UNIVERSIDADE DA CORUÑA

Teaching Guide			
Identifying Data			2023/24
Subject (*)	Security Business	Code	614530111
Study programme	Máster Universitario en Ciberseguridade		

Descriptors				
Cycle	Period	Year	Type	Credits
Official Master's Degree	2nd four-month period	First	Obligatory	4

Language	SpanishGalicianEnglish		
Teaching method	Face-to-face		
Prerequisites			
Department	Ciencias da Computación e Tecnoloxías da InformaciónComputaciónTecnoloxías da Información e as Comunicacións		
Coordinador	Carneiro Diaz, Victor Manuel	E-mail	victor.carneiro@udc.es
Lecturers	Carneiro Diaz, Victor Manuel	E-mail	victor.carneiro@udc.es
Web	moovi.uvigo.es		
General description	In the subject Business in cybersecurity and entrepreneurship, security is approached as a transversal element in the organization, from the strategic and business generation point of view. Different approaches to the monetization of data and their security are presented, as well as the different professional profiles present in the organization, focusing on the operation of a Security Operation Center (SOC) and its associated tools. Finally, different cases of success and business opportunities oriented to different productive sectors are addressed, with special attention to entrepreneurship.		

Study programme competences / results	
Code	Study programme competences / results
A16	CE16 - Ability for envisioning and driving the business operations in areas related to cybersecurity, with feasible monetization
A20	CE20 - Knowledge about the firms specialized in cybersecurity in the region
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 - Students will be able to apply their knowledge and their problem-solving ability in new or less familiar situations, within a broader context (or in multi-discipline contexts) related to their field of specialization
B4	CB4 - Students will learn to communicate their conclusions ---and the hypotheses and ultimate reasoning in their support--- to expert and nonexpert audiences in a clear and unambiguous way
B11	CG6 - Ability to do research. Ability to innovate and contribute to the advance of the principles, the techniques and the processes within their professional domain, designing new algorithms, devices, techniques or models which are useful for the protection public, private or commercial of digital assets
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 - Ability to ponder the importance of information security in the economic progress of society
C5	CT5 - Ability for oral and written communication in English
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.

Learning outcomes

Learning outcomes	Study programme competences / results		
Know the fundamental concepts about the business of digital security and its monetization	AJ16	BJ27	CJ4
Know clearly and unambiguously the correct channels of communication to specialized and non-specialized audiences.	AJ39	BJ4	CJ5
Knowing companies in the sector, their creation, development and orientation	AJ20	BJ27	CJ22
Understand that it is possible to guide a company in the field of security and even to more specific sectors within this field.	AJ20	BJ11	CJ23
Define the necessary profiles, specific to the company or external, associated with cybersecurity.	AJ31		
Learn the key competencies of entrepreneurship, such as the constant search for opportunities, the ability to take calculated risks, self-confidence and self-efficacy, critical and creative thinking, and leadership skills.	AJ38	BJ2	CJ21

Contents	
Topic	Sub-topic
Fundamentals of a Security Operation Center (SOC)	Definition of a SOC SOC types
Infrastructure of a SOC	Phases: Technology, Operational, Intelligence Tools of a SOC: SIEM Physical infrastructure of a SOC: private network, video walls, laboratories
Organization of a SOC	Organization: CISO, CIO, staff Profiles in a SOC
Metrics and intelligence	Monitoring metrics Prioritization of vulnerabilities Patch monitoring Blacklist and other lists Proactive monitoring
Monetization of security	Basics of a business model Market analysis Value proposition Market Product
Entrepreneurship	Fundamentals of entrepreneurship Tools and help for entrepreneurship

Planning				
Methodologies / tests	Competencies / Results	Teaching hours (in-person & virtual)	Student?s personal work hours	Total hours
Guest lecture / keynote speech	A16 A19 A20 B12 C4	15	30	45
Seminar	A16 A20 C4	10	0	10
Supervised projects	B2 B4 B8 B10 B11 C2 C5	4	36	40
Objective test	B4 B8 B10	1	2	3
Personalized attention		2	0	2
(*)The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.				

