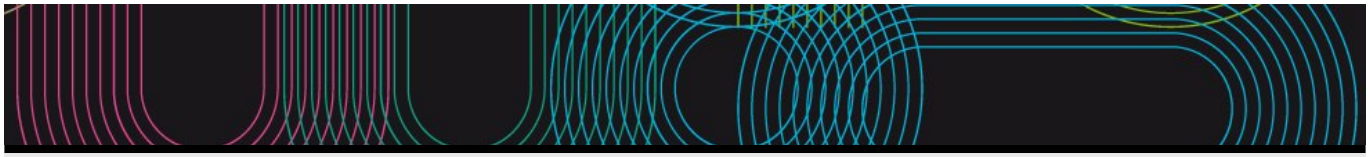

DATOS IDENTIFICATIVOS				
Trabajo Fin de Máster				
Asignatura	Trabajo Fin de Máster			
Código	V05M175V01107			
Titulacion	Máster Universitario en Ciberseguridad (en extinción)			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	15	OB	2	1c
Lengua Impartición	Castellano Gallego Inglés			
Departamento	Ingeniería telemática			
Coordinador/a	Caeiro Rodríguez, Manuel			
Profesorado	Caeiro Rodríguez, Manuel			
Correo-e	mcaeiro@det.uvigo.es			
Web	http://moovi.uvigo.es			
Descripción general	El Trabajo Fin de Máster (TFM) es un trabajo académico, personal y original que se debe presentar en público y que es evaluado por un tribunal. Se trata de un proyecto en el que el estudiante tiene que mostrar los conocimientos adquiridos durante el máster. Debe finalizar con la redacción por escrito de un conjunto de explicaciones, teorías, ideas, razonamientos, descripción de desarrollos o diseños, etc. sobre una temática elegida por el alumno, y supervisada por un tutor o tutores, que velarán por su progresión y por el nivel de calidad. No obstante, el Trabajo Fin de Máster es responsabilidad única del aspirante al título de máster.			

Resultados de Formación y Aprendizaje	
Código	
A1	Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y aplicación de ideas, a menudo en un contexto de investigación.
A2	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
A3	Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formar 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.
A4	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
A5	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
B1	Tener capacidad de análisis y síntesis. Tener capacidad para proyectar, modelar, calcular y diseñar soluciones de seguridad de la información, las redes y/o los sistemas de comunicaciones en todos los ámbitos de aplicación
B2	Resolución de problemas. Tener capacidad de resolver, con los conocimientos adquiridos, problemas específicos del ámbito técnico de la seguridad de la información, las redes y/o los sistemas de comunicaciones.
B3	Capacidad para el razonamiento crítico y la evaluación crítica de cualquier sistema de protección de la información, cualquier sistema de seguridad de la información, de la seguridad de las redes y/o los sistemas de comunicaciones
B4	Compromiso ético. Capacidad para diseñar e implantar soluciones técnicas y de gestión con criterios éticos de responsabilidad y deontología profesional en el ámbito de la seguridad de la información, las redes y/o los sistemas de comunicaciones
B5	Tener capacidad para aplicar los conocimientos teóricos en la práctica, en el marco de infraestructuras, equipamientos y aplicaciones concretos, y sujetos a requisitos de funcionamiento específicos
B6	Destreza para investigar. Capacidad para innovar y contribuir al avance de los principios, las técnicas y los procesos referidos a su ámbito profesional, diseñando nuevos algoritmos, dispositivos, técnicas o modelos útiles para la protección de los activos digitales públicos, privados o comerciales

