestre
Idioma de impartición asignatura		español			
Área	Derecho Procesal				
Departamento	Derecho Administrativo, Financiero y Procesal				
Plataforma virtual	Studium https://moodle.usal.es				

1.1.- Datos del profesorado*			
Profesor Coordinador	Lorenzo Mateo Bujosa Vadell	Grupo / s	Único
Departamento	Derecho Administrativo, Financiero y Procesal		
Área	Derecho Procesal		
Centro	Facultad de Derecho		
Despacho	285		
Horario de tutorías	Previa petición al correo electrónico: lbujosa@usal.es		
URL Web	*https://produccioncientifica.usal.es/investigadores/56612/detalle*		
E-mail	lbujosa@usal.es	Teléfono	Ext. 1652
Profesor Coordinador	Federico Bueno de Mata	Grupo / s	Único
Departamento	Derecho Administrativo, Financiero y Procesal		
Área	Derecho Procesal		
Centro	Facultad de Derecho		
Despacho	258		
Horario de tutorías	Previa petición al correo electrónico: febuma@usal.es		
URL Web	https://produccioncientifica.usal.es/investigadores/57438/detalle		
E-mail	febuma@usal.es	Teléfono	Ext. 1679

2.- Recomendaciones previas

- Haber cursado el Grado en derecho o en criminología
- Seguir los materiales aportados por el profesorado
- Tener presente la teoría general de la prueba.

3.- Objetivos de la asignatura

1. Examinar el marco constitucional aplicable a la cibercriminalidad desde una perspectiva probatoria, identificando los derechos fundamentales que pueden verse comprometidos durante la obtención y utilización de pruebas digitales (como la intimidad, la protección de datos personales y la inviolabilidad de las comunicaciones), así como los límites y garantías que rigen la actuación del Estado al recolectar evidencia electrónica.
2. Analizar los procedimientos procesales específicos relacionados con la obtención, conservación, validación y valoración de la prueba digital en la investigación y enjuiciamiento de delitos informáticos, abordando cuestiones como las medidas tecnológicas cautelares, la cadena de custodia de evidencias electrónicas y los mecanismos de cooperación internacional para el acceso legal a datos transfronterizos.
3. Identificar y clasificar los distintos tipos de pruebas electrónicas relevantes en la investigación de delitos informáticos, incluyendo registros de actividad digital, metadatos, comunicaciones electrónicas, archivos en la nube y rastros de navegación.
4. Examinar la jurisprudencia nacional e internacional sobre la prueba electrónica, identificando criterios clave sobre su validez, ilicitud, exclusión y contradicción en juicio.
5. Valorar el papel de los peritos informáticos forenses en la interpretación y certificación de pruebas electrónicas, así como la necesidad de conocimientos interdisciplinares entre Derecho y Tecnología para abordar eficazmente los desafíos probatorios del entorno digital.
6. Reflexionar críticamente sobre los riesgos de manipulación, pérdida o falsificación de evidencia digital, proponiendo buenas prácticas y estándares técnicos-jurídicos para asegurar su fiabilidad y legitimidad en el proceso penal.

4.- Competencias a adquirir / Resultados de aprendizaje

Resultados de aprendizaje

4.1: Conocimientos:

C1. Comprender y fundamentar las bases conceptuales de la ciberdelincuencia y su impacto en la obtención, tratamiento y valoración de pruebas digitales en el proceso penal.

C4. Evaluar herramientas legales y forenses necesarias para identificar, recolectar y asegurar evidencias electrónicas frente a diferentes modalidades de ciberamenazas y ciberdelitos.

C5. Interpretar la normativa nacional e internacional que regula la prueba digital, destacando el rol de autoridades, fiscales, jueces, cuerpos policiales y peritos en su obtención y utilización.

C6. Diferenciar las implicaciones probatorias derivadas de los delitos cometidos contra víctimas específicas (menores, colectivos vulnerables, víctimas de sextorsión, grooming, etc.) en entornos digitales.

C7. Contrastar jurisprudencia relevante (estatal y supranacional) sobre admisibilidad, ilicitud y valoración de pruebas tecnológicas en investigaciones de ciberdelitos

4.2: Habilidades:

H1. Identificar los principales riesgos jurídicos y técnicos asociados a la obtención y preservación de pruebas electrónicas en delitos informáticos, tanto en contextos nacionales como transnacionales, analizando cómo los nuevos entornos virtuales modifican los estándares probatorios tradicionales.

H2. Comprender el funcionamiento técnico de herramientas y entornos digitales (como redes, sistemas de cifrado, almacenamiento en la nube o registros de actividad), vinculándolos con las herramientas legales disponibles para asegurar la obtención legítima y eficaz de evidencia digital.

H3. Aplicar con precisión técnicas avanzadas de búsqueda, selección y análisis de legislación, doctrina y jurisprudencia relevante en materia de prueba electrónica, optimizando su uso en la investigación y litigación de delitos informáticos.

H4. Evaluar la viabilidad jurídica y técnica de diferentes medidas de investigación tecnológica (como registros remotos, captación de datos en tiempo real, interceptación de comunicaciones, etc.), atendiendo al tipo penal, la naturaleza de la prueba, la autoridad competente y la fase procesal.

H6. Identificar y argumentar con rigor jurídico las principales cuestiones procesales relacionadas con la admisibilidad, validez, contradicción y valoración de pruebas digitales en casos complejos de cibercriminalidad.

4.3: Competencias:

K1. Discriminar los distintos tipos de ciberdelito en función de las particularidades probatorias que presentan, comprendiendo los nuevos espacios virtuales en los que se generan las pruebas electrónicas, y aplicando la normativa vigente y la jurisprudencia relevante para su incorporación válida en el proceso penal.

K3. Analizar en profundidad los ciberdelitos desde la perspectiva probatoria, atendiendo a los perfiles diferenciados de víctimas y agresores, y evaluando el impacto que estas variables tienen sobre la forma de obtener, proteger y presentar la evidencia electrónica.

K5. Redactar documentos jurídicos relacionados con la prueba electrónica.

K6. Identificar con precisión las funciones y responsabilidades de los diferentes actores intervinientes en el proceso de obtención, análisis y presentación de pruebas electrónicas (fuerzas policiales, peritos informáticos, fiscales, jueces), así como los requisitos legales que garantizan la legalidad y validez del procedimiento probatorio.

K7 / E1. Seleccionar y aplicar de forma crítica conocimientos jurídicos, procesales y técnicos necesarios para salvaguardar los derechos fundamentales durante la investigación tecnológica, asegurando que las pruebas electrónicas se obtengan y utilicen conforme a los principios de legalidad, proporcionalidad, necesidad y respeto al debido proceso, tanto en contextos nacionales como internacionales.

5.- Contenidos (temario)

1: Fundamentos jurídicos de la prueba digital y la teoría general de la prueba
- 1.1. Concepto y características de la prueba electrónica
- 1.2. Principios rectores de la actividad probatoria
- 1.3. Prueba digital vs. prueba tradicional: similitudes y diferencias
- 1.4. Derechos fundamentales afectados (intimidad, privacidad, inviolabilidad de las comunicaciones, protección de datos)

2: Marco normativo y jurisprudencial
- 2.1. Normativa europea nacional sobre prueba digital en procesos penales
- 2.2. Instrumentos internacionales (Convenio de Budapest, propuestas de e-Evidence, cooperación judicial penal europea)
- 2.3. Jurisprudencia relevante (TC, TS, TEDH, TJUE) sobre obtención y validez de pruebas tecnológicas
- 2.4. Límites y garantías en la obtención de pruebas digitales

3: Tipología de evidencias digitales
- 3.1. Tipos de evidencia digital
- 3.2. Fuentes de prueba y medios de prueba
- 3.3. Preservación y aseguramiento de la prueba electrónica
- 3.4. Cadena de custodia digital

4: Técnicas y procedimientos de obtención y conservación de pruebas electrónicas
- 4.1. Diligencias de investigación tecnológica: intervención de comunicaciones, registros remotos, captación en tiempo real
- 4.2. Uso de herramientas forenses y software especializado
- 4.3. Medidas cautelares tecnológicas (bloqueo de cuentas, suspensión de servicios, congelación de datos)
- 4.4. Obtención transfronteriza de evidencia digital: mecanismos y cooperación internacional

5: Valoración y litigación de la prueba digital
- 5.1. Criterios de valoración judicial de la prueba electrónica
- 5.2. Nulidad, ilicitud e impugnación de pruebas digitales
- 5.3. Intervención del perito informático y presentación del informe pericial
- 5.4. Estrategias de defensa y acusación en torno a la prueba electrónica

6: Casos prácticos, litigación y simulaciones
- 6.1. Estudio de casos jurisprudenciales nacionales e internacionales
- 6.2. Análisis de evidencias digitales en supuestos de ciberdelitos comunes
- 6.3. Redacción de documentos procesales relacionados con la prueba digital
- 6.4. Simulación de vistas orales y debate sobre validez probatoria

6.- Metodologías docentes

En el desarrollo de la asignatura se compatibilizarán diversas metodologías. Así, se empleará la clase magistral durante las sesiones teóricas, mientras que en las sesiones prácticas se utilizarán diversas estrategias metodológicas, tales como el análisis y la discusión de textos legislativos y/o jurisprudenciales, el análisis crítico de supuestos prácticos y normativa concreta, con utilización, en su caso, de los medios audiovisuales pertinentes, además del planteamiento de debates y seminarios que permitan la profundización en aspectos concretos de la asignatura.

6.1.- Distribución de metodologías docentes					
		Horas dirigidas por el profesor		Horas de trabajo autónomo	HORAS TOTALES
		Horas presenciales.	Horas no presenciales.		
Sesiones magistrales		18		15	33
Prácticas	- En aula	4		10	14
	- En el laboratorio				
	- En aula de informática				
	- De campo				
	- Otras (detallar)				
Seminarios					
Exposiciones y debates		2		5	7
Tutorías		2		3	5
Actividades de seguimiento online		2		2	4
Preparación de trabajos					
Otras actividades (detallar)					
Exámenes					
TOTAL		**30**		**45**	**75**

7.- Recursos, bibliografía, referencias electrónicas o de otro tipo

- BUENO DE MATA, Federico. *Prueba electrónica y proceso 2.0: especial referencia al proceso civil*. Valencia: Tirant lo Blanch, 2014.
- BUJOSA VADELL, Lorenzo Mateo. “La valoración de la prueba electrónica.” En *Fodertics 3.0: Estudios sobre derecho y nuevas tecnologías*, coordinado por Federico BUENO DE MATA, 75–85. Granada: Comares, 2015.
- BUJOSA VADELL, Lorenzo Mateo. “La prueba digital producto de la vigilancia secreta: obtención, admisibilidad y valoración en el proceso penal en España y Colombia.” *Revista Brasileira de Direito Processual Penal* 7, no. 2 (2021): 1347–84.
- BUENO DE MATA, Federico, y LORENZO BUJOSA VADELL. *La prueba electrónica en el marco de una administración de justicia informatizada: especial referencia al proceso civil*. Tesis doctoral, Universidad de Salamanca, 2013.
- DELGADO MARTÍN, Joaquín. *Investigación tecnológica y prueba digital en todas las jurisdicciones*. Madrid: La Ley, 2.ª ed., 2018.
- DELGADO MARTÍN, Joaquín. “La prueba electrónica en el proceso penal.” *Diario La Ley*, nº 8167 (10 Octubre 2013): doctrina jurídica especializada
- PINTO PALACIOS, Fernando, y Purificación PUJOL CAPILLA. *La prueba en la era digital*. Madrid: La Ley, 2017.
- PICÓ I JUNOY, Joan, y Xavier ABEL LLUCH, eds. *La prueba electrónica*. Barcelona: J. M. Bosch Editor, 2011.

8.- Evaluación

8.1: Criterios de evaluación: La nota final corresponderá a:

- 70% Evaluación Final. Simulación de un caso práctico a repartir el primer día de clase (Por parejas o individual en función del número de estudiantes matriculados)
- 30% Realización de prácticas por parte del alumnado de manera presencial en clase.

Para poder acudir a la CONVOCATORIA ORDINARIA deberá superarse la parte práctica de la asignatura.

8.2: Sistemas de evaluación:

- Participar en las clases prácticas y aprobar al menos el 50% de los casos prácticos. La nota media de las prácticas se corresponde con el 30% de la nota de la asignatura
- Intervenir en las clases teóricas.
- Prueba final. Simulación de un caso práctico sobre los contenidos teóricos de la asignatura. La nota se corresponde con el 70% de la nota de la asignatura.

8.3: Consideraciones generales y recomendaciones para la evaluación y la recuperación:
A lo largo del curso se llevará a cabo un seguimiento y evaluación de las actividades presenciales y no presenciales.

Se realizará la parte de exposición y un examen práctico. La consideración global de ambas partes determinará la calificación final de la asignatura.

9.- Organización docente semanal

AUDITORÍA Y HERRAMIENTAS DE SEGURIDAD INFORMÁTICA BASADAS EN IA

1.- Datos de la Asignatura

Código	306.580	Plan	2025	ECTS	3
Carácter	Obligatoria de especialidad	Curso	1º	Periodicidad	2º Semestre
Idioma de impartición asignatura		Español			
Área	Ciencia de la Computación e Inteligencia Artificial				
Departamento	Informática y Automática				
Plataforma virtual	Studium https://moodle.usal.es				

1.1.- Datos del profesorado*

Profesor Coordinador	Guillermo Hernández González	Grupo / s	1
Departamento	Informática y Automática		
Área	Ciencia de la Computación e Inteligencia Artificial		
Centro	Facultad de Ciencias		
Despacho	F3013		
Horario de tutorías	Solicitar por correo electrónico		
URL Web	https://produccioncientifica.usal.es/investigadores/147991/detalle		
E-mail	guillehg@usal.es	Teléfono	923 294 500 Ext. 6059

2.- Recomendaciones previas

- Uso básico de herramientas informáticas: Familiaridad con el uso de sistemas operativos y software básico como editores de texto, terminal, y plataformas en la nube.

- **Conceptos básicos de seguridad informática**: Comprensión de principios fundamentales de la seguridad informática (por ejemplo, autenticación, criptografía, firewalls). Herramientas que generan datos con los que pretenden trabajar las herramientas de IA.

- Conocimientos básicos de programación: Es positivo contar con familiaridad con un lenguaje de programación (preferentemente Python, que es ampliamente usado en IA y ciberseguridad), aunque no será necesario para la asignatura.

3.- Objetivos de la asignatura

- Conocer los conceptos fundamentales de la inteligencia artificial y sus posibilidades de aplicación relacionadas con la auditoría y con las herramientas de seguridad informática.
- Conocer las técnicas principales de los paradigmas de aprendizaje supervisado y no supervisado, así como ser capaz de seleccionar las más adecuadas para un escenario.
- Conocer las metodologías para el entrenamiento y evaluación de los modelos de aprendizaje automático, así como las dificultades más frecuentes que pueden aparecer en este proceso.
- Entrenar y evaluar modelos sencillos que utilicen técnicas de aprendizaje supervisado y no supervisado.

4.- Competencias a adquirir / Resultados de aprendizaje

Resultados de aprendizaje

4.1: Conocimientos:

C1. Defender las bases conceptuales de la ciberdelincuencia, ciberamenazas y la seguridad informática

C2. Examinar el funcionamiento de las tecnologías disruptivas utilizadas por delincuentes y por profesionales que actúan ante la cibercriminalidad, así como los principios básicos de ciberespacio

C4. Evaluar las herramientas técnicas y legales necesarias para analizar y hacer frente a diferentes riesgos, ciberamenazas y ciberdelitos.

C8. E1 Seleccionar conocimientos jurídicos especializados de los diferentes tipos de ciberdelincuencia para poder asesorar a los profesionales que intervienen en el proceso penal, así como a otras instituciones públicas o privadas

4.2: Habilidades:

H1. Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales

H3. Practicar con pericia la búsqueda de legislación y jurisprudencia a través de diferentes técnicas que puedan favorecer la investigación, la prueba y la intervención ante ciberdelitos.

H5. Aplicar con dominio la normativa nacional e internacional que regula la ciberdelincuencia, así como su persecución, investigación y represión en casos concretos.

H7. E1 Ante casos específicos de ciberdelincuencia, elaborar, exponer y defender una solución jurídicamente fundamentada y adecuada al caso, de la que se deriven actuaciones concretas ante el delito.

H8. E1 Argumentar los derechos, garantías y principios que deben primar en atención al tipo delictivo concreto, así como las autoridades competentes para la práctica de diferentes funciones

4.3: Competencias:

K2. Aprender a actualizar de modo autónomo los conocimientos sobre las últimas tecnologías y herramientas de seguridad informática

K3. Analizar pormenorizadamente cada ciberdelito, incluyendo perfiles diferenciados de víctimas y agresores en el uso de la tecnología cibernética

K5. En casos de cibercriminalidad, redactar textos legales para los diferentes momentos procesales y desde el punto de vistas de diferentes profesiones implicadas, y que estos textos sean comprensibles tanto para un público especialista como para un público profano

K6. Discriminar las funciones de cada una de las autoridades y profesionales que intervienen en casos de ciberdelincuencia, identificando los requisitos formales que van ligados a todas ellas para poder poner en práctica las mismas

K7. E1 Seleccionar los conocimientos específicos y cualidades más idóneos necesarios para garantizar y salvaguardar los derechos y principios jurídicos que favorezcan la intervención eficaz de diferentes autoridades en casos de ciberdelincuencia nacional e internacional.

K8. E1 Realizar análisis críticos, auditorías y asesoramiento jurídico ante ciberamenazas, ciberataques u otro tipo de riesgos detectados

5.- Contenidos (temario)

Contenido teórico:

1. **Inteligencia artificial y principales paradigmas**
2. **Métodos de aprendizaje no supervisado**
   - Clustering
   - Reglas de asociación
   - Detección de anomalías
3. **Métodos de aprendizaje supervisado**
   - Clasificación
   - Regresión
   - Metodología de evaluación
   - Métodos de aprendizaje supervisado
   - Métodos de ensamble

Contenido práctico:

Utilización de herramientas de inteligencia artificial para el aprendizaje supervisado y no supervisado.

6.- Metodologías docentes

- Sesiones magistrales con apoyo de material audiovisual, en las que se desarrollará el contenido teórico de la asignatura. Se motivará a los alumnos a intervenir durante estas exposiciones para dinamizar y favorecer el aprendizaje.
- Prácticas en el aula, en las que se desarrollará el contenido práctico necesario para la realización del trabajo.
- Preparación del trabajo de la asignatura, relacionado principalmente con el contenido práctico, asistido de manera no presencial por el profesorado.
- Examen de la asignatura, relacionado con el contenido teórico.

6.1.- Distribución de metodologías docentes

		Horas dirigidas por el profesor		Horas de trabajo autónomo	HORAS TOTALES
		Horas presenciales.	Horas no presenciales.		
Sesiones magistrales		12		20	32
Prácticas	- En aula	12		25	37
	- En el laboratorio				
	- En aula de informática				
	- De campo				
	- Otras (detallar)				
Seminarios					
Exposiciones y debates					
Tutorías		4			4
Actividades de seguimiento online					
Preparación de trabajos					
Otras actividades (detallar)					
Exámenes		2			2
TOTAL		**30**		**45**	**75**

7.- Recursos, bibliografía, referencias electrónicas o de otro tipo

P. Norvig, S. Russell. Inteligencia Artificial: Un enfoque moderno. Pearson, 2004.

T. Hastie, R. Tibshirani, J. Friedman. The Elements of Statistical Learning: Data Mining, Inference, and Prediction. Springer, 2009.

A. Geron. Aprende Machine Learning con Scikit-Learn, Keras y Tensorflow. O'Reilly-Anaya, 2020.

Documentación de Orange Data Mining, disponible en https://orangedatamining.com/docs/.

8.- Evaluación

8.1: Criterios de evaluación:
La adquisición de los resultados de aprendizaje se evaluará mediante un examen escrito, centrado en los contenidos teóricos, y un trabajo escrito, centrado en los contenidos prácticos. En el examen se valorará el número de aciertos en el caso de preguntas de opción cerrada y la corrección, claridad y pertinencia en el caso de otro tipo de preguntas. En el trabajo escrito se valorará la corrección, pertinencia, claridad y originalidad.

