ANÁLISIS FORENSE

1.- Datos de la Asignatura					
Código	306558	Plan	M204-1	ECTS	6
Carácter	Optativa	Curso	1	Periodicidad	Semestre 2
Idioma de impartición asignatura		Español			
Área	Ciencia de la Computación e Inteligencia Artificial				
Departamento	Informática y Automática				
Plataforma virtual	Studium http://studium.usal.es				

1.1.- Datos del profesorado			
Profesor Coordinador	Emilio S. Corchado Rodríguez	Grupo / s	1
Departamento	Informática y Automática		
Área	Ciencia de la Computación e Inteligencia Artificial		
Centro	Facultad de Ciencias		
Despacho	Rector Tovar, nº 7-11, 1ªplanta		
Horario de tutorías	Lunes 11:00-15:00 y jueves de 12:00-16:00		
URL Web	https://produccioncientifica.usal.es/investigadores/57340/detalle		
E-mail	escorchado@usal.es	Teléfono	630736755

1.2.- Datos del profesorado			
Profesor	Davinia Carolina Zato Domínguez	Grupo / s	1
Departamento	Informática y Automática		
Área	Ciencia de la Computación e Inteligencia Artificial		
Centro	Facultad de Ciencias		
Despacho	Pasillo nuevo de Informática y Automática, Facultad de Ciencias		
Horario de tutorías	A demanda, consultar por correo electrónico		
URL Web	https://produccioncientifica.usal.es/investigadores/57537/detalle		
E-mail	carol_zato@usal.es	Teléfono	923 294 500 Ext. 6076

2.- Recomendaciones previas

- **Conocimientos básicos de ciberseguridad**: Familiaridad con los principios fundamentales de la ciberseguridad, como redes, protección de la información y control de accesos.
- **Conocimientos básicos en sistemas operativos**: Tener nociones de cómo funcionan los sistemas operativos, especialmente en relación con la gestión de archivos y registros, evidencias fundamentales en forense digital

- **Conocimientos básicos de redes**: Entender cómo funcionan las redes y los protocolos de comunicación, lo que facilitará la comprensión de incidentes relacionados con la red.

3.- Objetivos de la asignatura

- **Introducción al análisis forense**: Proporcionar una comprensión general sobre el análisis forense digital, su importancia y las prácticas legales involucradas en la investigación de ciberdelitos.
- **Evidencia digital**: Capacitar a los estudiantes para identificar, preservar y analizar evidencia digital de forma que se mantenga la integridad legal de la misma.
- **Análisis forense en sistemas operativos**: Enseñar a los estudiantes cómo realizar un análisis forense en sistemas operativos comprometidos, identificando y recuperando evidencia relevante.
- **Respuesta a incidentes**: Introducir las mejores prácticas en la gestión de incidentes de seguridad, con un enfoque en la respuesta efectiva ante incidentes forenses.
- **Análisis de malware**: Desarrollar competencias para analizar malware, con especial atención a los ransomware y su comportamiento.
- **Búsqueda de amenazas (threat hunting)**: Capacitar a los estudiantes para identificar amenazas en sus primeras fases, analizando comportamientos anómalos en redes y sistemas.

4.- Competencias a adquirir / Resultados de aprendizaje

Competencias *Complete esta columna si su titulación no ha sido adaptada al RD822/2021*	**Resultados de aprendizaje** *Complete esta columna si su titulación ha sido adaptada al RD822/2021*
4.1: Competencias Básicas:	**4.1: Conocimientos:** **C1**. Relacionar los fundamentos teóricos de la ciberseguridad, incluyendo conceptos básicos de la información, criptografía, redes y sistemas operativos para proteger la integridad y la confidencialidad de la información. **C2**. Identificar las amenazas y vulnerabilidades más comunes en entornos digitales, así como las técnicas y metodologías utilizadas para prevenir, detectar y responder a incidentes de seguridad. **C6**. Identificar protocolos de seguridad contra amenazas informáticas a partir de conocimientos especializados en ciberseguridad, centrándose en su desarrollo, implementación y evaluación. **C7**. Describir los aspectos técnicos e informáticos de la seguridad, incluyendo el diseño seguro de sistemas, la seguridad en redes y comunicaciones, la protección de datos y la gestión de incidentes de seguridad.
4.2: Competencias Específicas:	**4.2: Habilidades:** **H1.** Implementar medidas de seguridad en diferentes entornos y sistemas, incluyendo la configuración de firewalls, la gestión de accesos, la detección de intrusiones y el análisis forense digital. **H2.** Adquirir destrezas en el uso de herramientas y software especializados para evaluar la seguridad de sistemas y redes, así como para llevar a cabo pruebas de penetración y auditorías de seguridad. **H6.** Desarrollar habilidades técnicas para implementar soluciones de seguridad en sistemas y redes, realizar pruebas de penetración y responder a incidentes de seguridad de manera eficiente.

	H7. Adquirir destrezas en el uso de herramientas y software especializados para evaluar la seguridad de sistemas informáticos y redes.
4.3: Competencias Transversales:	**4.3: Competencias:** **K1**. Diseñar, desarrollar, evaluar y asegurar la seguridad de un sistema informático, con independencia de su tamaño y características. **K3**. Analizar, diseñar, construir y mantener aplicaciones de seguridad de forma robusta, segura y eficiente, eligiendo el paradigma y los lenguajes de programación más adecuados en cada caso, según el entorno de despliegue (entorno web, escritorio). **K4**. Diseñar, desplegar, administrar de forma segura y fiable servicios en una red de ordenadores. **K5**. Validar la garantía y seguridad de los sistemas informáticos pertinentes, como redes locales, servidores, bases de datos y sistemas de gestión de información. **K6**. Diseñar políticas de monitorización y copia de segura, para la recuperación de sistemas y el aseguramiento en la información en caso de malfuncionamiento. **K8**. Auditar las políticas de seguridad de una empresa a todos los niveles (sistemas, red, información, etc.).

5.- Contenidos (temario)

Contenido teórico:

1. Introducción al análisis forense.
2. Evidencia digital.
3. Análisis Forense en Sistemas Operativos.
4. Respuesta a incidentes.
5. Análisis de malware.
6. Búsqueda de amenazas (threat hunting).

Contenido práctico:

1. Taller de evidencia digital aplicado a ciberdelitos
2. Análisis y explotación de un malware (ransomware).
3. Análisis de un sistema comprometido.

6.- Metodologías docentes

- Sesiones magistrales: de carácter expositivo, se explicarán los conceptos clave de forma clara y estructurada, proporcionando el marco teórico necesario para el desarrollo del resto de las actividades. Se consideran el punto de partida para el análisis, la reflexión y la aplicación práctica.
- Prácticas o talleres en el aula de informática: permitirán al alumnado aplicar los conocimientos adquiridos mediante el uso de herramientas y recursos digitales específicos. Estas sesiones estarán orientadas a resolver ejercicios, realizar simulaciones o desarrollar proyectos relacionados con los contenidos de la materia.
- Seminarios: ofrecerán un espacio para el análisis en profundidad de temas seleccionados, con una dinámica más participativa y orientada al debate. En este formato se fomentará el pensamiento crítico, la discusión fundamentada y el intercambio de ideas.

- Exposiciones orales por parte del alumnado: contribuirán a compartir distintos enfoques sobre los temas tratados, enriqueciendo así el aprendizaje colectivo.
- Realización de trabajos individuales o en grupo: facilitará el desarrollo de competencias transversales como la búsqueda de información, el análisis crítico, la redacción académica y la gestión del tiempo. Estos trabajos estarán vinculados a los contenidos del curso y requerirán una implicación activa por parte del alumnado.
- Tutorías: sesiones personalizadas, individuales o en grupos pequeños, que permiten a los estudiantes aclarar dudas específicas y recibir orientación detallada del docente. Estas pueden realizarse de manera presencial o virtual, adaptándose a las necesidades de 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		4		10	14
Prácticas	- En aula				
	- En el laboratorio				
	- En aula de informática	6		40	48
	- De campo				
	- Otras (detallar)				
Seminarios		2	5		
Exposiciones y debates		4			
Tutorías			2		2
Actividades de seguimiento online			5	25	30
Preparación de trabajos			15	30	45
Otras actividades (detallar)					
Exámenes		2			
TOTAL		**18**	**27**	**105**	**150**

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

Bibliografía:
- Carvey, H. (2018). *Windows Forensics*. Syngress.
- Casey, E. (2011). *Handbook of Digital Forensics and Investigation*. Academic Press.
- Kim, S., & Solomon, M. (2018). *Fundamentals of Digital Forensics*. Wiley.

Repositorios y Herramientas:
- **SANS Forensics**: Recursos de capacitación en análisis forense digital. https://www.sans.org/cyber-security-courses/forensics/
- **Forensic Focus**: Comunidad y recursos para profesionales del análisis forense. https://www.forensicfocus.com/
- **Cellebrite**: Herramientas avanzadas para la recolección y análisis de evidencia digital. https://www.cellebrite.com/

Herramientas y software:
- **Autopsy**: Herramienta de análisis forense de código abierto. https://www.sleuthkit.org/autopsy/
- **FTK Imager**: Herramienta para la creación de imágenes forenses de discos. https://accessdata.com/product-download
- **Wireshark**: Herramienta para el análisis de tráfico de red. https://www.wireshark.org/

8.- Evaluación

8.1: Criterios de evaluación:

Realización de tareas:

- Las tareas estarán relacionadas con los contenidos abordados durante las clases presenciales y consistirán, en su mayoría, en el desarrollo de propuestas utilizando algunas de las herramientas y conceptos trabajados en el aula. En su evaluación se tendrá en cuenta no solo la calidad científica y técnica del contenido, sino también la destreza en el uso de las herramientas seleccionadas, la claridad comunicativa y la capacidad de análisis crítico y constructivo demostrada por el estudiante.
-

Prueba final:

- Consistirá en preguntas tipo test y de respuesta corta, e incluirá tanto preguntas de la parte teórica como de las sesiones prácticas, talleres y seminarios llevados a cabo.

La ponderación de las diferentes partes será la siguiente

- Asistencia y participación en actividades presenciales: 20%
- Tareas, trabajos, resolución de prácticas: 30%
- Prueba de evaluación final: 50%

8.2: Sistemas de evaluación:

- Participación en actividades presenciales.
- Entrega de informes de los talleres realizados y prácticas.
- Prueba final.

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

La evaluación se realizará de forma continua mediante la entrega de tareas o prácticas y tendrá en cuenta tanto el rendimiento individual como la participación activa en las distintas actividades propuestas. Se valorará la comprensión de los contenidos, la aplicación práctica de los conocimientos, la calidad en la realización de trabajos y exposiciones, así como la implicación en debates y seminarios. La asistencia regular, el cumplimiento de plazos y el compromiso con el aprendizaje también serán considerados. El objetivo es promover una evaluación formativa que refleje el progreso del alumnado a lo largo del curso.

Recuperación:

La asignatura se considerará superada cuando la media ponderada de las actividades propuestas en las diferentes partes sea igual a 5 o superior. En caso, contrario el alumno deberá volver a realizar aquellas partes necesarias para superar la calificación mínima exigida.

Aspectos legales de la ciberseguridad

1.- Datos de la Asignatura

Código	306552	Plan	M204-1	ECTS	3
Carácter	Obligatoria	Curso	1	Periodicidad	Primer semestre
Idioma de impartición asignatura		Castellano			
Área	Derecho Procesal				
Departamento	Derecho Administrativo, Financiero y Procesal				
Plataforma virtual	Studium http://studium.usal.es				

1.1.- Datos del profesorado

Profesor Coordinador	Federico Bueno de Mata	Grupo / s	1
Departamento	Derecho Administrativo, Financiero y Procesal		
Área	Derecho Procesal		
Centro	Facultad de Derecho		
Despacho	258		
Horario de tutorías	A acordar con el/la estudiante previa comunicación por e-mail.		
URL Web	*https://produccioncientifica.usal.es/investigadores/57438/detalle*		
E-mail	febuma@usal.es	Teléfono	923294500 Ext. 1679

Profesor	Paula María Tomé Domínguez	Grupo / s	1
Departamento	Derecho Administrativo, Financiero y Procesal		
Área	Derecho Administrativo		
Centro	E. Politécnica Superior de Ávila		
Despacho	282 (Facultad de Derecho)		
Horario de tutorías	A acordar con el/la estudiante previa comunicación por e-mail.		
URL Web	*https://produccioncientifica.usal.es/investigadores/148414/detalle*		

E-mail	paulatomedom@usal.es	Teléfono	923294500 Ext. 1639

2.- Recomendaciones previas

Es recomendable tener conocimientos previos en: nociones básicas de derecho, especialmente derecho constitucional, penal y civil; comprensión general del sistema jurídico y sus fuentes; familiaridad con derechos fundamentales como la intimidad, el honor y la protección de datos; conocimiento introductorio de legislación sobre tecnologías de la información, como el RGPD y la LOPDGDD; y comprensión básica del funcionamiento de internet y los sistemas informáticos, para entender el contexto técnico de las normas aplicables.

3.- Objetivos de la asignatura

1. Conocer el marco normativo español en materia de ciberseguridad y su evolución.
2. Comprender la estructura y funciones de los organismos nacionales responsables de la respuesta ante ciberataques.
3. Identificar y clasificar los principales ciberdelitos, fraudes y daños informáticos desde una perspectiva nacional y transnacional.
4. Analizar el tratamiento procesal de los incidentes de ciberseguridad, incluyendo competencias jurisdiccionales y actores implicados.
5. Aplicar los aspectos legales a casos prácticos relacionados con incidentes de ciberseguridad.
6. Desarrollar habilidades para gestionar incidentes de seguridad, integrando el componente jurídico en la toma de decisiones.

4.- Competencias a adquirir / Resultados de aprendizaje

Competencias	Resultados de aprendizaje
4.1: Competencias Básicas:	**4.1: Conocimientos:** C3, C9, C10 **C3**. Identificar las leyes, regulaciones y estándares nacionales e internacionales relacionados con la ciberseguridad. **C9**. Recopilar información pertinente de la legislación nacional e internacional que afecta a los sistemas de información y la ciberseguridad, así como en los aspectos legales y sociales relacionados. **C10**. Caracterizar normativas y regulaciones en materia de protección de datos, cumplimiento normativo y responsabilidad jurídica en casos de incidentes de seguridad.

4.2: Competencias Específicas:	**4.2: Habilidades:** H9, H11 **H9.** Adquirir habilidades para analizar y evaluar los aspectos legales de la ciberseguridad, asesorar en la implementación de políticas y normatives y colaborar con equipos técnicos en la resolución de casos jurídicos relacionados con la ciberseguridad. **H11.** Mejorar en habilidades de comunicación y argumentación legal, y desarrollar habilidades éticas y profesionales para enfrentar los desafíos éticos y legales en el ámbito de la ciberseguridad.
4.3: Competencias Transversales:	**4.3: Competencias:** K5, K7, K8, K9 **K5**. Validar la garantía y seguridad de los sistemas informáticos pertinentes, como redes locales, servidores, bases de datos y sistemas de gestión de información. **K7**. Elaborar la política de seguridad de una empresa. **K8**. Auditar las políticas de seguridad de una empresa a todos los niveles (sistemas, red, información, etc.). **K9**. Aplicar las restricciones legales asociados a la seguridad informática sobre el manejo y procesamiento de datos personales.