C1	Conocer, comprender y aplicar los métodos de criptografía y criptoanálisis, los fundamentos de identidad digital y los protocolos de comunicaciones seguras
C2	Conocer en profundidad las técnicas de ciberataque y ciberdefensa
C3	Conocer la normativa técnica y legal de aplicación en materia de ciberseguridad, sus implicaciones en el diseño de sistemas, en el uso de herramientas de seguridad y en la protección de la información
C4	Comprender y aplicar los métodos y técnicas de ciberseguridad aplicables a los datos, los equipos informáticos, las redes de comunicaciones, las bases de datos, los programas y los servicios de información
C5	Diseñar, implantar y mantener un sistema de gestión de la seguridad de la información utilizando metodologías de referencia
C6	Desarrollar y aplicar métodos de investigación forense para el análisis de incidentes o riesgos de ciberseguridad
C7	Tener capacidad para realizar la auditoría de seguridad de sistemas e instalaciones, el análisis de riesgos derivados de debilidades de ciberseguridad y desarrollar el proceso de certificación de sistemas seguros
C8	Tener capacidad para concebir, diseñar, poner en práctica y mantener sistemas de ciberseguridad
C9	Tener capacidad para elaborar planes y proyectos de trabajo en el ámbito de la ciberseguridad, claros, concisos y razonados
C10	Conocer los fundamentos matemáticos de las técnicas criptográficas y comprender su evolución y tendencias futuras.
C11	Reunir e interpretar datos relevantes dentro del área de la seguridad informática y de las comunicaciones.
C12	Conocer el papel de la ciberseguridad en el diseño de las nuevas industrias, así como las particularidades, restricciones y limitaciones que se han de acometer para obtener una infraestructura industrial segura.
C13	Tener capacidad de análisis, detección y eliminación de vulnerabilidades, y del malware susceptible de utilizarlas, en sistemas y redes
C14	Tener capacidad para desarrollar un plan de continuidad de negocio siguiendo normas y estándares de referencia.
C15	Tener capacidad de identificar el valor, tanto económico como de otra índole, de la información de la institución, sus procesos críticos y el impacto que produciría la interrupción de estos; y, también, las necesidades internas y externas que permitirán estar preparados ante ataques de seguridad.
C16	Tener capacidad para vislumbrar y enfocar el esfuerzo de negocio en temáticas relacionadas con la ciberseguridad, y con una monetización viable.
C17	Tener capacidad de planificar en el tiempo los periodos de detección de incidentes o desastres, y su recuperación
C18	Interpretar de una forma adecuada las fuentes de información en el ámbito del derecho penal informático (leyes, jurisprudencia y doctrina) de ámbito nacional e internacional.
C19	Saber identificar los perfiles de personal necesarios para una institución en función de sus características y su sector
C20	Conocimiento de las empresas orientadas específicamente al sector de seguridad de nuestro entorno.
D1	Tener capacidad para comprender el significado y aplicación de la perspectiva de género en los distintos ámbitos de conocimiento y en la práctica profesional con el objetivo de alcanzar una sociedad más justa e igualitaria.
D3	Incorporar en el ejercicio profesional criterios de sostenibilidad y compromiso ambiental. Incorporar a los proyectos el uso equitativo, responsable y eficiente de los recursos
D4	Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad
D5	Tener capacidad para comunicarse oralmente y por escrito en inglés.

Resultados previstos en la materia

Resultados previstos en la materia	Resultados de Formación y Aprendizaje
Capacidad de planificación y ejecución de un trabajo original en el ámbito de la ciberseguridad.	A1 A2 A3 A4 A5
Capacidad para la busca de información en el ámbito de la ciberseguridad, de su estudio y análisis, de cara a la obtención de resultados relevantes.	B1 B3 B5 B6 D1 D3 D4 D5

Resolución de problemas originales y con implicaciones reales en el ámbito de la ciberseguridad.	A1 A2 A3 B1 B2 B3 B4 B5 B6 C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 C12 C13 C14 C15 C16 C17 C18 C19 C20 D1 D3 D4 D5
Elaboración de una memoria de proyecto que recoja la situación actual, la problemática analizada, los objetivos, el trabajo completado, las conclusiones y las líneas futuras.	A1 A3 A4 B1 B2 B6
Presentación de un resumen de los principales resultados ante un tribunal y el público.	A4 D1 D4

Contenidos

Tema	
El Trabajo Fin de Máster es un trabajo académico, personal y original en el que el estudiante tiene que mostrar los conocimientos adquiridos durante el máster. Por lo tanto, el contenido de cada trabajo debe ser único, aunque deberá mostrar la capacidad del alumno para analizar un problema de una forma sistemática, proponer soluciones, analizar los resultados obtenidos y exponerlos de forma clara.	

Planificación

	Horas en clase	Horas fuera de clase	Horas totales
Trabajo tutelado	0	350	350
Presentación	1	24	25

*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado

Metodologías

	Descripción

Trabajo tutelado	El estudiante realizará un trabajo académico, personal y original en el que deberá mostrar los conocimientos adquiridos durante el máster. Debe concluir con la redacción por escrito de un conjunto de explicaciones, teorías, ideas, razonamientos, descripción de desarrollos o diseños, etc. sobre una temática elegida por el alumno, y supervisada por un tutor o tutores, que velarán por su progresión y por el nivel de calidad.

Atención personalizada

Metodologías	Descripción
Trabajo tutelado	Durante la realización del TFM se realizarán reuniones periódicas entre el estudiante y los tutores para definir, orientar, supervisar y delimitar el trabajo, así como para orientar la escritura de la memoria del mismo. El coordinador del TFM establecerá sus horarios de tutorías al principio del cuatrimestre que podrán consultarse en la página web de la asignatura en la plataforma de teledocencia https://moovi.uvigo.gal/.
Pruebas	**Descripción**
Presentación	Los directores del trabajo orientarán al estudiante en la preparación de la presentación y defensa del trabajo fin de máster. El coordinador del TFM establecerá sus horarios de tutorías al principio del cuatrimestre que podrán consultarse en la página web de la asignatura en la plataforma de teledocencia https://moovi.uvigo.gal/.

Evaluación

	Descripción	Calificación	Resultados de Formación y Aprendizaje
Trabajo tutelado	El trabajo será evaluado por un tribunal. El alumno pondrá a su disposición a memoria del trabajo, y realizará una presentación pública. El tribunal utilizará una rúbrica que estará disponible públicamente.	100	

Otros comentarios sobre la Evaluación

Fuentes de información

Bibliografía Básica

Bibliografía Complementaria

Manuel Ruiz-de-Luzuriaga-Peña, **Guía para citar y referenciar. Estilo IEEE**, Universidad Pública de Navarra, 2016

Recomendaciones