8.2: Sistemas de evaluación:
La calificación global de la asignatura se obtendrá mediante dos componentes:
Examen sobre el contenido teórico: 50 %
Trabajo sobre el contenido práctico: 50 %

En caso de que la calificación en **alguna de estas dos componentes sea inferior a 3** (sobre 10) la **calificación final de la asignatura no superará dicho umbral** (por ejemplo, con un 10 en el trabajo y un 2.9 en el examen, la calificación final será de 3.0).

8.3: Consideraciones generales y recomendaciones para la evaluación y la recuperación:
Los contenidos teóricos ayudan a la adquisición de las competencias prácticas y su demostración en el trabajo, por lo que se recomienda tener estos presentes en su elaboración. Se recomienda también la atención activa y la intervención en las clases para su aprovechamiento.

En la recuperación, podrán recuperarse las componentes suspensas en condiciones análogas. En los casos en que proceda la recuperación del trabajo escrito se podrá mejorar la entrega anterior.

9.- Organización docente semanal

CIBERDELINCUENCIA Y DERECHO PENAL

1.- Datos de la Asignatura					
Código	306571	Plan	2025	ECTS	6
Carácter	Obligatoria	Curso	1º	Periodicidad	1er Semestre
Idioma de impartición asignatura		Español			
Área	Derecho Penal				
Departamento	Derecho Público General				
Plataforma virtual	Studium https://moodle.usal.es				

1.1.- Datos del profesorado*			
Profesor Coordinador	Miriam Ruiz Arias	Grupo / s	Único
Departamento	Derecho Público General		
Área	Derecho Penal		
Centro	Facultad de Derecho		
Despacho	276		
Horario de tutorías	Jueves de 18.00 a 20.00. Escribir por email previamente para concertar cita		
URL Web	*https://produccioncientifica.usal.es/investigadores/157298/detalle*		
E-mail	miriam.ruiz@usal.es	Teléfono	923294500 Ext. 1621
Profesor Coordinador	María Luz Gutiérrez Francés	Grupo / s	Único
Departamento	Derecho Público General		
Área	Derecho Penal		
Centro	Facultad de Derecho		
Despacho	278		
Horario de tutorías	Lunes 14.30 a 18.30. Escribir por email previamente para concertar cita		
URL Web	*https://produccioncientifica.usal.es/investigadores/56906/detalle*		
E-mail	mgf@usal.es	Teléfono	+34 923 29 45 00 ext. 6958
Profesor Coordinador	Pendiente de asignar	Grupo / s	
Departamento			
Área			
Centro			
Despacho			

Horario de tutorías			
URL Web			
E-mail		Teléfono	

2.- Recomendaciones previas

Se requiere haber cursado y haber aprobado las siguientes asignaturas: Introducción al Derecho Penal, Teoría del delito y Derecho Penal. Parte Especial.

3.- Objetivos de la asignatura

El/la estudiante, al finalizar esta asignatura, será capaz de:
-Adquirir un conocimiento profundo y avanzado del marco teórico y la normativa internacional, europea penal de los ciberdelitos.
-Analizar críticamente los diferentes tipos de cibercrimen: elementos objetivos y subjetivos del tipo penal, autoría y participación y culpabilidad, etc.
-Analizar de manera crítica la legislación y la jurisprudencia nacional respectos a los ciberdelitos que se estudian.

4.- Competencias a adquirir / Resultados de aprendizaje

Resultados de aprendizaje *Complete esta columna si su titulación ha sido adaptada al RD822/2021*

4.1: Conocimientos: C1. Defender las bases conceptuales de la ciberdelincuencia, ciber amenazas y la seguridad informática.
C3. Identificar de forma exhaustiva el funcionamiento de los diferentes tipos de cibercrimen; modus operandi, autoría, víctimas, tecnología empleada.
C7. Contrastar la jurisprudencia estatal y supranacional en materia de ciberdelincuencia e investigación tecnológica.

4.2: Habilidades: H1. Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales.
H3. Practicar con pericia la búsqueda de legislación y jurisprudencia a través de diferentes técnicas que puedan favorecer la investigación, la prueba y la intervención ante ciberdelitos.
H5. Aplicar con dominio la normativa nacional e internacional que regula la ciberdelincuencia, así como su persecución, investigación y represión en casos concretos.
H6. Concluir las cuestiones jurídicas más relevantes implicadas en un conjunto complejo de hechos relacionados con casos de cibercriminalidad.

4.3: Competencias: K1. Discriminar los tipos de ciberdelito, comprendiendo los nuevos espacios virtuales y, en atención a ellos, aplicar la normativa vigente y las resoluciones jurisprudenciales vinculantes en cada caso en cuestión.
K3. Analizar pormenorizadamente cada ciberdelito, incluyendo perfiles diferenciados de víctimas y agresores en el uso de la tecnología cibernética
K4. Aplicar el ordenamiento jurídico español y la normativa internacional, con todas las garantías, ante riesgos, amenazas y ciberdelitos concretos.
K5. En casos de cibercriminalidad, redactar textos legales para los diferentes momentos procesales y desde el punto de vistas de diferentes profesiones implicadas, y que estos textos sean comprensibles tanto para un público especialista como para un público profano.
K6. Discriminar las funciones de cada una de las autoridades y profesionales que intervienen en casos de ciberdelincuencia, identificando los requisitos formales que van ligados a todas ellas para poder poner en práctica las mismas.

5.- Contenidos (temario)

Bloque General
Tema 1 Evolución del fenómeno del cibercrimen y estudio del concepto además de la categorización desde la criminología.
Tema 2 Convenios internacionales (Convenio de Budapest), europeos (Directivas y Reglamentos) además de programas (internacionales y europeos)

Bloque Específico
Tema 3 Ciberataques puros: Hacking (uso ilegal de redes y sistemas) y daños informáticos (arts. 264 y ss CP español).
Tema 4 Ciberataques réplica: ciber fraudes (colectivos o estafas a los consumidores, arts. 249, 284, entre otros del CP español) y delitos contra la libertad individual, privacidad e intimidad (Arts. 197 y ss. CP español)
Tema 5 Ciberataques de contenido: ciberpiratería intelectual (Arts. 270 y ss. CP español) y ciberterrorismo.

6.- Metodologías docentes

En el desarrollo de la asignatura se compatibilizarán diversas metodologías. Así, se empleará la clase magistral durante las sesiones teóricas, que se compatibilizará con otras estrategias metodológicas, tales como el análisis y la discusión de textos legislativos y/o jurisprudenciales, así como, el análisis crítico de artículos doctrinales y normativa concreta, con utilización, en su caso, de los medios audiovisuales pertinentes.

Las tutorías se basarán en la orientación personal sobre la asignatura a los alumnos.

6.1.- Distribución de metodologías docentes

		Horas dirigidas por el profesor		Horas de trabajo autónomo	HORAS TOTALES
		Horas presenciales.	Horas no presenciales.		
Sesiones magistrales		38		36	74
Prácticas	- En aula	8		4	12
	- En el laboratorio				
	- En aula de informática				
	- De campo				
	- Otras (detallar)				
Seminarios		2			2
Exposiciones y debates		6		8	14
Tutorías		2			2
Actividades de seguimiento online					
Preparación de trabajos					
Otras actividades (detallar)					
Exámenes		4		42	46
TOTAL		**60**		**90**	**150**

7.- Recursos, bibliografía, referencias electrónicas o de otro tipo

- Almenar Pineda, Francisco. Ciberdelincuencia. Porto: Editorial Juruá, 2018.
- Anguita Osuna, J. E. (2018). Análisis histórico-jurídico de la lucha contra la ciberdelincuencia en la Unión Europea.
- Atienza, G. M., & Bermejo, D. F. (2020). Ciberdelitos. Ediciones Experiencia.
- Bustos Rubio, M. (2023). La reforma de la ciberestafa y la incorporación de los medios de

pago digitales en el Código Penal.
- Castaño, E. N. (2022). La relevancia penal de las nuevas tecnologias y su incidencia en los denominados ciberdelitos: especial referencia a los delitos contra la intimidad. Revista General de Derecho Penal, 37.
- Fernández Bermejo, Daniel, y Gorgonio Martínez Atienza. Ciberdelitos. 1st ed. Barcelona: Ediciones Experiencia, 2020.
- Gómez Hervás, Nuria del Carmen. Normativa de ciberseguridad. 1st ed. Paracuellos de Jarama, Madrid: Ra-Ma, 2021.
- Ignacio Lledó Benito. «CIBERSEGURIDAD VERSUS CIBERDELINCUENCIA». El derecho penal, robots, IA y cibercriminalidad: desafíos éticos y jurídicos. ¿Hacia una distopía?. 1.a, 2/22/22 ed. Dykinson, 2022. 17-.
- Lledó Benito, Ignacio et al. «Visión del derecho penal en relación con la robótica, IA y la ciberdelincuencia». La robótica y la inteligencia artificial en la nueva era de la revolución industrial 4.0. Los desafíos jurídicos, éticos y tecnológicos de los robots inteligentes. 1.a, 8/24/21 ed. Madrid: Dykinson, 2021. 149-196.
- Lledó Benito, Ignacio. El derecho penal, robots, IA y cibercriminalidad : desafíos éticos y jurídicos : ¿hacia una distopía? 1st ed. Madrid, Spain: Editorial Dykinson, 2022.
- Miró Llinares, F. (2012). El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio.
- Muñoz, A. G. (2020). Los ciberdelitos en el ordenamiento español. Editorial UOC.
- Peña Labrin, Daniel Ernesto. «Ciberdelitos y criminalidad informática: Rol de la prevención en la expansión de la ciberdelincuencia». Informática y Derecho: Revista Iberoamericana de Derecho Informático 13 (2023): 57-72.
- Perrino Pérez, Ángel Luis. El derecho penal y las nuevas tecnologías : (aspectos sustantivos y procesales de la ciberdelincuencia). Primera edición: junio de 2024. Córdoba: CUNIEP Editorial, 2024.

Jurisprudencia del Tribunal Europeo de Derechos Humanso, Tribunal de Justicia de la Unión Europea además de Tribunal Supremo (sala segunda) y Audiencias Provinciales en España.

8.- Evaluación

8.1: Criterios de evaluación:
LA ASISTENCIA A LAS CLASES ES OBLIGATORIA**.**

8.2: Sistemas de evaluación:
Parte Práctica 40%. Se ajustará y dividirá en los siguientes métodos de evaluación:
a) Entrega de trabajos individuales: realización de casos, problemas o ejercicios prácticos en el aula, ya sea a través de las TIC, utilizando medidas en el medio offline o el aula invertida. 25% sobre 10 puntos.
b) Exposición de trabajos y/o presentaciones, resultado de trabajos de investigación. 15% sobre 10 puntos.

Parte teórica 60%. La evaluación consistirá en un examen teórico-práctico de preguntas desarrollo y/o preguntas cortas que se celebrará en el periodo de exámenes fijado por calendario académico, en virtud del cual se debe contestar de forma completa y adecuada el número de preguntas fijado sobre cualquiera de los temas estudiados en el temario impartido durante todo el semestre. Es necesario obtener un MÍNIMO DE 3/6 puntos EN EL EXAMEN PARA AÑADIR LOS OTROS CUATRO PUNTOS.

8.3: Consideraciones generales y recomendaciones para la evaluación y la recuperación:
Asistir a las clases teóricas para comprender los contenidos de la asignatura y realizar el examen además de las diferentes pruebas de la evaluación continua.
Se valorará la corrección jurídico-conceptual de las pruebas escritas y la entrega dentro del plazo preestablecido de las tareas encomendadas. Complementariamente, se apreciará la corrección lingüística, tanto ortográfica como gramatical y semántica.
En las exposiciones se valorará también el uso de lenguaje técnico y la claridad y sistematización de la presentación de las ideas.

Los estudiantes deben tener presente que la calificación de la asignatura depende de una combinación de elementos de evaluación continuada (entrega y exposición de trabajos individuales) y de un examen final (contenidos teóricos-prácticos).

Debido a su propia naturaleza, la evaluación continuada no es recuperable, dado que depende del trabajo permanente del alumno a lo largo de la asignatura. Por ello, los profesores establecerán con la suficiente antelación un plan de actividades que permita a los estudiantes planificar su participación, y se establecerán plazos y procedimientos lo suficientemente flexibles como para que todos los estudiantes dispongan de la oportunidad de realizar las tareas que se les encomienden.

En segunda convocatoria sólo será recuperable la nota del examen teórico-práctico (60%). En consecuencia, para aprobar la asignatura, los estudiantes deben tener presente que pueden necesitar más de un 50% de la nota del examen teórico-práctico si la nota de la entrega y exposición de trabajos es insuficiente, de modo que con el examen puedan compensarla.

Está terminante prohibido el plagio y el uso de inteligencia artificial o cualquier artificio semejante que haga que el examen o cualquiera de las pruebas durante el semestre no sea autoría del alumnado que lo presente.

9.- Organización docente semanal

Ciberperfilación criminológica

1.- Datos de la Asignatura					
Código	306.573	Plan	2025	ECTS	6
Carácter	Obligatoria	Curso	1º	Periodicidad	1er semestre
Idioma de impartición asignatura		español			
Área	Personalidad, Evaluación y Tratamiento Psicológicos				
Departamento	Personalidad, Evaluación y Tratamiento Psicológicos				
Plataforma virtual	Studium https://moodle.usal.es				

1.1.- Datos del profesorado*			
Profesor Coordinador	Luis Miguel Sánchez Gil	Grupo / s	
Departamento	Personalidad, Evaluación y Tratamiento Psicológicos		
Área	Personalidad, Evaluación y Tratamiento Psicológicos		
Centro	Facultad de Derecho		
Despacho	153		
Horario de tutorías	Previa consulta con el profesor		
URL Web	*https://produccioncientifica.usal.es/investigadores/262750/detalle*		
E-mail	lsangil@usal.es	Teléfono	611 84 51 84

2.- Recomendaciones previas

Se recomienda poseer conocimientos básicos en materia de perfilación criminológica y sobre las dinámicas de las redes sociales cibernéticas más utilizadas

3.- Objetivos de la asignatura

1. Comprender las técnicas de ciberperfilación criminal y su aplicación
2. Adquirir capacidades para el ciberperfilado criminal
3. Conocer los perfiles criminológicos vinculados a las distintas formas de cibercriminalidad

4.- Competencias a adquirir / Resultados de aprendizaje

Resultados de aprendizaje

4.1: Conocimientos:
C1. Defender las bases conceptuales de la ciberdelincuencia, ciberamenazas y la seguridad informática
C2. Examinar el funcionamiento de las tecnologías disruptivas utilizadas por delincuentes y por profesionales que actúan ante la cibercriminalidad, así como los principios básicos de ciberespacio
C3. Identificar de forma exhaustiva el funcionamiento de los diferentes tipos de cibercrimen; modus operandi, autoría, víctimas, tecnología empleada.
C6. Discriminar, por un lado, las particularidades de las personas víctimas de las actividades ilícitas que llevan a cabo los criminales utilizando tecnologías de la información y las comunicaciones; y, por otro, las necesidades de intervención que se derivan tras estos delitos.

4.2: Habilidades:
H1. Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales
H4. Evaluar la viabilidad de diferentes herramientas y medidas de investigación en atención al tipo de delictivo presentado, las autoridades involucradas y el momento procesal del caso.
H5. Aplicar con dominio la normativa nacional e internacional que regula la ciberdelincuencia, así como su persecución, investigación y represión en casos concretos.
H6. Concluir las cuestiones jurídicas más relevantes implicadas en un conjunto complejo de hechos relacionados con casos de cibercriminalidad

4.3: Competencias:
K1. Discriminar los tipos de ciberdelito, comprendiendo los nuevos espacios virtuales y, en atención a ellos, aplicar la normativa vigente y las resoluciones jurisprudenciales vinculantes en cada caso en cuestión
K3. Analizar pormenorizadamente cada ciberdelito, incluyendo perfiles diferenciados de víctimas y agresores en el uso de la tecnología cibernética K5. En casos de cibercriminalidad, redactar textos legales para los diferentes momentos procesales y desde el punto de vistas de diferentes profesiones implicadas, y que estos textos sean comprensibles tanto para un público especialista como para un público profano

5.- Contenidos (temario)

Parte 1. Aspectos generales

1. Criminal, víctima y delito como objetos de estudio
2. Conceptos básicos para el ciberperfilado criminológico
3. Análisis criminológico del contexto
4. Herramientas e intrumentos básicos

Parte 2. Ciberperfilado criminológico en formas específicas de criminalidad

1. Ciberperfilado criminológico en los ciberataques puros
    a. Perfil del criminal
    b. Perfil de la víctima
2. Ciberperfilado criminológico en los ciberataques de replica
    a. Perfil del criminal
    b. Perfil de la víctima
3. Criberperfilado en los ciberataques de contenido
    a. Perfil del criminal
    b. Perfil de la víctima
4. Ciberperfilado criminológico como complemento a los análisis de la criminalidad estructurada

6.- Metodologías docentes

Sesiones magistrales: exposición de los contenidos de la asignatura.
Prácticas en aula: formulación, análisis, resolución y debate de un problema o ejercicio, relacionado con la temática de la asignatura.
Seminarios: trabajo en profundidad sobre un tema. Ampliación de contenidos de sesiones magistrales.
Exposiciones y debates: presentación oral de un tema o trabajo.
Tutorías: tiempo para atender y resolver dudas.
Preparación de trabajos: preparación de trabajos. Exámenes:
pruebas de evaluación.

6.1.- Distribución de metodologías docentes

		Horas dirigidas por el profesor		Horas de trabajo autónomo	HORAS TOTALES
		Horas presenciales.	Horas no presenciales.		
Sesiones magistrales		30		20	50
Prácticas	- En aula	12		18	30
	- En el laboratorio				

	- En aula de informática				
	- De campo				
	- Otras (detallar)				
Seminarios		4			4
Exposiciones y debates		4		6	10
Tutorías		4			4
Actividades de seguimiento online					
Preparación de trabajos		4		6	10
Otras actividades (detallar)					
Exámenes		2		40	42
TOTAL		**60**		**90**	**150**

7.- Recursos, bibliografía, referencias electrónicas o de otro tipo

Brezo Fernández, F. y Rubio Viñuela, Y. (2019). *Manual de ciberinvestigación en fuentes abiertas. OSINT para analistas*.
Heuer Jr., R. J. y Pherson, R. H. (2015). *Técnicas Analísticas Estructuradas para el análisis de inteligencia*. Plaza y Valdés.

8.- Evaluación

8.1: Criterios de evaluación:

Se seguirá un sistema de evaluación continua, sustentado en los siguientes porcentajes y criterios generales:

A) 40% de la calificación se referirá a actividades prácticas desarrolladas a lo largo del curso (exposiciones, análisis de artículos doctrinales, supuestos prácticos, ensayos, comentarios críticos…). Todas ellas relacionadas con los contenidos teóricos expuestos durante las clases teóricas.
B) 60% de la calificación será un examen escrito final realizado en el aula. La modalidad de examen será:
   1) Desarrollo breve: 3 preguntas de desarrollo breve sobre conceptos básicos de la asignatura (6/10 puntos).
   2) Tipo test: 40 preguntas tipo test, con niveles variables de dificultad sobre aspectos generales, detallados y profundos de la asignatura (4/10).

Cada parte (A y B) deberá ser superada de forma individualizada con la calificación mínima de 5 sobre 10. En el caso de que alguna de las partes no se supere, esta fijará la calificación final de la asignatura.
La calificación final de la asignatura, superadas con éxito ambas partes (A y B), resultará de la suma ponderada de sus calificaciones.

8.2: Sistemas de evaluación:

- Prácticas evaluables.
- Asistencia a sesiones presenciales y seminarios.
- Examen final.

8.3: Consideraciones generales y recomendaciones para la evaluación y la recuperación:

- Participación en las sesiones presenciales: favorecerá la adquisición de conocimientos teóricoprácticos y se valorará positivamente para la evaluación.
- Trasladar las cuestiones y dudas sobre el contenido a través de las sesiones de tutoría.
- Estudiar contenidos teóricos y prácticos para la superación del examen final.
- Asistir a la consulta de los resultados del examen ordinario, en aquellos supuestos en que el estudiante no haya superado los mínimos requeridos. El objeto es poder determinar los principales puntos débiles detectados y planificar las estrategias para superar el examen en posteriores convocatorias.
- En la recuperación se mantendrán los porcentajes asignados para las prácticas y el examen. Se preservará la calificación de la parte superada y se podrá recuperar la restante a través de la correspondiente actividad establecida a tal fin.

