



Guía Docente				
Datos Identificativos				2022/23
Asignatura (*)	Seguridade como Negocio	Código	614530010	
Titulación	Máster Universitario en Ciberseguridade			
Descritores				
Ciclo	Período	Curso	Tipo	Créditos
Mestrado Oficial	2º cuatrimestre	Primeiro	Obrigatoria	3
Idioma	CastelánGalegoInglés			
Modalidade docente	Presencial			
Prerrequisitos				
Departamento	Ciencias da Computación e Tecnoloxías da InformaciónComputaciónTecnoloxías da Información e as Comunicaci3ns			
Coordinaci3n	Carneiro Diaz, Victor Manuel	Correo electr3nico	victor.carneiro@udc.es	
Profesorado	Carneiro Diaz, Victor Manuel	Correo electr3nico	victor.carneiro@udc.es	
Web	moovi.uvigo.es			
Descrici3n xeral	Seguridade como negocio aborda as competencias necesarias para comprender o funcionamento dun Security Operation Centre (SOC), desde o punto de vista tecnol3xico, operacional e de intelixencia. Profundarase na infraestrutura, organizaci3n, operaci3n e mecanismos de m3trica necesarios para a explotaci3n empresarial dos servizos asociados a un SOC. Estudaranse diferentes contornas de especializaci3n como o sector bancario, administraci3n p3blica ou o 3mbito militar.			

Competencias / Resultados do t3tulo	
C3digo	Competencias / Resultados do t3tulo
A9	CE9 - Ter capacidade para elaborar plans e proxectos de traballo no 3mbito da ciberseguridade, claros, concisos e razoados
A11	CE11 - Reunir e interpretar datos relevantes dentro do 3rea da seguridade inform3tica e das comunicaci3ns
A15	CE15 - Ter capacidade de identificar o valor, tanto econ3mico como doutra 3ndole, da informaci3n da instituci3n, os seus procesos cr3ticos e o impacto que producir3a a interrupci3n destes; e, tam3n, as necesidades internas e externas que permitir3n estar preparados ante ataques de seguridade
A16	CE16 - Ter capacidade para albiscaar e enfocar o esforzo de negocio en tem3ticas relacionadas coa ciberseguridade, e cunha monetizaci3n viable
A19	CE19 - Saber identificar os perf3s de persoal necesarios para unha instituci3n en funci3n das s3as caracter3sticas e o seu sector
A20	CE20 - Coñecemento das empresas orientadas especificamente ao sector de seguridade da nosa contorna
B1	CB1 - Posu3r e comprender coñecementos que aporten unha base ou oportunidade de ser orixinais no desenvolvemento e aplicaci3n de ideas, a mi3do nun contexto de investigaci3n
B4	CB4 - Que os estudantes saiban comunicar as s3as conclusi3ns ---e os coñecementos e raz3ns 3ltimas que as sustentan--- a p3blicos especializados e non especializados de un modo claro e sen ambigüidades
B8	CG3 - Capacidade para o razonamiento cr3tico e a evaluaci3n cr3tica de calquera sistema de protecci3n da informaci3n, calquera sistema de seguridade da informaci3n, da seguridade das redes e/ou os sistemas de comunicaci3ns
B11	CG6 - Destreza para investigar. Capacidade para innovar e contribuír ao avance dos principios, as t3cnicas e os procesos referidos o seu 3mbito profesional, deseñando novos algoritmos, dispositivos, t3cnicas ou modelos 3tiles para a protecci3n dos activos dixitais p3blicos, privados ou comerciais
C4	CT4 - Valorar a importancia da seguridade da informaci3n no avance socioecon3mico da sociedade
C5	CT5 - Ter capacidade para comunicarse oralmente e por escrito en ingl3s

Resultados da aprendizaxe			
Resultados de aprendizaxe			Competencias / Resultados do t3tulo
Coñecer os conceptos fundamentais sobre o negocio da seguridade dixital e a s3a monetizaci3n.			AP15 AP16
			BP1 BP11
Entender que 3 posible orientar unha empresa no 3mbito da seguridade e mesmo a sectores m3is específicos dentro deste 3mbito.			AP20
			CP4



Definir os perfís necesarios, propios da empresa ou externos, asociados á ciberseguridade.	AP19		
Coñecer empresas do sector, a súa creación, desenvolvemento e orientación	AP11 AP20		
Coñecer as canles correctas de comunicación na institución, especialmente coa xerencia	AP9	BP4 BP8	CP5

Contidos	
Temas	Subtemas
Fundamentos de un Security Operation Centre (SOC)	Deseño dun SOC Fases: Tecnoloxía, Operacional, Intelixencia Tipos de entradas: Logs, eventos, alertas, incidentes, problemas Falsos/verdadeiros positivos/negativos Tipos de clientes
Infraestrutura de un SOC	Mecanismos de defensa: rede, perimetral, host, aplicacións e datos SIEM/ Log manager Ferramentas de ticketing Infraestrutura física dun SOC: rede privada, vídeo walls, laboratorios
Organización de un SOC	Organigrama: CISO, CIO, staff Perfís nun SOC
Métricas e intelixencia	Métricas de supervisión Priorización de vulnerabilidades Monitoraxe de parches Blacklist e outra listas Monitoraxe proactiva
Tipos de SOC	Especialización de SOCs: banca, administración, militar. Outsourcing: MSSPs

