Guia docente				
Datos Identificativos				2024/25
Asignatura (*)	Seguridad como Negocio		Código	614530111
Titulación	Máster Universitario en Ciberseguridade			
Descriptores				
Ciclo	Periodo	Curso	Tipo	Créditos
Máster Oficial	2º cuatrimestre	Primero	Obligatoria	4
Idioma	CastellanoGallegoInglés			
Modalidad docente	Presencial			
Prerrequisitos				
Departamento	Ciencias da Computación e Tecnoloxías da InformaciónComputaciónTecnoloxías da Información e as Comunicacións			
Coordinador/a	Carneiro Diaz, Victor Manuel	Correo electrónico	victor.carneiro@udc.es	
Profesorado	Carneiro Diaz, Victor Manuel Fernández Vilas, Ana Nóvoa Manuel, Francisco Javier	Correo electrónico	victor.carneiro@udc.es francisco.javier.novoa@udc.es	
Web	moovi.uvigo.es			
Descripción general	En la asignatura Negocios en ciberseguridad y emprendimiento se aborda la seguridad como un elemento transversal en la organización, desde el punto de vista estratégico y de generación de negocio. Se presentan diferentes enfoques de la monetización de los datos y su seguridad, así como los diferentes perfiles profesionales presentes en la organización, centrándose en el funcionamiento de un Centro de Operaciones de Seguridad (SOC) y sus herramientas asociadas. Finalmente, se abordan diferentes casos de éxito y oportunidades de negocio orientadas a diferentes sectores productivos, con especial atención al emprendimiento.			

Competencias / Resultados del título	
Código	Competencias / Resultados del título
A16	CE16 - Tener capacidad para vislumbrar y enfocar el esfuerzo de negocio en temáticas relacionadas con la ciberseguridad, y con una monetización viable
A20	CE20 - Conocimiento de las empresas orientadas específicamente al sector de seguridad de nuestro entorno
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 los estudiantes sepan 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
B4	CB4 - Que los estudiantes sepan 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
B11	CG6 - Destreza para investigar. Capacidad para 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
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 la importancia de la seguridad de la información en el avance socioeconómico de la sociedad
C5	CT5 - Tener capacidad para comunicarse oralmente y 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 de aprendizaje			
Resultados de aprendizaje	Competencias / Resultados del título		
Conocer los conceptos fundamentales sobre el negocio de la seguridad digital y su monetización.	AP16	BP27	CP4
Conocer de manera clara y sin ambigüedades los canales correctos de comunicación a audiencias especializadas y no especializadas.	AP39	BP4	CP5
Conocer empresas del sector, su creación, desarrollo y orientación	AP20	BP27	CP22
Entender que es posible orientar una empresa en el ámbito de la seguridad e incluso a sectores más específicos dentro de este ámbito.	AP20	BP11	CP23
Definir los perfiles necesarios, propios de la empresa o externos, asociados a la ciberseguridad.	AP31		
Aprende las competencias clave del emprendimiento, como la búsqueda constante de oportunidades, la capacidad de asumir riesgos calculados, la confianza en uno mismo y la autoeficacia, el pensamiento crítico y creativo y las habilidades de liderazgo.	AP38	BP2	CP21

Contenidos	
Tema	Subtema
Fundamentos de un Centro de Operaciones de Seguridad (SOC)	Definición de un SOC Tipos de SOC
Infraestructura de un SOC	Fases: Tecnología, Operacional, Inteligencia Herramientas de un SOC: SIEM Infraestructura física de un SOC: red privada, videowalls, laboratorios
Organización de un SOC	Organigrama: CISO, CIO, staff Perfiles en un SOC
Métricas e inteligencia	Métricas de supervisión Priorización de vulnerabilidades Monitorización de parches Blacklist y otras listas Monitorización proactiva
Monetización de la seguridad	Conceptos básicos de un modelo de negocio Análisis de mercado Propuesta de valor Mercado Producto
Emprendimiento	Fundamentos del emprendimiento Herramientas y ayudas para el emprendimiento

Planificación				
Metodologías / pruebas	Competencias / Resultados	Horas lectivas (presenciales y virtuales)	Horas trabajo autónomo	Horas totales
Sesión magistral	A16 A20 B27 C4	15	30	45
Seminario	A16 A20 A31 C4 C23	10	0	10
Trabajos tutelados	A38 A39 B2 B4 B11 C5 C21 C22	4	36	40
Prueba objetiva	B4 B8 B10	1	2	3
Atención personalizada		2	0	2
(*)Los datos que aparecen en la tabla de planificación són de carácter orientativo, considerando la heterogeneidad de los alumnos				