9.- Organización docente semanal

Victimización de mujeres y menores en Internet: cuestiones penales

1.- Datos de la Asignatura					
Código	306.576	Plan	2025	ECTS	3
Carácter	Obligatoria de especialidad	Curso	1º	Periodicidad	2do Semestre
Idioma de impartición asignatura		español			
Área	DERECHO PENAL				
Departamento	DERECHO PÚBLICO GENERAL				
Plataforma virtual	Studium https://moodle.usal.es				

1.1.- Datos del profesorado*			
Profesor Coordinador	Lina Mariola Díaz Cortés	Grupo / s	
Departamento	Derecho Público General		
Área	Derecho penal		
Centro	Facultad de Derecho		
Despacho	231		
Horario de tutorías	Lunes de 12:00 a 14:00		
URL Web	*INDIQUE AQUÍ PREFERENTEMENTE EL ENLACE A SU PERFIL EN EL PORTAL DE PRODUCCIÓN CIENTÍFICA DE LA USAL https://produccioncientifica.usal.es/investigadores*		
E-mail		Teléfono	
Profesor Coordinador	María Concepción Gorjón Barranco	Grupo / s	
Departamento	Derecho Público General		
Área	Derecho penal		
Centro	Facultad de Derecho		
Despacho	277		
Horario de tutorías	Lunes de 9 a 11 h		
URL Web	*https://produccioncientifica.usal.es/investigadores/57491/detalle*		
E-mail	mcgb@usal.es	Teléfono	

*Replique esta tabla por cada profesor/a que imparte la asignatura

2.- Recomendaciones previas
No existen

3.- Objetivos de la asignatura

- Estudiar la cibervictimización de menores y mujeres en internet

Resultados de aprendizaje:

4.1: Conocimientos:

C1. Defender las bases conceptuales de la ciberdelincuencia, ciberamenazas y la seguridad informática

C3. Identificar de forma exhaustiva el funcionamiento de los diferentes tipos de cibercrimen; modus operandi, autoría, víctimas, tecnología empleada.

C6. Discriminar, por un lado, las particularidades de las personas víctimas de las actividades ilícitas que llevan a cabo los criminales utilizando tecnologías de la información y las comunicaciones; y, por otro, las necesidades de intervención que se derivan tras estos delitos.

C7. Contrastar la jurisprudencia estatal y supranacional en materia de ciberdelincuencia e investigación tecnológica

Especialidad en aspectos jurídicos de la cibercriminalidad[1]:

C8. E1 Seleccionar conocimientos jurídicos especializados de los diferentes tipos de ciberdelincuencia para poder asesorar a los profesionales que intervienen en el proceso penal, así como a otras instituciones públicas o privadas**.**

4.2: Habilidades:

H1. Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales

H3. Practicar con pericia la búsqueda de legislación y jurisprudencia a través de diferentes técnicas que puedan favorecer la investigación, la prueba y la intervención ante ciberdelitos.

H5. Aplicar con dominio la normativa nacional e internacional que regula la ciberdelincuencia, así como su persecución, investigación y represión en casos concretos.

H6. Concluir las cuestiones jurídicas más relevantes implicadas en un conjunto complejo de hechos relacionados con casos de cibercriminalidad.

H7. E1 Ante casos específicos de ciberdelincuencia, elaborar, exponer y defender una solución jurídicamente fundamentada y adecuada al caso, de la que se deriven actuaciones concretas ante el delito.

4.3: Competencias:

K1. Discriminar los tipos de ciberdelito, comprendiendo los nuevos espacios virtuales y, en atención a ellos, aplicar la normativa vigente y las resoluciones jurisprudenciales vinculantes en cada caso en cuestión

K3. Analizar pormenorizadamente cada ciberdelito, incluyendo perfiles diferenciados de víctimas y agresores en el uso de la tecnología cibernética

K5. En casos de cibercriminalidad, redactar textos legales para los diferentes momentos procesales y desde el punto de vistas de diferentes profesiones implicadas, y que estos textos sean comprensibles tanto para un público especialista como para un público profano

K6. Discriminar las funciones de cada una de las autoridades y profesionales que intervienen en casos de ciberdelincuencia, identificando los requisitos formales que van ligados a todas ellas para poder poner en práctica las mismas.

K7. E1 Seleccionar los conocimientos específicos y cualidades más idóneos necesarios para garantizar y salvaguardar los derechos y principios jurídicos que favorezcan la intervención eficaz de diferentes autoridades en casos de ciberdelincuencia nacional e internacional.

[1] En términos de codificación, "E1" es el código para las asignaturas de la Especialidad de "Aspectos jurídicos de la cibercriminalidad".

5.- Contenidos (temario)

BLOQUE I. VICTIMIZACIÓN DE MENORES EN INTERNET

1. Marco general. Ciber victimización menores.
    - 1.1. Contextualización
    - 1.2. Datos estadísticos
    - 1.3. Marco internacional:
        - 1.3.1. Marco Universal: Observación General 25/2021 Comité de los Derechos del Niño . Observación general núm. 25 (2021) relativa a los derechos de los niños en relación con el entorno digital.
        - 1.3.2. Marco Europeo: Recomendación (UE) 2024/1238 de la Comisión, de 23 de abril de 2024, sobre el desarrollo y el refuerzo de los sistemas integrados de protección de la infancia que redunden en el interés superior del niño.
    - 1.4. Marco legislativo nacional
        - 1.4.1. Ley Orgánica 8/ 2021. Ley Orgánica 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia.
        - 1.4.2. Proyecto 121/000052 de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales : aspectos generales.

2. Respuesta penal cibervictimización menores
    - 1.1. Delitos contra la libertad sexual:
        - 1.1.1. Agresiones sexuales online
        - 1.1.2. Online Child Grooming
        - 1.1.3. Pornografía infantil
    - 1.2. Delitos contra la intimidad. Especial referencia al sexting secundario.
    - 1.3. Delitos Digital *self harm*: la reforma de la LO 8 de 2021 .
    - 1.4. Nuevas propuestas de modificaciones Código Penal del Proyecto 121/000052 de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales.

BLOQUE II. VICTIMIZACIÓN DE MUJERES EN INTERNET

1. Marco general. Cibervictimización de mujeres
    - 1.1. Contextualización
    - 1.2. Datos estadísticos
    - 1.3. Marco internacional
        - 1.3.1. Especial consideración al Convenio del Consejo de Europa sobre prevención y lucha contra la violencia contra las mujeres y la violencia doméstica de 2011 (Convenio de Estambul)
        - 1.3.2. La Directiva (UE) 2024/1385 del Parlamento Europeo y del Consejo, de 14 de mayo de 2024, sobre la lucha contra la violencia contra las mujeres y la violencia doméstica.
    - 1.4. Marco legislativo nacional
        - 1.4.1. Estrategias
        - 1.4.2. Pacto de Estado contra la violencia de género
2. Respuesta penal cibervictimización de mujeres.
    - 1.1. Delitos contra la libertad sexual.
        - 1.1.1. Agresiones sexuales
        - 1.1.2. Fenómeno only fans: trata y prostitución en el ciberespacio
    - 1.2. Delitos contra la intimidad.
        - 1.2.1. Delitos de espionaje

1.2.2. Sexting secundario
1.3. Delitos contra la libertad: stalking
1.4. Delitos discriminatorios por razones de género: especial referencia al art. 510 CP

6.- Metodologías docentes

En el desarrollo de la asignatura se compatibilizarán diversas metodologías. Así, se empleará la clase magistral durante las sesiones teóricas, que se compatibilizará con diversas estrategias metodológicas, tales como el análisis y la discusión de textos legislativos y/o jurisprudenciales, y el análisis crítico de artículos doctrinales y normativa concreta, con utilización, en su caso, de los medios audiovisuales pertinentes.

Las tutorías se basarán en la orientación personal sobre la asignatura a l@s alumn@s

6.1.- Distribución de metodologías docentes

		Horas dirigidas por el profesor		Horas de trabajo autónomo	HORAS TOTALES
		Horas presenciales.	Horas no presenciales.		
Sesiones magistrales		24		5	29
Prácticas	- En aula				
	- En el laboratorio				
	- En aula de informática				
	- De campo				
	- Otras (detallar)				
Seminarios				8	8
Exposiciones y debates					
Tutorías		4			4
Actividades de seguimiento online					
Preparación de trabajos				4	4
Otras actividades (detallar)					
Exámenes		2		28	30
TOTAL		**30**		**45**	**75**

7.- Recursos, bibliografía, referencias electrónicas o de otro tipo

Se darán indicaciones al inicio del curso.

8.- Evaluación

8.1: Criterios de evaluación:

La evaluación consistirá en la realización de una prueba teórica y otra práctica que se preparará con los contenidos que se explicarán en las clases teóricas y el material que en cada uno de los bloques resulte de necesaria lectura.
Tomando en cuenta que es un Máster presencial, la asistencia a clase será controlada.

8.2: Sistemas de evaluación:

1. Trabajo/Prácticas: 4 puntos. Trabajo individual cuyas indicaciones serán dadas al inicio del curso. **La entrega de la prácticas es obligatoria** y se tomará en cuenta siempre y cuando el/la alumno/a supere el examen final. Práctica no presentada en el día señalado será evaluada con cero (0). Práctica en la que se detecte bibliografía falsa será valorada con 0.

2.Examen: prueba de conocimiento sobre contenidos teóricos: 6 puntos. Para superar la asignatura debe aprobarse esta parte. Solo una vez superado (3 puntos en adelante) se sumará la nota del trabajo práctico. El examen consistirá en preguntas tipo test y de desarrollo.

Ejemplo de la anterior valoración: tomando en cuenta que el examen se valora sobre 6.0, la práctica sobre 4.0 , el/la alumno/ que no presente la práctica tiene 0 en ésta, por lo cual para aprobar la asignatura deberá sacar 5.0 en el examen sobre 6.0.

8.3: Consideraciones generales y recomendaciones para la evaluación y la recuperación:

Se podrá recuperar la parte del examen pero no la del trabajo/práctica entregado/a.

9.- Organización docente semanal

COOPERACIÓN PROCESAL INTERNACIONAL EN MATERIA DE CIBERCRIMEN

1.- Datos de la Asignatura					
Código	306.579	Plan	2025	ECTS	3
Carácter	Obligatoria de especialidad	Curso	1º	Periodicidad	2º Semestre
Idioma de impartición asignatura		español			
Área	DERECHO PROCESAL				
Departamento	Derecho Administrativo, Financiero y Procesal				
Plataforma virtual	Studium https://moodle.usal.es				

1.1.- Datos del profesorado*			
Profesor Coordinador	Marta del Pozo Pérez	Grupo / s	Único
Departamento	Derecho Administrativo, Financiero y Procesal		
Área	Derecho Procesal		
Centro	Facultad de Derecho		
Despacho	284		
Horario de tutorías	Previa cita por correo electrónico		
URL Web	*https://produccioncientifica.usal.es/investigadores/56058/detalle*		
E-mail	tillo@usal.es	Teléfono	Ext. 6939
Profesor Coordinador	Alicia González Monje	Grupo / s	Único
Departamento	Derecho Administrativo, Financiero y Procesal		
Área	Derecho Procesal		
Centro	Facultad de Derecho		
Despacho	266		
Horario de tutorías	Previa cita por correo electrónico		
URL Web	*https://produccioncientifica.usal.es/investigadores/57155/detalle*		
E-mail	alicia.g.monje@usal.es	Teléfono	6101
Profesor Coordinador	Irene González Pulido	Grupo / s	Único
Departamento	Derecho Administrativo, Financiero y Procesal		
Área	Derecho Procesal		
Centro	Facultad de Derecho		
Despacho	283		
Horario de tutorías	Previa cita por correo electrónico		

URL Web	*https://produccioncientifica.usal.es/investigadores/148016/detalle*		
E-mail	irenegopu@usal.es	Teléfono	

*Replique esta tabla por cada profesor/a que imparte la asignatura

2.- Recomendaciones previas

Se recomienda conocimientos previos de Introducción al Derecho Procesal y Derecho Procesal Penal.

3.- Objetivos de la asignatura

- A partir de la transmisión de conocimiento teórico de esta materia proporcionar una comprensión activa sobre la relevancia y la función social de la Cooperación como sistema necesario de solución de conflictos surgidos en las relaciones sociales con componentes internacionales, comprender los conceptos fundamentales de la materia, conocer la especificidad de la metodología jurídica en esta materia, y proporcionar el conocimiento de las categorías e instituciones básicas de esta rama del conocimiento.
- A través de una adecuada y diversificada docencia práctica, potenciar en el estudiante una actitud más activa y autónoma, con la que pueda comprender las categorías e instituciones jurídicas en su aplicación práctica, y adquirir las formas de saber hacer, adecuadas a los modos y procedimientos de analizar y resolver supuestos en este campo del Derecho.

4.- Competencias a adquirir / Resultados de aprendizaje

Resultados de aprendizaje

4.1: Conocimientos:

C1. Defender las bases conceptuales de la ciberdelincuencia, ciberamenazas y la seguridad informática

C2. Examinar el funcionamiento de las tecnologías disruptivas utilizadas por delincuentes y por profesionales que actúan ante la cibercriminalidad, así como los principios básicos de ciberespacio

C4. Evaluar las herramientas técnicas y legales necesarias para analizar y hacer frente a diferentes riesgos, ciberamenazas y ciberdelitos.

C7. Contrastar la jurisprudencia estatal y supranacional en materia de ciberdelincuencia e investigación tecnológica

C8. E1 Seleccionar conocimientos jurídicos especializados de los diferentes tipos de ciberdelincuencia para poder asesorar a los profesionales que intervienen en el proceso penal, así como a otras instituciones públicas o privadas.

4.2: Habilidades:

H1. Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales

H3. Practicar con pericia la búsqueda de legislación y jurisprudencia a través de diferentes técnicas que puedan favorecer la investigación, la prueba y la intervención ante ciberdelitos.

H5. Aplicar con dominio la normativa nacional e internacional que regula la ciberdelincuencia, así como su persecución, investigación y represión en casos concretos.

H7. E1 Ante casos específicos de ciberdelincuencia, elaborar, exponer y defender una solución jurídicamente fundamentada y adecuada al caso, de la que se deriven actuaciones concretas ante el delito.

H8. E1 Argumentar los derechos, garantías y principios que deben primar en atención al tipo delictivo concreto, así como las autoridades competentes para la práctica de diferentes funciones

4.3: Competencias:

K1. Discriminar los tipos de ciberdelito, comprendiendo los nuevos espacios virtuales y, en

atención a ellos, aplicar la normativa vigente y las resoluciones jurisprudenciales vinculantes en cada caso en cuestión
K3. Analizar pormenorizadamente cada ciberdelito, incluyendo perfiles diferenciados de víctimas y agresores en el uso de la tecnología cibernética
K5. En casos de cibercriminalidad, redactar textos legales para los diferentes momentos procesales y desde el punto de vistas de diferentes profesiones implicadas, y que estos textos sean comprensibles tanto para un público especialista como para un público profano
K6. Discriminar las funciones de cada una de las autoridades y profesionales que intervienen en casos de ciberdelincuencia, identificando los requisitos formales que van ligados a todas ellas para poder poner en práctica las mismas
K7. E1 Seleccionar los conocimientos específicos y cualidades más idóneos necesarios para garantizar y salvaguardar los derechos y principios jurídicos que favorezcan la intervención eficaz de diferentes autoridades en casos de ciberdelincuencia nacional e internacional.
K8. E1 Realizar análisis críticos, auditorías y asesoramiento jurídico ante ciberamenazas, ciberataques u otro tipo de riesgos detectados

5.- Contenidos (temario)

I. Principios inspiradores de la cooperación procesal penal internacional.
II.- Diligencias de investigación y prueba transfronterizas
III.- La orden europea de detención y entrega.
IV.- La orden europea de investigación
V. Las órdenes europeas de producción y conservación de prueba electrónica en procesos penales

6.- Metodologías docentes

En el desarrollo de la asignatura se compatibilizarán diversas metodologías. Así, se empleará la clase magistral durante las sesiones teóricas, mientras que en las sesiones prácticas se utilizarán diversas estrategias metodológicas, tales como el análisis y la discusión de textos legislativos y/o jurisprudenciales, el análisis crítico de supuestos prácticos y normativa concreta, con utilización, en su caso, de los medios audiovisuales pertinentes, además del planteamiento de debates y seminarios que permitan la profundización en aspectos concretos de la asignatura.

6.1.- Distribución de metodologías docentes

		Horas dirigidas por el profesor		Horas de trabajo autónomo	HORAS TOTALES
		Horas presenciales.	Horas no presenciales.		
Sesiones magistrales		18		15	33
Prácticas	- En aula	4		10	14
	- En el laboratorio				
	- En aula de informática				
	- De campo				
	- Otras (detallar)				
Seminarios		2		5	7
Exposiciones y debates		2		3	5
Tutorías		2		2	4
Actividades de seguimiento online					
Preparación de trabajos					
Otras actividades (detallar)					
Exámenes		2		10	12
TOTAL		**30**		**45**	**75**

7.- Recursos, bibliografía, referencias electrónicas o de otro tipo

- GONZÁLEZ MONJE, A., *Cooperación jurídica internacional en materia penal e intervención de comunicaciones como técnica especial de investigación,* Comares, 2017.

- GRANDE-MARLASKA GÓMEZ, F. y POZO PÉREZ, M. DEL “La obtención de fuentes de prueba en la Unión Europea y su validez en el proceso penal español”, *Revista General de Derecho Europeo*, número 24, junio de 2011.
- POZO PÉREZ, M. DEL, "La entrega vigilada como técnica de investigación en el marco de la cooperación internacional", *Hacia un verdadero Espacio Judicial Europeo: Perspectivas para la construcción de un proceso penal europeo e instrumentos de cooperación policial y judicial en la Unión Europea*, COMARES, Granada, 2008, pp. 197-235
- POZO PÉREZ, M. DEL, “El agente encubierto como medio de investigación procesal en el ámbito de la cooperación jurídica internacional”, Constitución Europea: Aspectos Históricos, administrativos y procesales, TÓRCULO, Santiago de Compostela, 2006, 270-328.
- POZO PÉREZ, M. DEL, "La Orden Europea de detención y entrega: Un avance en el principio de reconocimiento mutuo de resoluciones judiciales entre los Estados de la Unión Europea", *Revista Jurídica LA LEY*, pp. 1-10, 2005.
- Atlas judicial europeo: https://e-justice.europa.eu/topics/trainings-judicial-networks-and-agencies/european-judicial-network-criminal-matters/judicial-atlas-criminal-matters_es
- Prontuario de Auxilio Judicial Internacional: https://www.prontuario.org/portal/site/prontuario
- Portal europeo e-Justicia: https://e-justice.europa.eu/home_es

8.- Evaluación

8.1: Criterios de evaluación:

Para poder superar la asignatura en la CONVOCATORIA ORDINARIA hay que:
1.- Participar en las clases prácticas y aprobar el 50% de las prácticas.
2.- Superar la prueba final oral de conocimientos teóricos.
La prueba final se hará al terminar el cuatrimestre y consistirá en una prueba oral de preguntas cortas sobre los contenidos teóricos de la asignatura.

8.2: Sistemas de evaluación:

Elementos Evaluables	**Valor con relación a la nota final (100%)**
Participar en las clases prácticas, y aprobar, al menos, el 50% de los casos prácticos	Hasta el 40%. Calculado en función de la nota media de las prácticas, así como de la participación en las clases prácticas
Prueba oral de preguntas cortas sobre los contenidos teóricos de la asignatura	Hasta el 60%. Calculado en función de la nota de la prueba oral

8.3: Consideraciones generales y recomendaciones para la evaluación y la recuperación:

Se deberá superar una prueba oral teórica y una escrita práctica que consistirá en:
1.- Una batería de preguntas cortas orales sobre los contenidos teóricos de la asignatura. (70% de la nota final)
2.- Un supuesto práctico. (30% de la nota final)
La nota final de la asignatura será la obtenida en ambas pruebas de acuerdo con el porcentaje establecido.

