Guia docente					
Datos Identificativos					2023/24
Asignatura (*)	Trabajo Fin de Máster			Código	614530017
Titulación	Máster Universitario en Ciberseguridade				
Descriptores					
Ciclo	Periodo	Curso		Tipo	Créditos
Máster Oficial	2º cuatrimestre	Segundo		Obligatoria	15
Idioma	CastellanoGallego				
Modalidad docente	Híbrida				
Prerrequisitos					
Departamento	Ciencias da Computación e Tecnoloxías da InformaciónEnxeñaría de Computadores				
Coordinador/a			Correo electrónico		
Profesorado			Correo electrónico		
Web	moovi.uvigo.gal				
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.				

Competencias / Resultados del título	
Código	Competencias / Resultados del título
A1	CE1 - Conocer, comprender y aplicar los métodos de criptografía y criptoanálisis, los fundamentos de identidad digital y los protocolos de comunicaciones seguras
A2	CE2 - Conocer en profundidad las técnicas de ciberataque y ciberdefensa
A3	CE3 - 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
A4	CE4 - 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
A5	CE5 - 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
A6	CE6 - Desarrollar y aplicar métodos de investigación forense para el análisis de incidentes o riesgos de ciberseguridad
A7	CE7 - 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
A8	CE8 - Tener capacidad para concebir, diseñar, poner en práctica y mantener sistemas de ciberseguridad
A9	CE9 - Tener capacidad para elaborar de planes y proyectos de trabajo en el ámbito de la ciberseguridad, claros, concisos y razonados
A10	CE10 - Conocer los fundamentos matemáticos de las técnicas criptográficas y comprender su evolución y tendencias futuras
A11	CE11 - Reunir e interpretar datos relevantes dentro del área de la seguridad informática y de las comunicaciones
A12	CE12 - 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
A13	CE13 - Tener capacidad de análisis, detección y eliminación de vulnerabilidades, y del malware susceptible de utilizarlas, en sistemas y redes
A14	CE14 - Tener capacidad para desarrollar un plan de continuidad de negocio siguiendo normas y estándares de referencia
A15	CE15 - 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

A16	CE16 - Tener capacidad para vislumbrar y enfocar el esfuerzo de negocio en temáticas relacionadas con la ciberseguridad, y con una monetización viable
A17	CE17 - Tener capacidad de planificar en el tiempo los periodos de detección de incidentes o desastres, y su recuperación
A18	CE18 - Interpretar de una forma adecuada las fuentes de información en el ámbito del derecho penal informático (leyes, jurispr
A19	CE19 - Saber identificar los perfiles de personal necesarios para una institución en función de sus características y su sector
A20	CE20 - Conocimiento de las empresas orientadas específicamente al sector de seguridad de nuestro entorno
B2	CB2 - 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
B3	CB3 - 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
B4	CB4 - 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
B5	CB5 - 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
B6	CG1 - 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
B7	CG2 - 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
B8	CG3 - 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 14 de comunicaciones
B9	CG4 - 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
B10	CG5 - 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
B11	CG6 - 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
B12	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
C1	CT1 - 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
C2	CT2 - Tener capacidad para comunicarse oralmente y por escrito en lengua gallega
C3	CT3 - Incorporar en el ejercicio profesional criterios de sostenibilidad y compromiso ambiental. Incorporar a los proyectos el uso equitativo, responsable y eficiente de los recursos
C4	CT4 - Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad
C5	CT5 - Tener capacidad para comunicarse oralmente y por escrito en inglés

Resultados de aprendizaje			
Resultados de aprendizaje	Competencias / Resultados del título		
Capacidad de planificación y ejecución de un trabajo original en el ámbito de la ciberseguridad.		BP2 BP3 BP4 BP5 BP12	
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.		BP6 BP8 BP10 BP11	CP1 CP3 CP4 CP5

Resolución de problemas originales y con implicaciones reales en el ámbito de la ciberseguridad.	AP1 AP2 AP3 AP4 AP5 AP6 AP7 AP8 AP9 AP10 AP11 AP12 AP13 AP14 AP15 AP16 AP17 AP18 AP19 AP20	BP2 BP3 BP6 BP7 BP8 BP9 BP10 BP11 BP12	
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.		BP3 BP4 BP6 BP7 BP11 BP12	CP2
Presentación de un resumen de los principales resultados ante un tribunal y el público.		BP4	CP1 CP4

Contenidos	
Tema	**Subtema**
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.	Polo tanto, o contido de cada traballo debe ser único, aínda que deberá mostrar a capacidade do alumno para analizar un problema dunha forma metódica, propoñer solucións, analizar os resultados obtidos e expoñelos de forma clara.

Planificación				
Metodologías / pruebas	**Competencias / Resultados**	**Horas lectivas (presenciales y virtuales)**	**Horas trabajo autónomo**	**Horas totales**
Presentación oral	B4 C5	1	24	25

Trabajos tutelados	A20 A19 A18 A17 A16 A15 A14 A13 A12 A11 A10 A9 A8 A7 A6 A5 A4 A3 A2 A1 B12 B2 B3 B4 B5 B6 B7 B8 B9 B10 B11 C1 C2 C3 C4 C5	0	350	350
Atención personalizada		0		0
(*)Los datos que aparecen en la tabla de planificación són de carácter orientativo, considerando la heterogeneidad de los alumnos				

Metodologías	
Metodologías	**Descripción**
Presentación oral	Defensa del trabajo realizado
Trabajos tutelados	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**
Trabajos tutelados Presentación oral	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. Los directores del trabajo orientarán al estudiante en la preparación de la presentación y defensa del trabajo fin de máster.

Evaluación			
Metodologías	**Competencias / Resultados**	**Descripción**	**Calificación**
Trabajos tutelados	A20 A19 A18 A17 A16 A15 A14 A13 A12 A11 A10 A9 A8 A7 A6 A5 A4 A3 A2 A1 B12 B2 B3 B4 B5 B6 B7 B8 B9 B10 B11 C1 C2 C3 C4 C5	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.	85
Presentación oral	B4 C5	Valoración especificada en la rúbrica	15

Observaciones evaluación

Fuentes de información	
Básica	
Complementária	Manuel Ruiz-de-Luzuriaga-Peña, Guía para citar y referenciar. Estilo IEEE, Universidad Pública de Navarra, 2016, http://www2.unavarra.es/gesadj/servicioBiblioteca/tutoriales/Citar_referenciar_(IEEE).pdf

Recomendaciones
Asignaturas que se recomienda haber cursado previamente

Asignaturas que se recomienda cursar simultáneamente
Asignaturas que continúan el temario
Otros comentarios

(*) La Guía Docente es el documento donde se visualiza la propuesta académica de la UDC. Este documento es público y no se puede modificar, salvo cosas excepcionales bajo la revisión del órgano competente de acuerdo a la normativa vigente que establece el proceso de elaboración de guías