5.- Contenidos (temario)

Contenido teórico:

1. Introducción.
2. Normativa de ciberseguridad nacional en España.
3. Gestión de incidentes de seguridad.
4. Organismos nacionales que dan respuesta a ataques cibernéticos.
5. Principales incidentes y ciberdelitos vinculados a la ciberseguridad: fraudes y daños informáticos desde la perspectiva transnacional.
6. Tratamiento procesal de los incidentes de ciberseguridad: orden jurisdiccional,competencia y operadores jurídicos en el ámbito penal y administrativo.

Contenido práctico:

1. Aplicabilidad de aspectos legales en un caso de estudio.
2. Taller sobre gestión de incidentes de seguridad.

6.- Metodologías docentes

Metodología jurídica clásica, a través de el análisis de legislación, jurisprudencia y bibliografía especializada, así como informes y cuestiones de softlaw relacionadas con la materia.
El enfoque de la asignatura combinará enfoques teóricos y aplicación práctica.

6.1.- Distribución de metodologías docentes

		Horas dirigidas por el profesor		Horas de trabajo autónomo	HORAS TOTALES
		Horas presenciales.	Horas no presenciales.		
Sesiones magistrales		8		20	28
Prácticas	- En aula				
	- En el laboratorio				
	- En aula de informática				
	- De campo				
	- Otras (detallar)				
Seminarios			8		8
Exposiciones y debates					
Tutorías			2		2
Actividades de seguimiento online					
Preparación de trabajos			3,5	32,5	36
Otras actividades (detallar)					
Exámenes		1			1
TOTAL		**9**	**13,5**	**52,5**	**75**

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

Tejerina Rodríguez, Ofelia. *Aspectos jurídicos de la ciberseguridad*. Madrid: Marcial Pons, 2023.Marcial Pons
Velasco, Eloy, coord. *Marco normativo de la UE para la transformación digital*. Madrid: La Ley, 2023.Revista SIC
Segura Serrano, Antonio, coord. *Global Cybersecurity and International Law*. Londres: Routledge, 2024.Revista SIC
Grupo Editorial RA-MA. *Aspectos jurídicos de la ciberseguridad*. Madrid: RA-MA, 2022.RA-MA

8.- Evaluación

Las pruebas de evaluación que se diseñen deben apreciar si se han adquirido las competencias o resultados de aprendizaje descritos en el apartado 3.

.1: Criterios de evaluación:

- Comprensión y dominio del marco jurídico aplicable a las diligencias de investigación y a la prueba electrónica.
- Capacidad para identificar y analizar los derechos fundamentales afectados.
- Aplicación adecuada de los conocimientos a supuestos prácticos.
- Claridad expositiva, argumentación jurídica y uso correcto del lenguaje técnico.
- Participación activa y fundamentada en clase (en convocatoria ordinaria).

8.2: Sistemas de evaluación:

Convocatoria ordinaria:

- **Participación activa en clase:** 30%
- **Trabajo expositivo individual o grupal:** 70%

Convocatoria extraordinaria:

- **Examen escrito con preguntas cortas:** 100%

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

-En la convocatoria ordinaria, se valorará especialmente la participación crítica y fundamentada en clase, así como la calidad y rigor del trabajo expositivo presentado.
- El trabajo expositivo debe mostrar comprensión teórica y capacidad de aplicación práctica, incluyendo referencias normativas y jurisprudenciales.
- En la convocatoria extraordinaria, el examen consistirá en preguntas cortas que evaluarán de forma directa los conocimientos teóricos y prácticos adquiridos.
- Se recomienda el seguimiento continuo de las clases, la lectura de los materiales indicados y la resolución de casos prácticos para facilitar tanto la evaluación ordinaria como la extraordinaria.
-El estudiante deberá demostrar, en ambos casos, un conocimiento suficiente de los contenidos esenciales de la asignatura y su aplicación conforme al marco legal vigente.

Ciberinteligencia

1.- Datos de la Asignatura					
Código	306551	Plan	M204-1	ECTS	6
Carácter	Obligatoria	Curso	1	Periodicidad	Primer semestre
Idioma de impartición asignatura		Español			
Área	Ciencia de la Computación e Inteligencia Artificial				
Departamento	Informática y Automática				
Plataforma virtual	Studium http://studium.usal.es				

1.1.- Datos del profesorado			
Profesor Coordinador	Pablo Chamoso Santos	Grupo / s	1
Departamento	Informática y Automática		
Área	Ciencia de la Computación e Inteligencia Artificial		
Centro	Facultad de Ciencias		
Despacho	F3012		
Horario de tutorías	Solicitar cita por correo electrónico		
URL Web	https://produccioncientifica.usal.es/investigadores/57686/detalle		
E-mail	chamoso@usal.es	Teléfono	923294500 Ext. 6591

1.2.- Datos del profesorado			
Profesor Coordinador	María Angélica González Arrieta	Grupo / s	1
Departamento	Informática y Automática		
Área	Ciencia de la Computación e Inteligencia Artificial		
Centro	Facultad de Ciencias		
Despacho	F3003		
Horario de tutorías	Solicitar cita por correo electrónico		
URL Web	https://produccioncientifica.usal.es/investigadores/56850/detalle		
E-mail	angelica@usal.es	Teléfono	923294500 Ext. 1302

2.- Recomendaciones previas

- Conocimientos básicos en ciberseguridad y redes.
- Familiaridad con la búsqueda de información en fuentes abiertas y redes sociales.
- Manejo básico de utilidades de consola y herramientas de software en entornos Windows y Unix

3.- Objetivos de la asignatura

- **Introducción a la ciberinteligencia**: Proporcionar una base sólida en el uso de fuentes abiertas (OSINT) y en el análisis de información en redes sociales (SOCMINT).
- **Análisis en entornos específicos**: Enseñar el uso de herramientas y metodologías para realizar análisis de amenazas en la deep web y dark web.
- **Inteligencia de amenazas**: Desarrollar competencias en el análisis de inteligencia sobre ciberamenazas, con un enfoque práctico en la identificación y seguimiento de riesgos emergentes.
- **Tendencias tecnológicas**: Analizar las últimas tendencias en ciberseguridad, como IoT, inteligencia artificial y aprendizaje automático, para aplicar estas tecnologías en la ciberinteligencia.
- **Trabajo práctico con herramientas**: Capacitar a los estudiantes a través de talleres prácticos en OSINT, SOCMINT y threat intelligence, permitiéndoles poner en práctica los conceptos aprendidos.

4.- Competencias a adquirir / Resultados de aprendizaje

Competencias	Resultados de aprendizaje
4.1: Competencias Básicas:	**4.1: Conocimientos:** C2, C5, C8 **C2**. Identificar las amenazas y vulnerabilidades más comunes en entornos digitales, así como las técnicas y metodologías utilizadas para prevenir, detectar y responder a incidentes de seguridad. **C5**. Examinar aspectos interdisciplinarios de la ciberseguridad, como la gestión de riesgos, la ética y la privacidad, con el fin de proporcionar una visión integral de la disciplina. **C8**. Distinguir las últimas tendencias y tecnologías en el campo de la ciberseguridad, como el Internet de las cosas (IoT), la inteligencia artificial (IA) y el aprendizaje automático (Machine Learning), para estar preparados ante los desafíos futuros
4.2: Competencias Específicas:	**4.2: Habilidades:** H2, H6, H7, H8 **H2.** Adquirir destrezas en el uso de herramientas y software especializados para evaluar la seguridad de sistemas y redes, así como para llevar a cabo pruebas de penetración y auditorías de seguridad. **H6.** Desarrollar habilidades técnicas para implementar soluciones de seguridad en sistemas y redes, realizar pruebas de penetración y responder a incidentes de seguridad de manera eficiente. **H7**. Adquirir destrezas en el uso de herramientas y software especializados para evaluar la seguridad de sistemas informáticos y redes. **H8**. Desarrollar habilidades de análisis y resolución de problemas en el ámbito de la seguridad informática, así como habilidades de comunicación y trabajo en equipo.
4.3: Competencias Transversales:	**4.3: Competencias:** K1, K2, K3, K5, K8 **K1.** Diseñar, desarrollar, evaluar y asegurar la seguridad de un sistema informático, con independencia de su tamaño y características.

	K2. Desarrollar, implantar y mantener sistemas, servicios y aplicaciones informáticas de seguridad empleando los métodos de la ingeniería del software como instrumento para el aseguramiento de su calidad. **K3**. Analizar, diseñar, construir y mantener aplicaciones de seguridad de forma robusta, segura y eficiente, eligiendo el paradigma y los lenguajes de programación más adecuados en cada caso, según el entorno de despliegue (entorno web, escritorio). **K5**. Validar la garantía y seguridad de los sistemas informáticos pertinentes, como redes locales, servidores, bases de datos y sistemas de gestión de información. **K8**. Auditar las políticas de seguridad de una empresa a todos los niveles (sistemas, red, información, etc.).

5.- Contenidos (temario)

Contenido teórico:

1. Introducción a inteligencia de fuentes abiertas (OSINT).
2. Ciberinteligencia en redes sociales y metadatos (SOCMINT).
3. Análisis en la *deep* web y *dark* web.
4. Inteligencia de amenazas (*threat Intelligence*).

Contenido práctico:

1. Taller de iniciación en OSINT y SOCMINT.
2. Taller de iniciación a *threat intelligence.*

6.- Metodologías docentes

La asignatura se plantea como una combinación equilibrada entre teoría y práctica, basada en un modelo constructivista y activo, donde el aprendizaje se logra mediante la resolución de problemas reales (que podrán ser simulados), el uso de herramientas técnicas y la discusión crítica de casos y datos. Esta asignatura se estructura a través de clases magistrales, talleres guiados con resolución de casos, fomentando tanto la adquisición de conocimientos como el desarrollo de competencias técnicas específicas con actividades de seguimiento en línea. En las tutorías se aclararán conceptos en los que el alumno requiera explicaciones avanzadas.

6.1.- Distribución de metodologías docentes

		Horas dirigidas por el profesor		Horas de trabajo autónomo	HORAS TOTALES
		Horas presenciales.	Horas no presenciales.		
Sesiones magistrales		8		30	38
Prácticas	- En aula	8		20	28
	- En el laboratorio				
	- En aula de informática				
	- De campo				
	- Otras (detallar)				
Seminarios			3		3
Exposiciones y debates					

Tutorías		4		4
Actividades de seguimiento online		5	25	30
Preparación de trabajos		15	30	45
Otras actividades (detallar)				
Exámenes	2			2
TOTAL	**18**	**27**	**105**	**150**

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

Bibliografía:

- McCoy, D., & Smith, R. (2019). *Open Source Intelligence Techniques*. CreateSpace.
- Manson, M. (2020). *The Art of Intelligence*. Wiley.
- Johnson, S. (2021). *Cyber Threat Intelligence*. O'Reilly Media.

Repositorios y recursos electrónicos:

- **OSINT Framework**: Plataforma que ofrece herramientas para el análisis de fuentes abiertas. https://osintframework.com/
- **Shodan**: Motor de búsqueda para dispositivos conectados a Internet. https://www.shodan.io/
- **CIRCL**: Centro de Ciberseguridad para el análisis de amenazas y la compartición de inteligencia. https://www.circl.lu/

8.- Evaluación

8.1: Criterios de evaluación:

La evaluación de la asignatura se basará en tres componentes principales: la participación activa en las actividades presenciales, la entrega y calidad de los informes correspondientes a los supuestos prácticos, y una prueba final que valorará los conocimientos teóricos adquiridos a lo largo del curso. Estos criterios permitirán medir tanto la implicación del estudiante como su capacidad para aplicar los conceptos y herramientas fundamentales de la ciberinteligencia.

8.2: Sistemas de evaluación:

- Participación en actividades presenciales: 10%
- Entrega de informes de los supuestos prácticos: 20%
- Prueba final: será de tipo test, con un peso del 70%

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

En la evaluación ordinaria, se valorarán la participación activa en clase, la entrega de los informes prácticos y la prueba final tipo test. Sin embargo, en la convocatoria de recuperación, la participación en clase no se tendrá en cuenta como criterio evaluable. En este caso, la calificación final se obtendrá exclusivamente a partir de la entrega de los informes prácticos pendientes (si corresponde) y de la realización de una nueva prueba final, que permitirá al estudiante demostrar la adquisición de los conocimientos fundamentales de la asignatura. Se recomienda revisar todos los materiales teóricos y prácticos trabajados durante el curso, así como reforzar el manejo de las herramientas presentadas en los talleres.

Compliance y cumplimiento normativo

1.- Datos de la Asignatura					
Código	306561	Plan	M204-1	ECTS	6
Carácter	Optativa	Curso	1	Periodicidad	Segundo semestre
Idioma de impartición asignatura		Castellano			
Área	Derecho Procesal, Derecho Administrativo y Economía Aplicada				
Departamento	Derecho Administrativo, Financiero y Procesal y Economía Aplicada				
Plataforma virtual	Studium http://studium.usal.es				

1.1.- Datos del profesorado			
Profesor Coordinador	Nicolás Rodríguez - García	Grupo / s	1
Departamento	Derecho Administrativo, Financiero y Procesal		
Área	Derecho Procesal		
Centro	Facultad de Derecho		
Despacho			
Horario de tutorías	A acordar con el/la estudiante previa comunicación por e-mail.		
URL Web	https://produccioncientifica.usal.es/investigadores/56955/detalle		
E-mail	nicolas@usal.es	Teléfono	923294500 Ext. 6944

Profesor Coordinador	Ana Carrillo Del Teso	Grupo / s	1
Departamento	Derecho Administrativo, Financiero y Procesal		
Área	Derecho Procesal		
Centro	Facultad de Derecho		
Despacho	234 (Facultad de Derecho)		
Horario de tutorías	A acordar con el/la estudiante previa comunicación por e-mail.		
URL Web	https://produccioncientifica.usal.es/investigadores/57685/detalle		
E-mail	ana_cdt@usal.es	Teléfono	923294500 Ext. 1688

Profesor Coordinador	Paula María Tomé Domínguez	Grupo / s	1
Departamento	Derecho Administrativo, Financiero y Procesal		
Área	Derecho Administrativo		
Centro	E. Politécnica Superior de Ávila		
Despacho	282 (Facultad de Derecho)		
Horario de tutorías	A acordar con el/la estudiante previa comunicación por e-mail.		

