

Teaching Guide						
Identifying Data 2021/22			2021/22			
Subject (*)	Security Business Code			614530010		
Study programme	Máster Universitario en Ciberseg	uridade			·	
		Descripto	rs			
Cycle	Period	Year		Туре	Credits	
Official Master's Degre	e 2nd four-month period	First		Obligatory	3	
Language	SpanishGalicianEnglish					
Teaching method	Hybrid					
Prerequisites						
Department	Ciencias da Computación e Tecr	oloxías da Informa	ciónComputac	iónTecnoloxías da Infori	mación e as Comunicacións	
Coordinador	Carneiro Diaz, Victor Manuel		E-mail	victor.carneiro@u	⊉udc.es	
Lecturers	Carneiro Diaz, Victor Manuel		E-mail	victor.carneiro@u	ıdc.es	
Web	moovi.uvigo.es					
General description	Security Business addresses the	necessary compet	encies to unde	rstand the operation of a	a Security Operation Center	
	(SOC), from a technological, ope	rational and intellig	ence point of v	iew. The infrastructure,	organization, operation and	
	metrics mechanisms necessary f	or the business exp	ploitation of the	services associated wit	h a SOC will be deepened.	
	Different specialization environments will be studied, such as the banking sector, public administration or the military					
	sector.					
Contingency plan	If it is not possible to carry out the	e teaching in persor	n or hybrid, bot	h the contents and the b	bibliography will not be altered.	
	For personalized attention, the te	lematic methods pr	rovided in the c	corresponding section of	this guide will be followed.	
	The master sessions foreseen in	the teaching metho	odology sectior	n will be covered through	n the provision in the faitic tool of	
	short videos that allow introducin	g the necessary co	ncepts. The pla	anned seminars will be h	neld through the videoconference	
	tool provided by the master's coo	rdinator.			5	
	The objective test will be carried	out on the date set	in the exam ca	llendar through a multipl	le response form available in the	
faitic tool.			•			
	The supervised works will not undergo changes in their teaching methodology.					
Nor will the evaluation and percentages specified in the corresponding section of this guide undergo changes.		e undergo changes.				

Study programme competences
Study programme competences
CE9 - Ability to write clear, concise and motivated projects and work plans in the field of cybersecurity
CE11 - Ability to collect and interpret relevant data the field of computer and communications security
CE15 - Ability to identify the value of information for an institution, economic or of other sort; ability to identify the critical procedures in an
institution, and the impact due to their disruption; ability to identify the internal and external requirements that guarantee readiness upon
security attacks
CE16 - Ability for envisioning and driving the business operations in areas related to cybersecurity, with feasible monetization
CE19 - To learn how to identify the best professional profiles for an institution as a functions of its features and activity sector
CE20 - Knowledge about the firms specialized in cybersecurity in the region
CB1 - To possess and understand the knowledge that provides the foundations and the opportunity to be original in the development and
application of ideas, frequently in a research context
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
CG3 - Capacity for critical thinking and critical evaluation of any system designed for protecting information, any information security
system, any system for network security or system for secure communication



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
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

Learning outcomes			
Learning outcomes	Study	/ progra	imme
	cor	npeten	ces
Know the fundamental concepts about the business of digital security and its monetization	AJ15	BJ1	CJ4
	AJ16	BJ11	
Understand that it is possible to guide a company in the field of security and even to more specific sectors within this field.	AJ20		
Define the necessary profiles, specific to the company or external, associated with cybersecurity.	AJ19		
Knowing companies in the sector, their creation, development and orientation			
	AJ20		
Know the correct channels of communication in the institution, especially with management	AJ9	BJ4	CJ5
		BJ8	

	Contents
Торіс	Sub-topic
Fundamentals of a Security Operation Center (SOC)	Design of a SOC
	Phases: Technology, Operational, Intelligence
	Types of entries: Logs, events, alerts, incidents, problems
	False / true positive / negative
	Types of clients
Infrastructure of a SOC	Defense mechanisms: network, perimeter, host, applications and data
	SIEM / Log manager
	Ticketing tools
	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
Types of SOC	Specialization of SOCs: banking, administration, military.
	Outsourcing: MSSPs

	Planning]		
Methodologies / tests	Competencies	Ordinary class	Student?s personal	Total hours
		hours	work hours	
Guest lecture / keynote speech	A15 A16 A19 B8	10	20	30
Supervised projects	A9 A11 A19 B1 B11	4	32	36
	C5			
Seminar	A19 A20 B8 C4	6	0	6
Objective test	B4	1	0	1
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 /	In which the theoretical content of the syllabus will be exposed including illustrative examples and with the support of
keynote speech	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.
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.
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.
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	Description	Qualification
Guest lecture /	A15 A16 A19 B8	At the end of the lectures will be an objective test, based on a test of closed answers,	40
keynote speech		where the acquired knowledge will be validated.	
Supervised projects	A9 A11 A19 B1 B11	The supervised works will be carried out individually or in groups by the students,	60
	C5	following the indications proposed by the teacher. They will affect specific aspects of	
		those developed during the lectures.	

Assessment comments

The final qualification of the student will be calculated based on the result of the objective test (40%) and the supervised work (60%).

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; 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

(*)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.