9.- Organización docente semanal

DERECHO PENAL Y CIBERDELINCUENCIA ECONÓMICA

1.- Datos de la Asignatura

Código	306577	Plan	2025	ECTS	3
Carácter	Obligatoria de especialidad	Curso	1º	Periodicidad	2do Semestre
Idioma de impartición asignatura		español			
Área	Derecho Penal				
Departamento	Derecho Público General				
Plataforma virtual	Studium https://moodle.usal.es				

1.1.- Datos del profesorado*

Profesor Coordinador	Javier Sánchez Bernal	Grupo / s	1
Departamento	Derecho Público General		
Área	Derecho Penal		
Centro	Facultad de Derecho		
Despacho	291		
Horario de tutorías	Contactar por email para concertar cita.		
URL Web	*https://produccioncientifica.usal.es/investigadores/57213/detalle*		
E-mail	jsbernal@usal.es.	Teléfono	923 29 45 00 Ext. 6976
Profesor	Julio Ballesteros Sánchez	Grupo / s	1
Departamento	Derecho Público General		
Área	Derecho Penal		
Centro	Facultad de Derecho		
Despacho	S-004		
Horario de tutorías	Contactar por email para concertar cita.		
URL Web	*https://produccioncientifica.usal.es/investigadores/107674/detalle*		
E-mail	jbs@usal.es	Teléfono	

2.- Recomendaciones previas

Se recomienda una aproximación a la asignatura a través de la lectura de la bibliografía recomendada.

3.- Objetivos de la asignatura

En lo referente a los resultados de aprendizaje, el/la estudiante, al finalizar esta asignatura, será capaz de:

- Conocer e identificar las bases conceptuales de la ciberdelincuencia económica y empresarial.
- Conocer los instrumentos jurídicos de que se sirve la Unión Europea y el Consejo de Europa en la lucha contra la cibercriminalidad económica.
- Identificar de forma exhaustiva el funcionamiento de los diferentes tipos de cibercrimen económico y empresarial, identificando los elementos típicos de las principales figuras delictivas en la materia.
- Identificar fortalezas y debilidades de la normativa española a través del estudio en clave de Derecho comparado.

4.- Competencias a adquirir / Resultados de aprendizaje

Resultados de aprendizaje

4.1: Conocimientos:

C1. Defender las bases conceptuales de la ciberdelincuencia, ciberamenazas y la seguridad informática

C3. Identificar de forma exhaustiva el funcionamiento de los diferentes tipos de cibercrimen; modus operandi, autoría, víctimas, tecnología empleada.

C5. Interpretar la normativa nacional e internacional que regula la ciberdelincuencia, así como las funciones de autoridades y profesionales en el marco de detección, prevención, actuación e intervención en casos de ciberdelincuencia.

C6. Discriminar, por un lado, las particularidades de las personas víctimas de las actividades ilícitas que llevan a cabo los criminales utilizando tecnologías de la información y las comunicaciones; y, por otro, las necesidades de intervención que se derivan tras estos delitos.

C7. Contrastar la jurisprudencia estatal y supranacional en materia de ciberdelincuencia e investigación tecnológica

C8. E1 Seleccionar conocimientos jurídicos especializados de los diferentes tipos de ciberdelincuencia para poder asesorar a los profesionales que intervienen en el proceso penal, así como a otras instituciones públicas o privadas.

4.2: Habilidades:

H1. Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales

H3. Practicar con pericia la búsqueda de legislación y jurisprudencia a través de diferentes técnicas que puedan favorecer la investigación, la prueba y la intervención ante ciberdelitos.

H5. Aplicar con dominio la normativa nacional e internacional que regula la ciberdelincuencia, así como su persecución, investigación y represión en casos concretos.

H6. Concluir las cuestiones jurídicas más relevantes implicadas en un conjunto complejo de hechos relacionados con casos de cibercriminalidad.

H7. E1 Ante casos específicos de ciberdelincuencia, elaborar, exponer y defender una solución jurídicamente fundamentada y adecuada al caso, de la que se deriven actuaciones concretas ante el delito.

4.3: Competencias:

K1. Discriminar los tipos de ciberdelito, comprendiendo los nuevos espacios virtuales y, en atención a ellos, aplicar la normativa vigente y las resoluciones jurisprudenciales vinculantes en cada caso en cuestión

K3. Analizar pormenorizadamente cada ciberdelito, incluyendo perfiles diferenciados de víctimas y agresores en el uso de la tecnología cibernética

K5. En casos de cibercriminalidad, redactar textos legales para los diferentes momentos procesales y desde el punto de vistas de diferentes profesiones implicadas, y que estos textos sean comprensibles tanto para un público especialista como para un público profano

K6. Discriminar las funciones de cada una de las autoridades y profesionales que intervienen en casos de ciberdelincuencia, identificando los requisitos formales que van ligados a todas ellas para poder poner en práctica las mismas

K7. E1. Seleccionar los conocimientos específicos y cualidades más idóneos necesarios para garantizar y salvaguardar los derechos y principios jurídicos que favorezcan la intervención eficaz

de diferentes autoridades en casos de ciberdelincuencia nacional e internacional.
K8. E1. Realizar análisis críticos, auditorías y asesoramiento jurídico ante ciberamenazas, ciberataques u otro tipo de riesgos detectados

5.- Contenidos (temario)

1. Análisis de documentos estratégicos en el ámbito tecnológico-empresarial.
2. Prevención de delitos en la empresa y tecnología. Normativa extrapenal y ciberseguridad.
3. La lucha contra la ciberdelincuencia económica en la Unión Europea y el Consejo de Europa.
4. Responsabilidad Penal de la Persona Jurídica y aspectos criminológicos de la criminalidad corporativa y tecnológica.
5. Blanqueo de capitales y criptoactivos.
6. Análisis de formas específicas de criminalidad:

6.1. Estafas informáticas.
6.2. Delitos informáticos de daños.
6.3. *Phreaking* o defraudación en telecomunicaciones.
6.4. Ciberdelitos contra la intimidad.
6.5. Ciberdelitos sexuales.
6.6. Amenazas
6.7. Acoso
6.8. Delito de odio
6.9. Apología del terrorismo
6.10. Injurias y calumnias
6.11. Delitos contra la propiedad intelectual.

6.- Metodologías docentes

Clases magistrales teórico-prácticas, seminarios especializados, comentarios jurisprudenciales y debate en el aula para fomentar el espíritu crítico.

6.1.- Distribución de metodologías docentes

		Horas dirigidas por el profesor		Horas de trabajo autónomo	HORAS TOTALES
		Horas presenciales.	Horas no presenciales.		
Sesiones magistrales		24			24
Prácticas	- En aula				
	- En el laboratorio				
	- En aula de informática				
	- De campo				
	- Otras (detallar)				
Seminarios				10	10
Exposiciones y debates				10	10
Tutorías		4		5	9
Actividades de seguimiento online					
Preparación de trabajos				20	20
Otras actividades (detallar)					
Exámenes		2			2
TOTAL		**30**		**45**	**75**

7.- Recursos, bibliografía, referencias electrónicas o de otro tipo

Ávila Trivelli, A.A., 2023. Análisis al Delito de Fraude Informático. Vox Juris, 42(1), pp. 161-175. Disponible en: https://portalrevistas.aulavirtualusmp.pe/index.php/VJ/article/view/2654/3534
Barrio Andrés, M., 2021. Criptoactivos. Retos y desafíos normativos. Madrid: Wolters Kluwer España.

Bustos Rubio, M., 2023. La reforma de la ciberestafa y la incorporación de los medios de pago digitales en el Código Penal. IDP: Revista de Internet, Derecho y Política, No. 38, pp. 1-11.

Chohan, U.W., 2021. Non-Fungible Tokens (NFTs): Early Thoughts and a Research Agenda. Critical Blockchain Research Initiative (CBRI) Working Papers, 2021-2024, pp. 4 y ss. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3822743

Chugá Montenegro, J.M., et al., 2024. Delitos informáticos de apropiación fraudulenta por medios y transferencia electrónicos de activo patrimonial. Iustitia Socialis, 9(1), pp. 220-229. Ed. Especial. Disponible en: https://fundacionkoinonia.com.ve/ojs/index.php/Iustitia_Socialis/article/view/3528/6103
Council of Europe, 2024. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Vilnius, 5.IX.2024. Disponible en: https://rm.coe.int/1680afae3c
Correia, P.M.A.R. y Andrade de Jesús, I.O., 2016. Combate às transferências bancárias ilegítimas pela Internet no direito português: entre as experiências domésticas e políticas globais concertadas. Revista Direito GV, 12(2), pp. 542–563. Disponible en: https://www.scielo.br/j/rdgv/a/6CjnmkZgQkkqZC7XVkrDXrv/abstract/?lang=pt
Council of Europe, 2024. Explanatory Report to the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Vilnius, 5.IX.2024. Disponible en: https://rm.coe.int/1680afae67

Europol, 2024. Internet Organized Crime Threat Assessment (IOCTA) 2024. Luxemburgo: Publications Office of the European Union, pp. 27 y ss. Disponible en: https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organized%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf
Fernández Amor, J.A., 2024. Apuntes sobre el tratamiento tributario de criptoactivos. Crónica Tributaria, 191(2), pp. 11–57. Disponible en: https://doi.org/10.47092/CT.24.2.1
Posada Maya, R., 2017. Los cibercrímenes: un nuevo paradigma de criminalidad: un estudio del Título VII bis del Código Penal colombiano. Bogotá D.C.: Ediciones Uniandes y Grupo Editorial Ibáñez.

Reinhart Schuller, R., 2022. Criptoactivos: Categorización Jurídica de Los Criptoactivos e Introducción a La Tecnología DLT/Blockchain. Cuadernos de Derecho Transnacional, 14(2), pp. 737–769. Disponible en: https://e-revistas.uc3m.es/index.php/CDT/article/view/7203/5642
Valdés Trapote, A., 2022. Estudio sobre la lucha contra el lavado de activos mediante criptoactivos. Madrid: El PAcTO. Disponible en: https://elpaccto.eu/wp-content/uploads/2022/07/Estudio-Lavado-Criptoactivos.pdf

8.- Evaluación

8.1: Criterios de evaluación: Para poder presentarse a la prueba teórica es preciso haber asistido al 80% de las clases y haber realizado el trabajo sobre la materia. Se controlará la asistencia.

8.2: Sistemas de evaluación:

60% de la calificación final: examen tipo test.
40% de la calificación final: realización personal de evaluación continua: trabajos, exposiciones, supuestos prácticos, etc. Para sumar la nota de prácticas, es preciso haber aprobado el examen. La detección de plagio o utilización de IA supondrá, automáticamente, suspender este elemento de evaluación.

8.3: Consideraciones generales y recomendaciones para la evaluación y la recuperación:

Se recomienda asistir y participar activamente en clase, así como realizar las actividades obligatorias y complementarias propuestas. En caso de dudas, se puede disponer de tutorías individuales y colectivas con los profesores de la asignatura.

Para la recuperación, en caso de no haber aprobado el examen en primera convocatoria, se guardará la nota obtenida en el apartado de evaluación continua para la convocatoria extraordinaria.
En caso de no haber realizado evaluación continua, **no** se guardará la nota del examen obtenida en primera convocatoria y, en segunda, además de realizar el examen, el apartado práctico se evaluará a través de un trabajo final realizado siguiendo las orientaciones del profesorado.

9.- Organización docente semanal

No aplica

PRINCIPALES EXPLICACIONES SOCIOCRIMINOLÓGICAS DEL CIBERDELITO

1.- Datos de la Asignatura

Código	306.583	Plan	2025	ECTS	3
Carácter	Obligatoria de especialidad	Curso	1º	Periodicidad	2do Semestre
Idioma de impartición asignatura		español			
Área	Sociología del crimen y la desviación				
Departamento	Sociología y Comunicación				
Plataforma virtual	Studium https://moodle.usal.es				

1.1.- Datos del profesorado

Profesor Coordinador	José Ignacio Antón Prieto	Grupo / s	
Departamento	Sociología y Comunicación		
Área	Sociología del crimen y la desviación		
Centro	Facultad de derecho		
Despacho	256		
Horario de tutorías	A determinar previa petición por email		
URL Web	*https://produccioncientifica.usal.es/investigadores/55918/detalle*		
E-mail	natxo@usal.es	Teléfono	923294400

2.- Recomendaciones previas

Además de los requisitos de acceso necesarios y del interés explícito por el mundo de la ciberdelincuencia, se recomienda una mentalidad abierta y una disposición relacional que nos ayuden a comprendernos y comprender la cibercriminalidad y la ciberdesviación en esta nueva realidad híbrida que habitamos.

NOTA: Por sociocriminología entendemos aquella parte de la criminología que comprende las explicaciones al delito y la desviación que se han aportado desde la sociología desde los inicios de ambas disciplinas.

3.- Objetivos de la asignatura

Vivimos en una realidad social híbrida en la que lo real y lo virtual se están fusionando a pasos agigantados. Se trata de un 'nuevo mundo' con nuevas normas, actores, relaciones... y, cómo no, desafíos sociales, criminológicos y jurídicos.

Partiendo de este nuevo escenario, esta asignatura tiene como objetivo genérico adentrarnos en los retos que el cibercrimen nos plantea como miembros de esa nueva sociedad y futuros profesionales de la cibercriminología; y en las explicaciones, análisis y estrategias que desde la sociocriminología se aportan para afrontar tales desafíos.

Para ello, específicamente:

- Accederemos al nivel especializado de la explicación sociocriminológica del ciberdelincuente y del ciberdelito,
- Aplicaremos los conceptos propios de la sociocriminología a la realidad de la ciberdesviación y la cibercriminalidad, aprendiendo a
  - detectar escenarios sociales criminógenos (actores, interacciones y contextos estructurales y situacionales)
  - Plantear estrategias de afrontamiento para estos escenarios.
  - Plantear estrategias de prevención para estos escenarios.

4.- Competencias a adquirir / Resultados de aprendizaje

Resultados de aprendizaje

4.1: Conocimientos:

C3. Identificar de forma exhaustiva el funcionamiento de los diferentes tipos de cibercrimen; modus operandi, autoría, víctimas, tecnología empleada.

C5. Interpretar la normativa nacional e internacional que regula la ciberdelincuencia, así como las funciones de autoridades y profesionales en el marco de detección, prevención, actuación e intervención en casos de ciberdelincuencia.

C6. Discriminar, por un lado, las particularidades de las personas víctimas de las actividades ilícitas que llevan a cabo los criminales utilizando tecnologías de la información y las comunicaciones; y, por otro, las necesidades de intervención que se derivan tras estos delitos.

C9. E2 Comparar conocimientos específicos para elaborar estudios e informes criminológicos en el ámbito de la ciberdelincuencia y profundizar en las teorías criminológicas que explican el delito en el ciberespacio, así como otros factores relacionados con el proceso penal.

4.2: Habilidades:

H1. Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales.

H3. Practicar con pericia la búsqueda de legislación y jurisprudencia a través de diferentes técnicas que puedan favorecer la investigación, la prueba y la intervención ante ciberdelitos.

H5. Aplicar con dominio la normativa nacional e internacional que regula la ciberdelincuencia, así como su persecución, investigación y represión en casos concretos.

H6. Concluir las cuestiones jurídicas más relevantes implicadas en un conjunto complejo de hechos relacionados con casos de cibercriminalidad.

H9. E2 Ante casos específicos de cibercriminalidad, elaborar, exponer y defender informes criminológicos jurídicamente fundamentados adecuados al caso y en relación con las exigencias procedimentales.

H10. E2 Desarrollar estrategias de prevención e intervención ante ciberataques u otro tipo de ciberdelitos, razonando y argumentando la propuesta con un enfoque interdisciplinar y teniendo en cuenta las particularidades de las víctimas para que la propuesta responda a las necesidades de éstas.

4.3: Competencias:

K1. Discriminar los tipos de ciberdelito, comprendiendo los nuevos espacios virtuales y, en atención a ellos, aplicar la normativa vigente y las resoluciones jurisprudenciales vinculantes en cada caso en cuestión

K3. Analizar pormenorizadamente cada ciberdelito, incluyendo perfiles diferenciados de víctimas y agresores en el uso de la tecnología cibernética

K5. En casos de cibercriminalidad, redactar textos legales para los diferentes momentos procesales y desde el punto de vistas de diferentes profesiones implicadas, y que estos textos sean comprensibles tanto para un público especialista como para un público profano

K6. Discriminar las funciones de cada una de las autoridades y profesionales que intervienen en casos de ciberdelincuencia, identificando los requisitos formales que van ligados a todas ellas para poder poner en práctica las mismas.

K10. E2 Determinar, tras su evaluación, el tratamiento individualizado de las víctimas de un cibercrimen, así como planes de prevención para hacer frente a los riesgos derivados de este tipo de criminalidad en diferentes sectores de la población.

5.- Contenidos (temario)

El temario de la asignatura se estructura en los siguientes 4 bloques

1. Ciberdelito y sociedad. Principales dimensiones explicativas:
    a. (hiper)riesgo e incertidumbre social
    b. El miedo
    c. La polarización y el odio
    d. La sociedad como algoritmo
2. La medición de la ciberdelincuencia en España
    a. MIR Informes sobre cibercriminalidad (2013–2023)
    b. MIR Balances trimestrales de criminalidad
    c. CIS Barómetro de febrero de 2024
    d. Eurobarómetro
    e. Los discursos de la ciberdesviación
3. Principales variables del cibercrimen
    a. Edad
    b. Sexo
    c. Tamaño del hábitat/comunidad autónoma
    d. Nacionalidad
    e. Evolución del cibercrimen y comparativa con el 'crimen analógico'
    f. Tasas de esclarecimiento
4. Principales explicaciones
    a. Ciberdesviación/cibercriminalidad. La 'normalidad' del cibercrimen y la ciberdesviación
        i. Aprendizaje y neutralización del ciberdelito.
    b. Desorganización social y situacional del ciberespacio
    c. Anomia y cibercrimen:
        i. Desvinculación moral
        ii. Tensión estructural y anomia institucional
    d. La desviación cultural y las subculturas en el entorno virtual
    e. La etiqueta de ciberdelincuente
        i. Pánicos morales en red.
    f. Cibercriminología crítica: explicaciones realistas e idealistas de la ciberdelincuencia.

En cada bloque se incorporarán distintos estudios de caso específicos para ejemplificar y aplicar los contenidos teóricos.

6.- Metodologías docentes

Las sesiones partirán del *planteamiento de dilemas* socio–ciber criminológicos presentes en la sociedad actual. A continuación, se aportarán claves sociocriminológicas conceptuales (*clases teóricas* propiamente dichas) que nos ayuden a resolverlos. Intercalados irán los *análisis de estudios de caso* que propicien el logro de los objetivos generales y específicos expuestos en el apartado tercero.

A lo largo de cada sesión se fomentará la *participación* y el *debate* sobre los casos, datos y conceptos que se vayan introduciendo.