URL Web	https://produccioncientifica.usal.es/investigadores/148414/detalle		
E-mail	paulatomedom@usal.es	Teléfono	923294500 Ext. 1639

Profesor Coordinador	José Ignacio Sánchez Macías	Grupo / s	1
Departamento	Economía aplicada		
Área	Economía aplicada		
Centro	Facultad de Derecho		
Despacho	131 (Facultad de Derecho)		
Horario de tutorías	A acordar con el/la estudiante previa comunicación por e-mail.		
URL Web	https://produccioncientifica.usal.es/investigadores/56487/detalle		
E-mail	macias@usal.es	Teléfono	923294500 Ex.t 3029

2.- Recomendaciones previas

Es recomendable tener conocimientos previos sobre economía y empresa y nociones legales: sistema de fuentes, derechos fundamentales, protección de datos, sistema penal y regulación administrativa.

3.- Objetivos de la asignatura

- Comprender los fundamentos del compliance y su relevancia en la prevención de riesgos legales y éticos en organizaciones públicas y privadas.
- Analizar el marco normativo aplicable, tanto en el sector privado como en el sector público, incluyendo regulaciones nacionales e internacionales.
- Identificar y gestionar riesgos de incumplimiento normativo en distintas áreas, como contratación pública, integridad institucional y anticorrupción.
- Conocer los elementos clave de un sistema de cumplimiento eficaz y su aplicación en entidades públicas y privadas.
- Desarrollar competencias para diseñar, implementar y supervisar programas de cumplimiento normativo adaptados al contexto organizacional.

4.- Competencias a adquirir / Resultados de aprendizaje

Competencias	Resultados de aprendizaje
4.1: Competencias Básicas:	**4.1: Conocimientos:** C3, C9, C10 **C3**. Identificar las leyes, regulaciones y estándares nacionales e internacionales relacionados con la ciberseguridad **C9**. Recopilar información pertinente de la legislación nacional e internacional que afecta a los sistemas de información y la ciberseguridad, así como en los aspectos legales y sociales relacionados. **C10**. Caracterizar normativas y regulaciones en materia de protección de datos, cumplimiento

	normativo y responsabilidad jurídica en casos de incidentes de seguridad.
4.2: Competencias Específicas:	**4.2: Habilidades:** H3, H9, H11 **H3.** Analizar y evaluar los riesgos de seguridad en entornos digitales, identificando posibles debilidades y proponiendo soluciones efectivas. **H9.** Adquirir habilidades para analizar y evaluar los aspectos legales de la ciberseguridad, asesorar en la implementación de políticas y normativas y colaborar con equipos técnicos en la resolución de casos jurídicos relacionados con la ciberseguridad. **H11.** Mejorar en habilidades de comunicación y argumentación legal, y desarrollar habilidades éticas y profesionales para enfrentar los desafíos éticos y legales en el ámbito de la ciberseguridad.
4.3: Competencias Transversales:	**4.3: Competencias:** K5, K6, K9 **K5**. Validar la garantía y seguridad de los sistemas informáticos pertinentes, como redes locales, servidores, bases de datos y sistemas de gestión de información. **K6**. Diseñar políticas de monitorización y copia de segura, para la recuperación de sistemas y el aseguramiento en la información en caso de malfuncionamiento. **K9**. Aplicar las restricciones legales asociados a la seguridad informática sobre el manejo y procesamiento de datos personales.

5.- Contenidos (temario)

Contenido teórico:

1. Elementos básicos del *compliance.*
2. Cultura del cumplimiento normativo y su importancia.
3. Aspectos procesales del *compliance.* Relevancia de las investigaciones internas
4. *Compliance* y entorno digital
5. Aspectos fundamentales de la contratación en el sector público
6. Detección y diagnóstico de riesgos en el sector público

Contenido práctico:

1. Desarrollo e implementación de sistemas de compliance.

6.- Metodologías docentes

- **Sesiones Magistrales**: Sesiones donde se presentan los fundamentos teóricos de los temas de la asignatura. Son de carácter expositivo y buscan proporcionar una visión amplia y detallada de los conceptos clave, fomentando al mismo tiempo el diálogo y la reflexión crítica entre los estudiantes.
- **Sesiones Prácticas**: A través de casos de estudio, los estudiantes pondrán en práctica los conceptos teóricos, desarrollando habilidades técnicas y analíticas aplicando de manera concreta los conocimientos adquiridos.
- **Actividades de seguimiento online**: Sesiones individualizadas o en pequeños grupos donde los estudiantes pueden resolver dudas específicas con el docente, recibir

orientación personalizada y profundizar en temas de interés. Estas sesiones son flexibles y se pueden llevar a cabo tanto de forma presencial como virtual.

- **Preparación de trabajos autónomos**: Asignaciones que los estudiantes deben realizar de manera independiente, aplicando los conocimientos adquiridos, con el objetivo de fomentar la capacidad de análisis, síntesis y crítica, así como el desarrollo de habilidades de investigación y escritura académica. Podrán ser individuales o de grupo.

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	40	72
Prácticas	- En aula	4		5	9
	- En el laboratorio				
	- En aula de informática				
	- De campo				
	- Otras (detallar)				
Seminarios					
Exposiciones y debates					
Tutorías			2		2
Actividades de seguimiento online			5	20	25
Preparación de trabajos				40	40
Otras actividades (detallar)					
Exámenes		2			2
TOTAL		**18**	**27**	**105**	**150**

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

SÁNCHEZ-MACÍAS, J. I. y RODRÍGUEZ -LÓPEZ, F. (2021). "Estudio Preliminar". En Rodríguez García (dir.), N., Tratado angloiberoamericano sobre compliance penal. Tirant Lo Blanch, págs. 27-58.
SÁNCHEZ-MACÍAS, J. I. (2024). "Rojo anaranjado o naranja rojizo: gestión empresarial y compliance". En Rodríguez-García, N., Carrillo del Teso, A. y Cerina, G. (eds.), Delincuencia corporativa: canales de denuncia y persecución penal. Valencia: Tirant Lo Blanch. LEO CASTELA, J. I. (2021). Gestión de riesgos legales y compliance corporativo. Valencia. Tirant Lo Blanch.
RODRÍGUEZ-LÓPEZ, F. y SÁNCHEZ-MACÍAS, J. I. (2021). "Normalización y certificación en compliance, de la autorregulación al valor social", en RODRÍGUEZ-GARCÍA N. y RODRÍGUEZ LÓPEZ, F. (eds.), Compliance y responsabilidad penal de las personas jurídicas. Tirant Lo Blanch, págs. 461-492.
COSO (2013). Control interno – Marco Integrado. Resumen Ejecutivo.pdf
IIA (2020). Modelo de las Tres Líneas. Disponible en three-lines-model-updated-spanish.pdf
CANALS AMETLLER, D. "Ciberseguridad. Un nuevo reto para el Estado y los Gobiernos Locales", 2021, Wolters Kluwer.
DÍAZ-FERNÁNDEZ, A. M., SOLARI-MERLO, M.N., "Tecnología y control social: el futuro de la gestión de la seguridad en las Smart cities", 2025, Aranzadi.
GOLLONET TERUEL, L.A. PÉREZ-PIAYA MORENO, C. Compliance en el derecho administrativo, 2020, Wolter Kluwer Aranzadi.
LLANEZA GONZÁLEZ, P. "Seguridad y responsabilidad en el Internet de las cosas (IoT)", 2018, Wolters Kluwer Aranzadi.
MATA, E. "Ciberseguridad: curso práctico", 2024, Ed. 1ª, RA-MA.
ORTEGO RUIZ, M. "Manual de privacidad, protección de datos y ciberseguridad", 2024, Tirant lo Blanch.
RAMÍREZ PASCUAL, B. "La ciberseguridad en la era de la Inteligencia Artificial", 2023, Ed.1ª, Aranzadi.
NEIRA PENA, A. M. (2017): *La instrucción de los procesos penales frente a las personas jurídicas*. Valencia: Tirant lo Blanch.

NEIRA PENA, A. M. (2018): *La defensa penal de la persona jurídica*: *representante defensivo, rebeldía, conformidad y compliance como objeto de prueba.* Cizur Menor: Aranzadi.
VILLEGAS GARCIA, M. A. & ENCINAR DEL POZO, M. A. (2020): *Lucha contra la corrupción,* compliance *e investigaciones internas. La influencia del Derecho estadounidense*. Cizur Menor: Aranzadi
RODRÍGUEZ GARCÍA, N. (Dir.) (2021): Tratado angloiberoamericano sobre compliance penal. Valencia: Tirant lo Blanch
RODRIGUEZ GARCÍA, N., RODRÍGUEZ LÓPEZ, F (Dirs.) (2021): Compliance y reponsabillidad de las personas jurídicas. Valencia: Tirant lo Blanch
RODRIGUEZ GARCÍA, N., CARRILLO DEL TESO, A., CERINA, G. (Dirs.) (2024): Delincuencia corporativa: compliance, canales de denuncia y persecución penal. Valencia: Tirant lo Blanch.

8.- Evaluación

8.1: Criterios de evaluación:

Participación activa: contribución en las actividades presenciales tanto teóricas como prácticas.

Entrega de trabajos y/o informes sobre supuestos prácticos:
- Dominio de los conceptos fundamentales del *compliance* y del marco normativo aplicable.
- Capacidad para explicar la función y objetivos de un programa de cumplimiento.
- Aplicación de los conocimientos a situaciones reales o simuladas en organizaciones públicas y privadas.
- Identificación de riesgos de cumplimiento y propuesta de medidas correctivas.
- Claridad, rigor y adecuación a la normativa vigente.

Prueba final:
- Evaluación del conocimiento adquirido mediante preguntas tipo test. Incluirá tanto preguntas de tipo teórico como práctico.

8.2: Sistemas de evaluación:

La nota final en ambas convocatorias se compondrá de:

- Participación en actividades presenciales: 15%
- Entrega de los trabajos y/o informes sobre supuestos prácticos: 25%
- Prueba final (tipo test): 60%

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

Con carácter general, se recomienda:
- asistir activamente a las sesiones presenciales de la asignatura.
- cumplir los plazos marcados para la entrega de tareas y trabajos.
- seguir las instrucciones para la elaboración de las entregas
- seguir las instrucciones para la prueba final.

Recomendaciones para la recuperación:

El alumno no superará la asignatura cuando no haya participado activamente en las actividades presenciales de la asignatura y/o no haya entregado las tareas obligatorias con un mínimo de calidad. Tampoco la superará si la prueba final no es satisfactoria. En consecuencia, deberá volver a realizar las tareas y la prueba final con el nivel de calidad exigido.

CRIPTOGRAFÍA, BLOCKCHAIN Y CRIPTOMONEDAS

1.- Datos de la Asignatura					
Código	306559	Plan		ECTS	6
Carácter	Optativa	Curso	1	Periodicidad	Semestre 2
Idioma de impartición asignatura		Español			
Área	Ciencia de la Computación e Inteligencia Artificial				
Departamento	Informática y Automática				
Plataforma virtual	Studium http://studium.usal.es				

1.1.- Datos del profesorado			
Profesor Coordinador	Javier Prieto Tejedor	Grupo / s	1
Departamento	Informática y Automática		
Área	Ciencia de la Computación e Inteligencia Artificial		
Centro	Facultad de Ciencias		
Despacho	F3006		
Horario de tutorías	Solicitar por correo electrónico		
URL Web	https://produccioncientifica.usal.es/investigadores/148044/detalle		
E-mail	javierp@usal.es	Teléfono	923 294 500 Ext. 6592

1.2.- Datos del profesorado			
Profesor	Javier Parra Domínguez	Grupo / s	1
Departamento	Administración y Economía de la Empresa		
Área	Economía Financiera y Contabilidad		
Centro	E.T.S. Ingeniería Industrial de Béjar		
Despacho	Planta Tercera		
Horario de tutorías	Solicitar por correo electrónico		
URL Web	https://produccioncientifica.usal.es/investigadores/57464/detalle		
E-mail	javierparra@usal.es	Teléfono	923 294 500 Ext. 2264

1.3.- Datos del profesorado			
Profesor	María Angélica González Arrieta	Grupo / s	1
Departamento	Informática y Automática		
Área	Ciencia de la Computación e Inteligencia Artificial		
Centro	Facultad de Ciencias		
Despacho	F3003		

Horario de tutorías	Se detallarán al inicio de la materia		
URL Web	https://produccioncientifica.usal.es/investigadores/56850/detalle		
E-mail	angelica@usal.es	Teléfono	923 294 500 Ext. 1302

2.- Recomendaciones previas

- **Conocimientos básicos de matemáticas**: comprensión de álgebra y teoría de números. Estos conocimientos son importantes para entender la criptografía.

- **Conceptos básicos de programación**: experiencia con un lenguaje de programación ayudará en la parte práctica del curso.

- **Conceptos generales de seguridad informática**: tener una idea básica sobre los principios de seguridad como autenticación, confidencialidad e integridad.

3.- Objetivos de la asignatura

- Proporcionar una comprensión profunda de los principios fundamentales de la criptografía y su aplicación en sistemas modernos como blockchain y criptomonedas.

- Desarrollar habilidades prácticas en el diseño e implementación de contratos inteligentes sobre plataformas blockchain.

- Analizar las vulnerabilidades comunes en los contratos inteligentes y en las redes blockchain, y cómo mitigar estos riesgos.

- Fomentar la comprensión de la interacción entre las criptomonedas, los contratos inteligentes y las plataformas de blockchain desde un punto de vista técnico.

4.- Competencias a adquirir / Resultados de aprendizaje

Competencias	Resultados de aprendizaje
4.1: Competencias Básicas:	**4.1: Conocimientos:** C1, C2, C6, C7
4.2: Competencias Específicas:	**4.2: Habilidades:** H1, H6, H7
4.3: Competencias Transversales:	**4.3: Competencias:** K1, K2, K3, K4, K5, K6, K7, K8

5.- Contenidos (temario)

Contenido teórico:

1. Introducción a la criptografía.
2. Introducción a *blockchain*.
3. Aspectos avanzados de *blockchain*.
4. Criptomonedas.
5. Vulnerabilidades en SmartContracts.

Contenido práctico:

1. Despliegue de contratos en *blockchain.*

Realización de trabajo con *blockchain* existente a elegir.

6.- Metodologías docentes

Sesiones magistrales: de carácter expositivo, en estas sesiones se presentarán los fundamentos teóricos de la criptografía, la tecnología blockchain y las criptomonedas. Se explicarán de forma estructurada los conceptos clave que permitirán a los estudiantes comprender el marco tecnológico y conceptual de la asignatura. Estas sesiones servirán como base para el análisis crítico y la aplicación práctica de los conocimientos.

Prácticas en el aula: orientadas al aprendizaje activo, permitirán a los estudiantes aplicar los conocimientos adquiridos mediante el uso de herramientas y lenguajes específicos para la implementación de algoritmos criptográficos, la interacción con redes blockchain y la creación de contratos inteligentes. Estas sesiones fomentarán la resolución de problemas, el pensamiento lógico y el aprendizaje por experimentación.

