



Guía Docente				
Datos Identificativos				2021/22
Asignatura (*)	Prácticas en Empresa	Código	614530016	
Titulación	Máster Universitario en Ciberseguridade			
Descritores				
Ciclo	Período	Curso	Tipo	Créditos
Mestrado Oficial	1º cuatrimestre	Segundo	Obrigatoria	15
Idioma	CastelánGalego			
Modalidade docente	Presencial			
Prerrequisitos				
Departamento	Ciencias da Computación e Tecnoloxías da InformaciónEnxeñaría de Computadores			
Coordinación	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			
Descrición xeral	A misión do máster é formar profesionais de alta cualificación en todos os procesos técnicos, organizativos, operativos e forenses relativos á seguridade dixital. O profesorado pertence ás áreas de Enxeñaría Telemática, Teoría da Sinal e Comunicacóns, Ciencias da Computación e Intelixencia Artificial, Enxeñaría de Sistemas e Dereito Penal das dúas universidades e complementase coa distribución de destacados profesionais de empresas do sector en Galicia e o compromiso destas en apoiar as prácticas dos estudantes.			
Plan de continxencia	<ol style="list-style-type: none"> <li>Modificacións nos contidos</li> <li>Metodoloxías <ul style="list-style-type: none"> <li>*Metodoloxías docentes que se manteñen</li> <li>*Metodoloxías docentes que se modifican</li> </ul> </li> <li>Mecanismos de atención personalizada ao alumnado</li> <li>Modificacións na avaliación <ul style="list-style-type: none"> <li>*Observacións de avaliación:</li> </ul> </li> <li>Modificacións da bibliografía ou webgrafía</li> </ol>			

Competencias / Resultados do título	
Código	Competencias / Resultados do título
A1	CE1 - Coñecer, comprender e aplicar os métodos de criptografía e criptoanálisis, os fundamentos de identidade dixital e os protocolos de comunicacións seguras
A2	CE2 - Coñecer en profundidade as técnicas de ciberataque e ciberdefensa
A3	CE3 - Coñecer a normativa técnica e legal de aplicación en materia de ciberseguridade, as súas implicacións no deseño de sistemas, no uso de ferramentas de seguridade e na protección da información
A4	CE4 - Comprender e aplicar os métodos e técnicas de ciberseguridade aplicables ós datos, os equipos informáticos, as redes de comunicacións, as bases de datos, os programas e os servizos de información
A5	CE5 - Diseñar, implantar e manter un sistema de xestión da seguridade da información utilizando metodoloxías de referencia



