Guía Docente: Trabajo Fin de Máster

DATOS GENERALES	
Facultad	Facultad de Ciencias y Tecnología
Titulación	Máster en Ciberseguridad
Plan de estudios	2018
Materia	Trabajo Fin de Máster
Carácter	Trabajo Fin de Máster
Período de impartición	Tercer Trimestre
Curso	Primero
Nivel/Ciclo	Máster
Créditos ECTS	6
Lengua en la que se imparte	Castellano
Prerrequisitos	La Universidad establecerá los requisitos que los estudiantes deberán reunir antes de poder matricularse en la asignatura de «Trabajo Fin de Máster», de acuerdo con la normativa universitaria correspondiente y vigente.

DATOS DEL PROFESORADO			
Profesor Responsable	Amalia Beatriz Orúe López	**Correo electrónico**	amaliabeatriz.orue@ui1.es
Área		**Facultad**	Facultad de Ciencias y Tecnología
Perfil Profesional 2.0	Google Academic		

CONTEXTUALIZACIÓN Y JUSTIFICACIÓN DE LA ASIGNATURA	
Asignaturas de la materia	• Trabajo Fin de Máster
Contexto y sentido de la asignatura en la titulación y perfil profesional	El Trabajo Fin de Máster (en adelante TFM) es una creación intelectual inédita y original, autónoma e individual, que sirve para acreditar que los alumnos del máster están en posesión de las competencias profesionales exigibles a un titulado universitario. Con su realización, el alumno deberá dejar constancia de la destreza adquirida en las competencias genéricas y específicas del Máster, así como su capacidad de transformar el saber en «saber hacer», siendo capaz de exponer un conjunto de ideas, teorías y explicaciones razonadas sobre un tema específico, fruto de sus conocimientos, indagación, investigación y experiencia obtenida en las prácticas realizadas. Por todo ello, resulta evidente que el trabajo debe estar orientado a la aplicación de las competencias profesionales asociadas a la titulación mediante su elaboración y posterior defensa pública ante un tribunal nombrado por la Universidad. De esta forma el TFM se sitúa como el escalón final en el camino hacia la obtención del título de Máster y su superación se presenta como la demostración fehaciente de la consecución de los objetivos del mismo y de la capacitación para desarrollar las funciones profesionales de su espectro laboral. La temática del TFM se adecúa a los diversos contenidos del plan de estudios, donde el alumno puede escoger entre un abanico de temáticas relacionadas con la aplicación la ciberseguridad. El peso específico de este TFM en el conjunto del programa de Máster es de 6 ECTS, lo que implica un volumen de 150 horas de trabajo personal del estudiante.

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE Y RESULTADOS DE APRENDIZAJE	
Competencias de la asignatura	• 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. • CB7: Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio. • CB9: 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. • CG1: Ser capaz de analizar, sintetizar y organizar la información dentro del área de seguridad informática y de las comunicaciones • CG3: Diseñar y elaborar concisa, clara y razonadamente planes y proyectos de trabajo en el ámbito de la ciberseguridad. • CE01: Analizar y detectar técnicas de ocultación de ataques a sistemas y redes en casos reales • CE02: Conocer las tendencias actuales en técnicas de ciberataque • CE03: Analizar sistemas para encontrar evidencias digitales de ciberataques y adoptar las medidas para mantener la cadena de custodia de dichas evidencias. • CE04: Comprender, aplicar y evaluar técnicas de hacking ético. • CE05: Conocer requisitos y procedimientos avanzados de certificación de sistemas seguros. • CE06: Comprender, aplicar y evaluar la gestión de la seguridad de sistemas altamente securizados por su naturaleza o criticidad. • CE07: Comprender, aplicar y evaluar las técnicas de seguridad en el desarrollo y uso de aplicaciones web y en los servicios basados en ellas. • CE08: Conocer, aplicar y evaluar técnicas avanzadas de autenticación biométrica de acceso a sistemas. • CE09: Analizar e identificar las vulnerabilidades de un sistema informático, y ser capaz de desarrollar métodos de protección de la información. • CE10: Conocer los conceptos básicos de los principales procesos y respuestas ante incidentes y su aplicación a casos reales. • CE11: Conocer, aplicar y evaluar métodos y técnicas para la seguridad de sistemas tecnológicos sociales (IoT) e industriales (IIoT). • CE12: Comprender y saber aplicar técnicas criptográ?cas avanzadas.
Resultados de aprendizaje de la asignatura	• Elaborar un «Trabajo Fin de Máster» que ponga de manifiesto el grado de adquisición de las competencias vinculadas con el proyecto. • Buscar de forma activa fuentes de información, actualizadas y relevantes, relacionadas con la temática del proyecto en diferentes lenguas, así como saber discriminar la pertinencia y fiabilidad de las mismas. • Desarrollar un trabajo con calidad científica. • Ser capaz de exponer de forma clara, tanto a nivel escrito como oral, las tesis expuestas en su proyecto.