Seminarios online: impartidos tanto por el profesorado de la asignatura como por expertos invitados, estos seminarios profundizarán en aspectos actuales y relevantes del sector, como la criptografía cuántica (QKD) y post-cuántica (PQC), la evolución de las criptomonedas, aplicaciones emergentes de blockchain o cuestiones legales y éticas. Tendrán un enfoque participativo y estarán orientados al debate, la reflexión crítica y la actualización profesional.

Actividades en la plataforma Studium: los estudiantes dispondrán de recursos interactivos y test de autoevaluación que les permitirán consolidar los conocimientos teóricos y hacer un seguimiento autónomo de su progreso. Estas actividades facilitarán el aprendizaje flexible y adaptado al ritmo individual.

Entrega de trabajo final: como parte de la evaluación continua, los estudiantes deberán desarrollar un proyecto final en el que se diseñe e implemente un contrato inteligente en una red blockchain. La entrega incluirá tanto el desarrollo técnico realizado como una memoria explicativa. Esta actividad permitirá aplicar los conocimientos adquiridos a un caso práctico y desarrollar competencias como la programación, la redacción técnica y la capacidad de análisis y síntesis.

Tutorías: se ofrecerán sesiones personalizadas, individuales o en pequeños grupos, que permitirán a los estudiantes resolver dudas, recibir orientación sobre las actividades prácticas y el trabajo final, y profundizar en aquellos contenidos que requieran refuerzo. Estas tutorías podrán realizarse de forma presencial o virtual, adaptándose a las necesidades del estudiantado.

6.1.- Distribución de metodologías docentes

		Horas dirigidas por el profesor		Horas de trabajo autónomo	HORAS TOTALES
		Horas presenciales.	Horas no presenciales.		
Sesiones magistrales		8		30	38
Prácticas	- En aula			20	28
	- En el laboratorio				
	- En aula de informática	8			
	- De campo				
	- Otras (detallar)				
Seminarios			5		5
Exposiciones y debates					
Tutorías			2		2
Actividades de seguimiento online			5	25	30
Preparación de trabajos			15	30	45
Otras actividades (detallar)					
Exámenes		2			2
TOTAL		**18**	**27**	**105**	**150**

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

- *Cryptography and Network Security* (William Stallings) - Referencia clave para entender los fundamentos de la criptografía.

- *Mastering Bitcoin* (Andreas M. Antonopoulos) - Guía práctica sobre el funcionamiento de las criptomonedas y la blockchain.

- *Blockchain Basics* (Daniel Drescher) - Un enfoque introductorio sobre blockchain.

- *Mastering Ethereum* (Andreas M. Antonopoulos y Gavin Wood) - Texto clave para trabajar con contratos inteligentes.

- *Mastering Blockchain: Unlocking the power of cryptocurrencies, smart contracts, and decentralized applications* (Imran Bashir). - Abarca los fundamentos, el desarrollo y las aplicaciones de la tecnología **blockchain**.

- Documentación oficial de Ethereum: https://ethereum.org/en/developers/docs/

- Tutoriales sobre Smart Contracts en Solidity (https://soliditylang.org/docs/)

- Artículos académicos sobre vulnerabilidades en contratos inteligentes (pueden encontrarse en Google Scholar, IEEE Xplore).

8.- Evaluación

8.1: Criterios de evaluación:

- Participación y realización de actividades:
  - Las competencias adquiridas en la aplicación de los conocimientos prácticos serán evaluadas a través de la participación en clase, y la realización de tareas a través de Studium. En esta parte se valorarán los resultados de aprendizaje relacionados con las competencias y conocimientos que deben adquirir a lo largo de la asignatura.
- Trabajo final:
  - El alumnado deberá desarrollar un trabajo final en el que se diseñe e implemente un contrato inteligente en una red blockchain, y que entregará junto con un informe sobre el trabajo realizado. En esta parte se valorarán los resultados de aprendizaje relacionados con las habilidades que deben desarrollar los estudiantes, además de las competencias y conocimientos.
- Prueba escrita:

- La comprensión de los conceptos básicos tratados tanto en las sesiones magistrales como en las sesiones prácticas será evaluada a través de una prueba escrita, tipo test. En esta parte se valorarán los resultados de aprendizaje relacionados con las competencias y los conocimientos que deben adquirir los estudiantes para su posterior aplicación en las sesiones prácticas.

8.2: Sistemas de evaluación:

Se propone una evaluación basada en tres mecanismos. **Cada parte debe aprobarse con un 5 sobre 10 para superar la asignatura y poder aplicar el porcentaje**:

- Participación y realización de actividades (20%): a lo largo del curso se pedirán distintas entregas obligatorias relacionadas con el contenido de la asignatura y los seminarios online. Estas serán evaluadas junto con la participación en clase.
- Trabajo final (20%): el trabajo versará sobre los contenidos vistos en los talleres de prácticas relacionados con el despliegue de contratos inteligentes. Junto con el trabajo obligatorio deberá entregarse informe sobre dicho desarrollo que también será evaluado.
- Prueba escrita (60%): consistirá en un examen tipo test sobre los conceptos básicos tratados tanto en las sesiones magistrales como en las sesiones prácticas.

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

La evaluación se realizará de forma continua mediante la entrega de tareas o prácticas y tendrá en cuenta tanto el rendimiento individual como la participación activa en las distintas actividades propuestas. Se valorará la comprensión de los contenidos, la aplicación práctica de los conocimientos, la calidad en la realización de trabajos y exposiciones, así como la implicación en debates y seminarios. La asistencia regular, el cumplimiento de plazos y el compromiso con el aprendizaje también serán considerados. El objetivo es promover una evaluación formativa que refleje el progreso del alumnado a lo largo del curso.

La asignatura se considerará superada cuando se alcance en cada una de las 3 partes anteriores una media ponderada igual a 5 o superior.

- Recuperación:
  - En caso de no superar la prueba escrita en convocatoria ordinaria, el alumno deberá volver a realizarla en convocatoria extraordinaria. En esta convocatoria extraordinaria, y siempre dentro del mismo curso académico, se mantendrá la nota de *Participación y realización de actividades* y del *Trabajo final*. En caso de no superar la asignatura en convocatoria extraordinaria, no se mantendrá ninguna nota para los siguientes cursos académicos.

Diligencias de Investigación y Prueba Electrónica

1.- Datos de la Asignatura

Código	306553	Plan	M204-1	ECTS	6
Carácter	Optativa	Curso	1	Periodicidad	Segundo semestre
Idioma de impartición asignatura		Castellano			
Área	Derecho Procesal				
Departamento	Derecho Administrativo, Financiero y Procesal				
Plataforma virtual	Studium http://studium.usal.es				

1.1.- Datos del profesorado

Profesor Coordinador	Federico Bueno de Mata	Grupo / s	1
Departamento	Derecho Administrativo, Financiero y Procesal		
Área	Derecho Procesal		
Centro	Facultad de Derecho		
Despacho	258		
Horario de tutorías			
URL Web	*https://produccioncientifica.usal.es/investigadores/57438/detalle*		
E-mail	febuma@usal.es	Teléfono	923294500 Ext. 1679

2.- Recomendaciones previas

Se recomienda tener conocimientos previos en Derecho Procesal Penal (especialmente sobre la fase de instrucción, diligencias previas, medidas cautelares y prueba), Derechos Fundamentales (como el derecho a la intimidad, al secreto de las comunicaciones y la protección de datos, recogidos en el art. 18 CE y desarrollados por el TC y el TEDH), y Derecho Penal Sustantivo (para entender el contexto de los delitos, especialmente los informáticos y los relacionados con la privacidad).

3.- Objetivos de la asignatura

- Conocer el marco jurídico que regula las diligencias de investigación en el proceso penal, incluyendo sus requisitos, límites y finalidad.
-Analizar los derechos fundamentales afectados por las diligencias de investigación y la obtención de prueba electrónica, especialmente el derecho a la intimidad, secreto de las comunicaciones y protección de datos.
- Identificar y comprender las principales diligencias de investigación (intervención de comunicaciones, registros, vigilancia, etc.) y su aplicación práctica.
- Estudiar la normativa y jurisprudencia aplicable a la prueba electrónica en el ámbito penal, tanto a nivel nacional como internacional.
- Evaluar la validez y eficacia probatoria de la prueba electrónica dentro del proceso penal, considerando su obtención, custodia y análisis.
-Desarrollar habilidades prácticas para la correcta interpretación jurídica y aplicación procesal de diligencias y pruebas electrónicas en casos reales.

4.- Competencias a adquirir / Resultados de aprendizaje

Competencias	Resultados de aprendizaje
4.1: Competencias Básicas:	**4.1: Conocimientos:** C3, C9, C10 **C3**. Identificar las leyes, regulaciones y estándares nacionales e internacionales relacionados con la ciberseguridad **C9**. Recopilar información pertinente de la legislación nacional e internacional que afecta a los sistemas de información y la ciberseguridad, así como en los aspectos legales y sociales relacionados. **C10**. Caracterizar normativas y regulaciones en materia de protección de datos, cumplimiento normativo y responsabilidad jurídica en casos de incidentes de seguridad.
4.2: Competencias Específicas:	**4.2: Habilidades:** H9, H10, H11 **H9.** Adquirir habilidades para analizar y evaluar los aspectos legales de la ciberseguridad, asesorar en la implementación de políticas y normatives y colaborar con equipos técnicos en la resolución de casos jurídicos relacionados con la ciberseguridad. **H10.** Desarrollar habilidades de investigación y análisis en materia de delitos informáticos para comprender los motivos e impacto en el entorno digital. **H11.** Mejorar en habilidades de comunicación y argumentación legal, y desarrollar habilidades éticas y profesionales para enfrentar los desafíos éticos y legales en el ámbito de la ciberseguridad.

4.3: Competencias Transversales:	4.3: Competencias: K5, K9 **K5**. Validar la garantía y seguridad de los sistemas informáticos pertinentes, como redes locales, servidores, bases de datos y sistemas de gestión de información. **K9**. Aplicar las restricciones legales asociados a la seguridad informática sobre el manejo y procesamiento de datos personales.

5.- Contenidos (temario)

Contenido teórico:

1. Introduccion a la investigación tecnológica
2. Marco lega internacional.
3. Marco legal nacional: especial referencia a Ley de Enjuiciamiento Criminal. LO 13/2015
4. Policía Judicial y competencias en la materia.
5. Tratamiento procesal y tipología de las diligencias de investigación tecnológica. (Interceptación de comunicaciones, captación y grabación de imágenes, dispositivos de escucha oral, registro masivo de dispositivos).
6. Introducción: Teoría general de la prueba
7. Marco legal internacional: especial referencia a las órdenes europeas sobre prueba elecrónica en procesos penales.
8. Conceptualización de prueba electrónica
9. Tipologías de prueba electrónica
10. Procedimiento probatorio de la prueba electrónica. Obtención, Aportación, Proposición, Admisión, Práctica y Valoración.

Contenido práctico:

1. Caso práctico sobre qué diligencias de investigación tecnológica se debe aplicar en función del ciberataque que se desea probar.
2. Caso práctico sobre sobre obtención de pruebas electrónicas, prueba ilícita y conexión de antijuridicidad.

6.- Metodologías docentes

Metodología jurídica clásica, a través de el análisis de legislación, jurisprudencia y bibliografía especializada, así como informes y cuestiones de softlaw relacionadas con la materia.
El enfoque de la asignatura combinará enfoques teóricos y aplicación práctica.

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	40	72
Prácticas	- En aula				
	- En el laboratorio				
	- En aula de informática				
	- De campo				

- Otras (detallar)				
Seminarios				
Exposiciones y debates	4		5	9
Tutorías		2		2
Actividades de seguimiento online		5		5
Preparación de trabajos			60	60
Otras actividades (detallar)				
Exámenes	2			2
TOTAL	**18**	**27**	**105**	**150**

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

BREZO FERNÁNDEZ, F.; RUBIO VIÑUELA, Y.; *Manual de ciberinvestigación en fuentes abiertas. OSINT para analistas*, Madrid, 2019.

BUENO DE MATA F., "Un centinela virtual para investigar delitos cometidos a través de las redes sociales: ¿deberían ampliarse las actuales funciones del agente encubierto en Internet?", *El proceso penal en la sociedad de la información. Las nuevas tecnologías para investigar el delito,* ed. La Ley, Madrid, 2012.

BUENO DE MATA, F. *Las diligencias de investigación penal en la cuarta revolución industrial*, Navarra, 2019.

BUENO DE MATA, F., *Investigación y prueba de delitos de odio en Redes Sociales: Técnicas OSINT e inteligencia policial,* Valencia, 2023.

BUJOSA VADELL, L., "ChatGPT y proceso", *Arbitraje y jurisdicción: homenaje a Miguel Ángel Fernández-Ballesteros*, Madrid, 2024, pp. 295-322.

CONTRERAS, M., "El amor como estrategia de explotación: Los loverboys*", Cambio de paradigma en la prevención y erradicación de la violencia de género*, Granada, 2017, pp. 107- 115.

DEL POZO PÉREZ M., "El agente encubierto como medio de investigación de la delincuencia organizada en la ley de enjuiciamiento criminal española, en Constitución Europea: aspectos históricos, administrativos y procesales", *Criterio Jurídico*, Santiago de Cali (Colombia), Nº 6, 2006.

DEL POZO PÉREZ, M., "La entrega vigilada como medio de investigación de la delincuencia organizada en la ley de enjuiciamiento criminal española", *Pensamiento Jurídico,* Número 21, 2008.

GONZÁLEZ PULIDO, I., "El uso de la inteligencia artificial generativa en la investigación de la ciberdelincuencia de género: ante el auge de los deepfakes", Ius et Scientia, Vol. 9, Nº 2, 2023, pp. 157-180. https://dx.doi.org/10.12795/IETSCIENTIA

GONZÁLEZ PULIDO, I., "European Cybercrime Centre (EC3) investigación de los delitos de alta tecnología*", FODERTICS 5.0: estudios sobre nuevas tecnologías y justicia,* Granada, 2016, pp. 223 y ss.

LÓPEZ GARCÍA, E., "Agente encubierto y agente provocador, ¿dos figuras incompatibles?" *Diario La Ley*, año XXIV número 5822. viernes, 11 de julio de 2003.

MARTÍN DIZ, F., “Derechos y garantías procesales penales fundamentales: una lectura en clave tecnológica” , *IUS ET SCIENTIA: Revista electrónica de Derecho y Ciencia*, (10) 1, 2024, pp. 52-81. https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i01.03

MIGUEL BARRIO, R., “El agente encubierto informático ante el anonimato del cibercrimen en la Deep Web”, *La justicia en la sociedad 4.0: nuevos retos para el siglo XXI*, 2023, pp. 589-618.

RODRIGUEZ RODRÍGUEZ, Y., “Inteligencia de fuentes abiertas (OSINT): Características, debilidades y engaño”, *Revista de Análisis GES*I, Nº11, 2019.