Metodologías	
Metodologías	**Descripción**
Sesión magistral	En las que se expondrá el contenido teórico del temario incluyendo ejemplos ilustrativos y con el soporte de medios audiovisuales. El alumno dispondrá del material de apoyo (notas, copias de las transparencias, artículos, etc.) con anterioridad y el profesor promoverá una actitud activa, recomendando la lectura previa de los puntos del temario a tratar en cada clase, así como realizando preguntas que permitan aclarar aspectos concretos y dejando cuestiones abiertas para la reflexión del alumno. Las sesiones magistrales se complementarán con la realización de conferencias en las que se traerá algún experto externo para tratar algún tema puntual con mayor profundidad.
Seminario	Presentaciones de empresas del sector, donde se desgrane su modelo de negocio e infraestructura de servicios orientados a la explotación mercantil del negocio de la ciberseguridad.
Trabajos tutelados	Propuesta de trabajos para su resolución individual o grupal y no presencial por parte de los alumnos. Estos trabajos permitirán a los alumnos profundizar en aspectos del temario relevantes y que no se habían podido tratar con el detalle suficiente durante las sesiones magistrales.
Prueba objetiva	Al final de las sesiones magistrales se le propondrá a los alumnos a realización de una pequeña prueba tipo test en la que se validen los conceptos introducidos a lo largo del curso.

Atención personalizada	
Metodologías	**Descripción**
Trabajos tutelados	Se recomendará a los alumnos a asistencia a tutorías como parte fundamental del apoyo al aprendizaje. Para llevar a cabo el trabajo supervisado, el profesor proporcionará las indicaciones iniciales necesarias, bibliografía para consulta y monitorearán el progreso que el estudiante está haciendo para proporcionar orientación relevante en cada caso, para garantizar la calidad del trabajo. según los criterios indicados Como herramientas telemáticas para la atención personalizada en línea, se utilizarán las proporcionadas por la coordinación del Máster: herramienta de correo electrónico, herramienta de teleformación (faitic) y herramienta de videoconferencia y trabajo en equipo (Teams).

Evaluación			
Metodologías	**Competencias / Resultados**	**Descripción**	**Calificación**
Seminario	A16 A20 A31 C4 C23	Este apartado evaluará la participación de los/as alumnos/as en las sesiones formativas de diversos actores del mercado.	20
Prueba objetiva	B4 B8 B10	Esta prueba, consistente en un cuestionario de prueba, evaluará los conocimientos adquiridos tanto en las sesiones magistrales como en los seminarios y trabajos tutelados.	40
Trabajos tutelados	A38 A39 B2 B4 B11 C5 C21 C22	Los trabajos tutelados serán realizados de forma individual o en grupo por los alumnos, siguiendo las indicaciones propuestas por el profesor.	40

Observaciones evaluación

La cualificación final del alumno se calculará en base al resultado de la prueba objetivo (40%), el trabajo tutelado (40%) y la participación de los seminarios del curso (20%). No existe nota mínima en ninguno de los apartados para superar la materia. Para la segunda oportunidad (convocatoria de julio) se aplicarán los mismos criterios de evaluación. Los alumnos tendrán la posibilidad de realizar una prueba objetiva tipo test sobre los contenidos tratados en las sesiones magistrales y una segunda fecha de entrega de los trabajos tutelados. Los estudiantes con matrícula a tiempo parcial podrán seguir la asignatura sin problemas, ya que la realización del trabajo tutelado evaluable no requiere presencialidad y la evaluación de los contenidos teóricos puede realizarse con una única asistencia para realizar la prueba objetiva en la fecha indicada en el calendario de exámenes. Importante: Las fechas válidas para la entrega de los trabajos tutelados será la publicada por el coordinador de la materia en la herramienta de teleformación del master. Otros Todos los aspectos relacionados con ?dispensa académica?, ?dedicación lo estudio?, ?permanencia? y ?fraude académica? se regirán de acuerdo con la normativa académica de la Universidad en la que se ha matridulado el o la estudiante.

Fuentes de información	
Básica	- David Nathans (2015). Designig and Building a Security Operations Center. Elsevier Inc. ISBN 978-0128008997
Complementária	- 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

Recomendaciones
Asignaturas que se recomienda haber cursado previamente
Gestión de la Seguridad de la Información/614530002
Asignaturas que se recomienda cursar simultáneamente
Test de Intrusión/614530008 Conceptos y Leyes en Ciberseguridad/614530001
Asignaturas que continúan el temario
Seguridad Ubicua/614530013 Gestión de Incidentes/614530015 Seguridad en Dispositivos Móviles/614530011 Ciberseguridad en Entornos Industriales/614530014
Otros comentarios

(*) La Guía Docente es el documento donde se visualiza la propuesta académica de la UDC. Este documento es público y no se puede modificar, salvo cosas excepcionales bajo la revisión del órgano competente de acuerdo a la normativa vigente que establece el proceso de elaboración de guías