PROGRAMACION DE CONTENIDOS	
Breve descripción de la asignatura	Se considera como requisito indispensable que evidencie claramente que el alumno ha adquirido el nivel y la variedad de competencias exigidos por la titulación de máster y, en concreto, por la especialización seguida. Los temas que se han de desarrollar en el Trabajo Fin de Máster serán propuestos por el profesor responsable de la asignatura al alumno, y de acuerdo con él. Hay que destacar en última instancia que la acción tutorial adquiere un enorme valor en el seguimiento del Trabajo Fin de Máster, de tal forma que a través de la relación profesor-alumno se da respuesta no solo a los requerimientos de información, sino también al asesoramiento científico, profesional y metodológico.
Temáticas	El TFM deberá enmarcarse en alguna de las temáticas relacionadas con el ámbito de la Ciberseguridad. El tema concreto a desarrollar en el TFM dependerá de los intereses del alumno. Algunos ejemplos de temáticas son los siguientes: • Ciberseguridad Social e Industrial • Técnicas Biométricas. • Redes y Sistemas Locales. • Técnicas Criptográficas. • Auditoría e Informática Forense • Sistemas Móviles y Servicios y Aplicaciones web • Hacking ético

METODOLOGÍA	
Proceso de aprendizaje	Para garantizar un adecuado desarrollo de los TFM y del proceso de aprendizaje del alumnado se han definido tres fases fundamentales, en las que se llevarán a cabo una serie de acciones educativas específicas. • **Fase previa** En esta fase se pretende que los estudiantes se familiaricen con la asignatura y su proceso de desarrollo. Así, el alumnado tendrá acceso a través del Aula Virtual a documentación imprescindible para la asignatura: guía didáctica, listado de temáticas, sistemas evaluativos y plantilla para el diseño del TFM. Se trata de que el alumno pueda previamente al desarrollo propiamente dicho del TFM: - Reflexionar sobre las temáticas propuestas para el desarrollo del TFM en función de sus intereses. - Elección de la temática de TFM y de la vía de seguimiento de la asignatura (ver sección «Sistema Evaluativo»). • **Fase de desarrollo** Esta fase implica el proceso de desarrollo del TFM propiamente dicho. Para desarrollar con eficacia dicho proceso, la Universidad asigna un tutor académico a cada estudiante. Todo el proceso de tutorización se desarrollará vía correo electrónico, empleando la dirección de correo electrónico corporativa de la Universidad.