SÁNCHEZ GÓMEZ, R., “El agente encubierto informático”, *La ley penal: revista de derecho penal, procesal y penitenciario*, ISSN 1697-5758, Nº. 118, 2016.

SANCHEZ GONZÁLEZ,S., *El agente encubierto en el proceso penal español*, Valencia, 2024.

VALIÑO CES, A., “Una lectura crítica en relación con el agente encubierto informático tras la Ley Orgánica 13/2015”, *Diario La Ley*, núm. 8731. Sección Tribuna, 30 de marzo de 2016.

VELASCO NUÑEZ, E., “Registros remotos sobre equipos informáticos. El agente encubierto virtual”, *Los medios técnicos e investigación criminal, Colección Criminología y Criminalística*, Madrid, 2019, pág. 230.

VILLAR FUENTES, “El agente encubierto informático: reto legislativo pendiente en un escenario digitalizado”, *Revista de Estudios Jurídicos y Criminológicos*, ISSN-e 2660-7964, Nº. 6, 2022, pp. 197-228.

8.- Evaluación

8.1: Criterios de evaluación:

· Comprensión y dominio del marco jurídico aplicable a las diligencias de investigación y a la prueba electrónica.
· Capacidad para identificar y analizar los derechos fundamentales afectados.
· Aplicación adecuada de los conocimientos a supuestos prácticos.
· Claridad expositiva, argumentación jurídica y uso correcto del lenguaje técnico.
· Participación activa y fundamentada en clase (en convocatoria ordinaria).

8.2: Sistemas de evaluación:

Convocatoria ordinaria:
· **Participación activa en clase:** 30%
· **Trabajo expositivo individual o grupal:** 70%

Convocatoria extraordinaria:
· **Examen escrito con preguntas cortas:** 100%

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

-En la convocatoria ordinaria, se valorará especialmente la participación crítica y fundamentada en clase, así como la calidad y rigor del trabajo expositivo presentado.
- El trabajo expositivo debe mostrar comprensión teórica y capacidad de aplicación práctica, incluyendo referencias normativas y jurisprudenciales.
- En la convocatoria extraordinaria, el examen consistirá en preguntas cortas que evaluarán de forma directa los conocimientos teóricos y prácticos adquiridos.
- Se recomienda el seguimiento continuo de las clases, la lectura de los materiales indicados y la resolución de casos prácticos para facilitar tanto la evaluación ordinaria como la extraordinaria.
-El estudiante deberá demostrar, en ambos casos, un conocimiento suficiente de los contenidos esenciales de la asignatura y su aplicación conforme al marco legal vigente.

Economía y empresa digital

1.- Datos de la Asignatura					
Código	306556	Plan	M204-1	ECTS	3
Carácter	Optativa	Curso	1	Periodicidad	Primer semestre
Idioma de impartición asignatura		Castellano			
Área	Historia e Instituciones Económicas				
Departamento	Economía e Historia Económica				
Plataforma virtual	Studium http://studium.usal.es				

1.1.- Datos del profesorado			
Profesor Coordinador	Santiago Manuel López García	Grupo / s	1
Departamento	Economía e Historia Económica		
Área	Historia e Instituciones Económicas		
Centro	Facultad de Economía y Empresa		
Despacho	IECYT, Edificio I+D+i		
Horario de tutorías			
URL Web	*https://produccioncientifica.usal.es/investigadores/57037/detalle*		
E-mail	slopez@usal.es	Teléfono	923294500 Ext. 4694

Profesor Coordinador	José Ortega Mohedano	Grupo / s	1
Departamento	Administración y Economía de la Empresa		
Área	Economía Financiera y Contabilidad		
Centro	Facultad de Economía y Empresa		
Despacho			
Horario de tutorías			
URL Web	*https://produccioncientifica.usal.es/investigadores/57405/detalle*		
E-mail	lito@usal.es	Teléfono	923294500

Profesor Coordinador	Cristina Almaraz López	Grupo / s	1
Departamento	Economía e Historia Económica		
Área	Historia e Instituciones Económicas		
Centro	Facultad de Economía y Empresa		
Despacho	IECYT, Edificio I+D+i		

Horario de tutorías			
URL Web	https://produccioncientifica.usal.es/investigadores/807078/detalle		
E-mail	cristina.almaraz@usal.es	Teléfono	923294500

2.- Recomendaciones previas

- No se requieren conocimientos especializados previos.
- Conocimientos de inglés para la comprensión de textos académicos.

3.- Objetivos de la asignatura

- Analizar el impacto de la digitalización y la economía intensiva en datos sobre los mercados, el sector público y las dinámicas de innovación y desigualdad.
- Comprender los fundamentos económicos de la empresa digital y los retos que plantea la economía del dato, incluyendo los fallos de mercado y el papel de las políticas públicas y de ciberseguridad.
- Evaluar el papel de la ciberseguridad en la empresa desde una perspectiva económica y financiero-contable, valorando su impacto en la organización, la gestión y la protección de activos digitales.
- Aplicar criterios de valoración económico-financiera en la gestión de la ciberseguridad empresarial y en la toma de decisiones en entornos digitales.

4.- Competencias a adquirir / Resultados de aprendizaje

Competencias	Resultados de aprendizaje
4.1: Competencias Básicas:	**4.1: Conocimientos:** C4 **C4**. Valorar el impacto de la ciberseguridad sobre la economía, la empresa y la ciudadanía.
4.2: Competencias Específicas:	**4.2: Habilidades:** H4, H5 **H4.** Trabajar en equipo para colaborar con otros profesionales de la ciberseguridad, así como para educar a usuarios finales y promover buenas prácticas de seguridad. **H5.** Trabajar en equipo en entornos multidisciplinares, para el análisis y resolución de problemas concretos de inseguridad en equipos y sistemas informáticos.
4.3: Competencias Transversales:	**4.3: Competencias:** K9 **K9**. Aplicar las restricciones legales asociados a la seguridad informática sobre el manejo y procesamiento de datos personales.

5.- Contenidos (temario)

Contenido teórico:

1. La economía intensiva en datos: caracterización y fallos de mercado.
2. El rol del sector público en la economía intensiva en datos.
3. El paradigma de la destrucción creativa.
4. Innovación, desigualdad y políticas de ciberseguridad.
5. La digitalización en la empresa.
6. El mercado de la ciberseguridad.
7. La ciberseguridad en la empresa desde una perspectiva económica.
8. Valoración económico-financiera de la ciberseguridad en la empresa.

Contenido práctico:

1. Elección entre las lecturas propuestas por el profesor y realización de comentarios de texto.
2. Participación en seminarios de argumentación y contraargumentación.

6.- Metodologías docentes

- **Sesiones Magistrales**: Sesiones donde se presentan los fundamentos teóricos de los temas de la asignatura. Son de carácter expositivo y buscan proporcionar una visión amplia y detallada de los conceptos clave, fomentando al mismo tiempo el diálogo y la reflexión crítica entre los estudiantes.
- **Seminarios**: Sesiones en grupos más reducidos, donde los estudiantes tienen la oportunidad de discutir y profundizar en los temas tratados. Se trata de fomentar la participación, el intercambio de ideas y la construcción colaborativa del conocimiento.
- **Sesiones Prácticas**: A través de casos de estudio, los estudiantes pondrán en práctica los conceptos teóricos, desarrollando habilidades técnicas y analíticas aplicando de manera concreta los conocimientos adquiridos.
- **Actividades de seguimiento online**: Sesiones individualizadas o en pequeños grupos donde los estudiantes pueden resolver dudas específicas con el docente, recibir orientación personalizada y profundizar en temas de interés. Estas sesiones son flexibles y se pueden llevar a cabo tanto de forma presencial como virtual.
- **Preparación de trabajos autónomos**: Asignaciones que los estudiantes deben realizar de manera independiente, aplicando los conocimientos adquiridos, con el objetivo de fomentar la capacidad de análisis, síntesis y crítica, así como el desarrollo de habilidades de investigación y escritura académica. Podrán ser individuales o de grupo.

6.1.- Distribución de metodologías docentes

		Horas dirigidas por el profesor		Horas de trabajo autónomo	HORAS TOTALES
		Horas presenciales.	Horas no presenciales.		
Sesiones magistrales		8		15	23
Prácticas	- En aula			10	10
	- En el laboratorio				
	- En aula de informática				
	- De campo				
	- Otras (detallar)				
Seminarios			3		3
Exposiciones y debates					
Tutorías					
Actividades de seguimiento online			3	13	16
Preparación de trabajos			7,5	14,5	22
Otras actividades (detallar)					
Exámenes		1			1

TOTAL	**9**	**13,5**	**52,5**	75

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

- Anderson, R. et al. (2013). Measuring the Cost of Cybercrime. In: Böhme, R. (eds) The Economics of Information Security and Privacy. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-39498-0_12
- Anderson, R., & Moore, T. (2007). Information Security Economics – and Beyond. Lecture Notes in Computer Science, 68–91. https://doi.org/10.1007/978-3-540-74143-5_5
- Baeza, E. O., Sabater, V. L., Delgado, D. V., Paniagua, M. R., & Pinto, A. L. (2018). Economía de los Datos: riqueza 4.0. https://www.fundacioncarolina.es/wp-content/uploads/2018/11/Libro-Economia-de-los-Datos-Ontiveros.pdf
- Caballero, R.J. (2010). creative destruction. In: Durlauf, S.N., Blume, L.E. (eds) Economic Growth. The New Palgrave Economics Collection. Palgrave Macmillan, London. https://doi.org/10.1057/9780230280823_5
- Cobos, E. V. (2024). Cybersecurity Economics for Emerging Markets. World Bank Publications-Books.
- Comisión Europea. Políticas de ciberseguridad. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies
- Evans, A. (2022). Enterprise Cybersecurity in Digital Business. Taylor & Francis. https://bookshelf.vitalsource.com/books/9781000459371
- Goldfarb, A., & Tucker, C. (2019). Digital economics. Journal of Economic Literature, 57(1), 3-43. https://doi.org/10.1257/jel.20171452
- Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. ACM Transactions on Information and System Security, 5(4), 438–457. https://doi.org/10.1145/581271.581274
- INCIBE. (2024). Directorio de estudios del mercado de la ciberseguridad de ICEX. https://www.incibe.es/internacionalizacion/nuevos-mercados/estudios-de-mercado-de-la-ciberseguridad-internacionales
- Kianpour, M., Kowalski, S. J., & Øverby, H. (2021). Systematically Understanding Cybersecurity Economics: A Survey. Sustainability, 13(24), 13677. https://doi.org/10.3390/su132413677
- Rashid, Z., Noor, U., & Altmann, J. (2021). Economic model for evaluating the value creation through information sharing within the cybersecurity information sharing ecosystem. Future Generation Computer Systems, 124, 436-466. https://doi.org/10.1016/j.future.2021.05.033
- Rogers, D. L. (2016). The digital transformation playbook: Rethink your business for the digital age. Columbia University Press.
- Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. Sensors, 23(15), 6666. https://doi.org/10.3390/s23156666
- Taskin, N., Yıldırım, A. Ö., Ercan, H. D., Wynn, M., & Metin, B. (2025). Cyber Insurance Adoption and Digitalisation in Small and Medium-Sized Enterprises. Information, 16(1), 66. https://doi.org/10.3390/info16010066
- World Economic Forum, in collaboration with Accenture. Global Cybersecurity Outlook 2025. https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

8.- Evaluación

8.1: Criterios de evaluación:

La nota final se compondrá de:

- 10% participación en actividad presencial

- 40% de entrega de los trabajos y/o informes sobre supuestos prácticos
- 50% de la prueba final

8.2: Sistemas de evaluación:

El examen final sobre conocimientos teóricos será tipo test.

En cuanto a los supuestos prácticos, se entregarán 2 informes realizados a partir de un trabajo grupal. Ambos tendrán el mismo peso en la nota final de la parte práctica de la asignatura.

También se evaluará la participación en los debates que se generen en clase y/o en los foros online.

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

Se recomienda participar en las actividades de seguimiento online para la preparación de los trabajos y/o informes y en el caso de no aprobar una de las dos evaluaciones (teórica y práctica) de la asignatura. De esta forma el alumno puede consultar con el profesor la mejor manera de preparar el examen de recuperación.

GESTIÓN Y ADMINISTRACIÓN DE LA CIBERSEGURIDAD

1.- Datos de la Asignatura					
Código	306550	Plan	M204-1	ECTS	6
Carácter	Obligatoria	Curso	1	Periodicidad	Semestre 1
Idioma de impartición asignatura		Español			
Área	Ciencia de la Computación e Inteligencia Artificial				
Departamento	Informática y Automática				
Plataforma virtual	Studium http://studium.usal.es/				

1.1.- Datos del profesorado			
Profesor Coordinador	Sara Rodríguez González	Grupo / s	1
Departamento	Ciencias de la computación e inteligencia artificial		
Área	Informática y Automática		
Centro	Facultad de Ciencias		
Despacho	D1514		
Horario de tutorías	A demanda, consultar por correo electrónico		
URL Web	https://produccioncientifica.usal.es/investigadores/57246/detalle		
E-mail	srg@usal.es	Teléfono	923294500 Ext. 6096 6588

1.2.- Datos del profesorado			
Profesor Coordinador	Fernando de la Prieta Pintado	Grupo / s	1
Departamento	Ciencias de la computación e inteligencia artificial		
Área	Informática y Automática		
Centro	Facultad de Ciencias		
Despacho	D1514		
Horario de tutorías	A demanda, consultar por correo electrónico		
URL Web	https://produccioncientifica.usal.es/investigadores/57460/detalle		
E-mail	fer@usal.es	Teléfono	923294500 Ext. 6088 6590

2.- Recomendaciones previas

- Conocimientos básicos de ciberseguridad, redes, criptografía y sistemas operativos.
- Familiaridad con las metodologías de investigación científica.
- Comprensión básica de la gestión de riesgos y principios de privacidad en ciberseguridad.
- Conocimientos básicos de inglés para la búsqueda de información

3.- Objetivos de la asignatura

- **Fundamentos teóricos de ciberseguridad**: Introducción a conceptos básicos como criptografía, redes y protección de la información.
- **Identificación de amenazas y vulnerabilidades**: Analizar las amenazas más comunes en entornos digitales y las técnicas para prevenir, detectar y responder ante incidentes de seguridad.
- **Investigación en ciberseguridad**: Desarrollar habilidades en la búsqueda y análisis de artículos científicos y recursos académicos relevantes en ciberseguridad.
- **Gestión de riesgos y privacidad**: Examinar los aspectos de gestión de riesgos, ética y privacidad en la ciberseguridad, considerando su impacto en la protección de la información.
- **Trabajo colaborativo y resolución de problemas**: Fomentar el trabajo en equipo en el análisis y resolución de problemas de seguridad informática, así como en la argumentación y defensa de soluciones.

