



1. Identificación

1.1. De la asignatura

Curso Académico	2024/2025
Titulación	MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD / MASTER IN CYBERSECURITY
Nombre de la asignatura	TFM MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD / MASTER IN CYBERSECURITY
Código	7844
Curso	SEGUNDO
Carácter	TRABAJO FIN DE MÁSTER
Número de grupos	1
Créditos ECTS	24.0
Estimación del volumen de trabajo	600.0
Organización temporal	1º Cuatrimestre
Idiomas en que se imparte	Inglés, Español

1.2. Del profesorado: Equipo docente

LOPEZ MILLAN, GABRIEL

Coordinación de los grupos:

Coordinador de la asignatura

Categoría

PROFESORES TITULARES DE UNIVERSIDAD

Área

INGENIERÍA TELEMÁTICA

Departamento

INGENIERÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES

Correo electrónico / Página web / Tutoría electrónica

gabilm@um.es <https://umurcia.zoom.us/j/7426898280?pwd=Vmt1NkVkbVVwZE1vUTBSbnMvV2Z2dz09> Tutoría electrónica : Sí

Teléfono, horario y lugar de atención al alumnado

Duración:	Día:	Horario:	Lugar:
C1	Martes	12:00-13:30	868888504, Facultad de Informática B1.1.014

Observaciones:
No consta

Duración:	Día:	Horario:	Lugar:
C1	Viernes	09:00-10:30	868888504, Facultad de Informática B1.1.014

Observaciones:
Las tutorías de los viernes serán principalmente online, salvo que el profesor diga lo contrario. El enlace para tutorías es el siguiente: <https://umurcia.zoom.us/j/7426898280?pwd=Vmt1NkVkbVVwZE1vUTBSbnMvV2Z2dz09>

Duración:	Día:	Horario:	Lugar:
C2	Miércoles	15:30-17:00	868888504, Facultad de Informática B1.1.014

Observaciones:
No consta

Duración:	Día:	Horario:	Lugar:
C2	Viernes	09:00-10:30	868888504, Facultad de Informática B1.1.014 (DESPACHO PROF. GABRIEL LÓPEZ MILLÁN)

Observaciones:
Para tutorías electrónicas: <https://umurcia.zoom.us/j/7426898280?pwd=Vmt1NkVkbVVwZE1vUTBSbnMvV2Z2dz09>

2. Presentación

El Trabajo Fin de Máster (TFM) es una asignatura obligatoria que el alumno debe cursar para la obtención del título de Máster. Es un trabajo personal y autónomo del estudiante cuya realización tiene por objeto dar cuenta de forma integrada de los contenidos y competencias que se han adquirido con el resto de asignaturas y/o materias que conforman el plan de estudios. Siempre se desarrollará bajo la supervisión de un tutor o tutora que orientará al estudiante en su elaboración, y debe presentarse y defenderse de forma individual y pública.

3. Condiciones de acceso a la asignatura

3.1. Incompatibilidades

No constan

3.2. Requisitos

No constan

3.3. Recomendaciones

No constan

4. Competencias

4.1. Competencias básicas

- CB6: Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación
- CB8: Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios
- CB9: Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades
- CB10: Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

4.2. Competencias de la titulación

- CG4: Que los estudiantes sean capaces de elaborar documentación clara, concisa y razonada sobre aspectos relacionados con el ámbito de la ciberseguridad.
- CG5: Que los estudiantes conozcan los conceptos y tecnologías utilizadas en la implantación de la Ciberseguridad en una organización, considerando la definición de estrategias, políticas y normas para la seguridad corporativa.
- CE3: Ser capaz de diseñar, monitorizar y evaluar arquitecturas y servicios de seguridad de sistemas, infraestructuras críticas y redes de comunicaciones.
- CE5: Identificar y conocer las nuevas tendencias, buenas prácticas, normas, regulación y aspectos humanos relacionados con la ciberseguridad.

4.3. Competencias transversales y de materia

No constan

5. Líneas de investigación o temas de trabajo

[Oferta de líneas de investigación](#)

6. Actividades Formativas

Actividad Formativa	Metodología	Horas	Presencialidad
A10: Pruebas de evaluación: Incluye cualquier tipo de evaluación que sea necesaria en la asignatura, como pruebas parciales o finales, ya sean de teoría o prácticas.	MD1: Lección Magistral: Exposición oral de un tema estructurado para facilitar los contenidos sobre la materia objeto de estudio de forma organizada. Se realizan a través de sesiones síncronas de teoría online o sesiones síncronas de laboratorio online.	2.0	0.0
AF6: Tutorías: Tutorías individuales o grupales donde el profesorado resuelve dudas particulares, orienta, apoya y ayuda a los estudiantes en el desarrollo de su trabajo y en la adquisición de competencias.	MD2: Estudio de Casos: Análisis de un problema o suceso real para conocerlo, interpretarlo, resolverlo, generar hipótesis, contrastar datos, reflexionar, completar conocimientos, diagnosticarlo y buscar las soluciones.	18.0	0.0
AF9: Trabajo autónomo: Dedicación del estudiante a revisar y estudiar los contenidos teórico/prácticos de la asignatura, búsqueda de información bibliográfica, realización de lecturas, etc.	MD5: Aprendizaje Orientado a Proyectos (AOP): Los estudiantes llevan a cabo la realización de un proyecto en un tiempo determinado abordando una tarea mediante la planificación, diseño y realización de una serie de actividades. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, casos prácticos, tutorías grupales, etc.	580.0	0.0
Totales		600,00	