6.1.- Distribución de metodologías docentes

		Horas dirigidas por el profesor		Horas de trabajo autónomo	HORAS TOTALES
		Horas presenciales.	Horas no presenciales.		
Sesiones magistrales		12			12
Prácticas	- En aula	8			20
	- En el laboratorio				
	- En aula de informática				
	- De campo				
	- Otras (detallar)				
Seminarios					

Exposiciones y debates	4			24
Tutorías	4			28
Actividades de seguimiento online				
Preparación de trabajos	45			73
Otras actividades (detallar)				
Exámenes	2			75
TOTAL				**75**

7.- Recursos, bibliografía, referencias electrónicas o de otro tipo

Bibliografía

- AEBI, Marcelo Fernando; MIRÓ–LLINARES, Fernando; CANEPPELE, Stefano (eds.), *Understanding Crime Trends in a Hybrid Society The Digital Drift*, ed. Springer, Luxemburg, 2025.
- AL-KHATEEB, Sahadi; AGARWAL, Naman, "Case Studies of Deviance in Social Media", in. *Deviance in Social Media and Social Cyber Forensics. Uncovering Hidden Relations Using Open Source Information (OSINF)*, ed. Springer, Luxemburg, 2019.
- ANTÓN PRIETO, José Ignacio "El proceso de avatarización social" en CURIEL, Aitor (comp.) Síndrome Avatar. Distintas versiones de una misma realidad ed. Ed. Asociación HELPTIC de Afectados por el uso de las Tecnologías de la Información y la Comunicación Valladolid, 2016, pp. 81–98.
- ANTÓN PRIETO, José Ignacio ET. AL *Informe sobre las percepciones de seguridad e inseguridad derivadas del uso de las Tecnologías de la Información y la Comunicación* ed. Catedra telefónica, Salamanca, 2011, 46 pp.
- ANTÓN PRIETO, José Ignacio, "Ciberdelincuencia de género. Análisis sociocriminológico descriptivo de la situación española 2013–2022", ed. Tirant lo Blanch, México, 2024.
- ANTÓN PRIETO, José Ignacio, "Delitos de odio en la España multipolarizada (2013–2022). Diez años de estadísticas", en FIGUERUELO BURRIEZA, Ángela (dir.) Desinformación, odio y polarización (II) ed. Aranzadi Thomson Reuters, Madrid.
- BUIL–GIL, David; TRAJTENBERG, Nicolas; AEBI, Marcelo Fernando "Measuring cybercrime and cyberdeviance in surveys" in GRAHAM, Roderick S. ET. AL. (eds.), *The routledge international handbook of online deviance*, ed. Routledge, London, 2025.
- GALANTINO, Maria Grazia "Organised Irresponsibility in the Post-Truth Era: Beck's Legacy in Today's World at Risk", rev. *Italian Sociological Review*, ed. University of Verona, Verona, 2022, pp. 971—990.
- GONZÁLEZ, María Laura "La cibercriminalidad como instrumento para la expansión y empoderamiento del crimen organizado", rev. Análisis GESI. Grupo de Estudios en seguridad internacional, nº 47, ed. Universidad de Granada, Granada, 2017.
- GOODMAN, Marc, *Los delitos del futuro. Todo está conectado, todos somos vulnerables, ¿qué podemos hacer al respecto?*, ed. Ariel S. A., Barcelona, 2015.
- HIKAL, Wael "La teoría de la asociación diferencial para la explicación de la criminalidad y la articulación de una política criminal" rev. Derecho y cambio social, ed. Sociedad Mexicana de Criminología capítulo Nuevo León, Nuevo León, 2017, pp. 1—15.
- LUKNAR, Ivana "Social control theory and cybercrime" rev. *Nationalni interés*, vol. 41, pp. 147/159.
- MARAS, Marie-Helen, *Cybercriminology*, Ed. Oxford University Press, Oxford, 2016.
- MIRÓ–LLINARES, Fernando, "Crimen, cibercrimen y COVID–19: desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos", rev. Revista de los Estudios de Derecho y Ciencia Política, nº 32, ed. UOC, Barcelona, 2021, pp. 1—17.
- MIRÓ–LLINARES, Fernando, "La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen", rev. Revista Electrónica de Ciencia Penal y Criminología, vol. 7, nº 13, 55 pp.
- MIRÓ–LLINARES, Fernando, *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, ed. Marcial Pons, Madrid, 2012.
- UNODC *Compendio de ciberdelincuencia organizada*, Viena, 2022.
- UNODC *Comprehensive study on cybercrime*, Vienna, 2013.

Fuentes estadísticas

- WEF The global Risk reports (2009–2023)
- MIR Informes sobre cibercriminalidad (2013–2023)

- MIR Balances trimestrales de criminalidad
- CIS Barómetros y estudios
- UE Eurobarómetro.

8.- Evaluación

8.1: Criterios de evaluación:
La evaluación pretende dar cuenta de los conocimientos y derezas adquiridos en el máster. Para ello se utilizarán

8.2: Sistemas de evaluación:
Evaluación continua: Participación, entrega y exposición de actividades y trabajos (60%)
Examen final: tipo test (40%).

8.3: Consideraciones generales y recomendaciones para la evaluación y la recuperación: la asistencia, además de obligatoria, es indispensable para superar la materia.

9.- Organización docente semanal

FACTOR HUMANO DEL CIBERDELITO

1.- Datos de la Asignatura					
Código	306584	Plan	2025	ECTS	3
Carácter	Obligatoria de especialidad	Curso	1º	Periodicidad	2º Semestre
Idioma de impartición asignatura		español			
Área	Psicología Social				
Departamento	Psicología Social y Antropología				
Plataforma virtual	Studium https://moodle.usal.es				

1.1.- Datos del profesorado*			
Profesor Coordinador	Pendiente de asignar	Grupo / s	--
Departamento	Psicología Social y Antropología		
Área	Psicología Social		
Centro	--		
Despacho	Pendiente de asignar		
Horario de tutorías	Pendiente de determinar		
URL Web	--		
E-mail	--	Teléfono	--

Profesor Coordinador	Pendiente de asignar	Grupo / s	--
Departamento	Psicología Social y Antropología		
Área	Psicología Social		
Centro	--		
Despacho	Pendiente de asignar		
Horario de tutorías	Pendiente de determinar		
URL Web	--		
E-mail	--	Teléfono	--

*Replique esta tabla por cada profesor/a que imparte la asignatura

2.- Recomendaciones previas

Sin recomendaciones previas

3.- Objetivos de la asignatura

- Conocer las explicaciones psicológicas, psicosociales y criminológicas de la ciberdelincuencia.
- Conocer los factores de riesgo de cibervictimización y el impacto del ciberdelito sobre la

víctima.
- Entender el factor humano detrás de distintos ciberdelitos concretos.
- Conocer cuáles son las respuestas adecuadas ante la ciberdelincuencia.
- Razonar y proporcionar argumentos sobre los métodos más adecuados para prevenir y reaccionar ante el ciberdelito.
- Proponer soluciones a casuísticas específicas respecto a cómo reaccionar ante un ciberdelito.
- Reconocer los factores criminógenos que contribuyen al desarrollo de un ciberdelito concreto.
- Programar actuaciones acordes con las áreas de interés y objetivos estratégicos nacionales de lucha contra el ciberdelito desde la perspectiva del factor humano.
- Interiorizar el uso de medios y procedimientos que se hallen suficientemente contrastados, dentro de los límites del conocimiento científico vigente.

4.- Competencias a adquirir / Resultados de aprendizaje

Resultados de aprendizaje

4.1: Conocimientos:

C3. Identificar de forma exhaustiva el funcionamiento de los diferentes tipos de cibercrimen; modus operandi, autoría, víctimas, tecnología empleada.

C4. Evaluar las herramientas técnicas y legales necesarias para analizar y hacer frente a diferentes riesgos, ciberamenazas y ciberdelitos.

C5. Interpretar la normativa nacional e internacional que regula la ciberdelincuencia, así como las funciones de autoridades y profesionales en el marco de detección, prevención, actuación e intervención en casos de ciberdelincuencia.

C6. Discriminar, por un lado, las particularidades de las personas víctimas de las actividades ilícitas que llevan a cabo los criminales utilizando tecnologías de la información y las comunicaciones; y, por otro, las necesidades de intervención que se derivan tras estos delitos.

C9. E2 Comparar conocimientos específicos para elaborar estudios e informes criminológicos en el ámbito de la ciberdelincuencia y profundizar en las teorías criminológicas que explican el delito en el ciberespacio, así como otros factores relacionados con el proceso penal.

4.2: Habilidades:

H1. Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales

H3. Practicar con pericia la búsqueda de legislación y jurisprudencia a través de diferentes técnicas que puedan favorecer la investigación, la prueba y la intervención ante ciberdelitos.

H5. Aplicar con dominio la normativa nacional e internacional que regula la ciberdelincuencia, así como su persecución, investigación y represión en casos concretos.

H6. Concluir las cuestiones jurídicas más relevantes implicadas en un conjunto complejo de hechos relacionados con casos de cibercriminalidad.

H9. E2 Ante casos específicos de cibercriminalidad, elaborar, exponer y defender informes criminológicos jurídicamente fundamentados adecuados al caso y en relación con las exigencias procedimentales.

H10. E2 Desarrollar estrategias de prevención e intervención ante ciberataques u otro tipo de ciberdelitos, razonando y argumentando la propuesta con un enfoque interdisciplinar y teniendo en cuenta las particularidades de las víctimas para que la propuesta responda a las necesidades de éstas.

4.3: Competencias:

K1. Discriminar los tipos de ciberdelito, comprendiendo los nuevos espacios virtuales y, en atención a ellos, aplicar la normativa vigente y las resoluciones jurisprudenciales vinculantes en cada caso en cuestión

K3. Analizar pormenorizadamente cada ciberdelito, incluyendo perfiles diferenciados de víctimas y agresores en el uso de la tecnología cibernética

K5. En casos de cibercriminalidad, redactar textos legales para los diferentes momentos procesales y desde el punto de vistas de diferentes profesiones implicadas, y que estos textos

sean comprensibles tanto para un público especialista como para un público profano
K6. Discriminar las funciones de cada una de las autoridades y profesionales que intervienen en casos de ciberdelincuencia, identificando los requisitos formales que van ligados a todas ellas para poder poner en práctica las mismas
Especialidad en aspectos jurídicos de la cibercriminalidad:
K9. E2 Elaborar informes criminológicos relacionados con el ciberdelito, en los que se seleccione los conocimientos específicos y las cualidades más idóneos y en los que se identifiquen los factores que favorecen la criminalidad y se defina y reconstruya el modus operandi o la actuación posterior.
K10. E2 Determinar, tras su evaluación, el tratamiento individualizado de las víctimas de un cibercrimen, así como planes de prevención para hacer frente a los riesgos derivados de este tipo de criminalidad en diferentes sectores de la población

5.- Contenidos (temario)

INTRODUCCIÓN
1. El factor humano y su relación con el ciberdelito.
2. El yo en el ciberespacio.
3. Aplicación de teorías criminológicas a la explicación del ciberdelito.

LA VÍCTIMA
4. Factores de riesgo de la cibervictimización.
5. Impacto de los ciberdelitos sobre las víctimas.

EL CIBERDELITO
6. Ciberdelitos interpersonales: Bullying, stalking, citas, abuso de pareja y delitos de odio.
7. Ciberdelitos financieros.
8. Ciberdelitos sexuales.

LAS RESPUESTAS AL CIBERDELITO
9. La respuesta policial al ciberdelito.
10. Intervenciones para ciberdelincuentes.

6.- Metodologías docentes

Se emplearán las siguientes metodologías docentes:

- Clases teóricas: exposición, explicación y análisis crítico de contenidos fundamentales por parte del profesorado. Sesiones de obligatoria asistencia, se fomentará la reflexión crítica del alumnado y su participación.
- Clases prácticas: planteamiento, desarrollo y resolución de problemas y de casos prácticos. Sesiones de obligatoria asistencia
- Elaboración de trabajos individuales o grupales: aplicando los contenidos teóricos a casos prácticos más elaborados. En trabajos individuales se perseguirá trabajar la capacidad individual de análisis, reflexión y síntesis. En trabajos grupales se fomentará que los alumnos colaboren y desarrollen habilidades de comunicación, liderazgo y gestión de conflictos.
- Tutorías: se pondrá a disposición de los estudiantes la solicitud de tutorías para el seguimiento y asesoramiento individual en relación con el desarrollo de la asignatura.

También podrán emplearse, si se considera oportuno, las siguientes:

- Debates: presentación y defensa de posturas contrarias sobre temas tratados, ya sean previamente preparados o improvisados en el transcurso de la clase. También son de obligatoria asistencia.
- Seminarios: se profundizará en diferentes aspectos que rodean a la ciberdelincuencia con expertos en la materia. Se podrá requerir la lectura previa de textos científicos. Se

incentivará la participación del alumnado, así como la eventual práctica de debates o la resolución de problemas.

- Talleres y exposiciones: se profundizará en aspectos propios de la asignatura a través de talleres didácticos con expertos y, eventualmente, se complementarán con exposiciones del alumnado.

6.1.- Distribución de metodologías docentes

		Horas dirigidas por el profesor		Horas de trabajo autónomo	HORAS TOTALES
		Horas presenciales.	Horas no presenciales.		
Sesiones magistrales		16			16
Prácticas	- En aula	4			4
	- En el laboratorio				
	- En aula de informática				
	- De campo				
	- Otras (detallar)				
Seminarios		4			4
Exposiciones y debates					
Tutorías		4			4
Actividades de seguimiento online					
Preparación de trabajos				8	8
Otras actividades (detallar)				7	7
Exámenes		2		30	32
TOTAL		**30**		**45**	**75**

7.- Recursos, bibliografía, referencias electrónicas o de otro tipo

Bada, M. (2021). Psychology of cybercrime. En Jajodia, S., Samarati, P., Yung, M. (Eds.), Encyclopedia of cryptography, security and privacy. Springer. https://doi.org/10.1007/978-3-642-27739-9_1589-1

Bada, M., & Nurse, J. R. C. (2020). The social and psychological impact of cyberattacks. In V. Benson & J. McAlaney (Eds.), *Emerging cyber threats and cognitive vulnerabilities* (pp. 73–92). Academic Press. https://doi.org/10.1016/B978-0-12-816203-3.00004-6

Benson, V., & McAlaney, J. (Eds.). (2020). *Emerging cyber threats and cognitive vulnerabilities*. Academic Press. https://doi.org/10.1016/C2017-0-04243-X

Borwell, J., Jansen, J., & Stol, W. (2021). The psychological and financial impact of cybercrime victimization: A novel application of the Shattered Assumptions Theory. *Social Science Computer Review*, *40*(4), 933-954. https://doi.org/10.1177/0894439320983828

Cross, C., & Layt, R. (2021). "I suspect that the pictures are stolen": Romance fraud, identity crime, and responding to suspicions of inauthentic identities. *Social Science Computer Review*, *40*(4), 955-973. https://doi.org/10.1177/0894439321999311

Fissel, E. R., Graham, A., Butler, L. C., & Fisher, B. S. (2021). A new frontier: The development and validation of the intimate partner cyber abuse instrument. *Social Science Computer Review*, *40*(4), 974-993. https://doi.org/10.1177/0894439321994618

Jeffries, S., & Apeh, E. (2020). Standard operating procedures for cybercrime investigations: A systematic literature review. En V. Benson & J. McAlaney (Eds.), *Emerging cyber threats and cognitive vulnerabilities* (pp. 145–162). Academic Press. https://doi.org/10.1016/B978-0-12-816203-3.00007-1

Leukfeldt, R., & Holt, T. J. (Eds.). (2019). *The human factor of cybercrime.* Taylor & Francis.

Pica, E., Ross, D., & Pozzulo, J. (Eds.). (2024). *The impact of technology on the criminal justice system: A psychological overview*. Routledge.

Weulen Kranenbarg, M., & Leukfeldt, R. (Eds.). (2021). *Cybercrime in context: The human factor in victimization, offending, and policing*. Springer.

Whitty, M. T., & Young, G. (2017). *Cyberpsychology: The study of individuals, society and digital technologies.* Wiley.

8.- Evaluación

8.1: Criterios de evaluación:

8.2: Sistemas de evaluación:

- Evaluación continua. Estrega de trabajos, exposición de trabajos, clases, participación en clase, etc.: 30% de la calificación.
- Prueba de evaluación final (examen): 70% de la calificación
- En la convocatoria extraordinaria se realizará una prueba de evaluación (examen)

8.3: Consideraciones generales y recomendaciones para la evaluación y la recuperación:

9.- Organización docente semanal

FUNDAMENTOS DE LA SEGURIDAD INFORMÁTICA

1.- Datos de la Asignatura

Código	306.572	Plan	2025	ECTS	6
Carácter	Obligatorio	Curso	1º	Periodicidad	1er Semestre
Idioma de impartición asignatura		español			
Área	Ciencias de la Computación e Inteligencia Artificial				
Departamento	Informática y Automática				
Plataforma virtual	Studium https://moodle.usal.es				

1.1.- Datos del profesorado*

Profesor Coordinador	Alfonso González Briones	Grupo / s	
Departamento	Informática y Automática		
Área	Ciencias de la Computación e Inteligencia Artificial		
Centro	Facultad de Ciencias		
Despacho	F3012		
Horario de tutorías	Cita previa (email)		
URL Web	*https://produccioncientifica.usal.es/investigadores/148408/detalle*		
E-mail	alfonsogb@usal.es	Teléfono	923 294 500 extensión 5479
Profesor Coordinador	Pendiente de designar	Grupo / s	
Departamento	Informática y Automática		
Área			
Centro	Facultad de Ciencias		
Despacho			
Horario de tutorías			
URL Web			
E-mail		Teléfono	
Profesor Coordinador		Grupo / s	

2.- Recomendaciones previas

No se requieren conocimientos previos.

3.- Objetivos de la asignatura

• **Comprensión de los fundamentos de la seguridad informática**: Proporcionar una base sólida sobre los principios esenciales de la seguridad de la información, tales como la confidencialidad, integridad, disponibilidad, autenticación y control de acceso.

• **Evaluación de riesgos y amenazas en entornos digitales**: Capacitar al estudiante para identificar y clasificar amenazas, vulnerabilidades y riesgos presentes en sistemas y redes, así como entender su impacto potencial en distintos contextos tecnológicos y organizativos.
• **Diseño y análisis de arquitecturas seguras**: Instruir en los modelos y estrategias de diseño seguro, incluyendo la defensa en profundidad, segmentación de redes, políticas de acceso y uso de firewalls, con aplicación a infraestructuras tecnológicas modernas.
• **Uso de mecanismos criptográficos**: Introducir los fundamentos de criptografía aplicada, gestión de claves, certificados digitales y protocolos seguros para la protección de comunicaciones y datos sensibles.
• **Seguridad en sistemas operativos y software**: Enseñar los principios del hardening de sistemas operativos y la aplicación de buenas prácticas de desarrollo seguro, prestando especial atención a las vulnerabilidades más comunes.
• **Formación práctica en técnicas defensivas**: Dotar al alumnado de habilidades para aplicar herramientas y metodologías básicas de detección y mitigación de amenazas, análisis forense inicial y respuesta a incidentes en entornos simulados.
• **Familiarización con estándares y marcos regulatorios**: Introducir al estudiante en las principales normativas y estándares de seguridad y su aplicación en auditorías de cumplimiento y gestión de riesgos.

4.- Competencias a adquirir / Resultados de aprendizaje

Resultados de aprendizaje

4.1: Conocimientos:

C1. Defender las bases conceptuales de la ciberdelincuencia, ciberamenazas y la seguridad informática
C2. Examinar el funcionamiento de las tecnologías disruptivas utilizadas por delincuentes y por profesionales que actúan ante la cibercriminalidad, así como los principios básicos de ciberespacio
C3. Identificar de forma exhaustiva el funcionamiento de los diferentes tipos de cibercrimen; modus operandi, autoría, víctimas, tecnología empleada.
C4. Evaluar las herramientas técnicas y legales necesarias para analizar y hacer frente a diferentes riesgos, ciberamenazas y ciberdelitos.

4.2: Habilidades:

H1. Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales
H2. Identificar el funcionamiento técnico de las ciberamenazas y ciberdelitos, en relación con las herramientas técnicas y legales disponibles para su cese y represión.
H4. Evaluar la viabilidad de diferentes herramientas y medidas de investigación en atención al tipo de delictivo presentado, las autoridades involucradas y el momento procesal del caso**.**

4.3: Competencias:

K1. Discriminar los tipos de ciberdelito, comprendiendo los nuevos espacios virtuales y, en atención a ellos, aplicar la normativa vigente y las resoluciones jurisprudenciales vinculantes en cada caso en cuestión
K2. Aprender a actualizar de modo autónomo los conocimientos sobre las últimas tecnologías y herramientas de seguridad informática
K4. Aplicar el ordenamiento jurídico español y la normativa internacional, con todas las garantías, ante riesgos, amenazas y ciberdelitos concretos
K6. Discriminar las funciones de cada una de las autoridades y profesionales que intervienen en casos de ciberdelincuencia, identificando los requisitos formales que van ligados a todas ellas para poder poner en práctica las mismas
Especialidad en aspectos jurídicos de la cibercriminalidad:

5.- Contenidos (temario)

Contenido teórico

1. Principios y objetivos de la seguridad informática
2. Modelos de seguridad y arquitectura defensiva
3. Criptografía y gestión de claves
4. Sistemas operativos seguros
5. Seguridad en redes de datos
6. Seguridad en aplicaciones y ciclo de vida del software
7. Malware y técnicas de evasión
8. Normativas, estándares y cumplimiento

Contenido práctico

1. Análisis de políticas de seguridad
2. Configuración segura de sistemas
3. Gestión de claves y certificados
4. Análisis de tráfico y detección de ataques
5. Laboratorio de seguridad en red
6. Evaluación de aplicaciones inseguras

6.- Metodologías docentes

Las sesiones magistrales serán exposiciones claras y estructuradas que presentarán los conceptos teóricos fundamentales para el desarrollo del curso. Las prácticas o talleres en aula informática permitirán aplicar estos conocimientos mediante ejercicios, simulaciones o proyectos con herramientas digitales específicas. Los seminarios facilitarán un análisis profundo y participativo, promoviendo el debate y el pensamiento crítico. Las exposiciones orales por parte del alumnado aportarán diferentes perspectivas, enriqueciendo el aprendizaje colectivo. La realización de trabajos individuales o grupales favorecerá competencias como la búsqueda de información, análisis crítico, redacción y gestión del tiempo, vinculados a los contenidos del curso. Finalmente, las tutorías ofrecerán atención personalizada para resolver dudas y orientar a los estudiantes, de forma presencial o virtual.