	El tutor académico: - Acompañará al estudiante en su proceso de trabajo, orientándole, asesorándole, supervisándole y resolviendo las posibles dudas que vayan surgiendo. - Evaluará el trabajo del alumno/a, en función de la vía de evaluación seleccionada. - Emitirá el visto bueno para la defensa del TFM. Por su parte, el alumno/a realizará las siguientes acciones formativas en esta fase: - Mantendrá un contacto continuo y fluido con el tutor vía correo electrónico corporativo. - Revisará de manera continuada el Aula Virtual. - Desarrollará el TFM en base a las directrices establecidas. - Cumplirá con los plazos de entrega establecidos en la temporalización (según la opción de evaluación elegida). - Atenderá a las recomendaciones y correcciones aportadas por el tutor. En el caso de que el alumno/a elija una temática que involucre diversas áreas de conocimiento de distintas facultades (p.ej.: biotecnología) además del tutor del máster de Big Data asignado se le asignará un cotutor académico, especialista en dicho área. El cotutor académico compartirá las funciones tutor realizadas específicamente en el área de conocimiento en que es especialista. • **Fase de defensa** La defensa del TFM es la última fase en la que se organiza la asignatura y se desarrollará **tras la finalización del tercer trimestre**. **Es requisito indispensable para poder acceder a la defensa del TFM estar en posesión del visto bueno por parte del tutor, lo que no implica ni garantiza la superación de la asignatura.** El acto de defensa del TFM se desarrollará ante un tribunal por videoconferencia salvo expreso deseo del alumno de hacerlo presencial (en la sede central de la Universidad Isabel I en Burgos). En el aula virtual se deberá proporcionar toda la información necesaria para la preparación y desarrollo de la defensa del trabajo.

EVALUACIÓN	
Sistema evaluativo	**Sistema de evaluación** La asignatura se presenta bajo dos modalidades de seguimiento: **a. Vía de evaluación continua y formativa** En esta vía de seguimiento de la asignatura, el desarrollo del TFM y el proceso de tutorización implican una serie de entregas obligatorias y pautadas en la temporización

publicada en el Aula Virtual, acompañadas de una evaluación continua y formativa. La selección de esta vía de evaluación continua implica una serie de **compromisos** por parte de alumnos y tutores:

- Respetar la temporización de las entregas obligatorias establecidas. Dichas entregas deberán cumplir criterios de tiempo, forma y contenido [1].
- En cada una de las entregas obligatorias el tutor realizará una valoración, aportando correcciones y feedbacks que permitirán al alumno la mejora continua del TFM.
- Para la adecuada coordinación docente, los tutores compartirán con la comisión de TFM informes parciales de seguimiento de las entregas de cada uno de los tutorandos.
- Todas las dudas que puedan ir surgiendo se resolverán a través del correo electrónico corporativo, siendo imprescindible el contacto continuo alumno-tutor.

b. Vía de evaluación final

En esta vía de seguimiento de la asignatura existen dos **entregas obligatorias**, que garantizan así el desarrollo de un proceso de **evaluación formativa** (valoración y revisión por parte del tutor para la mejora del TFM).

Las fechas de las entregas aparecen determinadas en la temporización del Aula Virtual y deberán reunir las siguientes condiciones:

- Las entregas del TFM se realizarán completas (no se permitirán entregas parciales o incompletas).
- Se deberá cumplir con los criterios de tiempo y forma establecidos para la entrega.
- La **entrega final** para la evaluación final se realizará por la vía que se establezca y el tutor realizará una revisión completa y aportará feedback con las posibles mejoras del trabajo. Una vez recibida la corrección, el alumno tendrá el plazo establecido para realizar las mejoras propuestas por el tutor. El incumplimiento de esta entrega implica la imposibilidad de realizar la entrega definitiva.
- La **entrega definitiva** se realizará a través del Aula Virtual, cumplimentando los campos requeridos en la entrega y adjuntando el documento en **formato PDF** y otro documento adicional que incluya anexos en el caso de que existan. Tras esta entrega, el tutor valorará el trabajo realizado y se comunicará al estudiante si obtiene o no el visto bueno para la realización de la defensa.

Con independencia de la elección de esta vía de evaluación final, el contacto con el tutor será continuo y se garantizará en todo momento la resolución de cualquier duda que pueda surgir durante el proceso de elaboración del TFM.

Todos los estudiantes, independientemente de la opción seleccionada, que no superen la convocatoria ordinaria tienen derecho a una convocatoria extraordinaria.

El procedimiento de tutorización y entrega del TFM en la convocatoria extraordinaria sigue las mismas directrices y condiciones establecidas para la vía de evaluación final.

Sistema de calificación

El sistema de calificación se apoyará en dos ítems básicos, ambos deberán ser superados por el alumno con al menos una calificación de 5 sobre 10:

- Tutorización de Trabajo Fin de Máster, que supondrá un 50 % de la calificación final del alumno.
- Tribunal de defensa de Trabajo Fin de Máster, que implicará un 50 % de la evaluación final, dentro de la cual se contemplarán dos aspectos:
    - Valoración del trabajo escrito.

