Guía Docente				
Datos Identificativos				2018/19
Asignatura (*)	Fortificación de Sistemas Operativos		Código	614530007
Titulación	Máster Universitario en Ciberseguridade			
Descriptores				
Ciclo	Período	Curso	Tipo	Créditos
Mestrado Oficial	2º cuadrimestre	Primeiro	Obrigatoria	5
Idioma	CastelánGalegoInglés			
Modalidade docente	Presencial			
Prerrequisitos				
Departamento	Computación			
Coordinación	Yañez Izquierdo, Antonio Fermin	Correo electrónico	antonio.yanez@udc.es	
Profesorado	Yañez Izquierdo, Antonio Fermin	Correo electrónico	antonio.yanez@udc.es	
Web	www.dc.fi.udc.es/~afyanez			
Descrición xeral	Por favor, ver guía na versión en inglés.			

Competencias do título	
Código	Competencias do título
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 - Deseñar, implantar e manter un sistema de xestión da seguridade da información utilizando metodoloxías de referencia
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
A11	CE11 - Reunir e interpretar datos relevantes dentro do área da seguridade informática e das comunicacións
A13	CE13 - Ter capacidade de análisis, detección e eliminación de vulnerabilidades, e do malware susceptible de utilizalas, en sistemas e redes
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 más amplos (ou multidisciplinares) relacionados coa súa área de estudo
B5	CB5 - Que os estudantes posúan as habilidades de aprendizaxe que lles permitan continuar estudando dun modo que haberá de ser en gran medida autodirixido ou autónomo
B6	CG1 - Ter capacidade de análisis e síntesis. Ter capacidade para proxectar, modelar, calcular e diseñar 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 evaluación crítica de calquera sistema de protección da información, calquera sistema de seguridade da información, da seguridade das redes e/ou os sistemas de comunicacións
B10	CG5 - Ter capacidade para aplicar os coñecementos teóricos na práctica, no marco de infraestructuras, equipamientos e aplicacións concretos, e suxeitos a requisitos de funcionamento específicos
C3	CT3 - Incorporar no exercicio profesional criterios de sostenibilidade 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

Resultados da aprendizaxe	
Resultados de aprendizaxe	Competencias do título

		BP2 BP5 BP6 BP7 BP10	
	AP8	BP2 BP5 BP6 BP7 BP10	
	AP3 AP4 AP5 AP8 AP9 AP11 AP13	BP2 BP5 BP6 BP7 BP8	CP3 CP4

Contidos	
Temas	Subtemas

Planificación				
Metodoloxías / probas	Competencias	Horas presenciais	Horas non presenciais / traballo autónomo	Horas totais
Actividades iniciais	A8 A11 A13 B6	1	2	3
Sesión maxistral	A3 A4 A11 A13 B5 B6 B8 B10 C3	16	32	48
Solución de problemas	A3 A4 A5 B2 B5 B7 B8 B10 C3	5	15	20
Prácticas de laboratorio	A4 A5 A8 A9 A11 A13 B2 B5 B6 B7 B8 B10 C3	16	16	32
Proba obxectiva	A3 A4 A5 A8 A9 A11 A13 B2 B5 B6 B7 B8 B10 C3 C4	2	20	22
Atención personalizada		0		0
*Os datos que aparecen na táboa de planificación son de carácter orientativo, considerando a heteroxeneidade do alumnado				

Metodoloxías	
Metodoloxías	Descrición
Actividades iniciais	
Sesión maxistral	

Solución de problemas	
Prácticas de laboratorio	
Proba obxectiva	

Atención personalizada	
Metodoloxías	**Descrición**
Sesión maxistral Solución de problemas Prácticas de laboratorio	

Avaliación			
Metodoloxías	**Competencias**	**Descrición**	**Cualificación**
Proba obxectiva	A3 A4 A5 A8 A9 A11 A13 B2 B5 B6 B7 B8 B10 C3 C4		50
Prácticas de laboratorio	A4 A5 A8 A9 A11 A13 B2 B5 B6 B7 B8 B10 C3		50

Observacións avaliación

Fontes de información	
Bibliografía básica	- Donald A. Tevault (2018). Mastering Linux Security and Hardening. Packt Publishing - James Turnbull (2008). Hardening Linux . Apress - Carlos Álvarez Martín y Pablo González Pérez 0xWord (2016). Hardening de servidores GNU / Linux (3a Edicion). 0xWord - Tajinder Kalsi (2018). Practical Linux Security Cookbook: Secure your Linux environment from modern-day attacks with practical recipes, 2nd Edition. Packt Publishing - Gris, Myriam (2017). Windows 10. ENI - Aprea, Jean-François (2017). Windows Server 2016 : Arquitectura y Administración de los servicios de dominio Active Directory. ENI - Bonnet, Nicolas (2017). Windows Server 2016 : las bases imprescindibles para administrar y configurar su servido. ENI - De los Santos, Sergio (). Máxima Seguridad en Windows: Secretos Técnico. 0xWord - Núñez, Ángel (). Windows Server 2016: Administración, seguridad y operaciones. 0xWord - Yuri Diogenes, Erdal Ozkaya (2018). Cybersecurity - Attack and Defense Strategies. Packt Publishing - Salvy, Pierre (2017). Windows 10 : despliegue y gestión a través de los servicios de empresa. ENI - Deman, Thierry (2018). Windows Server 2016 : Administración avanzada. ENI - García, Carlos. González, Pablo (). Hacking Windows: Ataques a sistemas y redes Microsoft. 0xWord
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