4.- Competencias a adquirir / Resultados de aprendizaje

Competencias	Resultados de aprendizaje
4.1: Competencias Básicas:	**4.1: Conocimientos:** C1, C2, C3, C5, C6, C7 **C1**. Relacionar los fundamentos teóricos de la ciberseguridad, incluyendo conceptos básicos de la información, criptografía, redes y sistemas operativos para proteger la integridad y la confidencialidad de la información. **C2**. Identificar las amenazas y vulnerabilidades más comunes en entornos digitales, así como las técnicas y metodologías utilizadas para prevenir, detectar y responder a incidentes de seguridad. **C3**. Identificar las leyes, regulaciones y estándares nacionales e internacionales relacionados con la ciberseguridad. **C5**. Examinar aspectos interdisciplinarios de la ciberseguridad, como la gestión de riesgos, la ética y la privacidad, con el fin de proporcionar una visión integral de la disciplina. **C6**. Identificar protocolos de seguridad contra amenazas informáticas a partir de conocimientos especializados en ciberseguridad, centrándose en su desarrollo, implementación y evaluación. **C7**. Describir los aspectos técnicos e informáticos de la seguridad, incluyendo el diseño seguro de sistemas, la seguridad en redes y comunicaciones, la protección de datos y la gestión de incidentes de seguridad.
4.2: Competencias Específicas:	**4.2: Habilidades:** H3, H4, H5, H8 **H3.** Analizar y evaluar los riesgos de seguridad en entornos digitales, identificando posibles debilidades y proponiendo soluciones efectivas. **H4.** Trabajar en equipo para colaborar con otros profesionales de la ciberseguridad, así como para educar a usuarios finales y promover buenas prácticas de seguridad.

	H5. Trabajar en equipo en entornos multidisciplinares, para el análisis y resolución de problemas concretos de inseguridad en equipos y sistemas informáticos. **H8**. Desarrollar habilidades de análisis y resolución de problemas en el ámbito de la seguridad informática, así como habilidades de comunicación y trabajo en equipo.
4.3: Competencias Transversales:	**4.3: Competencias:** K5, K6, K7, K8 **K5**. Validar la garantía y seguridad de los sistemas informáticos pertinentes, como redes locales, servidores, bases de datos y sistemas de gestión de información. **K6**. Diseñar políticas de monitorización y copia de segura, para la recuperación de sistemas y el aseguramiento en la información en caso de malfuncionamiento. **K7**. Elaborar la política de seguridad de una empresa. **K8**. Auditar las políticas de seguridad de una empresa a todos los niveles (sistemas, red, información, etc.).

5.- Contenidos (temario)

Contenido teórico:

1. Introducción a la investigación en ciberseguridad.
2. Metodologías en investigación.
3. Repositorios de artículos de investigación.
4. Situación de la ciberseguridad en el I+D+i.
5. Organismos e instituciones de ciberseguridad.

Contenido práctico:

1. Taller práctico de bibliometría.
2. Participación en seminarios de argumentación y contraargumentación.

6.- Metodologías docentes

-Sesiones Magistrales: sesiones de carácter expositivo donde se presentan los fundamentos teóricos de los temas la asignatura. Las sesiones podrán tener aplicabilidad tanto de forma presencial como en formatos no presenciales, utilizando plataformas de videoconferencia para su realización u otros canales.

-Sesiones Prácticas (en aula): sesiones en aula diseñadas para aplicar de manera concreta los conocimientos adquiridos. A través de ejercicios y el uso de herramientas y software específico, los estudiantes pondrán en práctica los conceptos teóricos, desarrollando habilidades técnicas y analíticas.

- Seminarios: Sesiones donde los estudiantes tienen la oportunidad de profundizar en los temas tratados en la asignatura. Se utilizarán metodologías activas, como el debate, el análisis de casos o la resolución de problemas, adaptable tanto a modalidades presenciales como a distancia.

- Tutorías: sesiones personalizadas, individuales o en grupos pequeños, que permiten a los estudiantes aclarar dudas específicas y recibir orientación detallada del docente. Estas pueden realizarse de manera presencial o virtual, adaptándose a las necesidades de los alumnos.

- Preparación de trabajos autónomos (individuales y en grupo): Consisten en tareas que los estudiantes desarrollan de forma independiente para aplicar y profundizar en los conocimientos. Los trabajos en grupo implican actividades colaborativas en las que los estudiantes aplican conocimientos de manera conjunta. Los trabajos incluyen exposiciones que tratan de fomentar habilidades sociales como comunicación, liderazgo, negociación y manejo de conflictos, potenciando el trabajo en equipo.
Prueba final. Se convierte en un instrumento para determinar el grado de asimilación de la asignatura. Consistirá mayoritariamente en preguntas de tipo test y/o respuesta corta.

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		30	36
Prácticas	- En aula	6		20	26
	- En el laboratorio				
	- En aula de informática				
	- De campo				
	- Otras (detallar)				
Seminarios			5		5
Exposiciones y debates		4			4
Tutorías					
Actividades de seguimiento online			7	25	32
Preparación de trabajos			15	30	45
Otras actividades (detallar)					
Exámenes		2			2
TOTAL		**18**	**27**	**105**	**150**

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

Bibliografía:
- Stallings, W. (2017). *Network Security Essentials*. Pearson.
- Anderson, R. (2020). *Security Engineering*. Wiley.
- Jouini, M. & Abeni, A. (2013). *Cyber Security and IT Infrastructure Protection*. Springer.
Recursos adicionales:
- SANS Institute, NIST.

8.- Evaluación

8.1: Criterios de evaluación:

Elaboración de tareas obligatorias:

- Las tareas versarán sobre los contenidos vistos en las clases presenciales. En general se tratará de realizar desarrollos con algunas de las herramientas y contenidos vistos en clase. En las tareas entregadas se valorará, además de la calidad científica y técnica del contenido, la destreza en el uso de la herramienta o herramientas elegidas, la capacidad de comunicación y el espíritu crítico y constructivo.

Prueba final:

- Consistirá mayoritariamente en preguntas tipo test y de respuesta corta, e incluirá tanto preguntas de la parte teórica como de las sesiones prácticas y demostraciones llevadas a cabo.

La ponderación de las diferentes partes será la siguiente

- Asistencia y participación en actividades presenciales: 20%
- Tareas, resolución de prácticas: 30%
- Prueba de evaluación final: 50%

8.2: Sistemas de evaluación:

- Participación en actividades presenciales.
- Entrega de informes de los supuestos prácticos.
- Prueba final.

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

Recomendaciones para la evaluación:

Con carácter general, se recomienda:

- asistir activamente a las sesiones presenciales de la asignatura.
- cumplir los plazos marcados para la entrega de tareas y trabajos.
- seguir las instrucciones para la elaboración de los informes.
- seguir las instrucciones para las tareas y la prueba final.

Recomendaciones para la recuperación:

El alumno no superará la asignatura cuando no haya participado activamente en las actividades presenciales de la asignatura y/o no haya entregado las tareas obligatorias con un mínimo de calidad. Tampoco la superará si la prueba final no es satisfactoria. En consecuencia, deberá volver a realizar las tareas y la prueba final con el nivel de calidad exigido.

HACKING ÉTICO

1.- Datos de la Asignatura					
Código	306554	Plan	M204-1	ECTS	6
Carácter	Obligatoria	Curso	1	Periodicidad	Semestre 1
Idioma de impartición asignatura		Español			
Área	Ciencia de la Computación e Inteligencia Artificial				
Departamento	Informática y Automática				
Plataforma virtual	Studium http://studium.usal.es				

1.1.- Datos del profesorado			
Profesor Coordinador	Alfonso González Briones	Grupo / s	1
Departamento	Informática y Automática		
Área	Ciencia de la Computación e Inteligencia Artificial		
Centro	Facultad de Ciencias		
Despacho	F3012		
Horario de tutorías	Solicitar cita por correo electrónico		
URL Web	https://produccioncientifica.usal.es/investigadores/148408/detalle		
E-mail	alfonsogb@usal.es	Teléfono	923294500

2.- Recomendaciones previas

- **Conocimientos avanzados de sistemas operativos**: Familiaridad con el uso de terminal y comandos avanzados en sistemas operativos, tanto Linux como Windows.
- **Experiencia en redes y protocolos de comunicación**: Comprensión de cómo funcionan las redes, los protocolos de comunicación y la seguridad asociada.
- **Conocimientos básicos en ciberseguridad**: Familiaridad con conceptos de protección de sistemas, redes y aplicaciones.

3.- Objetivos de la asignatura

- **Introducción al hacking ético**: Proporcionar una comprensión clara de los principios del hacking ético, con énfasis en la legalidad y las buenas prácticas.
- ***Information gathering* ("*footprinting*")**: Enseñar a obtener información sobre objetivos de manera legal y ética, mediante técnicas y herramientas específicas.
- **Explotación de vulnerabilidades**: Capacitar a los estudiantes en el análisis y explotación de vulnerabilidades en sistemas informáticos, con la aplicación de herramientas prácticas.
- **Post-explotación**: Instruir en técnicas de post-explotación para mantener el acceso a sistemas comprometidos y obtener información adicional de manera controlada.
- **Uso de herramientas especializadas**: Familiarizar a los estudiantes con herramientas como para la resolución de retos prácticos en un entorno controlado.

4.- Competencias a adquirir / Resultados de aprendizaje

Competencias	Resultados de aprendizaje
4.1: Competencias Básicas:	**4.1: Conocimientos:** C1, C2, C6, C7
4.2: Competencias Específicas:	**4.2: Habilidades:** K1, K2, K3, K4, K5, K6, K8
4.3: Competencias Transversales:	**4.3: Competencias:** H1, H2, H6, H7

5.- Contenidos (temario)

Contenido teórico:

1. Introducción al *hacking* ético.
2. *Information gathering* o "*footprinting*".
3. Herramientas para la obtención de información.
4. Análisis y explotación de vulnerabilidades.
5. Herramientas para la explotación de vulnerabilidades.
6. Post-explotación.

Contenido práctico:

1. Iniciación en *information gathering*.
2. Taller de explotación de vulnerabilidades.
3. Taller de post-explotación.

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		8		30	38
Prácticas	- En aula	8		20	28
	- En el laboratorio				
	- En aula de informática				
	- De campo				
	- Otras (detallar)				
Seminarios			5		5
Exposiciones y debates					
Tutorías			2		2
Actividades de seguimiento online			7	25	32
Preparación de trabajos			15	30	45
Otras actividades (detallar)					
Exámenes		2			2
TOTAL		**18**	**27**	**105**	**150**

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

Bibliografía:

- SANS Institute (2019). *The Web Application Hacker's Handbook*. Wiley.
- Michael, M., & Miller, R. (2020). *Hacking: The Art of Exploitation*. No Starch Press.
- McClure, S., & Scambray, J. (2017). *Hacking Exposed: Network Security Secrets & Solutions*. McGraw-Hill.

Repositorios y recursos electrónicos:

- **Hack The Box**: Plataforma de retos de hacking ético para practicar habilidades de penetration testing. https://www.hackthebox.eu/
- **picoCTF**: Competición de hacking ético orientada a estudiantes, con ejercicios prácticos de ciberseguridad. https://picoctf.org/
- **Atenea**: Plataforma de simulación y retos de ciberseguridad aplicada. https://www.atenea.com/

8.- Evaluación

8.1: Criterios de evaluación:

Examen: Evaluación del conocimiento teórico sobre hacking ético, vulnerabilidades y post-explotación.
Trabajo práctico: Entrega de un informe sobre las actividades prácticas realizadas durante los talleres de explotación de vulnerabilidades y post-explotación.

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.

INVESTIGACIÓN EN SEGURIDAD

1.- Datos de la Asignatura					
Código	306553	Plan	M204-1	ECTS	6
Carácter	Obligatoria	Curso	1	Periodicidad	Semestre 1
Idioma de impartición asignatura		Español			
Área	Ciencia de la Computación e Inteligencia Artificial				
Departamento	Informática y Automática				
Plataforma virtual	Studium http://studium.usal.es				

1.1.- Datos del profesorado			
Profesor Coordinador	Juan Manuel Corchado Rodríguez	Grupo / s	1
Departamento	Informática y Automática		
Área	Ciencia de la Computación e Inteligencia Artificial		
Centro	Facultad de Ciencias		
Despacho	Edificio Multiusos I+D+i, 24.1		
Horario de tutorías	A demanda, consultar por correo electrónico		
URL Web	https://produccioncientifica.usal.es/investigadores/55867/detalle		
E-mail	corchado@usal.es	Teléfono	923 294 500 Ext. 1525

1.2.- Datos del profesorado			
Profesor	Davinia Carolina Zato Domínguez	Grupo / s	1
Departamento	Informática y Automática		
Área	Ciencia de la Computación e Inteligencia Artificial		
Centro	Facultad de Ciencias		
Despacho	Pasillo nuevo de Informática y Automática, Facultad de Ciencias		
Horario de tutorías	A demanda, consultar por correo electrónico		
URL Web	https://produccioncientifica.usal.es/investigadores/57537/detalle		
E-mail	carol_zato@usal.es	Teléfono	923 294 500 Ext. 6076

2.- Recomendaciones previas

- Conocimientos básicos de ciberseguridad, redes y sistemas informáticos.
- Familiaridad con la búsqueda de artículos científicos
- Habilidades básicas en la redacción técnica

3.- Objetivos de la asignatura

- **Fundamentos de investigación en ciberseguridad**: Introducir a los estudiantes en las metodologías de investigación aplicadas a la ciberseguridad.
- **Metodologías en investigación**: Enseñar diferentes metodologías de investigación que son relevantes en el campo de la ciberseguridad, incluyendo enfoques cualitativos y cuantitativos.
- **Acceso y uso de repositorios de investigación**: Capacitar a los estudiantes para acceder y utilizar repositorios científicos como Google Scholar, IEEE Xplore y ACM Digital Library para encontrar artículos relevantes en ciberseguridad.
- **Situación actual de la ciberseguridad en I+D+i**: Analizar cómo la investigación y el desarrollo en ciberseguridad contribuyen a la innovación en el campo, abordando tanto las tendencias como los desafíos actuales.
- **Interacción con organismos de ciberseguridad**: Familiarizar a los estudiantes con los principales organismos e instituciones internacionales y nacionales que lideran la investigación en ciberseguridad.
- **Desarrollo de habilidades prácticas**: Fomentar la capacidad de realizar una revisión del estado del arte en ciberseguridad, con énfasis en el análisis crítico de la literatura científica.