	◦ La defensa del TFM. Es requisito indispensable para poder acceder a la defensa del TFM **estar en posesión del visto bueno por parte del tutor**, lo que no implica ni garantiza la superación de la asignatura. El acto de defensa del TFM se desarrollará ante un tribunal por videoconferencia, salvo expreso deseo del alumno de hacerlo presencial (en la sede central de la Universidad Isabel I en Burgos). Dicho tribunal, que actúa de forma colegiada, está compuesto por un presidente y dos vocales, todos ellos profesores de la Universidad. En ningún caso el tutor del TFM puede formar parte de un tribunal que evalúe a alguno de sus alumnos dirigidos. [1] El incumplimiento, por parte del alumno, de alguno de los compromisos establecidos implicará la pérdida del derecho a la evaluación continua, pasando de manera forzosa a la vía de evaluación final.

BIBLIOGRAFÍA Y OTROS RECURSOS	
Bibliografía básica	Jhon R. Vacca (2017). Computer and Information Security Handbook. (3ª ed.). Kaufmann. Esta publicación proporciona una referencia actual y completa sobre seguridad informática, ofreciendo una amplia informacion sobre todo tipo de seguridad aplicada en sistemas, redes, auditorias, etc. Nadean H. Tanner (2019). Cybersecurity Blue Team Toolkit. Wiley. Este libro presenta de manera simple las mejores prácticas y estrategias que debe conocer todo profesional de la ciberseguridad.
Bibliografía complementaria	1.- Cunha, I. (2016). El trabajo de fin de grado y de máster: redacción, defensa y publicación. Editorial UOC. 2.- M Carmen Rodríguez Otero (2011). Guía de uso de Mendeley. https://biblioteca.ucm.es/data/cont/docs/397-2013-12-12-guiadeusodemendeley2.pdf 3.- Baelo A?lvarez, Manuel (2017). El arte de presentar trabajos académicos ante un tribunal: TFG, TFM y tesis doctoral: guía práctica para estudiantes universitarios. 4.- Oded Goldreich (2015). How to write a paper. http://www.wisdom.weizmann.ac.il/~oded/R2/re-writing.pdf 5.- McClure, S., Scambray, J. y Kurtz, G. (2012). *Hacking exposed. Network security secrets and solutions.* Nueva York: McGraw-Hill. 6.- Lal, N.A., Prasad, S., Farik, M. (2016) A review of authentication methods. *International journal of scientific & technology research, 5*, (11). 7.- Chell, D. (2015). *The mobile application hacker's handbook* (1.ª ed.). Indianapolis, Wiley. 8.- Salas, A. (2015). Los hombres que susurran a las máquinas: hackers, espías e intrusos en tu ordenador. Espasa.

	9.- Jhon R. Vacca (2013). Cyber Security and IT Infrastructure Protection 1st Edition. SYNGRESS. 10.- Stuttard, D, Pinto, M. (2011). The Web Application Hacker's Book, Finding and Exploiting Security Flaws (2nd edition). Wiley Publishing.
Otros recursos	Manual básico con las normas de referencia APA(American Psychological Association): http://www.apastyle.org Cómo buscar y utilizar información científica Guía para estudiantes universitarios / Luis Javier Martínez, 2013 http://eprints.rclis.org/20141/1/Como_buscar_usar_informacion.pdf Fuentes de información especializadas: aspectos prácticos y teóricos / Manuel Blázquez Ochando, 2015 http://mblazquez.es/wp-content/uploads/ebook-mbo-fuentes-especializadas.pdf Sitio oficial para descargar GNS3 y ver tutoriales. https://www.gns3.com/ David Santo Orcero. Pentesting con Kali: Aprende a dominar la herramienta Kali de pentesting, hacking y auditorías activas de seguridad. CreateSpace Independent Publishing Platform (15 de junio de 2017) Chris McNab. Network Security Assessment: Know Your Network. O'Reilly Media; 3 edition (25 Feb. 2016)