Guia docente				
Datos Identificativos				2021/22
Asignatura (*)	Prácticas en Empresa		Código	614530016
Titulación	Máster Universitario en Ciberseguridade			
Descriptores				
Ciclo	Periodo	Curso	Tipo	Créditos
Máster Oficial	1º cuatrimestre	Segundo	Obligatoria	15
Idioma	CastellanoGallego			
Modalidad docente	Presencial			
Prerrequisitos				
Departamento	Ciencias da Computación e Tecnoloxías da InformaciónEnxeñaría de Computadores			
Coordinador/a	Dafonte Vazquez, Jose Carlos		Correo electrónico	carlos.dafonte@udc.es
Profesorado	Carballal Mato, Adrián Dafonte Vazquez, Jose Carlos Fernández Caramés, Tiago Manuel Fernández Iglesias, Diego López Rivas, Antonio Daniel Nóvoa Manuel, Francisco Javier		Correo electrónico	adrian.carballal@udc.es carlos.dafonte@udc.es tiago.fernandez@udc.es diego.fernandez@udc.es daniel.lopez@udc.es francisco.javier.novoa@udc.es
Web	faitic.uvigo.es			
Descripción general	La misión del máster es formar profesionales de alta cualificación en todos los procesos técnicos, organizativos, operativos y forenses relativos a la seguridad digital. El profesorado pertenece a las áreas de Ingeniería Telemática, Teoría de la Señal y Comunicaciones, Ciencias de la Computación e Inteligencia Artificial, Ingeniería de Sistemas y Derecho Penal de las dos universidades, y se complementa con la contribución de destacados profesionales de empresas del sector en Galicia y el compromiso de éstas en apoyar las prácticas de los estudiantes.			
Plan de contingencia	1. Modificaciones en los contenidos 2. Metodologías *Metodologías docentes que se mantienen *Metodologías docentes que se modifican 3. Mecanismos de atención personalizada al alumnado 4. Modificacines en la evaluación *Observaciones de evaluación: 5. Modificaciones de la bibliografía o webgrafía			

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
B1	CB1 - 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
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
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		
Experiencia no desempeño da profesión e das súas funcións máis habituais nunha contorna real de empresa	AP1	BP1	CP1
	AP2	BP2	CP2
	AP3	BP3	CP3
	AP4	BP4	CP4
	AP5	BP5	CP5
	AP6	BP6	
	AP7	BP7	
	AP8	BP8	
	AP9	BP9	
	AP10	BP10	
	AP11	BP11	
	AP12		
	AP13		
	AP14		
	AP15		
	AP16		
	AP17		
	AP18		
	AP19		
	AP20		

Contenidos	
Tema	Subtema
El alumno realizará una estancia en la empresa desarrollando funciones propias de un Master en Ciberseguridad	

Planificación				
Metodologías / pruebas	Competencias / Resultados	Horas lectivas (presenciales y virtuales)	Horas trabajo autónomo	Horas totales
Prácticas clínicas	A1 A2 A3 A4 A5 A6 A7 A8 A9 A10 A11 A12 A13 A14 A15 A16 A17 A18 A19 A20 B1 B2 B3 B4 B5 B6 B7 B8 B9 B10 B11 C1 C2 C3 C4 C5	375	0	375
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
Prácticas clínicas	Prácticas externas: Estancia en empresas desarrollando funciones propias de un Master en Ciberseguridad

Atención personalizada	
Metodologías	**Descripción**
Prácticas clínicas	Los alumnos tendrán un tutor en la empresa y un tutor en la Universidad, a quienes los alumnos podrán consultar dudas sobre la actividad a desarrollar y a quienes tendrán que presentar los resultados del trabajo realizado.

Evaluación			
Metodologías	**Competencias / Resultados**	**Descripción**	**Calificación**
Prácticas clínicas	A1 A2 A3 A4 A5 A6 A7 A8 A9 A10 A11 A12 A13 A14 A15 A16 A17 A18 A19 A20 B1 B2 B3 B4 B5 B6 B7 B8 B9 B10 B11 C1 C2 C3 C4 C5	La evaluación la realizará el tutor en la Universidad en función de la memoria del trabajo realizado en la empresa y de la evaluación del alumno por parte del tutor en la empresa.	0

Observaciones evaluación

Fuentes de información	
Básica	
Complementária	

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