Guia docente				
Datos Identificativos				2018/19
Asignatura (*)	Seguridad como Negocio		Código	614530010
Titulación	Máster Universitario en Ciberseguridade			
Descriptores				
Ciclo	Periodo	Curso	Tipo	Créditos
Máster Oficial	2º cuatrimestre	Primero	Obligatoria	3
Idioma	CastellanoGallegoInglés			
Modalidad docente	Presencial			
Prerrequisitos				
Departamento	ComputaciónTecnoloxías da Información e as Comunicacións			
Coordinador/a	Carneiro Diaz, Victor Manuel	Correo electrónico	victor.carneiro@udc.es	
Profesorado	Carneiro Diaz, Victor Manuel	Correo electrónico	victor.carneiro@udc.es	
Web	www.munics.es			
Descripción general	Seguridad como negocio aborda las competencias necesarias para comprender el funcionamiento de un Security Operation Centre (SOC), desde el punto de vista tecnológico, operacional y de inteligencia. Se profundizará en la infraestructura, organización, operación y mecanismos de métrica necesarios para la explotación empresarial de los servicios asociados a un SOC. Se estudiarán diferentes entornos de especialización como el sector bancario, administración pública o el ámbito militar.			

Competencias del título	
Código	Competencias del título
A9	CE9 - Tener capacidad para elaborar de planes y proyectos de trabajo en el ámbito de la ciberseguridad, claros, concisos y razonados
A11	CE11 - Reunir e interpretar datos relevantes dentro del área de la seguridad informática y de las comunicaciones
A15	CE15 - Tener capacidad de identificar el valor, tanto económico como de otra índole, de la información de la institución, sus procesos críticos y el impacto que produciría la interrupción de estos; y, también, las necesidades internas y externas que permitirán estar preparados ante ataques de seguridad
A16	CE16 - Tener capacidad para vislumbrar y enfocar el esfuerzo de negocio en temáticas relacionadas con la ciberseguridad, y con una monetización viable
A19	CE19 - Saber identificar los perfiles de personal necesarios para una institución en función de sus características y su sector
A20	CE20 - Conocimiento de las empresas orientadas específicamente al sector de seguridad de nuestro entorno
B1	CB1 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y aplicación de ideas, a menudo en un contexto de investigación
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
B8	CG3 - Capacidad para el razonamiento crítico y la evaluación crítica de cualquier sistema de protección de la información, cualquier sistema de seguridad de la información, de la seguridad de las redes y/o los sistemas 14 de comunicaciones
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
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

Resultados de aprendizaje			
Resultados de aprendizaje	Competencias del título		
Conocer los conceptos fundamentales sobre el negocio de la seguridad digital y su monetización.	AP15 AP16	BP1 BP11	CP4

Entender que es posible orientar una empresa en el ámbito de la seguridad e incluso a sectores más específicos dentro de este ámbito.	AP20		
Definir los perfiles necesarios, propios de la empresa o externos, asociados a la ciberseguridad.	AP19		
Conocer empresas del sector, su creación, desarrollo y orientación	AP11 AP20		
Conocer los cauces correctos de comunicación en la institución, especialmente con la gerencia	AP9	BP4 BP8	CP5

Contenidos	
Tema	**Subtema**
Fundamentos de un Security Operation Centre (SOC)	Diseño de un SOC Fases: Tecnología, Operacional, Inteligencia Tipos de entradas: Logs, eventos, alertas, incidentes, problemas Falsos/verdaderos positivos/negativos Tipos de clientes
Infraestructura de un SOC	Mecanismos de defensa: red, perimetral, host, aplicaciones y datos SIEM/Log manager Herramientas de ticketing Infraestructura física de un SOC: red privada, video walls, 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
Tipos de SOC	Especialización de SOCs: banca, administración, militar. Outsourcing: MSSPs

Planificación				
Metodologías / pruebas	**Competéncias**	**Horas presenciales**	**Horas no presenciales / trabajo autónomo**	**Horas totales**
Sesión magistral	A15 A16 A19 B8	10	20	30
Trabajos tutelados	A9 A11 A19 B1 B11 C5	4	32	36
Seminario	A19 A20 B8 C4	6	0	6
Prueba objetiva	B4	1	0	1
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.

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.
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.
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	Para la realización de los trabajos tutelados los profesores proporcionarán las indicaciones iniciales necesarias, bibliografía para consulta y realizarán un seguimiento de los avances que el alumno vaya realizando para ofrecer las orientaciones pertinentes en cada caso, de modo que se asegure la calidad de los trabajos de acuerdo a los criterios que se indiquen. Los profesores de la materia propondrán además un horario de tutorías en el que los alumnos podrán resolver cualquier duda relacionada con el desarrollo de la misma. Se recomendará a los alumnos a asistencia a tutorías como parte fundamental del apoyo al aprendizaje.

Evaluación			
Metodologías	**Competéncias**	**Descripción**	**Calificación**
Sesión magistral	A15 A16 A19 B8	Al final de las sesiones magistrales se realizará una prueba objetiva, basada en un test de respuestas cerradas, donde se validarán los conocimientos adquiridos. Para superar la materia será necesario obtener 4 sobre 10 puntos en este apartado.	40
Trabajos tutelados	A9 A11 A19 B1 B11 C5	Los trabajos tutelados serán realizados de forma individual o en grupo por los alumnos, siguiendo las indicaciones propuestas por el profesor. Incidirán en aspectos concretos de los desarrollados durante las sesiones magistrales.	60

Observaciones evaluación
La cualificación final del alumno se calculará en base al resultado de la prueba objetivo (40%) y el trabajo tutelado (60%). Para superar la materia será necesario obtener, al menos, 4 sobre 10 puntos en la prueba objetiva, independientemente de la cualificación obtenida en el trabajo tutelado. 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. FRAUDEEn caso de detectarse algún fraude en las pruebas evaluables se aplicarán las medidas sancionadoras previstas en la normativa de la Universidad.

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