6.1.- Distribución de metodologías docentes

		Horas dirigidas por el profesor		**Horas de trabajo autónomo**	**HORAS TOTALES**
		Horas presenciales.	**Horas no presenciales.**		
Sesiones magistrales		24		15	39
Prácticas	- En aula	24		10	26
	- En el laboratorio				
	- En aula de informática	16			
	- De campo				
	- Otras (detallar)				
Seminarios		4		6	10
Exposiciones y debates		4		6	10
Tutorías		2		4	6
Actividades de seguimiento online			4	8	12
Preparación de trabajos				23	23
Otras actividades (detallar)				5	5
Exámenes		3			3
TOTAL		**53**	**4**	**93**	**150**

7.- Recursos, bibliografía, referencias electrónicas o de otro tipo

Bibliografía

- Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems (3.ª ed.). Wiley.
- Stallings, W. (2022). Computer Security: Principles and Practice (5.ª ed.). Pearson.
- Bishop, M. (2018). Computer Security: Art and Science (2.ª ed.). Addison-Wesley.
- Viega, J., & McGraw, G. (2011). Building Secure Software: How to Avoid Security Problems the Right Way. Addison-Wesley.
- Pfleeger, C. P., & Pfleeger, S. L. (2015). Security in Computing (5.ª ed.). Prentice Hall.

Repositorios y recursos electrónicos:

- NIST National Vulnerability Database (NVD): Base de datos oficial sobre vulnerabilidades y configuraciones inseguras. https://nvd.nist.gov/
- OWASP (Open Web Application Security Project): Proyecto abierto sobre buenas prácticas en seguridad de aplicaciones. https://owasp.org/
- CIS Benchmarks (Center for Internet Security): Guías de configuración segura para múltiples sistemas. https://www.cisecurity.org/cis-benchmarks/
- MITRE ATT&CK Framework: Base de conocimientos sobre técnicas de adversarios para análisis y defensa. https://attack.mitre.org/
- TryHackMe: Plataforma de entrenamiento en ciberseguridad con entornos virtuales interactivos. https://tryhackme.com/
- Red Team Tools: Colección actualizada de herramientas y recursos orientados a profesionales de ciberseguridad ofensiva y defensiva. https://github.com/yeyintminthuhtut/Awesome-Red-Teaming
- Seguridad Lógica INCIBE: Repositorio español de contenidos técnicos sobre seguridad TIC. https://www.incibe.es/protege-tu-empresa/guias-y-recursos

8.- Evaluación

8.1: Criterios de evaluación:
-**Examen**: Evaluación del conocimiento teórico sobre Fundamentos de la Seguridad Informática.
-**Trabajo práctico**: Entrega de un informe sobre las actividades prácticas realizadas durante los talleres de las prácticas.

8.2: Sistemas de evaluación:
-Examen tipo test: Evaluación escrita para comprobar los conocimientos adquiridos.
-Trabajo práctico: Evaluación del desempeño en las prácticas y la calidad del informe entregado. Participación en las actividades.

8.3: Consideraciones generales y recomendaciones para la evaluación y la recuperación:
En caso de no aprobar el examen o el trabajo práctico, los estudiantes tendrán una oportunidad de recuperación, donde podrán presentar una versión revisada del trabajo o realizar un nuevo examen en segunda convocatoria

9.- Organización docente semanal

MEDIDAS DE INVESTIGACIÓN TECNOLÓGICA

1.- Datos de la Asignatura					
Código	306.574	Plan	2025	ECTS	6
Carácter	Obligatorio	Curso	1º	Periodicidad	1er Semestre
Idioma de impartición asignatura		español			
Área	DERECHO PROCESAL				
Departamento	Derecho Administrativo, Financiero y Procesal				
Plataforma virtual	Studium https://moodle.usal.es				

1.1.- Datos del profesorado*			
Profesor Coordinador	Marta del Pozo Pérez	Grupo / s	Único
Departamento	Derecho Administrativo, Financiero y Procesal		
Área	Derecho Procesal		
Centro	Facultad de Derecho		
Despacho	284		
Horario de tutorías	Previa cita por correo electrónico		
URL Web	*https://produccioncientifica.usal.es/investigadores/56058/detalle*		
E-mail	tillo@usal.es	Teléfono	Ext. 6939
Profesor Coordinador	Alicia González Monje	Grupo / s	Único
Departamento	Derecho Administrativo, Financiero y Procesal		
Área	Derecho Procesal		
Centro	Facultad de Derecho		
Despacho	266		
Horario de tutorías	Previa cita por correo electrónico		
URL Web	*https://produccioncientifica.usal.es/investigadores/57155/detalle*		
E-mail	alicia.g.monje@usal.es	Teléfono	6101
Profesor Coordinador	Irene González Pulido	Grupo / s	Único
Departamento	Derecho Administrativo, Financiero y Procesal		
Área	Derecho Procesal		
Centro	Facultad de Derecho		
Despacho	283		
Horario de tutorías	Previa cita por correo electrónico		
URL Web	*https://produccioncientifica.usal.es/investigadores/148016/detalle*		
E-mail	irenegopu@usal.es	Teléfono	

2.- Recomendaciones previas

Se recomienda conocimientos previos de Introducción al Derecho Procesal y Derecho Procesal Penal.

3.- Objetivos de la asignatura

Aprender y asimilar el contenido de las diligencias de investigación tecnológicas que pueden practicarse en el seno de una investigación criminal.
Analizar el marco jurídico que regula las técnicas especiales de investigación tecnológica en el proceso penal, con especial atención a su compatibilidad con los derechos fundamentales.
Valorar críticamente el uso de diligencias de investigación tecnológicas, considerando su eficacia frente al cibercrimen y los riesgos que comportan para los derechos del investigado.

4.- Competencias a adquirir / Resultados de aprendizaje

Resultados de aprendizaje

4.1: Conocimientos:
C2. Examinar el funcionamiento de las tecnologías disruptivas utilizadas por delincuentes y por profesionales que actúan ante la cibercriminalidad, así como los principios básicos de ciberespacio
C3. Identificar de forma exhaustiva el funcionamiento de los diferentes tipos de cibercrimen; modus operandi, autoría, víctimas, tecnología empleada.
C4. Evaluar las herramientas técnicas y legales necesarias para analizar y hacer frente a diferentes riesgos, ciberamenazas y ciberdelitos.
C5. Interpretar la normativa nacional e internacional que regula la ciberdelincuencia, así como las funciones de autoridades y profesionales en el marco de detección, prevención, actuación e intervención en casos de ciberdelincuencia.
C7. Contrastar la jurisprudencia estatal y supranacional en materia de ciberdelincuencia e investigación tecnológica

4.2: Habilidades:
H1. Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales
H2. Identificar el funcionamiento técnico de las ciberamenazas y ciberdelitos, en relación con las herramientas técnicas y legales disponibles para su cese y represión.
H4. Evaluar la viabilidad de diferentes herramientas y medidas de investigación en atención al tipo de delictivo presentado, las autoridades involucradas y el momento procesal del caso**.**

4.3: Competencias:
K1. Discriminar los tipos de ciberdelito, comprendiendo los nuevos espacios virtuales y, en atención a ellos, aplicar la normativa vigente y las resoluciones jurisprudenciales vinculantes en cada caso en cuestión
K2. Aprender a actualizar de modo autónomo los conocimientos sobre las últimas tecnologías y herramientas de seguridad informática
K4. Aplicar el ordenamiento jurídico español y la normativa internacional, con todas las garantías, ante riesgos, amenazas y ciberdelitos concretos
K6. Discriminar las funciones de cada una de las autoridades y profesionales que intervienen en casos de ciberdelincuencia, identificando los requisitos formales que van ligados a todas ellas para poder poner en práctica las mismas

5.- Contenidos (temario)

I. Investigación tecnológica y derechos fundamentales
II. Interceptación de comunicaciones telefónicas y telemáticas
III. Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos
IV. Utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización
V. Registro de dispositivos y equipos informáticos
VI. Agente encubierto informático y entrega vigilada informática

6.- Metodologías docentes

En el desarrollo de la asignatura se compatibilizarán diversas metodologías. Así, se empleará la clase magistral durante las sesiones teóricas, mientras que en las sesiones prácticas se utilizarán diversas estrategias metodológicas, tales como el análisis y la discusión de textos legislativos y/o jurisprudenciales, el análisis crítico de supuestos prácticos y normativa concreta, con utilización, en su caso, de los medios audiovisuales pertinentes, además del planteamiento de debates y seminarios que permitan la profundización en aspectos concretos de la asignatura.

6.1.- Distribución de metodologías docentes

		Horas dirigidas por el profesor		Horas de trabajo autónomo	HORAS TOTALES
		Horas presenciales.	Horas no presenciales.		
Sesiones magistrales		38		50	88
Prácticas	- En aula	8		10	18
	- En el laboratorio				
	- En aula de informática				
	- De campo				
	- Otras (detallar)				
Seminarios		4		6	10
Exposiciones y debates		6		10	16
Tutorías		2		2	4
Actividades de seguimiento online					
Preparación de trabajos					
Otras actividades (detallar)					
Exámenes		2		12	14
TOTAL		**60**		**90**	**150**

7.- Recursos, bibliografía, referencias electrónicas o de otro tipo

BUENO DE MATA, F., *Las diligencias de investigación penal en la cuarta revolución industrial: principios teóricos y problemas prácticos*, Thomson Reuters Aranzadi, 2019.
DEL POZO PÉREZ, M., *Diligencias de investigación y cadena de custodia*, Sepin, 2014.
GONZÁLEZ MONJE, A., *Cooperación jurídica internacional en materia penal e intervención de comunicaciones como técnica especial de investigación,* Comares, 2017.
GONZÁLEZ PULIDO, I., *El registro remoto como diligencia de investigación tecnológica de la ciberdelincuencia*. Aranzadi, 2023.
CENDOJ. Centro de Documentación Judicial. https://www.poderjudicial.es/search/indexAN.jsp
FISCALÍA GENERAL DEL ESTADO. https://www.fiscal.es/

8.- Evaluación

8.1: Criterios de evaluación: La nota final corresponderá a:

- 70% Evaluación Final. Simulación de un caso práctico a repartir el primer día de clase (Por parejas o individual en función del número de estudiantes matriculados)
- 30% Realización de prácticas por parte del alumnado de manera presencial en clase.

Para poder acudir a la CONVOCATORIA ORDINARIA deberá superarse la parte práctica de la asignatura.

8.2: Sistemas de evaluación:

- Participar en las clases prácticas y aprobar al menos el 50% de los casos prácticos. La nota media de las prácticas se corresponde con el 30% de la nota de la asignatura
- Intervenir en las clases teóricas.
- Prueba final. Simulación de un caso práctico sobre los contenidos teóricos de la asignatura. La nota se corresponde con el 70% de la nota de la asignatura.

8.3: Consideraciones generales y recomendaciones para la evaluación y la recuperación:
A lo largo del curso se llevará a cabo un seguimiento y evaluación de las actividades presenciales y no presenciales.
Se realizará la parte de exposición y un examen práctico. La consideración global de ambas partes determinará la calificación final de la asignatura.
Repasar el contenido teórico de la materia

9.- Organización docente semanal

Prueba electrónica e informes periciales en el proceso penal

1.- Datos de la Asignatura					
Código	306.578	Plan	2025	ECTS	6
Carácter	Obligatoria de especialidad	Curso	1º	Periodicidad	2º Semestre
Idioma de impartición asignatura		español			
Área	Derecho Procesal				
Departamento	Derecho Administrativo, Financiero y Procesal				
Plataforma virtual	Studium https://moodle.usal.es				

1.1.- Datos del profesorado*			
Profesor Coordinador	Irene González Pulido	Grupo / s	Único
Departamento	Derecho Administrativo, Financiero y Procesal		
Área	Derecho Procesal		
Centro	Facultad de Derecho		
Despacho	283		
Horario de tutorías	Previa petición al correo electrónico: irenegopu@usal.es		
URL Web	https://produccioncientifica.usal.es/investigadores/148016/detalle		
E-mail	irenegopu@usal.es	Teléfono	Ext. 1652
Profesor Coordinador	Elena Gómez de Liaño	Grupo / s	Único
Departamento	Derecho Administrativo, Financiero y Procesal		
Área	Derecho Procesal		
Centro	Facultad de Derecho		
Despacho	283		
Horario de tutorías	Previa petición al correo electrónico: elenagomezdeliano@usal.es		
URL Web	https://produccioncientifica.usal.es/investigadores/57108/detalle		
E-mail	elenagomezdeliano@usal.es	Teléfono	Ext. 1652

2.- Recomendaciones previas

- Haber cursado el Grado en derecho o en criminología
- Seguir los materiales aportados por el profesorado

3.- Objetivos de la asignatura

1. Examinar el marco constitucional aplicable a la prueba electrónica en el ámbito de la cibercriminalidad, identificando los derechos fundamentales que pueden verse comprometidos durante su obtención y utilización —como el derecho a la intimidad, la protección de datos personales y la inviolabilidad de las comunicaciones—. Se analizarán los límites y garantías constitucionales que rigen la actuación estatal al recolectar evidencia digital, prestando especial atención al papel que cumple el perito informático forense en asegurar que dichas pruebas se obtengan conforme al debido proceso y a los principios de legalidad y proporcionalidad.
2. Analizar los procedimientos procesales específicos vinculados a la obtención, conservación, autenticación y valoración de la prueba digital en el marco de investigaciones penales por delitos informáticos. Este análisis incluirá el rol técnico-jurídico del perito informático en etapas clave como la preservación de la cadena de custodia, la implementación de medidas tecnológicas cautelares y la elaboración de informes periciales. Asimismo, se abordarán los mecanismos de cooperación internacional requeridos para acceder legalmente a datos electrónicos almacenados en jurisdicciones extranjeras.
3. Identificar y clasificar los diversos tipos de evidencia electrónica utilizados en la investigación penal, tales como registros de actividad digital, metadatos, archivos almacenados en la nube, comunicaciones electrónicas o rastros de navegación. Se destacará cómo el perito informático forense interviene en su extracción, análisis y presentación técnica mediante informes que deben cumplir criterios de claridad, integridad, trazabilidad y replicabilidad.
4. Examinar la jurisprudencia nacional e internacional relevante sobre la prueba electrónica, analizando los criterios adoptados por los tribunales en relación con su licitud, validez, exclusión o contradicción en juicio. Se prestará especial atención a los casos en que la intervención del perito informático ha resultado determinante para establecer la autenticidad o manipulación de las evidencias digitales.
5. Valorar el papel del perito informático forense como auxiliar técnico del órgano judicial, encargado de interpretar y certificar el contenido y la integridad de las pruebas electrónicas. Se analizará la relevancia de su informe pericial como medio de prueba, así como la necesidad de fortalecer las competencias interdisciplinares entre Derecho y Tecnología para afrontar con garantías los desafíos que plantea el entorno digital.
6. Reflexionar críticamente sobre los riesgos inherentes a la manipulación, pérdida o falsificación de evidencia digital, y proponer buenas prácticas, estándares técnico-jurídicos y protocolos periciales que garanticen la fiabilidad, legalidad y legitimidad de las pruebas electrónicas en el proceso penal, reforzando así la confianza judicial en el dictamen del perito informático.

4.- Competencias a adquirir / Resultados de aprendizaje

Resultados de aprendizaje

4.1: Conocimientos:

C1. Comprender y fundamentar las bases conceptuales de la ciberdelincuencia y su impacto en la obtención, tratamiento y valoración de pruebas digitales en el proceso penal.

C4. Evaluar herramientas legales y forenses necesarias para identificar, recolectar y asegurar evidencias electrónicas frente a diferentes modalidades de ciberamenazas y ciberdelitos.

C5. Interpretar la normativa nacional e internacional que regula la prueba digital, destacando el rol de autoridades, fiscales, jueces, cuerpos policiales y peritos en su obtención y utilización.

C6. Diferenciar las implicaciones probatorias derivadas de los delitos cometidos contra víctimas específicas (menores, colectivos vulnerables, víctimas de sextorsión, grooming, etc.) en entornos digitales.

C7. Contrastar jurisprudencia relevante (estatal y supranacional) sobre admisibilidad, ilicitud y valoración de pruebas tecnológicas en investigaciones de ciberdelitos

4.2: Habilidades:

H1. Identificar los principales riesgos jurídicos y técnicos asociados a la obtención y preservación de pruebas electrónicas en delitos informáticos, tanto en contextos nacionales como transnacionales, analizando cómo los nuevos entornos virtuales modifican los estándares probatorios tradicionales.

H2. Comprender el funcionamiento técnico de herramientas y entornos digitales (como redes, sistemas de cifrado, almacenamiento en la nube o registros de actividad), vinculándolos con las herramientas legales disponibles para asegurar la obtención legítima y eficaz de evidencia digital.

H3. Aplicar con precisión técnicas avanzadas de búsqueda, selección y análisis de legislación, doctrina y jurisprudencia relevante en materia de prueba electrónica, optimizando su uso en la investigación y litigación de delitos informáticos.

H4. Evaluar la viabilidad jurídica y técnica de diferentes medidas de investigación tecnológica (como registros remotos, captación de datos en tiempo real, interceptación de comunicaciones, etc.), atendiendo al tipo penal, la naturaleza de la prueba, la autoridad competente y la fase procesal.

H6. Identificar y argumentar con rigor jurídico las principales cuestiones procesales relacionadas con la admisibilidad, validez, contradicción y valoración de pruebas digitales en casos complejos de cibercriminalidad.

4.3: Competencias:

K1. Discriminar los distintos tipos de ciberdelito en función de las particularidades probatorias que presentan, comprendiendo los nuevos espacios virtuales en los que se generan las pruebas electrónicas, y aplicando la normativa vigente y la jurisprudencia relevante para su incorporación válida en el proceso penal.

K3. Analizar en profundidad los ciberdelitos desde la perspectiva probatoria, atendiendo a los perfiles diferenciados de víctimas y agresores, y evaluando el impacto que estas variables tienen sobre la forma de obtener, proteger y presentar la evidencia electrónica.

K5. Redactar documentos jurídicos relacionados con la prueba electrónica, incluyendo solicitudes de diligencias probatorias tecnológicas, valoraciones jurídicas sobre informes periciales informáticos y recursos procesales vinculados a la admisibilidad o licitud de evidencias digitales.

K6. Identificar con precisión las funciones y responsabilidades de los actores involucrados en el ciclo probatorio digital: fuerzas policiales encargadas de la intervención tecnológica, peritos informáticos responsables del análisis forense y elaboración de informes, fiscales que orientan la estrategia probatoria, y jueces que valoran la licitud y eficacia de la prueba. Conocer los requisitos legales y procesales que garantizan la validez del procedimiento, así como la importancia del trabajo conjunto entre pericia técnica e interpretación jurídica.

K7 / E1. Seleccionar y aplicar de forma crítica conocimientos jurídicos, procesales y técnicos necesarios para salvaguardar los derechos fundamentales durante la investigación tecnológica, asegurando que las pruebas electrónicas se obtengan y utilicen conforme a los principios de legalidad, proporcionalidad, necesidad y respeto al debido proceso, tanto en contextos nacionales como internacionales.

5.- Contenidos (temario)

1: Fundamentos jurídicos de la prueba electrónica y la teoría general de la prueba
- Concepto y características de la prueba electrónica
- Prueba digital vs. prueba tradicional: similitudes y diferencias

2: Marco normativo y jurisprudencial
- Normativa europea nacional sobre prueba digital en procesos penales
- Instrumentos internacionales (Convenio de Budapest, propuestas de e-Evidence, cooperación judicial penal europea)
- Jurisprudencia relevante (TC, TS, TEDH, TJUE) sobre obtención y validez de pruebas tecnológicas

3: Tipología de pruebas electrónica
- Tipos de evidencia digital
- Fuentes de prueba electrónicas y medios de prueba
- Preservación y aseguramiento de la prueba electrónica
- Cadena de custodia digital

4.. El perito informático: perfil y funciones
- Requisitos técnicos y legales.
- Perito judicial vs. perito de parte.
- Designación, recusación, deberes y responsabilidad.

