Guía Docente					
Datos Identificativos					2023/24
Asignatura (*)	Seguridade como Negocio			Código	614530111
Titulación	Máster Universitario en Ciberseguridade				
Descriptores					
Ciclo	Período		Curso	Tipo	Créditos
Mestrado Oficial	2º cuadrimestre		Primeiro	Obrigatoria	4
Idioma	CastelánGalegoInglés				
Modalidade docente	Presencial				
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	Na materia Negocio en ciberseguridade e emprendemento abordase a seguridade como elemento transversal na organización, dende o punto de vista estratéxico e de xeración de negocio. Presentanse distintos enfoques para a monetización dos datos e da seguridade dos mesmos, así como os distintos perfís profesionais presentes na organización, centrándonos no funcionamento dun Security Operation Centre (SOC) e as suas ferramentas asocidas. Finalmente abordanse distintos casos de éxito e oportunidades de negocio orientados a diferentes sectores productivos, con especial atención ao emprendemento.				

Competencias / Resultados do título	
Código	Competencias / Resultados do título
A16	CE16 - Ter capacidade para albiscar e enfocar o esforzo de negocio en temáticas relacionadas coa ciberseguridade, e cunha monetización viable
A20	CE20 - Coñecemento das empresas orientadas específicamente ao sector de seguridade da nosa contorna
A31	HD-11 - Valorar una empresa en el ámbito de la seguridad e incluso a sectores más específicos dentro de este ámbito, así como definir los perfiles necesarios, propios de la empresa o externos, asociados a la ciberseguridad
A38	HD-18 - Saber 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
A39	HD-19 - Saber 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
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
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
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
B27	K-11 - Comprender los conceptos fundamentales sobre el negocio de la seguridad digital y, en este contexto, el funcionamiento de las empresas, las formas de monetización y la comunicación de productos a públicos especializados y no especializados
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
C21	C-16 - 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
C22	C-17 - Incorporar en el ejercicio profesional criterios de sostenibilidad y compromiso ambiental mediante el uso equitativo, responsable y eficiente de los recursos
C23	C-18 - Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad y tener capacidad para elaborar de planes y proyectos de trabajo claros, concisos y razonados en el ámbito de la ciberseguridad.

Resultados da aprendizaxe			
Resultados de aprendizaxe	Competencias / Resultados do título		
Coñecer os conceptos fundamentais sobre o negocio da seguridade dixital e a súa monetización.	AP16	BP27	CP4
Coñecer de forma clara e sen ambigüedades as canles correctas de comunicación a públicos especializados e non especializados.	AP39	BP4	CP5
Coñecer empresas do sector, a súa creación, desenvolvemento e orientación	AP20	BP27	CP22
Entender que é posible orientar unha empresa no ámbito da seguridade e mesmo a sectores máis específicos dentro deste ámbito.	AP20	BP11	CP23
Definir os perfís necesarios, propios da empresa ou externos, asociados á ciberseguridade.	AP31		
Coñecer as competencias clave do emprendemento, como a busca constante de oportunidades, a capacidade de asumir riscos calculados, a autoconfianza e a autoeficiencia, o pensamento crítico e creativo e as habilidades de liderado.	AP38	BP2	CP21

Contidos	
Temas	Subtemas
Fundamentos dun Security Operation Centre (SOC)	Definición dun SOC Tipos de SOC
Infraestructura dun SOC	Fases: Tecnoloxía, Operacional, Intelixencia Ferramentas dun SOC: SIEM 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
Monetización da seguridade	Fundamentos dun modelo de negocio Análisis de mercado Proposta de valor Mercado Producto
Emprendemento	Fundamentos do emprendemento Ferramentas e axudas ao emprendemento

Planificación				
Metodoloxías / probas	Competencias / Resultados	Horas lectivas (presenciais e virtuais)	Horas traballo autónomo	Horas totais
Sesión maxistral	A16 A19 A20 B12 C4	15	30	45
Seminario	A16 A20 C4	10	0	10
Traballos tutelados	B2 B4 B8 B10 B11 C2 C5	4	36	40
Proba obxectiva	B4 B8 B10	1	2	3
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.
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.
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.
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	
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**
Seminario	A16 A20 C4	Este apartado avaliará a participación do alumno nas sesións formativas presentadas por diversos actores do mercado da ciberseguridade.	20
Proba obxectiva	B4 B8 B10	Esta proba, consistente nun cuestionario test, avaliará os coñecementos adquiridos tanto nas sesións maxistrais como nos seminarios e traballos tutelados.	40
Traballos tutelados	B2 B4 B8 B10 B11 C2 C5	Os traballos tutelados serán realizados de forma individual ou en grupo polos alumnos, seguindo as indicacións propostas polo profesor.	40

Observacións avaliación

A cualificación final do alumno calcularase en base ao resultado da proba obxectivo (40%), o traballo tutelado (40%) e a participación nos seminarios (20%). 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