Planificación				
Metodoloxías / probas	Competencias / Resultados	Horas lectivas (presenciais e virtuais)	Horas traballo autónomo	Horas totais
Sesión maxistral	A15 A16 A19 B8	10	20	30
Traballos tutelados	A9 A11 A19 B1 B11 C5	4	32	36
Seminario	A19 A20 B8 C4	6	0	6
Proba obxectiva	B4	1	0	1
Atención personalizada		2	0	2

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

Metodoloxías	
Metodoloxías	Descrición
Sesión maxistral	Nas que se expoñerá o contido teórico do temario incluíndo exemplos ilustrativos e co soporte de medios audiovisuais. O alumno dispoñerá do material de apoio (notas, copias das transparencias, artigos, etc.) con anterioridade e o profesor promoverá unha actitude activa, recomendando a lectura previa dos puntos do temario para tratar en cada clase, así como realizando preguntas que permitan aclarar aspectos concretos e deixando cuestións abertas para a reflexión do alumno. As sesións maxistras complementaranse coa realización de conferencias nas que se traerá algún experto externo para tratar algún tema puntual con maior profundidade.
Traballos tutelados	Proposta de traballos para a súa resolución individual ou grupal e non presencial por parte dos alumnos. Estes traballos permitirán aos alumnos profundar en aspectos do temario relevantes e que non se puideron tratar co detalle suficiente durante as sesións maxistras.



Seminario	Presentacións de empresas do sector, onde se debulle o seu modelo de negocio e infraestrutura de servizos orientados á explotación mercantil do negocio da ciberseguridade.
Proba obxectiva	Ao final das sesións maxistras propoñeráse aos alumnos a realización dunha pequena proba tipo test na que se validen os conceptos introducidos ao longo do curso.

Atención personalizada

Metodoloxías	Descrición
Traballos tutelados	<p>Recomendarase aos estudantes que asistan á titoría como parte fundamental do apoio á aprendizaxe.</p> <p>Para a realización dos traballos supervisados, os profesores proporcionarán as indicacións iniciais necesarias, bibliografía para consulta e vixiarán os avances que o alumno está a realizar para ofrecer as orientacións pertinentes en cada caso, para asegurar a calidade do traballo. segundo os criterios indicados.</p> <p>Como ferramentas telemáticas para a atención en liña personalizada utilizaranse as facilitadas pola coordinación do Master: Ferramenta de correo electrónico, ferramenta de teleformación (faitic) e videoconferencia e ferramenta de traballo en equipo (Teams).</p>

Avaliación

Metodoloxías	Competencias / Resultados	Descrición	Cualificación
Sesión maxistral	A15 A16 A19 B8	Ao final das sesións maxistras realizarase unha proba obxectiva, baseada nun test de respostas pechadas, onde se validarán os coñecementos adquiridos.	40
Traballos tutelados	A9 A11 A19 B1 B11 C5	Os traballos tutelados serán realizados de forma individual ou en grupo polos alumnos, seguindo as indicacións propostas polo profesor.	50
Seminario	A19 A20 B8 C4	Este apartado avaliará a participación do alumno nas sesións formativas presentadas por diversos actores do mercado da ciberseguridade.	10

Observacións avaliación

A cualificación final do alumno calcularase en base ao resultado da proba obxectivo (40%), o traballo tutelado (50%) e a participación nos seminarios (10%). Non existe nota mínima para superar cada apartado.

Para a segunda oportunidade (convocatoria de xullo) aplicaranse os mesmos criterios de avaliación. Os alumnos terán a posibilidade de realizar unha proba obxectiva tipo test sobre os contidos tratados nas sesións maxistras e unha segunda data de entrega dos traballos tutelados.

Os estudantes con matrícula a tempo parcial poderán seguir a materia sen problemas, xa que a realización do traballo tutelado avaliable non require presencialidade e a avaliación dos contidos teóricos pode realizarse cunha única asistencia para realizar a proba obxectiva na data indicada no calendario de exames.

IMPORTANTE:

As datas válidas para a entrega dos traballos tutelados será a publicada polo coordinador da materia na ferramenta de teleformación do master.

FRAUDE

En caso de detectarse algun fraude nas probas avaliáveis aplicaranse as medidas sancionadoras previstas na normativa da Universidade.

Fontes de información

Bibliografía básica	- David Nathans (2015). Designing and Building a Security Operations Center. Elsevier Inc. ISBN 978-0128008997
----------------------------	--



Bibliografía complementaria	- Joseph Muniz (2016). Security Operations Center: Building, Operating, and Maintaining your SOC. Cisco Press, ISBN 978-0134052014 - Gegory Jarpey & R. Scott McCoy (2017). Security Operations Center Guidebook: A Practical Guide for a Successful SOC. Elsevier Inc., ISBN 978-0128036570
------------------------------------	---

Recomendacións

Materias que se recomenda ter cursado previamente

Xestión da Seguridade da Información/614530002

Materias que se recomenda cursar simultaneamente

Test de Intrusión/614530008

Conceptos e Leis en Ciberseguridade/614530001

Materias que continúan o temario

Seguridade Ubicua/614530013

Xestión de Incidentes/614530015

Seguridade en Dispositivos Móviles/614530011

Ciberseguridade en Contornos Industriais/614530014

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