7. Horario de la asignatura

<https://www.um.es/en/web/estudios/masteres/ciberseguridad/2024-25#horarios>

8. Sistemas de Evaluación

Identificador	Denominación del instrumento de evaluación	Criterios de Valoración	Ponderación
IE5	Informe TFM: Este instrumento incluye los resultados de actividades relacionadas con el desarrollo del Trabajo Fin de Máster, junto con su memoria descriptiva.		55.0
IE6	Exposición y Defensa TFM: Este instrumento se refiere a la presentación o exposición oral del Trabajo Fin de Máster realizada de forma individual ante uno o varios profesores a modo de tribunal, y posibles turnos en los que los candidatos respondan a preguntas relacionadas con el trabajo.		45.0

9. Fechas de exámenes

<https://www.um.es/en/web/estudios/masteres/ciberseguridad/2024-25#exámenes>

10. Resultados del Aprendizaje

- Diseñar escenarios, soluciones, o sistemas de ciberseguridad incluyendo aspectos originales o innovadores.
- Planifica tareas de trabajo autónomo y procesos de autoaprendizaje ejecutándose en los tiempos previstos.
- Identificar los principales aspectos a comunicar a la hora de presentar los resultados de un estudio o análisis relacionado con la ciberseguridad y al público al que va dirigido
- Diseñar una presentación que incluye las principales ideas a comunicar y los materiales audiovisuales que permitirán reforzar los mensajes a transmitir con respecto a un escenario de ciberseguridad
- Exponer sus conocimientos de una forma clara, concisa, sin ambigüedades y adaptándose al tiempo establecido para la presentación.
- Identificar, organizar y planificar las tecnologías a estudiar y/o recursos bibliográficos a analizar para abordar un determinado problema dentro del ámbito de la ciberseguridad
- Diseñar soluciones a problemas de ciberseguridad utilizando pensamiento creativo.
- Colaborar a la hora de resolver un problema del ámbito de la ciberseguridad, trabajo en equipo y liderazgo.
- Elaborar documentación clara, concisa y razonada sobre aspectos relacionados con el ámbito de la ciberseguridad.
- Identificar modelos de gestión de la ciberseguridad y procesos asociados para llevar a cabo el seguimiento y la gestión de la ciberseguridad dentro de una organización.
- Diseñar arquitecturas y servicios de seguridad de sistemas, infraestructuras críticas y redes de comunicaciones que estén de acuerdo a las políticas de la organización, consideren aspectos técnicos, de negocio (económicos, legales, medioambientales, etc) y de innovación.
- Argumentar y asesorar sobre las razones de la introducción de nuevas tecnologías, buenas prácticas, normas, regulación y aspectos en un escenario de ciberseguridad.
- Evaluar las implicaciones de la adopción de nuevas tecnologías, buenas prácticas, normas, regulación y aspectos humanos de la ciberseguridad en escenarios concretos de negocio.

11. Bibliografía

Bibliografía básica

No constan

Bibliografía complementaria

No constan

12. Observaciones

Toda la información sobre la normativa, incluyendo proceso de elaboración, evaluación y defensa TFM se encuentra publicada en: <https://www.um.es/web/estudios/masteres/ciberseguridad/tfm>

NECESIDADES EDUCATIVAS ESPECIALES

Aquellos estudiantes con discapacidad o necesidades educativas especiales podrán dirigirse al Servicio de Atención a la Diversidad y Voluntariado (ADYV - <https://www.um.es/adyv>) para recibir orientación sobre un mejor aprovechamiento de su proceso formativo y, en su caso, la adopción de medidas de equiparación y de mejora para la inclusión, en virtud de la Resolución Rectoral R-358/2016. El tratamiento de la información sobre este alumnado, en cumplimiento con la LOPD, es de estricta confidencialidad.

REGLAMENTO DE EVALUACIÓN DE ESTUDIANTES

El artículo 8.6 del Reglamento de Evaluación de Estudiantes (REVA) prevé que "salvo en el caso de actividades definidas como obligatorias en la guía docente, si el o la estudiante no puede seguir el proceso de evaluación continua por circunstancias sobrevenidas debidamente justificadas, tendrá derecho a realizar una prueba global".

Se recuerda asimismo que el artículo 22.1 del Reglamento de Evaluación de Estudiantes (REVA) estipula que "el o la estudiante que se valga de conductas fraudulentas, incluida la indebida atribución de identidad o autoría, o esté en posesión de medios o instrumentos que faciliten dichas conductas, obtendrá la calificación de cero en el procedimiento de evaluación y, en su caso, podrá ser objeto de sanción, previa apertura de expediente disciplinario".