Teaching Guide				
Identifying Data				2021/22
Subject (*)	Incident Management		Code	614530015
Study programme	Máster Universitario en Ciberseguridade			
Descriptors				
Cycle	Period	Year	Type	Credits
Official Master's Degree	2nd four-month period	First	Optional	3
Language	SpanishGalician			
Teaching method	Face-to-face			
Prerequisites				
Department	Ciencias da Computación e Tecnoloxías da InformaciónComputación			
Coordinador	López Rivas, Antonio Daniel	E-mail	daniel.lopez@udc.es	
Lecturers	Dafonte Vazquez, Jose Carlos López Rivas, Antonio Daniel	E-mail	carlos.dafonte@udc.es daniel.lopez@udc.es	
Web	moovi.uvigo.es			
General description	The management of cybersecurity incidents focuses on managing proactivity to prevent and mitigate possible consequences. The necessary knowledge about tools that can facilitate the management of incidents and recoveries, the justification of the proposed plans for recovery and resilience, the identification and classification of possible incidents and the definition of the channels for their management and resolution will be obtained.			

Contingency plan	Contingency plan A: total or partial confinement of students and / or teachers. 1. Modification in the contents: there is no modification. 2. Methodologies * Teaching methodologies that are modified - Master session, taught through videoconference. - Practices through ICT, taught through the use of the students' own tools and / or remote access to classroom equipment. - Objective test, through Faitic, Moodle or other tool provided by UVigo and / or UDC. 3. Mechanisms for personalized attention to students - Moodle: always. All teaching resources (slides, practice statement, announcements, software, etc.) are available through Moodle. - Teams: weekly. The tutorials will be attended by Teams at the official hours of each teacher. - Email: always. To answer any question. 4. Modifications in the evaluation: none * Observations of the evaluation: in the event that it cannot be done in person, the following will be carried out: - Objective test: through Faitic and Remote Campus or Teams. 5. Modifications of the bibliography or webgraphy: none. Contingency plan B: number of students exceeds the capacity of the classroom. 1. Modification in the contents: there is no 2. Methodologies * Teaching methodologies that are modified - Master session, two groups will be established that will attend in person every other week. A video conferencing solution (remote Campus or Teams) will be searched to access the sessions remotely. - Practices through ICT, two groups will be established that will attend in person every other week. A remote access solution or similar will be sought for the group that cannot attend in person. It is taught through the use of the students' own tools and / or remote access to classroom equipment. - Objective test, a classroom with sufficient capacity will be enabled. 3. Mechanisms for personalized attention to students - Moodle: always. All teaching resources (slides, practice statement, announcements, software, etc.) are available through Moodle. - Teams: weekly. The tutorials will be attended by Teams at the official hours of each teacher. - Email: always. To answer any question. 4. Modifications in the evaluation: none * Observations of the evaluation: if it cannot be done in person, the following will be carried out: - Objective test: through Faitic and Remote Campus or Teams. 5. Modifications of the bibliography or webgraphy: none.

Study programme competences	
Code	Study programme competences
A3	CE3 - Knowledge of the legal and technical standards used in cybersecurity, their implications in systems design, in the use of security tools and in the protection of information
A9	CE9 - Ability to write clear, concise and motivated projects and work plans in the field of cybersecurity

A14	CE14 - Ability to develop a continuity business plan on the guidelines of commonly accepted norms and standards
A15	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
A17	CE17 - Ability to plan a time schedule containing the detection periods of incidents or disasters, and their recovery
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
B3	CB3 - Students will be able to integrate diverse knowledge areas, and address the complexity of making statements on the basis of information which, notwithstanding incomplete or limited, may include thoughts about the ethical and social responsibilities entailed to the application of their professional capabilities and judgements
B5	CB5 - Students will apprehend the learning skills enabling them to study in a style that will be selfdriven and autonomous to a large extent
B6	CG1 - To have skills for analysis and synthesis. To have ability to project, model, calculate and design solutions in the area of information, network or system security in every application area
B10	CG5 - Students will have ability to apply theoretical knowledge to practical situations, within the scope of infrastructures, equipment or specific application domains, and designed for precise operating requirements
C4	CT4 - Ability to ponder the importance of information security in the economic progress of society

Learning outcomes			
Learning outcomes	Study programme competences		
Manage proactivity to prevent and mitigate possible security incidents	AJ9 AJ14 AJ17	BJ2 BJ3 BJ5 BJ6 BJ10	CJ4
Obtain the necessary knowledge about tools that can facilitate the management of incidents and recoveries	AJ3 AJ14 AJ17	BJ2 BJ3 BJ5 BJ6 BJ10	
Justify proposed plans for recovery and resilience	AJ3 AJ9 AJ14 AJ15	BJ2 BJ3 BJ5 BJ6 BJ10	CJ4
Identify and classify possible incidents and define the channels for their management and resolution	AJ3 AJ9 AJ17	BJ2 BJ3 BJ5 BJ6 BJ10	CJ4

Contents	
Topic	Sub-topic
1. Fundamentals: resilience and the value of information	1.1. Introduction 1.2. Fundamentals
2. Incident detection and response management	2.1. Detection and notification of incidents 2.2. Response management, containment and mitigation of impact
3. Standards: continuity and recovery plans	3.1. ISO / IEC standards 3.2. Guidelines for incident management

4. Disaster recovery	4.1. Mechanisms 4.2. Phases of recovery 4.3. Protection of critical infrastructures
5. Legislation	5.1. Specific legislation: National Security Scheme, National Cybersecurity Strategy

Planning				
Methodologies / tests	Competencies	Ordinary class hours	Student?s personal work hours	Total hours
Laboratory practice	A9 A14 A17 B2 B3 B10	10	25	35
Guest lecture / keynote speech	A3 A14 A15 A17 B5 B6 C4	10	20	30
Supervised projects	A3 A9 A14 A15 A17 B2 B3 B5 B6 B10 C4	1	9	10
Objective test	A3 A9 A14 A15 A17 B2 B3 B5 B6 B10 C4	1.5	0	1.5
Personalized attention		0		0
(*)The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.				