A6	CE6 - Desenvolver e aplicar métodos de investigación forense para o análisis de incidentes ou riscos de ciberseguridade
A7	CE7 - Ter capacidade para realizar a auditoría de seguridade de sistemas e instalacións, o análisis de riscos derivados de debilidades de ciberseguridade e desenvolver o proceso de certificación de sistemas seguros
A8	CE8 - Ter capacidade para concibir, deseñar, poñer en práctica e manter sistemas de ciberseguridade
A9	CE9 - Ter capacidade para elaborar plans e proxectos de traballo no ámbito da ciberseguridade, claros, concisos e razoados
A10	CE10 - Coñecer os fundamentos matemáticos das técnicas criptográficas e comprender a súa evolución e tendencias futuras
A11	CE11 - Reunir e interpretar datos relevantes dentro do área da seguridade informática e das comunicacións
A12	CE12 - Coñecer o papel da ciberseguridade no deseño das novas industrias, así como as particularidades, restricións e limitacións que teñen que acometerse para obter unha infraestrutura industrial segura
A13	CE13 - Ter capacidade de análisis, detección e eliminación de vulnerabilidades, e do malware susceptible de utilizalas, en sistemas e redes
A14	CE14 - Ter capacidade para desenvolver un plan de continuidade de negocio seguindo normas e estándares de referencia
A15	CE15 - Ter capacidade de identificar o valor, tanto económico como doutra índole, da información da institución, os seus procesos críticos e o impacto que produciría a interrupción destes; e, tamén, as necesidades internas e externas que permitirán estar preparados ante ataques de seguridade
A16	CE16 - Ter capacidade para albisca e enfocar o esforzo de negocio en temáticas relacionadas coa ciberseguridade, e cunha monetización viable
A17	CE17 - Ter capacidade de planificar no tempo os períodos de detección de incidentes ou desastres, e a súa recuperación
A18	CE18 - Interpretar dunha forma axeitada as fontes de información no ámbito do dereito penal informático (leis, xurisprudencia e doutrina) de ámbito nacional e internacional
A19	CE19 - Saber identificar os perfís de persoal necesarios para unha institución en función das súas características e o seu sector
A20	CE20 - Coñecemento das empresas orientadas especificamente ao sector de seguridade da nosa contorna
B1	CB1 - Posuír e comprender coñecementos que aporten unha base ou oportunidade de ser orixinais no desenvolvemento e aplicación de ideas, a miúdo nun contexto de investigación
B2	CB2 - Que os estudantes saiban aplicar os coñecementos adquiridos e a súa capacidade de resolución de problemas en contornas novas ou pouco coñecidas dentro de contextos máis amplos (ou multidisciplinares) relacionados coa súa área de estudo
B3	CB3 - Que os estudantes sexan capaces de integrar coñecementos e enfrontarse á complexidade de formar xuízos a partir dunha información que, sendo incompleta ou limitada, inclúa reflexións sobre as responsabilidades sociais e éticas vinculadas á aplicación dos seus coñecementos e xuízos
B4	CB4 - Que os estudantes saiban comunicar as súas conclusións ---e os coñecementos e razóns últimas que as sustentan--- a públicos especializados e non especializados de un modo claro e sen ambigüidades
B5	CB5 - Que os estudantes posúan as habilidades de aprendizaxe que lles permitan continuar estudando dun modo que habrá de ser en gran medida autodirixido ou autónomo
B6	CG1 - Ter capacidade de análisis e síntesis. Ter capacidade para proxectar, modelar, calcular e deseñar solucións de seguridade da información, as redes e/ou os sistemas de comunicacións en todos os ámbitos de aplicación
B7	CG2 - Resolución de problemas. Ter capacidade de resolver, cos coñecementos adquiridos, problemas específicos do ámbito técnico da seguridade da información, as redes e/ou os sistemas de comunicacións
B8	CG3 - Capacidade para o razonamiento crítico e a avaliación crítica de calquera sistema de protección da información, calquera sistema de seguridade da información, da seguridade das redes e/ou os sistemas de comunicacións
B9	CG4 - Compromiso ético. Capacidad para diseñar e implantar solucións 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 - Ter capacidade para aplicar os coñecementos teóricos na práctica, no marco de infraestructuras, equipamentos e aplicacións concretos, e suxeitos a requisitos de funcionamento específicos
B11	CG6 - Destreza para investigar. Capacidade para innovar e contribuir ao avance dos principios, as técnicas e os procesos referidos o seu ámbito profesional, deseñando novos algoritmos, dispositivos, técnicas ou modelos útiles para a protección dos activos dixitais públicos, privados ou comerciais
C1	CT1 - Ter capacidade para comprender o significado e aplicación da perspectiva de xénero nos distintos ámbitos de coñecemento e na práctica profesional co obxectivo de acadar unha sociedade máis xusta e igualitaria
C2	CT2 - Ter capacidade para comunicarse oralmente e por escrito en lingua galega



C3	CT3 - Incorporar no exercicio profesional criterios de sustentabilidade e compromiso ambiental. Incorporar aos proxectos o uso equitativo, responsable e eficiente dos recursos
C4	CT4 - Valorar a importancia da seguridade da información no avance socioeconómico da sociedade
C5	CT5 - Ter capacidade para comunicarse oralmente e por escrito en inglés

Resultados da aprendizaxe			
Resultados de aprendizaxe		Competencias / Resultados do título	
Experiencia en el desempeño de la profesión y de sus funciones mas habituales en un entorno 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	

Contidos	
Temas	Subtemas
O alumno realizará unha estancia na empresa desenvolvendo funcións propias dun Máster en Ciberseguridade	

Planificación				
Metodoloxías / probas	Competencias / Resultados	Horas lectivas (presenciais e virtuais)	Horas traballo autónomo	Horas totais
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

\*Os datos que aparecen na táboa de planificación son de carácter orientativo, considerando a heteroxeneidade do alumnado

Metodoloxías
--------------



Metodoloxías	Descrición
Prácticas clínicas	Prácticas externas: Estancia en empresas desenvolvendo funcións propias dun Master en Ciberseguridad

### Atención personalizada

Metodoloxías	Descrición
Prácticas clínicas	Os alumnos terán un titor na empresa e un titor na Universidade cos que poderán consultar dúbidas sobre as actividades a desenvolver e ademais son os que terán que presentar os resultados do traballo realizado.

### Avaliación

Metodoloxías	Competencias / Resultados	Descrición	Cualificación
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	A Avaliación será realizada polo titor na Universidade en función da memoria de traballo realizado na empresa e da avaliación do alumno por parte do titor da empresa.	0

### Observacións avaliación

--

### Fontes de información

Bibliografía básica	
Bibliografía complementaria	

### Recomendacións

Materias que se recomenda ter cursado previamente

Materias que se recomenda cursar simultaneamente

Materias que continúan o temario

### Observacións

--

(\*)A Guía docente é o documento onde se visualiza a proposta académica da UDC. Este documento é público e non se pode modificar, salvo casos excepcionais baixo a revisión do órgano competente dacordo coa normativa vixente que establece o proceso de elaboración de guías