4.- Competencias a adquirir / Resultados de aprendizaje

Competencias	Resultados de aprendizaje
4.1: Competencias Básicas:	**4.1: Conocimientos:** **C2**. Identificar las amenazas y vulnerabilidades más comunes en entornos digitales, así como las técnicas y metodologías utilizadas para prevenir, detectar y responder a incidentes de seguridad. **C5**. Examinar aspectos interdisciplinarios de la ciberseguridad, como la gestión de riesgos, la ética y la privacidad, con el fin de proporcionar una visión integral de la disciplina. **C6**. Identificar protocolos de seguridad contra amenazas informáticas a partir de conocimientos especializados en ciberseguridad, centrándose en su desarrollo, implementación y evaluación. **C7**. Describir los aspectos técnicos e informáticos de la seguridad, incluyendo el diseño seguro de sistemas, la seguridad en redes y comunicaciones, la protección de datos y la gestión de incidentes de seguridad. **C8.** Distinguir las últimas tendencias y tecnologías en el campo de la ciberseguridad, como el Internet de las cosas (IoT), la inteligencia artificial (IA) y el aprendizaje automático (Machine Learning), para estar preparados ante los desafíos futuros.
4.2: Competencias Específicas:	**4.2: Habilidades:** **H1.** Implementar medidas de seguridad en diferentes entornos y sistemas, incluyendo la configuración de firewalls, la gestión de accesos, la detección de intrusiones y el análisis forense digital. **H2.** Adquirir destrezas en el uso de herramientas y software especializados para evaluar la seguridad de sistemas y redes, así como para llevar a cabo pruebas de penetración y auditorías de seguridad. **H6.** Desarrollar habilidades técnicas para implementar soluciones de seguridad en sistemas y

	redes, realizar pruebas de penetración y responder a incidentes de seguridad de manera eficiente. **H7**. Adquirir destrezas en el uso de herramientas y software especializados para evaluar la seguridad de sistemas informáticos y redes. **H8**. Desarrollar habilidades de análisis y resolución de problemas en el ámbito de la seguridad informática, así como habilidades de comunicación y trabajo en equipo.
4.3: Competencias Transversales:	**4.3: Competencias:** **K5**. Validar la garantía y seguridad de los sistemas informáticos pertinentes, como redes locales, servidores, bases de datos y sistemas de gestión de información. **K6**. Diseñar políticas de monitorización y copia de segura, para la recuperación de sistemas y el aseguramiento en la información en caso de malfuncionamiento. **K7**. Elaborar la política de seguridad de una empresa. **K8**. Auditar las políticas de seguridad de una empresa a todos los niveles (sistemas, red, información, etc.). **K9**. Aplicar las restricciones legales asociados a la seguridad informática sobre el manejo y procesamiento de datos personales.

5.- Contenidos (temario)

Contenido teórico:

1. Introducción a la investigación en ciberseguridad.
2. Metodologías en investigación.
3. Repositorios de artículos de investigación.
4. Situación de la ciberseguridad en el I+D+i.
5. Organismos e instituciones de ciberseguridad.

Contenido práctico:

1. Taller práctico de bibliometría.
2. Elaboración de una revisión del estado del arte en aspectos de ciberseguridad.

6.- Metodologías docentes

La asignatura combina clases magistrales (8 horas) para impartir los fundamentos de la investigación en ciberseguridad, junto con seminarios (4 horas) y talleres prácticos de bibliometría (4 horas). En función de disponibilidades, se podrá contar con expertos en el área que compartirán su experiencia con el 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		8		30	38
Prácticas	- En aula	4			4
	- En el laboratorio				
	- En aula de informática				

	- De campo				
	- Otras (detallar)				
Seminarios		4	5	20	29
Exposiciones y debates					
Tutorías					
Actividades de seguimiento online			7	25	32
Preparación de trabajos			15	30	45
Otras actividades (detallar)					
Exámenes		2			2
TOTAL		**18**	**27**	**105**	**150**

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

Repositorios y recursos electrónicos:
- **Scopus**: Motor de búsqueda de artículos científicos.
- **Web of Science**: Motor de búsqueda de artículos científicos.
- **IEEE Xplore**: Base de datos de investigación en informática y ciberseguridad. https://ieeexplore.ieee.org/
- **ACM Digital Library**: Repositorio de artículos académicos de la ACM. https://dl.acm.org/

Recursos adicionales:
- **SANS Institute**: Plataforma educativa con recursos y formaciones sobre ciberseguridad. https://www.sans.org/

8.- Evaluación

8.1: Criterios de evaluación:
La nota final se compondrá: 50% de la nota parte teórica, 50% de la nota parte práctica.

8.2: Sistemas de evaluación:
Examen tipo test: Evaluación del conocimiento teórico sobre metodologías de investigación y ciberseguridad.
Trabajo escrito: Entrega de una revisión del estado del arte en ciberseguridad en general o específico sobre un tema a proponer, evaluada por su calidad y profundidad.

8.3: Consideraciones generales y recomendaciones para la evaluación y la recuperación:
Las dos partes serán consideradas de forma independiente, por lo que la recuperación será únicamente las partes suspensas. En caso de haber superado una parte, se guardará la nota de la parte superada para la segunda convocatoria.

La ciberseguridad en la sociedad del riesgo: economía y protección del dato

1.- Datos de la Asignatura					
Código	306557	Plan	M204-1	ECTS	3
Carácter	Optativa	Curso	1	Periodicidad	Primer semestre
Idioma de impartición asignatura		Castellano			
Área	Historia e Instituciones Económicas				
Departamento	Economía e Historia Económica				
Plataforma virtual	Studium http://studium.usal.es				

1.1.- Datos del profesorado			
Profesor Coordinador	Santiago Manuel López García	Grupo / s	1
Departamento	Economía e Historia Económica		
Área	Historia e Instituciones Económicas		
Centro	Facultad de Economía y Empresa		
Despacho	Edificio Multiusos I+D+i		
Horario de tutorías			
URL Web	https://produccioncientifica.usal.es/investigadores/57037/detalle		
E-mail	slopez@usal.es	Teléfono	923294500 Ext. 4694

Profesor Coordinador	José Ortega Mohedano	Grupo / s	1
Departamento	Administración y Economía de la Empresa		
Área	Economía Financiera y Contabilidad		
Centro	Facultad de Economía y Empresa		
Despacho			
Horario de tutorías			
URL Web	https://produccioncientifica.usal.es/investigadores/57405/detalle		
E-mail	lito@usal.es	Teléfono	923294500

Profesor Coordinador	Stefano De Marco	Grupo / s	1
Departamento	Sociología y Comunicación		
Área	Sociología		
Centro	Facultad de Ciencias Sociales		
Despacho			
Horario de tutorías			

URL Web	https://produccioncientifica.usal.es/investigadores/58037/detalle		
E-mail	s.demarco@usal.es	Teléfono	

Profesor Coordinador	Cristina Almaraz López	Grupo / s	1
Departamento	Economía e Historia Económica		
Área	Historia e Instituciones Económicas		
Centro	Facultad de Economía y Empresa		
Despacho			
Horario de tutorías			
URL Web	https://produccioncientifica.usal.es/investigadores/807078/detalle		
E-mail	cristina.almaraz@usal.es	Teléfono	923294500

2.- Recomendaciones previas

No se requieren conocimientos especializados previos.

Conocimientos de inglés para la comprensión de textos académicos.

3.- Objetivos de la asignatura

Analizar el impacto de la ciberseguridad en la economía y la sociedad, especialmente en el contexto de la sociedad del riesgo y la economía del dato.

Comprender los fundamentos económicos y sociales de la ciberseguridad, así como los riesgos que plantea para las democracias y la ciudadanía.

Evaluar el papel de la ciberseguridad en la gestión y organización empresarial, como parte de la elaboración, auditoría y aplicación de políticas de seguridad en la empresa.

4.- Competencias a adquirir / Resultados de aprendizaje

Competencias	Resultados de aprendizaje
4.1: Competencias Básicas:	**4.1: Conocimientos:** C3, C4, C9, C10 **C3**. Identificar las leyes, regulaciones y estándares nacionales e internacionales relacionados con la ciberseguridad **C4**. Valorar el impacto de la ciberseguridad sobre la economía, la empresa y la ciudadanía. **C9**. Recopilar información pertinente de la legislación nacional e internacional que afecta a los sistemas de información y la ciberseguridad,

	así como en los aspectos legales y sociales relacionados. **C10**. Caracterizar normativas y regulaciones en materia de protección de datos, cumplimiento normativo y responsabilidad jurídica en casos de incidentes de seguridad.
4.2: Competencias Específicas:	**4.2: Habilidades:** H3, H9 **H3.** Analizar y evaluar los riesgos de seguridad en entornos digitales, identificando posibles debilidades y proponiendo soluciones efectivas. **H9.** Adquirir habilidades para analizar y evaluar los aspectos legales de la ciberseguridad, asesorar en la implementación de políticas y normatives y colaborar con equipos técnicos en la resolución de casos jurídicos relacionados con la ciberseguridad.
4.3: Competencias Transversales:	**4.3: Competencias:** K5, K6, K7, K8, K9 **K5**. Validar la garantía y seguridad de los sistemas informáticos pertinentes, como redes locales, servidores, bases de datos y sistemas de gestión de información. **K6**. Diseñar políticas de monitorización y copia de segura, para la recuperación de sistemas y el aseguramiento en la información en caso de malfuncionamiento. **K7**. Elaborar la política de seguridad de una empresa. **K8**. Auditar las políticas de seguridad de una empresa a todos los niveles (sistemas, red, información, etc.). **K9**. Aplicar las restricciones legales asociados a la seguridad informática sobre el manejo y procesamiento de datos personales.

5.- Contenidos (temario)

Contenido teórico:

1. Introducción a la sociedad de riesgo
2. Sociedad de la Información, economía del dato y ciberseguridad: riesgos para las democracias
3. Ciberseguridad y economía.
4. Ciberseguridad y empresa.

Contenido práctico:

1. Elección entre las lecturas propuestas por el profesor y realización de comentarios de texto.
2. Videos para profundizar conceptos/generar reflexiones.

6.- Metodologías docentes

- **Sesiones Magistrales**: Sesiones donde se presentan los fundamentos teóricos de los temas de la asignatura. Son de carácter expositivo y buscan proporcionar una visión amplia y detallada de los conceptos clave, fomentando al mismo tiempo el diálogo y la reflexión crítica entre los estudiantes.
- **Seminarios**: Sesiones en grupos más reducidos, donde los estudiantes tienen la oportunidad de discutir y profundizar en los temas tratados. Se trata de fomentar la participación, el intercambio de ideas y la construcción colaborativa del conocimiento.
- **Sesiones Prácticas**: A través de casos de estudio, los estudiantes pondrán en práctica los conceptos teóricos, desarrollando habilidades técnicas y analíticas aplicando de manera concreta los conocimientos adquiridos.
- **Actividades de seguimiento online**: Sesiones individualizadas o en pequeños grupos donde los estudiantes pueden resolver dudas específicas con el docente, recibir orientación personalizada y profundizar en temas de interés. Estas sesiones son flexibles y se pueden llevar a cabo tanto de forma presencial como virtual.
- **Preparación de trabajos autónomos**: Asignaciones que los estudiantes deben realizar de manera independiente, aplicando los conocimientos adquiridos, con el objetivo de fomentar la capacidad de análisis, síntesis y crítica, así como el desarrollo de habilidades de investigación y escritura académica. Podrán ser individuales o de grupo.

6.1.- Distribución de metodologías docentes

		Horas dirigidas por el profesor		Horas de trabajo autónomo	HORAS TOTALES
		Horas presenciales.	Horas no presenciales.		
Sesiones magistrales		8		15	23
Prácticas	- En aula			10	10
	- En el laboratorio				
	- En aula de informática				
	- De campo				
	- Otras (detallar)				
Seminarios			3		3
Exposiciones y debates					
Tutorías					
Actividades de seguimiento online			3	13	16
Preparación de trabajos			7,5	14,5	22
Otras actividades (detallar)					
Exámenes		1			1
TOTAL		**9**	**13,5**	**52,5**	75

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

- Beck, U. (1998). *La sociedad del riesgo*. Barcelona: Paidós.
- Castells, M. (1996). *The Information Age: Economy, Society and Culture*. Blackwell Publishers, Cambridge, MA; Oxford, UK. (Solo para consultar conceptos puntuales). Más en específico: Volume I. *The rise of the network society* y Volume II. *The power of Identity*
- Cobos, E. V. (2024). Cybersecurity Economics for Emerging Markets. *World Bank Publications-Books*.
- Gordon, L.A.; Loeb, M.P. (2002). The economics of information security investment. ACM Trans. Inf. Syst. Secur. (TISSEC), 5, 438–457.
- Iriarte, D (2025). *Guerras Cognitivas*. Arpa Editores.
- Moore, T. (2010). The economics of cybersecurity: Principles and policy options. International Journal of Critical Infrastructure Protection, 3(3-4), 103-117.
- Goldfarb, A., & Tucker, C. (2019). Digital economics. Journal of Economic Literature, 57(1), 3-43. https://doi.org/10.1257/jel.20171452

8.- Evaluación

8.1: Criterios de evaluación:

La nota final se compondrá de:

- 10% participación en actividad presencial
- 40% de entrega de los trabajos y/o informes sobre supuestos prácticos
- 50% de la prueba final

8.2: Sistemas de evaluación:

El examen final sobre conocimientos teóricos será tipo test.

En cuanto a los supuestos prácticos, se entregarán 2 informes realizados a partir de un trabajo grupal. Ambos tendrán el mismo peso en la nota final de la parte práctica de la asignatura.

También se evaluará la participación en los debates que se generen en clase y/o en los foros online.

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

Se recomienda participar en las actividades de seguimiento online para la preparación de los trabajos y/o informes y en el caso de no aprobar una de las dos evaluaciones (teórica y práctica) de la asignatura. De esta forma el alumno puede consultar con el profesor la mejor manera de preparar el examen de recuperación.

Taller de investigación en inteligencia artificial y ciberseguridad

1.- Datos de la Asignatura					
Código	306555	Plan	M204-1	ECTS	3
Carácter	Obligatoria	Curso	1	Periodicidad	Semestre 2
Idioma de impartición asignatura		Español			
Área	Ciencia de la Computación e Inteligencia Artificial				
Departamento	Informática y Automática				
Plataforma virtual	Studium http://studium.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

- **Conocimientos básicos de programación**: Familiaridad con un lenguaje de programación (preferentemente Python, que es ampliamente usado en IA y ciberseguridad).

- **Conceptos básicos de ciberseguridad**: 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.

- **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.

3.- Objetivos de la asignatura

- Introducir los conceptos fundamentales de la inteligencia artificial y su aplicación en el campo de la ciberseguridad.

- Explorar metodologías y enfoques de la inteligencia artificial aplicados a la detección y prevención de amenazas en ciberseguridad.

- Analizar tendencias actuales de investigación en inteligencia artificial y ciberseguridad, así como su impacto en la protección de sistemas informáticos.

- Desarrollar habilidades prácticas para utilizar herramientas de inteligencia artificial en escenarios de ciberseguridad.

4.- Competencias a adquirir / Resultados de aprendizaje

Competencias	Resultados de aprendizaje
4.1: Competencias Básicas:	**4.1: Conocimientos:** C1, C2, C8
4.2: Competencias Específicas:	**4.2: Habilidades:** H2, H56, H7, H8
4.3: Competencias Transversales:	**4.3: Competencias:** K1, K2, K3, K4, K8

5.- Contenidos (temario)

Contenido teórico:

1. Conceptos básicos de inteligencia artificial.
2. Metodologías de inteligencia artificial aplicada a la ciberseguridad.
3. Revisión de tendencias de investigación en inteligencia artificial y ciberseguridad: casos de estudio.