Methodologies	
Methodologies	Description
Laboratory practice	Practical computer sessions associated with incident scenarios and tools for cyberincidents. The objective is to put into practice the knowledge of the master sessions promoting autonomous learning.
Guest lecture / keynote speech	Guest lecture. Presentations of the theoretical knowledge of the subjects of the matter promoting the interaction with the students. NOTE: it will be possible to use any of these sessions to carry out a company workshop or invite a collaborating person of recognised competence.
Supervised projects	Work to be developed by the student on any of the subjects of the matter proposed by the student or professor. This work will have a follow-up by the faculty and the student will make a brief presentation of the same.
Objective test	Written test to assess the knowledge acquired. Although it will focus on the material of expository teaching, it can incorporate some issues related to the practical sessions.

Personalized attention	
Methodologies	Description
Laboratory practice Supervised projects	The personalized attention is focused on supporting the student in the understanding of the different techniques through the support in the tutorials and the resolution of doubts that may arise in the lectures. Help will also be provided to respond to doubts that may arise during the realization of the practices or learning through the supervised works for a better use and understanding of the knowledge acquired in class.

Assessment			
Methodologies	Competencies	Description	**Qualification**
Laboratory practice	A9 A14 A17 B2 B3 B10	Practical computer sessions associated with incident scenarios and management of tools for cyber incidents. The objective is to put the knowledge from the master sessions into practice, promoting autonomous learning. The evaluation will be continuous throughout the sessions. NOTE: it will be possible to use some of the face-to-face sessions to carry out a workshop of a collaborating entity.	30

Supervised projects	A3 A9 A14 A15 A17 B2 B3 B5 B6 B10 C4	Work to be carried out by the student on any of the subjects of the subject at the proposal of the student or the teacher. This work will be followed up by the teaching staff and the student will make a brief face-to-face defense of it.	20
Objective test	A3 A9 A14 A15 A17 B2 B3 B5 B6 B10 C4	Written test to assess the knowledge acquired. Although it will focus on the expository teaching material, it will be able to incorporate some questions related to the practical sessions.	50

Assessment comments
In order to pass the subject, it will be necessary to obtain a minimum of 5 out of 10 in both the objective test and the practical work. Otherwise, the maximum note that can be obtained will be 4.5. The grade obtained in the continuous assessment of practices and supervised project will be maintained throughout the academic year.STUDENTS WHO DID NOT PARTICIPATE IN THE CONTINUOUS EVALUATION OF PRACTICES AND SUPERVISED PROJECTS:i) When the student presents himself to the first opportunity call, his grade will be 0 in both methodologies.ii) When the student presents himself to the second opportunity call or extraordinary call, without having participated in the continuous evaluation process, using these methodologies, he / she will be able to individually perform the practices with the material available in the virtual teaching platform and through the request of tutorials with the professors of the subject. Also individually, the student will specify with the professor the date of the exam of practices that, in this case, will be essential.STUDENTS WHO DID NOT PARTICIPATE IN THE OBJECTIVE PROOF AT THE FIRST OPPORTUNITY: Whether or not they have participated in the process of continuous assessment of practices and supervised project, their grade will be "No Presented".PLAGIARISM: Plagiarism is regarded as serious dishonest behavior. If any form of plagiarism is detected in any of the exams or provided material, the final grade will be FAIL (0), and the incident will be reported to the corresponding academic authorities for prosecution.

Sources of information	
Basic	- ISO/IEC 27035:2016 - Information technology - Security techniques - Information security incident management. http://www.iso27001security.com/html/27035.html- Gestión de incidentes de seguridad informática, Álvaro Gómez Vieites, 978-84-92650-77-4, RA-MA Editorial, 2014- Gestión de incidentes de seguridad informática (MF0488_3), Ester Chicano Tejada, 978-84-16351-70-1, IC Editorial, 2014- Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad, Luis Gómez Fernández y Pedro Pablo Fernández Rivero, 978-84-81439-63-2 AENOR, 2018- Sistema de Información para gestionar un SGSI basado en ISO 27001:2013: Cómo tener trazabilidad de un Sistema de Gestión de Seguridad de la información a través de una herramienta Informática, Lorena Mahecha Guzmán y Gabriel Coello F., 978-620-2-25000-9, EAE, 2017- Implementing the ISO/IEC 27001 ISMS Standard 2016 (Information Security), Edward Humphreys, 978-1-60807-930-8, Artech House Publishers, 2016- Infosec Management Fundamentals, Henry Dalziel, 978-0-12-804187-1, Syngress, 2015- Information Security Incident Management: A Methodology, Neil Hare-Brown, 978-0-580-50720-5, BSI Standards, 2007
Complementary	

Recommendations
Subjects that it is recommended to have taken before
Subjects that are recommended to be taken simultaneously
Subjects that continue the syllabus
Other comments
The student is recommended, for an optimal use of the subject, to actively attend classes as well as participate in the different activities and the use of personalized attention for the resolution of doubts or questions that may arise.