5. Tipos de peritaje en el ámbito digital
- Forense informático (informática forense).
- Análisis de redes y tráfico.
- Análisis de dispositivos móviles.
- Peritaje en delitos de propiedad intelectual, fraude, acoso, intrusión, etc.

6.. El dictamen pericial informático
- Estructura del informe técnico.
- Lenguaje claro y técnico-jurídico.
- Presentación y defensa en juicio (ratificación y contrainterrogatorio).

7. Procedimiento probatorio y prueba electrónica
- Criterios de valoración judicial de la prueba electrónica
- Nulidad, ilicitud e impugnación de pruebas electrónicas
- Intervención del perito informático y presentación del informe pericial
- Estrategias de defensa y acusación en torno a la prueba electrónica

8. Cadena de custodia digital y peritaje forense
- Principios de conservación, integridad y trazabilidad.
- Uso de hash, imagen forense y duplicados exactos.
- Valor probatorio del informe pericial: estándares técnicos vs. estándares jurídicos.
- Estándares internacionales (ISO 27037, ENISA, NIST) y su aplicación práctica.

6.- Metodologías docentes

En el desarrollo de la asignatura se compatibilizarán diversas metodologías. Así, se empleará la clase magistral durante las sesiones teóricas, mientras que en las sesiones prácticas se utilizarán diversas estrategias metodológicas, tales como el análisis y la discusión de textos legislativos y/o jurisprudenciales, el análisis crítico de supuestos prácticos y normativa concreta, con utilización, en su caso, de los medios audiovisuales pertinentes, además del planteamiento de debates y seminarios que permitan la profundización en aspectos concretos de la asignatura.

6.1.- Distribución de metodologías docentes

		Horas dirigidas por el profesor		Horas de trabajo autónomo	HORAS TOTALES
		Horas presenciales.	Horas no presenciales.		
Sesiones magistrales		18		15	33
Prácticas	- 4		10	14	23
	- En el laboratorio				
	- En aula de informática				
	- De campo				
	- Otras (detallar)				
Seminarios					
Exposiciones y debates		2		5	7
Tutorías		2		3	5
Actividades de seguimiento online		2		2	4
Preparación de trabajos					
Otras actividades (detallar)					
Exámenes					
TOTAL		**30**		**45**	**75**

7.- Recursos, bibliografía, referencias electrónicas o de otro tipo

- BUENO DE MATA, Federico. *Prueba electrónica y proceso 2.0: especial referencia al proceso civil*. Valencia: Tirant lo Blanch, 2014.
- BUJOSA VADELL, Lorenzo Mateo. “La valoración de la prueba electrónica.” En *Fodertics 3.0: Estudios sobre derecho y nuevas tecnologías*, coordinado por Federico BUENO DE MATA, 75–85. Granada: Comares, 2015.
- BUJOSA VADELL, Lorenzo Mateo. “La prueba digital producto de la vigilancia secreta: obtención, admisibilidad y valoración en el proceso penal en España y Colombia.” *Revista Brasileira de Direito Processual Penal* 7, no. 2 (2021): 1347–84.
- BUENO DE MATA, Federico, y LORENZO BUJOSA VADELL. *La prueba electrónica en el marco de una administración de justicia informatizada: especial referencia al proceso civil*. Tesis doctoral, Universidad de Salamanca, 2013.
- DELGADO MARTÍN, Joaquín. *Investigación tecnológica y prueba digital en todas las jurisdicciones*. Madrid: La Ley, 2.ª ed., 2018.
- DELGADO MARTÍN, Joaquín. “La prueba electrónica en el proceso penal.” *Diario La Ley*, nº 8167 (10 Octubre 2013): doctrina jurídica especializada
- PINTO PALACIOS, Fernando, y Purificación PUJOL CAPILLA. *La prueba en la era digital*. Madrid: La Ley, 2017.
- PICÓ I JUNOY, Joan, y Xavier ABEL LLUCH, eds. *La prueba electrónica*. Barcelona: J. M. Bosch Editor, 2011.

8.- Evaluación

8.1: Criterios de evaluación: La nota final corresponderá a:

- 70% Evaluación Final. Simulación de un caso práctico a repartir el primer día de clase (Por parejas o individual en función del número de estudiantes matriculados)
- 30% Realización de prácticas por parte del alumnado de manera presencial en clase.

Para poder acudir a la CONVOCATORIA ORDINARIA deberá superarse la parte práctica de la asignatura.

8.2: Sistemas de evaluación:

- Participar en las clases prácticas y aprobar al menos el 50% de los casos prácticos. La nota media de las prácticas se corresponde con el 30% de la nota de la asignatura
- Intervenir en las clases teóricas.
- Prueba final. Simulación de un caso práctico sobre los contenidos teóricos de la asignatura. La nota se corresponde con el 70% de la nota de la asignatura.

8.3: Consideraciones generales y recomendaciones para la evaluación y la recuperación:
A lo largo del curso se llevará a cabo un seguimiento y evaluación de las actividades presenciales y no presenciales.

Se realizará la parte de exposición y un examen práctico. La consideración global de ambas partes determinará la calificación final de la asignatura.

9.- Organización docente semanal

TALLERES DE ACTUALIZACIÓN CRIMINOLÓGICA

1.- Datos de la Asignatura					
Código	306.587	Plan	2025	ECTS	3
Carácter	Obligatoria de especialidad	Curso	1º	Periodicidad	2do Semestre
Idioma de impartición asignatura		español			
Área	- Derecho penal, - Área de Ciencias de la computación e IA - Psicología social				
Departamento	- Departamento de Derecho Público General - Departamento de Informática y Automática - Departamento de Psicología Social y antropología				
Plataforma virtual	Studium https://moodle.usal.es				

1.1.- Datos del profesorado*			
Profesor Coordinador	Isabel García Domínguez	Grupo / s	Único
Departamento	Derecho público general		
Área	Derecho penal		
Centro	Facultad de Derecho		
Despacho	Seminario de Derecho penal, 291		
Horario de tutorías	A petición del alumnado a través del correo electrónico		
URL Web	*https://produccioncientifica.usal.es/investigadores/148226/detalle*		
E-mail	isabelgarciadominguez@usal.es	Teléfono	
Profesor Coordinador	Pendiente de asignación	Grupo / s	
Departamento	Departamento de Informática y Automática		
Área	Área de Ciencias de la computación e IA		
Centro	Facultad de Ciencias		
Despacho			
Horario de tutorías			
URL Web			
E-mail		Teléfono	
Profesor Coordinador	CARMEN HERRERO ALONSO	Grupo / s	
Departamento	Departamento de Psicología Social y antropología		
Área	Psicología Social		
Centro	Facultad de Psicología		
Despacho	114		

Horario de tutorías	A concretar con el alumnado previa petición por mail		
URL Web	*https://produccioncientifica.usal.es/investigadores/56941/detalle*		
E-mail	cherrero@usal.es	Teléfono	

2.- Recomendaciones previas

Superar las asignaturas obligatorias del primer cuatrimestre relativas a la ciberdelincuencia y el Derecho penal, los fundamentos de la seguridad informática y aspectos legales de la ciberdelincuencia

3.- Objetivos de la asignatura

- Profundizar en fenómenos delictivos en el ámbito de la cibercriminalidad
- Fomentar el pensamiento crítico sobre las estrategias adoptadas de prevención e intervención de la ciberdelincuencia
- Identificar y valorar los principales procesos psicológicos y el impacto de la cultura en las entrevistas de investigación con víctimas y testigos.
- Reconocer algunos de los sesgos fundamentales en la investigación policial y en la utilización las ciencias forenses.
- Familiarizarse con el impacto de la tecnología en el sistema de justicia.

4.- Competencias a adquirir / Resultados de aprendizaje

Resultados de aprendizaje

4.1: Conocimientos:
C3. Identificar de forma exhaustiva el funcionamiento de los diferentes tipos de cibercrimen; modus operandi, autoría, víctimas, tecnología empleada.
C4. Evaluar las herramientas técnicas y legales necesarias para analizar y hacer frente a diferentes riesgos, ciberamenazas y ciberdelitos.
C6. Discriminar, por un lado, las particularidades de las personas víctimas de las actividades ilícitas que llevan a cabo los criminales utilizando tecnologías de la información y las comunicaciones; y, por otro, las necesidades de intervención que se derivan tras estos delitos.
C7. Contrastar la jurisprudencia estatal y supranacional en materia de ciberdelincuencia e investigación tecnológica
C9. E2 Comparar conocimientos específicos para elaborar estudios e informes criminológicos en el ámbito de la ciberdelincuencia y profundizar en las teorías criminológicas que explican el delito en el ciberespacio, así como otros factores relacionados con el proceso penal.

4.2: Habilidades:
H1. Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales
H3. Practicar con pericia la búsqueda de legislación y jurisprudencia a través de diferentes técnicas que puedan favorecer la investigación, la prueba y la intervención ante ciberdelitos.
H5. Aplicar con dominio la normativa nacional e internacional que regula la ciberdelincuencia, así como su persecución, investigación y represión en casos concretos.
H6. Concluir las cuestiones jurídicas más relevantes implicadas en un conjunto complejo de hechos relacionados con casos de cibercriminalidad.
H9. E2 Ante casos específicos de cibercriminalidad, elaborar, exponer y defender informes criminológicos jurídicamente fundamentados adecuados al caso y en relación con las exigencias procedimentales.
H10. E2 Desarrollar estrategias de prevención e intervención ante ciberataques u otro tipo de ciberdelitos, razonando y argumentando la propuesta con un enfoque interdisciplinar y teniendo en cuenta las particularidades de las víctimas para que la propuesta responda a las necesidades de éstas.

4.3: Competencias:
K1. Discriminar los tipos de ciberdelito, comprendiendo los nuevos espacios virtuales y, en atención a ellos, aplicar la normativa vigente y las resoluciones jurisprudenciales vinculantes en cada caso en cuestión
K3. Analizar pormenorizadamente cada ciberdelito, incluyendo perfiles diferenciados de víctimas y agresores en el uso de la tecnología cibernética
K5. En casos de cibercriminalidad, redactar textos legales para los diferentes momentos procesales y desde el punto de vistas de diferentes profesiones implicadas, y que estos textos sean comprensibles tanto para un público especialista como para un público profano
K6. Discriminar las funciones de cada una de las autoridades y profesionales que intervienen en casos de ciberdelincuencia, identificando los requisitos formales que van ligados a todas ellas para poder poner en práctica las mismas
K9. E2 Elaborar informes criminológicos relacionados con el ciberdelito, en los que se seleccione los conocimientos específicos y las cualidades más idóneos y en los que se identifiquen los factores que favorecen la criminalidad y se defina y reconstruya el modus operandi o la actuación posterior.
K10. E2 Determinar, tras su evaluación, el tratamiento individualizado de las víctimas de un cibercrimen, así como planes de prevención para hacer frente a los riesgos derivados de este tipo de criminalidad en diferentes sectores de la población

5.- Contenidos (temario)

Parte A. Derecho penal
- Inteligencia Artificial
- Discursos y delitos de odio *online*
- Delitos contra la libertad sexual en el ciberespacio
- Retos criminológicos en la prevención de la ciberdelincuencia

Parte B. Psicología Social y Jurídica
- Procesos psicológicos, cultura y entrevistas de investigación (víctimas y testigos)
- Sesgos (cognitivos) en la investigación policial y en la utilización de las ciencias forenses.
- Impacto de la tecnología en el sistema de justicia

Parte C. Pendiente de designar

6.- Metodologías docentes

Las clases consistirán en seminarios con debates y comentarios críticos. También se trabajarán sentencias y análisis de casos relevantes.

6.1.- Distribución de metodologías docentes

		Horas dirigidas por el profesor		Horas de trabajo autónomo	HORAS TOTALES
		Horas presenciales.	Horas no presenciales.		
Sesiones magistrales		10		10	20
Prácticas	- En aula				
	- En el laboratorio				
	- En aula de informática				
	- De campo				
	- Otras (detallar)				
Seminarios		12		10	22
Exposiciones y debates					
Tutorías					
Actividades de seguimiento online			6	10	16
Preparación de trabajos					
Otras actividades (detallar)					
Exámenes		2		15	17

TOTAL	**24**	**6**	**45**	**75**

7.- Recursos, bibliografía, referencias electrónicas o de otro tipo

DeMatteo, D. y Scherr, K. C. (2023) (Eds.). *The Oxford Handbook of Psychology and law*. Oxford University Press.

Dror, I. (2020). Cognitive and human factors in expert decisión making. *Analytical Chemistry, 92*, 7998-8004. https://dx.doi.org/10.1021/acs.analchem.0c00704.

Elmer et al. (2024). Acoso Sexual en Videojuegos en Línea. *RISTI: Revista Ibérica de Sistemas e Tecnologias de Informação (*75), 314-325

García Domínguez, I. (2025). Delitos de odio online en España. Una revisión sistemática de sentencias (años 2018-2022). *Revista Española De Investigación Criminológica*, *22*(2), e890. https://doi.org/10.46381/reic.v22i2.890

Koen, W. J. y Bowers, C. M. (Ed.) (2018). *The psychology and sociology of wrongful convictions: forensic science reform*. Academic Press.

Leukfeldt, R. y Holt, T. J. (2020). *The Human Factor of Cybercrime*. Routledge.

Miró Llinares. (2023). Digitalización y algoritmización de la justicia introducción a un monográfico en tiempos de regulación de la IA. *IDP: revista de Internet, derecho y política = revista d'Internet, dret i política* (39).

Oxburgh, G. et al. (2016*). Communication in investigative and legal contexts*. Wiley

Pica, E., Ross, D. y Pozzulo, J. (2024) *The Impact of Technology on the Criminal Justice System: A Psychological Overview.* Routledge.

Villacampa Estiarte y Gómez Adillon. (2016). Nuevas tecnologías y victimización sexual de menores por online grooming. *Revista electrónica de ciencia penal y criminología*, (18).

Whitty, M. T y Young, G. (2027). *Cyberpsychology: the study of individuals, society and digital technologies*. Wiley.

8.- Evaluación

8.1: Criterios de evaluación:

Se seguirá un sistema de evaluación continua con la realización de un examen final, siendo los porcentajes los siguientes

- 30-40% de la calificación se obtendrá de la asistencia a los seminarios y resolución de casos prácticos, debates y otras actividades propuestas por el profesorado.
- 70-60% examen final: dependiendo de las partes podrán utilizarse preguntas tipo test y/o preguntas cortas de desarrollo, tanto en convocatoria ordinaria como extraordinaria..

Es necesario obtener un 5/10 en el examen final para superar la asignatura. El 30-40% de la evaluación continua no es recuperable.

8.2: Sistemas de evaluación:

- Asistencia seminarios
- Resolución de casos prácticos y realización de otras actividades propuestas
- Examen final

8.3: Consideraciones generales y recomendaciones para la evaluación y la recuperación:

Se recomienda la asistencia a los seminarios con el fin de obtener los conocimientos teórico-prácticos necesarios para superar la asignatura.

9.- Organización docente semanal

Los seminarios se desarrollarán a lo largo del segundo cuatrimestre en sesiones con diferentes horarios y días. Estos se fijarán al final del primer cuatrimestre

Teorías criminológicas y ciberespacio

1.- Datos de la Asignatura					
Código	306.582	Plan	2025	ECTS	3
Carácter	Obligatoria de especialidad	Curso	1º	Periodicidad	Segundo Semestre
Idioma de impartición asignatura		español			
Área	Derecho Penal				
Departamento	Derecho Público General				
Plataforma virtual	Studium https://moodle.usal.es				

1.1.- Datos del profesorado*			
Profesor Coordinador	LAURA PASCUAL MATELLÁN	Grupo / s	Único
Departamento	Derecho Público General		
Área	Derecho Penal		
Centro	Facultad de Derecho		
Despacho	259		
Horario de tutorías	Se solicitará cita por correo electrónico		
URL Web	https://produccioncientifica.usal.es/investigadores/107719/detalle https://jeanmonnetprisons.usal.es/		
E-mail	nicte@usal.es	Teléfono	+34 923 29 45 00 ext. 6966

2.- Recomendaciones previas

Tener conocimientos de Derecho penal y/o de Criminología

3.- Objetivos de la asignatura

- Comprender las teorías criminológicas clásicas y su evolución hacia enfoques contemporáneos.
- Evaluar cómo estas teorías pueden adaptarse al contexto delictivo digital.
- Explorar las características propias del ciberespacio como nuevo escenario criminológico.
- Relacionar las teorías criminológicas con las tipologías delictivas en el entorno digital.
- Aplicar marcos teóricos a delitos como el hacking, phishing, grooming, ciberacoso, delitos financieros, etc.
- Evaluar su utilidad y limitaciones en contextos virtuales.
- Analizar críticamente los enfoques actuales sobre ciberdelincuencia desde una perspectiva interdisciplinaria.
- Fomentar la reflexión sobre nuevas necesidades teóricas.
- Fomentar una perspectiva crítica y ética frente al uso de herramientas tecnológicas en la prevención e investigación del ciberdelito.
- Promover el pensamiento crítico ante los discursos alarmistas o reduccionistas sobre el crimen en línea.

4.- Competencias a adquirir / Resultados de aprendizaje

Resultados de aprendizaje

4.1: Conocimientos:

C3. Identificar de forma exhaustiva el funcionamiento de los diferentes tipos de cibercrimen; modus operandi, autoría, víctimas, tecnología empleada.

C5. Interpretar la normativa nacional e internacional que regula la ciberdelincuencia, así como las funciones de autoridades y profesionales en el marco de detección, prevención, actuación e intervención en casos de ciberdelincuencia.

C6. Discriminar, por un lado, las particularidades de las personas víctimas de las actividades ilícitas que llevan a cabo los criminales utilizando tecnologías de la información y las comunicaciones; y, por otro, las necesidades de intervención que se derivan tras estos delitos. el proceso penal, así como a otras instituciones públicas o privadas.

C9. E2 Comparar conocimientos específicos para elaborar estudios e informes criminológicos en el ámbito de la ciberdelincuencia y profundizar en las teorías criminológicas que explican el delito en el ciberespacio, así como otros factores relacionados con el proceso penal.

4.2: Habilidades:

H1. Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales

H3. Practicar con pericia la búsqueda de legislación y jurisprudencia a través de diferentes técnicas que puedan favorecer la investigación, la prueba y la intervención ante ciberdelitos.

H5. Aplicar con dominio la normativa nacional e internacional que regula la ciberdelincuencia, así como su persecución, investigación y represión en casos concretos.

H6. Concluir las cuestiones jurídicas más relevantes implicadas en un conjunto complejo de hechos relacionados con casos de cibercriminalidad.

H9. E2 Ante casos específicos de cibercriminalidad, elaborar, exponer y defender informes criminológicos jurídicamente fundamentados adecuados al caso y en relación con las exigencias procedimentales.

4.3: Competencias:

K1. Discriminar los tipos de ciberdelito, comprendiendo los nuevos espacios virtuales y, en atención a ellos, aplicar la normativa vigente y las resoluciones jurisprudenciales vinculantes en cada caso en cuestión

K3. Analizar pormenorizadamente cada ciberdelito, incluyendo perfiles diferenciados de víctimas y agresores en el uso de la tecnología cibernética

K5. En casos de cibercriminalidad, redactar textos legales para los diferentes momentos procesales y desde el punto de vistas de diferentes profesiones implicadas, y que estos textos sean comprensibles tanto para un público especialista como para un público profano

K6. Discriminar las funciones de cada una de las autoridades y profesionales que intervienen en casos de ciberdelincuencia, identificando los requisitos formales que van ligados a todas ellas para poder poner en práctica las mismas

K10. E2 Determinar, tras su evaluación, el tratamiento individualizado de las víctimas de un cibercrimen, así como planes de prevención para hacer frente a los riesgos derivados de este tipo de criminalidad en diferentes sectores de la población

5.- Contenidos (temario)

Tema 1. Las teorías criminológicas
Tema 2. La Escuela Clásica
Tema 3. Teorías biológicas
Tema 4. Teoría de la desorganización social
Tema 5. Teoría de la asociación diferencial
Tema 6. Teoría de la anomia
Tema 7. Teoría de las subculturas delictivas
Tema 8. Teorías del control
Tema 9. Teoría del etiquetamiento

Tema 10. Criminología Crítica
Tema 11. Las teorías criminológicas y el ciberespacio

6.- Metodologías docentes

Clases magistrales, seminarios especializados y debate en el aula para fomentar el espíritu crítico.