Contenido práctico:

Utilización de herramientas de inteligencia artificial.

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		4		15	19
Prácticas	- En aula	4		10	14
	- En el laboratorio				
	- En aula de informática				
	- De campo				
	- Otras (detallar)				
Seminarios			3.5		3.5
Exposiciones y debates					
Tutorías					
Actividades de seguimiento online					
Preparación de trabajos			10	27.5	37.5
Otras actividades (detallar)					
Exámenes		1			1
TOTAL		**9**	**13.5**	**52.5**	**75**

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

- *Artificial Intelligence: A Modern Approach* (Stuart Russell y Peter Norvig) - Texto introductorio clave sobre los fundamentos de la IA.

- *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow* (Aurélien Géron) - Guía práctica sobre el uso de IA para resolver problemas.

- Artículos sobre IA aplicada a la ciberseguridad en revistas académicas como *IEEE Transactions on Information Forensics and Security*.

- Documentación oficial sobre herramientas de IA de código abierto como *TensorFlow* y *Keras* (https://www.tensorflow.org/).

- Blogs y recursos sobre ciberseguridad y IA, como *Dark Reading* (https://www.darkreading.com/) y *Krebs on Security* (https://krebsonsecurity.com/).

- *Machine Learning for Cybersecurity* (publicaciones y libros sobre el uso de IA en seguridad informática).

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 compentencias 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.

TRABAJO DE FIN DE MÁSTER

1.- Datos de la Asignatura					
Código	306562	Plan	M204-1	ECTS	15
Carácter	Obligatoria	Curso	1	Periodicidad	Semestre 2
Idioma de impartición asignatura		Español / Inglés			
Área	Ciencia de la Computación e Inteligencia Artificial				
Departamento	Informática y Automática				
Plataforma virtual	Studium http://studium.usal.es				

1.1.- Datos del profesorado*			
Profesor Coordinador	Cada TFM tendrá un tutor (o dos máximo) asignado entre los profesores del Máster	Grupo / s	-
Departamento	Informática y Automática Administración y Economía de la Empresa Economía e Historia Económica Derecho Administrativo, Financiero y Procesal Economía Aplicada Sociología y Comunicación		
Área	Ciencia de la Computación e Inteligencia Artificial Economía Financiera y Contabilidad Economía e Historia Económica Derecho Administrativo Derecho Procesal Economía Aplicada Sociología		
Centro	Facultad de Ciencias		
Despacho	-		
Horario de tutorías	Dependerá de cada profesor		
URL Web	*https://ciberseguridad.usal.es*		
E-mail	-	Teléfono	-

2.- Recomendaciones previas

Haber superado las asignaturas del primer semestre, garantizando una base sólida en conceptos fundamentales y técnicos de la ciberseguridad.

3.- Objetivos de la asignatura

Diseñar una solución completa en uno de los ejes temáticos ofertados por el profesorado o propuesta del alumno aprobada por el profesorado, teniendo en cuenta los conocimientos adquiridos sobre ciberseguridad en el resto de asignaturas de la oferta académica del máster.

4.- Competencias a adquirir / Resultados de aprendizaje	
Competencias	**Resultados de aprendizaje**
4.1: Competencias Básicas:	**4.1: Conocimientos:** C1. Relacionar los fundamentos teóricos de la ciberseguridad, incluyendo conceptos básicos de la información, criptografía, redes y sistemas operativos para proteger la integridad y la confidencialidad de la información. C2. Identificar las amenazas y vulnerabilidades más comunes en entornos digitales, así como las técnicas y metodologías utilizadas para prevenir, detectar y responder a incidentes de seguridad. C3. Identificar las leyes, regulaciones y estándares nacionales e internacionales relacionados con la ciberseguridad C4. Valorar el impacto de la ciberseguridad sobre la economía, la empresa y la ciudadanía. C5. Examinar aspectos interdisciplinarios de la ciberseguridad, como la gestión de riesgos, la ética y la privacidad, con el fin de proporcionar una visión integral de la disciplina. C6. Identificar protocolos de seguridad contra amenazas informáticas a partir de conocimientos especializados en ciberseguridad, centrándose en su desarrollo, implementación y evaluación. C7. Describir los aspectos técnicos e informáticos de la seguridad, incluyendo el diseño seguro de sistemas, la seguridad en redes y comunicaciones, la protección de datos y la gestión de incidentes de seguridad. C8. Distinguir las últimas tendencias y tecnologías en el campo de la ciberseguridad, como el Internet de las cosas (IoT), la inteligencia artificial (IA) y el aprendizaje automático (Machine Learning), para estar preparados ante los desafíos futuros C9. Recopilar información pertinente de la legislación nacional e internacional que afecta a los sistemas de información y la ciberseguridad, así como en los aspectos legales y sociales relacionados. C10. Caracterizar normativas y regulaciones en materia de protección de datos, cumplimiento normativo y responsabilidad jurídica en casos de incidentes de seguridad.
4.2: Competencias Específicas:	**4.2: Habilidades:** H1. Implementar medidas de seguridad en diferentes entornos y sistemas, incluyendo la configuración de firewalls, la gestión de accesos, la detección de intrusiones y el análisis forense digital. H2. Adquirir destrezas en el uso de herramientas y software especializados para evaluar la seguridad

	de sistemas y redes, así como para llevar a cabo pruebas de penetración y auditorías de seguridad. H3. Analizar y evaluar los riesgos de seguridad en entornos digitales, identificando posibles debilidades y proponiendo soluciones efectivas. H4. Trabajar en equipo para colaborar con otros profesionales de la ciberseguridad, así como para educar a usuarios finales y promover buenas prácticas de seguridad. H5. Trabajar en equipo en entornos multidisciplinares, para el análisis y resolución de problemas concretos de inseguridad en equipos y sistemas informáticos. H6. Desarrollar habilidades técnicas para implementar soluciones de seguridad en sistemas y redes, realizar pruebas de penetración y responder a incidentes de seguridad de manera eficiente. H7. Adquirir destrezas en el uso de herramientas y software especializados para evaluar la seguridad de sistemas informáticos y redes. H8. Desarrollar habilidades de análisis y resolución de problemas en el ámbito de la seguridad informática, así como habilidades de comunicación y trabajo en equipo. H9. Adquirir habilidades para analizar y evaluar los aspectos legales de la ciberseguridad, asesorar en la implementación de políticas y normatives y colaborar con equipos técnicos en la resolución de casos jurídicos relacionados con la ciberseguridad. H10. Desarrollar habilidades de investigación y análisis en materia de delitos informáticos para comprender los motivos e impacto en el entorno digital. H11. Mejorar en habilidades de comunicación y argumentación legal, y desarrollar habilidades éticas y profesionales para enfrentar los desafíos éticos y legales en el ámbito de la ciberseguridad.
4.3: Competencias Transversales:	**4.3: Competencias:** K1. Diseñar, desarrollar, evaluar y asegurar la seguridad de un sistema informático, con independencia de su tamaño y características. K2. Desarrollar, implantar y mantener sistemas, servicios y aplicaciones informáticas de seguridad empleando los métodos de la ingeniería del software como instrumento para el aseguramiento de su calidad. K3. Analizar, diseñar, construir y mantener aplicaciones de seguridad de forma robusta, segura y eficiente, eligiendo el paradigma y los lenguajes de programación más adecuados en cada caso, según el entorno de despliegue (entorno web, escritorio).

	K4. Diseñar, desplegar, administrar de forma segura y fiable servicios en una red de ordenadores. K5. Validar la garantía y seguridad de los sistemas informáticos pertinentes, como redes locales, servidores, bases de datos y sistemas de gestión de información. K6. Diseñar políticas de monitorización y copia de segura, para la recuperación de sistemas y el aseguramiento en la información en caso de malfuncionamiento. K7. Elaborar la política de seguridad de una empresa. K8. Auditar las políticas de seguridad de una empresa a todos los niveles (sistemas, red, información, etc.). K9. Aplicar las restricciones legales asociados a la seguridad informática sobre el manejo y procesamiento de datos personales.

5.- Contenidos (temario)

El contenido del Trabajo Fin de Máster se fundamenta en los conocimientos teóricos y prácticos adquiridos a lo largo de las distintas asignaturas cursadas en el programa del máster universitario en ciberseguridad. A partir de esta base formativa, el estudiante ha puede llevar a cabo, bajo la dirección del profesorado correspondiente, un proceso riguroso de investigación y trabajo autónomo con el fin de profundizar en el eje temático seleccionado, aplicando metodologías, herramientas y marcos de referencia estudiados durante el máster para abordar una problemática real o simulado del ámbito de la seguridad informática. Este trabajo se desarrollará integrando conocimientos multidisciplinares y enfoques técnicos avanzados, lo que permite no solo demostrar la competencia profesional del alumno, sino también su capacidad para generar soluciones innovadoras y fundamentadas dentro del ámbito específico de estudio.

6.- Metodologías docentes

La realización del Trabajo Fin de Máster se basa en una metodología docente activa dirigida por el profesorado, pero centrada en el aprendizaje autónomo, la investigación aplicada y el desarrollo competencial del estudiante.

Esta metodología se articula en torno al trabajo individual guiado por un tutor académico, con el objetivo de fomentar la capacidad de análisis crítico, la toma de decisiones fundamentadas y la resolución de problemas complejos en el ámbito de la ciberseguridad.

La supervisión continua, el *feedback* formativo y la elaboración progresiva del trabajo permiten integrar de forma coherente los contenidos teóricos y prácticos adquiridos durante el máster, consolidando así las competencias profesionales del estudiante en el entorno de la seguridad informática.

6.1.- Distribución de metodologías docentes

	Horas dirigidas por el profesor		**Horas de trabajo autónomo**	**HORAS TOTALES**
	Horas presenciales.	**Horas no presenciales.**		

Sesiones magistrales					
Prácticas	- En aula				
	- En el laboratorio				
	- En aula de informática				
	- De campo				
	- Otras (detallar)				
Seminarios					
Exposiciones y debates					
Tutorías			10		
Actividades de seguimiento online			10		
Preparación de trabajos			88,5	262,5	351
Otras actividades (detallar): Sesión de presentaciones ante el tribunal		4			
Exámenes					
TOTAL		4	108,5	262,5	375

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

Bibliografía, recursos y materiales proporcionados en el resto de las asignaturas del máster.

8.- Evaluación

8.1: Criterios de evaluación:

La evaluación del Trabajo Fin de Máster se llevará a cabo conforme a criterios técnicos, académicos y competenciales, que permitan valorar de forma integral tanto el producto final como el proceso de elaboración y su defensa pública. Los principales criterios son los siguientes:

- Rigor técnico y calidad del trabajo desarrollado: se valorará la solidez de la solución propuesta, el uso adecuado de herramientas y tecnologías de ciberseguridad, así como la correcta aplicación de metodologías técnicas.
- Documentación técnica entregada: se tendrá en cuenta la claridad, organización, precisión y exhaustividad de la memoria, incluyendo el diseño de la arquitectura, resultados obtenidos, análisis de viabilidad, pruebas realizadas y conclusiones.
- Dominio del eje temático: se evaluará la comprensión profunda del problema tratado, así como la capacidad de contextualizarlo dentro del ámbito actual de la ciberseguridad.
- Originalidad e innovación: se valorará la capacidad del alumno para proponer soluciones novedosas o enfoques no triviales, así como la iniciativa en el planteamiento y resolución del problema.
- Calidad de la defensa oral: se evaluará la capacidad de comunicación técnica del estudiante, la estructuración de la presentación, el uso de recursos visuales, y la solvencia en la respuesta a las preguntas del tribunal.

8.2: Sistemas de evaluación:

La evaluación del Trabajo Fin de Máster se realizará mediante un sistema estructurado que permite valorar la adquisición de las competencias asociadas a la asignatura, mediante la consideración de distintos aspectos técnicos, documentales y expositivos del trabajo realizado. La calificación final se obtendrá aplicando las siguientes ponderaciones, conforme a los criterios definidos por la normativa académica del máster:

- Dificultad técnica y complejidad del trabajo (40% – 65%): se valorará el grado de dificultad asumido, el uso adecuado y avanzado de herramientas de ciberseguridad, la profundidad técnica de la solución propuesta y el nivel de autonomía del estudiante.
- Calidad de la documentación técnica entregada (15% – 30%): se tendrá en cuenta la estructura lógica de la memoria, la claridad expositiva, el nivel de detalle técnico, la calidad de las evidencias aportadas y la correcta justificación metodológica.

- Presentación y exposición oral de la memoria (10% – 20%): se evaluará la capacidad del estudiante para comunicar de forma eficaz y técnica los contenidos principales del trabajo, mediante una exposición estructurada, clara y apoyada en recursos visuales adecuados.
- Defensa del trabajo ante el tribunal (10% – 20%): se valorará la solidez de las respuestas ante las preguntas formuladas por el tribunal, la defensa argumentada de las decisiones adoptadas y la capacidad crítica del estudiante en relación con su propio trabajo.

Para garantizar la transparencia y objetividad del proceso de evaluación, se publicará una rúbrica detallada que recogerá los porcentajes exactos, comunes a todos los tribunales del curso académico. Esta rúbrica estará disponible con antelación suficiente antes de la entrega de la documentación y de la defensa pública, y será el instrumento de referencia que utilizarán los miembros del tribunal evaluador.

El tribunal estará compuesto por tres docentes del máster: un presidente, un vocal y un secretario, quienes evaluarán de manera colegiada el trabajo desarrollado, siguiendo los parámetros establecidos en la rúbrica y conforme a los estándares académicos del programa.

8.3: Consideraciones generales y recomendaciones para la evaluación y la recuperación:
El proceso de evaluación del Trabajo Fin de Máster debe entenderse como una culminación del aprendizaje adquirido a lo largo del programa, por lo que se recomienda al estudiante abordar su desarrollo con planificación, rigor técnico y responsabilidad académica. A tal efecto, es imprescindible que se respeten los plazos de entrega establecidos por la coordinación del máster, así como los requisitos formales exigidos para la documentación escrita (estructura, formato, extensión, normas de citación y anexos técnicos).

Se recomienda mantener un contacto regular con el tutor académico, con el fin de garantizar un seguimiento adecuado del trabajo, resolver dudas metodológicas y alinear los avances con los objetivos formativos de la asignatura.

En caso de no superar la evaluación en la convocatoria ordinaria, se habilitará una convocatoria de recuperación en los términos establecidos por la normativa del máster. Esta recuperación podrá implicar la mejora del contenido técnico de la memoria, la revisión o ampliación de la documentación entregada o incluso un nuevo enfoque, en función de los motivos específicos de la calificación no superada. Se recomienda al estudiante atender cuidadosamente a las observaciones del tribunal y del tutor para orientar adecuadamente el proceso de mejora.