UNIVERSIDADE DA CORUÑA

Guía Docente				
Datos Identificativos				2021/22
Asignatura (*)	Seguridade como Negocio		Código	614530010
Titulación				

Descriptores				
Ciclo	Período	Curso	Tipo	Créditos
Mestrado Oficial	2º cuadrimestre	Primeiro	Obrigatoria	3

Idioma	CastelánGalegoInglés		
Modalidade docente	Híbrida		
Prerrequisitos			
Departamento	Ciencias da Computación e Tecnoloxías da InformaciónComputaciónTecnoloxías da Información e as Comunicacións		
Coordinación	Carneiro Diaz, Victor Manuel	Correo electrónico	victor.carneiro@udc.es
Profesorado	Carneiro Diaz, Victor Manuel	Correo electrónico	victor.carneiro@udc.es
Web	moovi.uvigo.es		
Descrición xeral	Seguridade como negocio aborda as competencias necesarias para comprender o funcionamento dun Security Operation Centre (SOC), desde o punto de vista tecnolóxico, operacional e de intelixencia. Profundarase na infraestrutura, organización, operación e mecanismos de métrica necesarios para a explotación empresarial dos servizos asociados a un SOC. Estudaranse diferentes contornas de especialización como o sector bancario, administración pública ou o ámbito militar.		
Plan de continxencia	Se non é posible levar a cabo a docencia de xeito presencial ou híbrido, non se alterarán nin os contidos ni a bibliografía recomendada. Para a atención personalizada, seguiránse os métodos telemáticos proporcionados no apartado correspondente desta guía. As sesións maxistrais previstas na sección de metodoloxía docente cubriranse mediante a provisión na ferramenta faitic de vídeos curtos que permitan introducir os conceptos necesarios. Os seminarios previstos realizaránse a través da ferramenta de videoconferencia proporcionada pola coordinación do máster. A proba obxectiva realizarase na data establecida no calendario de exames a través dun formulario de resposta múltiple dispoñible na ferramenta faitic. Os traballos supervisados ??non sufrirán cambios na súa metodoloxía docente. Tampouco se modificará a avaliación e as porcentaxes especificadas no apartado correspondente desta guía.		

Competencias / Resultados do título	
Código	Competencias / Resultados do título

Resultados da aprendizaxe			
Resultados de aprendizaxe	Competencias / Resultados do título		
Coñecer os conceptos fundamentais sobre o negocio da seguridade dixital e a súa monetización.	AP15 AP16	BP1 BP11	CP4
Entender que é posible orientar unha empresa no ámbito da seguridade e mesmo a sectores máis específicos dentro deste ámbito.	AP20		
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
Infraestructura 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 maxistrais 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 maxistrais.
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 maxistrais propoñeráselle aos alumnos a realización dunha pequena proba tipo test na que se validen os conceptos introducidos ao longo do curso.

Atención personalizada

UNIVERSIDADE DA CORUÑA

Metodoloxías	Descrición
Traballos tutelados	Recomendarase aos estudantes que asistan á titoría como parte fundamental do apoio á aprendizaxe. 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. 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).

Avaliación			
Metodoloxías	Competencias / Resultados	Descrición	**Cualificación**
Sesión maxistral	A15 A16 A19 B8	Ao final das sesións maxistrais 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.	60

Observacións avaliación
A cualificación final do alumno calcularase en base ao resultado da proba obxectivo (40%) e o traballo tutelado (60%). 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 maxistrais 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 avaliables aplicaranse as medidas sancionadoras previstas na normativa da Universidade.

Fontes de información	
Bibliografía básica	- David Nathans (2015). Designig 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 Móbiles/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