6.1.- Distribución de metodologías docentes

		Horas dirigidas por el profesor		Horas de trabajo autónomo	HORAS TOTALES
		Horas presenciales.	Horas no presenciales.		
Sesiones magistrales		18			
Prácticas	- En aula	3			
	- En el laboratorio				
	- En aula de informática				
	- De campo				
	- Otras (detallar)				
Seminarios		1		10	
Exposiciones y debates		2		10	
Tutorías		4		5	
Actividades de seguimiento online					
Preparación de trabajos					
Otras actividades (detallar)					
Exámenes		2		20	
TOTAL		**30**		**45**	

7.- Recursos, bibliografía, referencias electrónicas o de otro tipo

1. Fernando Miró: "La victimización por cibercriminalidad social. Un estudio a partir de la Teoría de las Actividades Cotidianas en el Ciberespacio", *Revista Española de Investigación Criminológica*, 2013.
2. Stephen Pfohl: *Images of Desviance and Social Control*, New York, McGraw-Hill, 1994.
3. Elena Larrauri: *La Herencia de la Criminología Crítica*, Madrid, Siglo XXI, 1991.
4. Antonio García Pablos de Molina: *Tratado de Criminología*, Valencia, Tirant Lo Blanch, 1999.
5. Albert Cohen: "An Elaboration of Anomie Theory", en N. Passas; R. Agnew (eds.), *The Future of Anomie Theory,* Boston, Northeastern University Press.
6. Stanley Cohen: *Visions of Social Control,* Cambridge, Polity Press, 1985.
7. Vicente Garrido, Per Stangeland y Santiago Redondo: *Principios de Criminología*, Valencia, Tirant Lo Blanch, 1999.
8. Laura Pascual Matellán: *Pedro Dorado Montero y el correccionalismo español. El difícil desafío de humanizar el Derecho penal*, Valencia, Tirant Lo Blanch, 2021.
9. Nieves Sanz Mulas: *Evolución de la política criminal y sus protagonistas. Del totalitarismo de la raza al totalitarismo del dinero*, Valencia, Tirant Lo Blanch, 2021.
10. Alfonso Serrano Maíllo: *Teoría criminológica. La explicación del delito en la sociedad contemporánea*, Editorial Dykinson, 2021.

8.- Evaluación

8.1: Criterios de evaluación: Para poder presentarse al examen es preciso haber asistido al 80% de las clases.
8.2: Sistemas de evaluación: El examen escrito representa el 100% de la calificación, tanto para la convocatoria ordinaria como extraordinaria
8.3: Consideraciones generales y recomendaciones para la evaluación y la recuperación: Se recomienda asistir a las clases y participar activamente.

9.- Organización docente semanal

LA VÍCTIMA EN EL CIBERESPACIO: CUESTIONES PENALES Y PROCESALES

1.- Datos de la Asignatura					
Código	306.575	Plan	2025	ECTS	3
2	Obligatoria	Curso	1º	Periodicidad	2do semestre
Idioma de impartición asignatura		español			
Área	Derecho penal y Derecho procesal				
Departamento	Derecho público general				
Plataforma virtual	Studium https://moodle.usal.es				

1.1.- Datos del profesorado*			
Profesor Coordinador	Isabel García Domínguez	Grupo / s	Único
Departamento	Derecho público general		
Área	Derecho penal		
Centro	Facultad de Derecho		
Despacho	Seminario de Derecho penal, 291		
Horario de tutorías	A petición del alumnado a través del correo electrónico		
URL Web	*https://produccioncientifica.usal.es/investigadores/148226/detalle*		
E-mail	isabelgarciadominguez@usal.es	Teléfono	
Profesor Coordinador	Irene González Pulido	Grupo / s	Único
Departamento	Derecho Administrativo, Financiero y Procesal		
Área	Derecho procesal		
Centro	Facultad de Derecho		
Despacho	283		
Horario de tutorías	Solicitud a través de email: irenegopu@usal.es		
URL Web	*https://produccioncientifica.usal.es/investigadores/148016/detalle*		
E-mail	irenegopu@usal.es	Teléfono	
Profesor Coordinador	Elena Gómez De Liaño Diego	Grupo / s	Único
Departamento	Derecho Administrativo, Financiero y Procesal		
Área	Derecho procesal		
Centro	Facultad de Derecho		
Despacho	283		
Horario de tutorías	Solicitud a través de email		
URL Web	*https://produccioncientifica.usal.es/investigadores/57108/detalle*		

E-mail	elenagomezdeliano@usal.es	Teléfono	

2.- Recomendaciones previas

Se recomiendan nociones sobre las bases del Derecho procesal, el Derecho penal y la Criminología

3.- Objetivos de la asignatura

Parte A

- Conocer los derechos de las víctimas en el ciberespacio y las medidas de protección disponibles.
- Examinar la victimización secundaria que pueden experimentar las cibervíctimas y las oportunidades tecnológicas para minimizarla.
- Analizar los instrumentos y las vías de reparación del daño ocasionado por la ciberdelincuencia.

Parte B

- Identificar y conocer las características de las víctimas en el espacio, así como sus tipologías principales
- Estudiar los factores de riesgo y vulnerabilidad de la cibervictimización
- Conocer las consecuencias psico-sociales de las víctimas en el espacio
- Identificar y analizar las estadísticas de cibervictimización
- Diseñar estrategias de prevención de la victimización digital

4.- Competencias a adquirir / Resultados de aprendizaje

Resultados de aprendizaje

4.1: Conocimientos:

C1. Defender las bases conceptuales de la ciberdelincuencia, ciberamenazas y la seguridad informática

C3. Identificar de forma exhaustiva el funcionamiento de los diferentes tipos de cibercrimen; modus operandi, autoría, víctimas, tecnología empleada.

C6. Discriminar, por un lado, las particularidades de las personas víctimas de las actividades ilícitas que llevan a cabo los criminales utilizando tecnologías de la información y las comunicaciones; y, por otro, las necesidades de intervención que se derivan tras estos delitos.

4.2: Habilidades:

H1. Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales

H3. Practicar con pericia la búsqueda de legislación y jurisprudencia a través de diferentes técnicas que puedan favorecer la investigación, la prueba y la intervención ante ciberdelitos

H4. Evaluar la viabilidad de diferentes herramientas y medidas de investigación en atención al tipo de delictivo presentado, las autoridades involucradas y el momento procesal del caso

H6. Concluir las cuestiones jurídicas más relevantes implicadas en un conjunto complejo de hechos relacionados con casos de cibercriminalidad.

4.3: Competencias:

K1. Discriminar los tipos de ciberdelito, comprendiendo los nuevos espacios virtuales y, en atención a ellos, aplicar la normativa vigente y las resoluciones jurisprudenciales vinculantes en cada caso en cuestión

K3. Analizar pormenorizadamente cada ciberdelito, incluyendo perfiles diferenciados de víctimas y agresores en el uso de la tecnología cibernética

K5. En casos de cibercriminalidad, redactar textos legales para los diferentes momentos procesales y desde el punto de vistas de diferentes profesiones implicadas, y que estos textos sean comprensibles tanto para un público especialista como para un público profano

K6. Discriminar las funciones de cada una de las autoridades y profesionales que intervienen en

casos de ciberdelincuencia, identificando los requisitos formales que van ligados a todas ellas para poder poner en práctica las mismas

5.- Contenidos (temario)

PARTE A. CUESTIONES PROCESALES

1. Los derechos de las víctimas de ciberdelitos en el proceso
2. Victimización secundaria en casos de ciberdelincuencia: oportunidades de la tecnología.
3. Medidas de protección para las cibervíctimas: marco nacional, europeo e internacional.
4. Particularidades de las cibervíctimas menores de edad y proceso
5. Reparación del daño en casos de ciberdelincuencia

PARTE B. CUESTIONES PENALES

1. La víctima en el ciberespacio: conceptos clave
2. Tipologías generales, factores de riesgo y vulnerabilidad
3. Impacto de la cibervictimización
4. Fuentes de datos oficiales y extraoficiales
5. Prevención del ciberdelito y buenas prácticas

6.- Metodologías docentes

Las clases consistirán en sesiones magistrales combinadas con prácticas, seminarios, debates y comentarios de artículos de investigación relevantes. También se trabajarán sentencias y análisis de casos relevantes.
Se podrán incorporar sistemas de innovación docente para la consecución de los objetivos.

6.1.- Distribución de metodologías docentes

		Horas dirigidas por el profesor		Horas de trabajo autónomo	HORAS TOTALES
		Horas presenciales.	Horas no presenciales.		
Sesiones magistrales		16		10	26
Prácticas	- En aula	8		15	23
	- En el laboratorio				
	- En aula de informática				
	- De campo				
	- Otras (detallar)				
Seminarios		2		5	7
Exposiciones y debates					
Tutorías					
Actividades de seguimiento online		2		5	7
Preparación de trabajos					
Otras actividades (detallar)					
Exámenes		2		10	12
TOTAL		**30**		**45**	**75**

7.- Recursos, bibliografía, referencias electrónicas o de otro tipo

PARTE A

BUENO DE MATA, F. “Bases legales y puntos clave para la configuración de un protocolo de videograbación de la declaración de menores víctimas de violencia de género”. *Proceso penal y víctimas especialmente vulnerables: aspectos interdisciplinares* / coord. por Alicia González Monje; Lorenzo Mateo Bujosa Vadell (dir.), Marta del Pozo Pérez (dir.), 2019, ISBN 9788413091013, págs. 281-297

GONZÁLEZ PULIDO, I. “Víctimas de ciberdelincuencia de género y proceso penal: victimización secundaria”. *Proceso penal y víctimas especialmente vulnerables: aspectos interdisciplinares* / coord. por Alicia González Monje; Lorenzo Mateo Bujosa Vadell (dir.), Marta del Pozo Pérez (dir.), 2019, ISBN 9788413091013, págs. 353-376

RODRÍGUEZ TIRADO, A.M. *Vulnerabilidad y proceso penal de menores por delitos sexuales.* Aranzadi, 2021.
RODRÍGUEZ TIRADO, A.M. "Las víctimas menores de delitos de pornografía infantil y de delitos de child grooming y su protección en el proceso penal. Las TICs y las diligencias de investigación tecnológica". *Justicia: revista de derecho procesal*, ISSN 0211-7754, Nº 1, 2018, págs. 137-200.
JULIEN DE ASÍS, J. *La participación de la víctima menor de edad en el proceso penal.* Tirant lo Blanch, 2025.
SEMPERE FAUS, S. *La participación de la víctima en el proceso penal y la victimización secundaria.* Tirant lo Blanch, 2025.

PARTE B

Espinosa Sánchez. (2019). Ciberdelincuencia. Aproximación criminológica de los delitos en la red. La razón histórica. *Revista hispanoamericana de Historia de las Ideas* (44), 153-173.
Miró-Llinares. (2012). *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio*. Marcial Pons.
Morillas Fernández et al. (2011). *Victimología: un estudio sobre la víctima y los procesos de victimización.* Dykinson. ISBN 978-84-15454-25-0
Torres Manrique. (2024). *Nuevos desafíos de la criminalidad en el ciberpesacio*. Editorial Bosh

8.- Evaluación

8.1: Criterios de evaluación:

Se seguirá un sistema de evaluación continua con la realización de un examen final, siendo los porcentajes los siguientes

- 40% de la calificación se obtendrá a través de los casos prácticos realizados en clase, en *studium* y otras actividades que se propongan a lo largo de las clases. De esta calificación un 20% corresponderá a la parte A de procesal y el 20% restante a la parte B de penal.
- 60% examen final. De preguntas cortas de la Parte A y tipo test de la parte B.

Es obligatorio obtener un 5 tanto en las prácticas de la parte A de procesal, como en la parte B referente a penal. También es necesario tener aprobadas las dos partes del examen, tanto la de la Parte A como de la B, se considerara cada parte aprobada a partir del 5/10 para poder hacer media con la otra parte.

En el caso de que no se superase la asignatura en convocatoria ordinaria, se realizará un examen tipo preguntas cortas de la parte A y tipo test de la parte B.

Se reservará la nota de prácticas para la convocatoria extraordinaria en caso de haber sido superada. Si no se hubieran superado será necesario realizar un examen práctico en la convocatoria extraordinaria (en la convocatoria ordinaria no habrá examen de prácticas, ya que se habrán evaluado de forma continua a lo largo de la asignatura).

8.2: Sistemas de evaluación:

- Prácticas evaluables, casos prácticos y comentarios de artículos
- Asistencia a prácticas, seminarios, talleres y/o congresos indicados por el profesorado.
- Examen final

8.3: Consideraciones generales y recomendaciones para la evaluación y la recuperación:

Se recomienda y se valorará positivamente la asistencia a las clases con el fin de obtener los conocimientos teórico-prácticos necesarios para superar la asignatura.

9.- Organización docente semanal

El mes de febrero se impartirá el contenido procesal y, subsiguientemente, en el mes de marzo se centrará en los aspectos penales

MODELO ÚNICO de guía docente de asignaturas de Grado y Máster Universitario
Curso 2025-2026

Talleres de actualización jurídica

1.- Datos de la Asignatura					
Código	306.581	Plan	2025	ECTS	6
Carácter	Obligatoria de especialidad	Curso	1º	Periodicidad	2º Semestre
Idioma de impartición asignatura		español			
Área	Derecho Constitucional, Derecho Administrativo y Derecho Procesal				
Departamento	Derecho Administrativo, Financiero y Procesal y Derecho Público General				
Plataforma virtual	Studium https://moodle.usal.es				

1.1.- Datos del profesorado*			
Profesor Coordinador	Federico Bueno de Mata	Grupo / s	Único
Departamento	Derecho Administrativo, Financiero y Procesal		
Área	Derecho Procesal		
Centro	Facultad de Derecho		
Despacho	2		
Horario de tutorías	Previa petición al correo electrónico: fmdiz@usal.es		
URL Web			
E-mail	febuma@usal.es	Teléfono	Ext. 1698
Profesor Coordinador	Daniel Terrón Santos	Grupo / s	Único
Departamento	Derecho Administrativo, Financiero y Procesal		
Área	Derecho Administrativo		
Centro	Facultad de Derecho		
Despacho	255		
Horario de tutorías	Previa petición por correo electrónico datersa@usal.es		
URL Web			
E-mail	datersa@usal.es	Teléfono	Ext. 1645
Profesor Coordinador	José Luis Mateos Crespo	Grupo/s	Único
Departamento	Derecho Público General		
Área	Derecho Constitucional		
Centro	Facultad de Derecho		
Despacho	105		

Horario de tutorías	Previa petición por correo electrónico		
URL Web			
E-mail	joseluismateos@usal.es	Teléfono	923 29 45 00 (Ext. 6950)

2.- Recomendaciones previas

- Haber cursado el Grado en Derecho o en Criminología
- Seguir los materiales aportados por el profesorado

3.- Objetivos de la asignatura

1. Analizar, desde una perspectiva multidisciplinaria, los desafíos jurídicos que plantea el cibercrimen, mediante el estudio y aplicación de normas, principios y procedimientos propios del derecho procesal, constitucional y administrativo, con el fin de formar profesionales capaces de interpretar, prevenir y abordar jurídicamente las nuevas formas delictivas en el entorno digital.
2. Promover la constante actualización del marco normativo, doctrinal y jurisprudencial frente a las transformaciones tecnológicas que inciden en la comisión, prevención e investigación del cibercrimen, desde una perspectiva integral del derecho constitucional, procesal y administrativo.
3. Incentivar el análisis jurídico de fenómenos emergentes en el ámbito digital (como inteligencia artificial, blockchain, deepfakes, Internet de las cosas, etc.) y su vinculación con nuevas formas delictivas, garantizando la protección de derechos fundamentales y el cumplimiento del debido proceso.
4. Consolidar habilidades prácticas y argumentativas para aplicar el derecho a casos reales y simulados de cibercrimen, considerando las transformaciones anuales del ecosistema tecnológico y su efecto en la interpretación y aplicación de las normas jurídicas.

4.- Competencias a adquirir / Resultados de aprendizaje

Resultados de aprendizaje

4.1: Conocimientos:

C1. Conocer los principios, normas y procedimientos aplicables al cibercrimen desde el derecho procesal, constitucional y administrativo.

C2. Identificar los distintos tipos de delitos informáticos y su clasificación doctrinal y normativa, en función de su evolución anual.

C3. Comprender los derechos fundamentales afectados por el uso indebido de tecnologías digitales, incluyendo privacidad, protección de datos, libertad de expresión y acceso a la información.

C4. Conocer las facultades y limitaciones de las autoridades administrativas y judiciales en la persecución y prevención del cibercrimen.

C5. Reconocer la incidencia de nuevas tecnologías (IA, blockchain, IoT, etc.) en la transformación del fenómeno criminal y su tratamiento jurídico.

C6. Comprender los desafíos jurídicos que implica la obtención, admisibilidad y valoración de la prueba digital en el proceso penal.

4.2: Habilidades:

H1. Analizar críticamente casos reales o simulados de cibercrimen desde diversas ópticas jurídicas.

H2. Aplicar criterios jurídicos actualizados para interpretar normas procesales, constitucionales y administrativas en escenarios tecnológicos emergentes.

H3. Formular estrategias legales frente a delitos informáticos, considerando aspectos procedimentales, jurisdiccionales y de protección de derechos.
H4. Evaluar la constitucionalidad y legalidad de medidas administrativas o judiciales en contextos de vigilancia y control digital.
H5. Investigar y sistematizar información jurídica y técnica sobre nuevas tecnologías aplicadas al crimen digital.
H6. Diseñar propuestas de mejora normativa o institucional adaptadas al avance tecnológico.
H7. Resolver problemas jurídicos mediante el trabajo colaborativo, la argumentación y el uso de entornos digitales.

4.3: Competencias:
K1. Integrar conocimientos jurídicos multidisciplinarios para abordar de forma eficaz el tratamiento jurídico del cibercrimen en un entorno cambiante.
K2. Adaptar la interpretación y aplicación del derecho a los retos éticos, jurídicos y sociales derivados del uso de tecnologías disruptivas.
K3. Emitir juicios jurídicos informados y fundamentados frente a casos complejos que involucren delitos informáticos y derechos fundamentales.
K4. Proponer reformas legales o soluciones administrativas ante lagunas normativas derivadas del avance tecnológico.
K5. Comunicar eficazmente argumentos jurídicos sobre cibercrimen a distintos públicos, tanto técnicos como no especializados.
K6. Colaborar con profesionales del derecho, la informática y la administración pública para prevenir, investigar y sancionar el cibercrimen.
K7. Evaluar la eficacia de las políticas públicas y marcos regulatorios frente al cibercrimen, con base en principios de legalidad, proporcionalidad y derechos humanos**.**
.

5.- Contenidos (temario)

El contenido de los talleres será dinámico en función de la evolución normativa y tecnológica. Cada año podrá sufrir modificaciones por cuestiones propias de oportunidad. Se darán talleres en las tres áreas de conocimiento implicadas a través de formatos como charlas conferencias debates etc.

6.- Metodologías docentes

Clases magistrales teórico-prácticas, seminarios especializados, comentarios jurisprudenciales y debate en el aula para fomentar el espíritu crítico.

6.1.- Distribución de metodologías docentes

		Horas dirigidas por el profesor		Horas de trabajo autónomo	HORAS TOTALES
		Horas presenciales.	Horas no presenciales.		
Sesiones magistrales		6			6
Prácticas	- En aula	12		40	52
	- En el laboratorio				
	- En aula de informática				
	- De campo				
	- Otras (detallar)				
Seminarios		18		20	
Exposiciones y debates		12		10	22
Tutorías		2		5	7
Actividades de seguimiento online		10		15	25

Preparación de trabajos				
Otras actividades (detallar)				
Exámenes				
TOTAL	**60**		**90**	**150**

7.- Recursos, bibliografía, referencias electrónicas o de otro tipo

Cada taller proporcionará talleres autónomos en función del tema tratado que estará disponible a través de la plataforma moodle

8.- Evaluación

8.1: Criterios de evaluación:

8.2: Sistemas de evaluación:

- Ordinaria. Asistencia y participación activa en cada una de las tareas de actualización a través de la entrega de trabajos y resúmenes o trabajos vinculados. 100%

8.3: Consideraciones generales y recomendaciones para la evaluación y la recuperación:

Examen con preguntas cortas vinculados a los contenidos de los talleres planteados.

9.- Organización docente semanal

Organización vinculada al calendario de cada año, utilizando horas del horario planteado y avisando al alumnado con una antelación de dos semanas de su realización.