Methodologies	
Methodologies	Description

Guest lecture / keynote speech	In which the theoretical content of the syllabus will be exposed including illustrative examples and with the support of audiovisual media. The student will have support material (notes, transparencies, articles, etc.) previously and the teacher will promote an active attitude, recommending the previous reading of the topics to be dealt with in each class, as well as asking questions that allow to clarify specific aspects and leaving open questions for the reflection of the student. The magisterial sessions will be complemented with the conferences in which an external expert will be brought to discuss a specific topic in greater depth.
Seminar	Presentations of companies in the sector, where their business model and infrastructure of services aimed at the commercial exploitation of the business of cybersecurity.
Supervised projects	Proposal of works for individual or group and non-face-to-face resolution by the students. These works will allow the students to delve into relevant aspects of the syllabus and that could not be dealt with in sufficient detail during the lectures.
Objective test	At the end of the lectures the students will be proposed to carry out a small test type test in which the concepts introduced throughout the course are validated.

Personalized attention	
Methodologies	Description
Supervised projects	Students will be recommended to attend tutoring as a fundamental part of learning support. To carry out the supervised work, the teacher will provide the necessary initial indications, bibliography for consultation and will monitor the progress that the student is making to provide relevant guidance in each case, to guarantee the quality of the work. according to the indicated criteria As telematic tools for personalized online attention, those provided by the Master's coordinator will be used: email tool, learning tool (faitic) and videoconference and teamwork tool (Teams).

Assessment			
Methodologies	Competencies / Results	Description	Qualification
Seminar	A16 A20 C4	This section will evaluate the participation of the students in the training sessions of various market players.	20
Objective test	B4 B8 B10	This test, consisting of a test questionnaire, will evaluate the knowledge acquired both in the master sessions and in the seminars and supervised work.	40
Supervised projects	B2 B4 B8 B10 B11 C2 C5	The supervised works will be carried out individually or in groups by the students, following the indications proposed by the teacher. They will affect specific aspects of those developed during the lectures.	40

Assessment comments
The final qualification of the student will be calculated based on the result of the objective test (40%), the supervised work (40%) and events participation (20%). For the second opportunity (July call) the same evaluation criteria will be applied. Students will have the opportunity to perform an objective test type test on the content discussed in the lectures and a second date of delivery of the supervised works. Students with part-time enrollment can follow the subject without problems, since the realization of the supervised tutorial work does not require face-to-face and the evaluation of the theoretical contents can be done with a single assistance to perform the objective test on the date indicated in the calendar of exams. FRAUD: In case of detecting any fraud in the evaluable tests, the sanctioning measures provided for in the regulations of the University will be applied.

Sources of information	
Basic	- David Nathans (2015). Designig and Building a Security Operations Center. Elsevier Inc. ISBN 978-0128008997

Complementary	- Joseph Muniz (2016). Security Operations Center: Building, Operating, and Maintaining your SOC. Cisco Press, ISBN 978-0134052014 - Gegory Jarpey &amp;amp; R. Scott McCoy (2017). Security Operations Center Guidebook: A Practical Guide for a Successful SOC. Elsevier Inc., ISBN 978-0128036570

Recommendations
Subjects that it is recommended to have taken before
Information Security Mangement/614530002
Subjects that are recommended to be taken simultaneously
Penetration Testing/614530008 Cibersecurity Concepts and Laws/614530001
Subjects that continue the syllabus
Ubiquitous Security/614530013 Incident Management/614530015 Security in Mobile Devices/614530011 Cybersecurity in Industrial Environments /614530014
Other comments

(*)The teaching guide is the document in which the URV publishes the information about all its courses. It is a public document and cannot be modified. Only in exceptional cases can it be revised by the competent agent or duly revised so that it is in line with current legislation.