



| Guía Docente          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                    |                        |           |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------------------|-----------|
| Datos Identificativos |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                    | 2019/20                |           |
| 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 Comunicacóns                                                                                                                                                                                                                                                                                                                                                                          |                    |                        |           |
| Coordinación          | Carneiro Diaz, Victor Manuel                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Correo electrónico | victor.carneiro@udc.es |           |
| Profesorado           | Carneiro Diaz, Victor Manuel                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Correo electrónico | victor.carneiro@udc.es |           |
| Web                   | faitic.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. |                    |                        |           |

| Competencias do título |                                                                                                                                                                                                                                                                                                           |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Código                 | Competencias do título                                                                                                                                                                                                                                                                                    |
| A9                     | CE9 - Ter capacidade para elaborar plans e proxectos de traballo no ámbito da ciberseguridade, claros, concisos e razoados                                                                                                                                                                                |
| A11                    | CE11 - Reunir e interpretar datos relevantes dentro do área da seguridade informática e das comunicacións                                                                                                                                                                                                 |
| A15                    | CE15 - Ter capacidade de identificar o valor, tanto económico como doutra índole, da información da institución, os seus procesos críticos e o impacto que produciría a interrupción destes; e, tamén, as necesidades internas e externas que permitirán estar preparados ante ataques de seguridade      |
| A16                    | CE16 - Ter capacidade para albisca e enfocar o esforzo de negocio en temáticas relacionadas coa ciberseguridade, e cunha monetización viable                                                                                                                                                              |
| A19                    | CE19 - Saber identificar os perfís de persoal necesarios para unha institución en función das súas características e o seu sector                                                                                                                                                                         |
| A20                    | CE20 - Coñecemento das empresas orientadas especificamente ao sector de seguridade da nosa contorna                                                                                                                                                                                                       |
| B1                     | CB1 - Posuír e comprender coñecementos que aporten unha base ou oportunidade de ser orixinais no desenvolvemento e aplicación de ideas, a miúdo nun contexto de investigación                                                                                                                             |
| 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                                                                                                 |
| B8                     | CG3 - Capacidade para o razonamiento crítico e a avaliación crítica de calquera sistema de protección da información, calquera sistema de seguridade da información, da seguridade das redes e/ou os sistemas de comunicacións                                                                            |
| 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 |
| 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                                                                                                                                                                                                                                   |

| Resultados da aprendizaxe                                                                                                     |  |                        |             |
|-------------------------------------------------------------------------------------------------------------------------------|--|------------------------|-------------|
| Resultados de aprendizaxe                                                                                                     |  | Competencias do título |             |
| Coñecer os conceptos fundamentais sobre o negocio da seguridade dixital e a súa monetización.                                 |  | AP15<br>AP16           | BP1<br>BP11 |
| 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         |            |     |
| Cofecer empresas do sector, a súa creación, desenvolvemento e orientación                  | AP11<br>AP20 |            |     |
| Cofecer as canles correctas de comunicación na institución, especialmente coa xerencia     | AP9          | BP4<br>BP8 | CP5 |

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

| Planificación          |                         |                   |                                           |              |
|------------------------|-------------------------|-------------------|-------------------------------------------|--------------|
| Metodoloxías / probas  | Competencias            | Horas presenciais | Horas non presenciais / traballo autónomo | Horas totais |
| Sesión maxistral       | A15 A16 A19 B8          | 10                | 20                                        | 30           |
| Traballos tutelados    | A9 A11 A19 B1 B11<br>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 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    | <p>Para a realización dos traballos tutelados os profesores proporcionarán as indicacións iniciais necesarias, bibliografía para consulta e realizarán un seguimento dos avances que o alumno vaia realizando para ofrecer as orientacións pertinentes en cada caso, de modo que se asegure a calidade dos traballos de acordo aos criterios que se indiquen.</p> <p>Os profesores da materia propoñerán ademais un horario de titorías no que os alumnos poderán resolver calquera dúbida relacionada co desenvolvemento da mesma. Recomendarase aos alumnos a asistencia a titorías como parte fundamental do apoio á aprendizaxe.</p> |

| Avaliación          |                         |                                                                                                                                                                                                                                       |               |
|---------------------|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| Metodoloxías        | Competencias            | 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. Para superar a materia será necesario obter 4 sobre 10 puntos neste apartado. | 40            |
| Traballos tutelados | A9 A11 A19 B1 B11<br>C5 | Os traballos tutelados serán realizados de forma individual ou en grupo polos alumnos, seguindo as indicacións propostas polo profesor. Para superar a materia será necesario obter 4 sobre 10 puntos neste apartado.                 | 60            |

| Observacións avaliación                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>A cualificación final do alumno calcularase en base ao resultado da proba obxectivo (40%) e o traballo tutelado (60%). Para superar a materia será necesario obter, ao menos, 4 sobre 10 puntos en cada un dos apartados, independentemente da media global obtida. Se a media global é superior a 5 puntos, pero un dos apartados (teoría ou práctica) non supera a puntuación mínima, nas actas aparecerá como Suspenso (4.0).</p> <p>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.</p> <p>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.</p> <p><b>IMPORTANTE:</b></p> <p>As datas válidas para a entrega dos traballos tutelados será a publicada polo coordinador da materia na ferramenta de teleformación do master.</p> <p><b>FRAUDE</b></p> <p>En caso de detectarse algun fraude nas probas avaliáveis aplicaranse as medidas sancionadoras previstas na normativa da Universidade.</p> |

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



|                                    |                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Bibliografía complementaria</b> | <ul style="list-style-type: none"><li>- Joseph Muniz (2016). Security Operations Center: Building, Operating, and Maintaining your SOC. Cisco Press, ISBN 978-0134052014</li><li>- Gegory Jarpey &amp; R. Scott McCoy (2017). Security Operations Center Guidebook: A Practical Guide for a Successful SOC. Elsevier Inc., ISBN 978-0128036570</li></ul> |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## 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