Teaching Guide				
Identifying Data				2023/24
Subject (*)	Intelligent Cibersecurity		Code	614544024
Study programme	Máster Universitario en Intelixencia Artificial			
Descriptors				
Cycle	Period	Year	Type	Credits
Official Master's Degree	1st four-month period	Second	Optional	3
Language	English			
Teaching method	Hybrid			
Prerequisites				
Department	Ciencias da Computación e Tecnoloxías da Información			
Coordinador	Garabato Míguez, Daniel	E-mail	daniel.garabato@udc.es	
Lecturers	Garabato Míguez, Daniel	E-mail	daniel.garabato@udc.es	
Web				
General description	This subject introduces the student to the development of strategies based on Artificial Intelligence applied to protect computer systems and networks against malicious attacks that seek to control them or to get access to the information behind them. The students will be trained in prevention, detection, analysis and elimination of security threats in a context of continuous evolution. Typical use cases of Artificial Intelligence in cybersecurity scenarios will be reviewed.			

Study programme competences	
Code	Study programme competences
A5	CE04 - Knowing the fundamentals and basic techniques of Artificial Intelligence, plus their practical application
A9	CE08 - Ability to design and develop secure intelligent systems, in terms of integrity, confidentiality and robustness
A20	CE19 - Knowledge of the different environments where AI based technologies can be applied and awareness of their capability to provide a differentiating added value
A21	CE20 - Ability to combine and adapt different techniques, extrapolating knowledge among different application domains
A22	CE21 - Knowledge of the techniques that facilitate the efficient organisation and management of AI projects in real environments, including resources management and tasks scheduling and taking into account the concepts of knowledge dissemination and open science
A23	CE22 - Knowledge of the techniques that facilitate the security of data, applications and communications and the derived consequences on different application domains in AI
A31	CE30 - Being able to set out, model and solve problems that require the application of AI methods, techniques and technologies
B1	CG01 - Maintaining and extending theoretical foundations to allow the introduction and exploitation of new and advanced technologies in the field of AI
B2	CG02 - Successfully addressing each and every stage of an AI project
B4	CG04 - Suitably elaborating written essays or motivated arguments, including some point of originality, writing plans, work projects, scientific papers and formulating reasonable hypotheses in the field
B5	CG05 - Working in teams, especially of multidisciplinary nature, and being skilled in the management of time, people and decision making
B6	CB01 - Acquiring and understanding knowledge that provides a basis or opportunity to be original in the development and/or application of ideas, frequently in a research context
B7	CB02 - The students will be able to apply the acquired knowledge and to use their capacity of solving problems in new or poorly explored environments inside wider (or multidisciplinary) contexts related to their field of study
B9	CB04 - The students will be able to communicate their conclusions, their premises and their ultimate justifications, both to specialised and non-specialised audiences, using a clear style language, free from ambiguities
B10	CB05 - The students will acquire learning abilities to allow them to continue studying in way that will mostly be self-directed or autonomous
C5	CT05 - Understanding the importance of the entrepreneurial culture and knowledge of the resources within the entrepreneur person's means
C8	CT08 - Appreciating the importance of research, innovation and technological development in the socioeconomic and cultural progress of society
C9	CT09 - Being able to manage time and resources: outlining plans, prioritising activities, identifying criticisms, fixing deadlines and sticking to them

Learning outcomes			
Learning outcomes	Study programme competences		
Know different techniques and tools to implement AI-based solutions for automated detection of vulnerabilities, attacks and fraudulent content and applications	AC4 AC8 AC19 AC20 AC22 AC30	BC1 BC6 BC7 BC10	CC5 CC8
Know, understand and analyze real application cases of AI techniques in different cybersecurity fields	AC4 AC8 AC19 AC20 AC21 AC22 AC30	BC2 BC4 BC5 BC6 BC7 BC9 BC10	CC5 CC8 CC9
Know techniques that facilitate security by design and that allow secure system and network communications administration, risk management and a fast recovery upon cybersecurity events	AC8 AC20 AC21 AC22 AC30	BC1 BC2 BC4 BC5 BC7 BC9	CC8 CC9
Understand the importance of identity as a concept and know techniques that guarantee access to the data and their privacy	AC4 AC8 AC21 AC22 AC30	BC1 BC2 BC6 BC7 BC9 BC10	CC8

Contents	
Topic	Sub-topic
Theory	- Cybersecurity: concepts and introduction - Threat detection and attack prevention models - Detection of fraudulent content and applications - Data mining in event management systems - Identity control, biometrics and behavioral patterns - Anomaly detection and clustering for attack detection in communications - Risk management in AI, critical risks and regular profiles, malicious uses, and contingency and recovery plans
Practice	- Use of specific tools related to cybersecurity environments - Application of AI techniques to solve cybersecurity problems

Planning				
Methodologies / tests	Competencies	Ordinary class hours	Student?s personal work hours	Total hours
Guest lecture / keynote speech	A5 A9 A20 A21 A22 A23 B1 B2 B6 B10 C5 C8	10	10	20

Laboratory practice	A5 A9 A20 A21 A22 A23 A31 B1 B2 B4 B5 B6 B7 B9 C9	5.25	15.75	21
Problem solving	A5 A9 A20 A21 A22 A23 A31 B1 B2 B4 B5 B6 B7 B9 C9	5.25	15.75	21
Objective test	A5 A9 A20 A21 A22 A23 A31 B1 B2 B4 B6 B7 B9 B10	2	10	12
Personalized attention		1	0	1
(*)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	Oral presentation complemented by the use of audiovisual media and bringing up some questions addressed to the students, in order to transmit knowledge and facilitate learning. In addition to the oral presentation carried out by the professor, this activity requires the students to dedicate time to prepare and review the class materials on their own.
Laboratory practice	Classes dedicated to the development of practical work involving the resolution of complex problems, as well as the analysis and design of solutions that constitute a means for their resolution. This activity may require students to make an oral presentation of the work done. These works can be carried out, depending on the case, either individually or in working groups.
Problem solving	These are sessions in which the objective is that students acquire certain competencies based on the resolution of exercises, case studies and projects that require the application of the knowledge and competencies developed during the course. This activity may require students to make an oral presentation of the work done. This work may be done, depending on the case, either individually or in work groups.
Objective test	Examination in which both theoretical and practical aspects seen during the course can be evaluated.

Personalized attention	
Methodologies	**Description**
Guest lecture / keynote speech Laboratory practice Problem solving	The development of the practices will be monitored during the reserved hours in the schedule (laboratory sessions). In addition, to address those particularly difficult problems, the time slots available for student's attention can also be used.

Assessment			
Methodologies	**Competencies**	**Description**	**Qualification**
Laboratory practice	A5 A9 A20 A21 A22 A23 A31 B1 B2 B4 B5 B6 B7 B9 C9	Assessment of practical assignments (E2)	40
Objective test	A5 A9 A20 A21 A22 A23 A31 B1 B2 B4 B6 B7 B9 B10	Final examination (E1)	20
Problem solving	A5 A9 A20 A21 A22 A23 A31 B1 B2 B4 B5 B6 B7 B9 C9	Assessment of supervised projects (E3)	40

Assessment comments

In order to pass (and release) both laboratory practices and supervised projects, it is necessary to reach 40% of the maximum score foreseen for these evaluation items. There is no minimum required for the objective test.In order to pass the subject it is necessary to reach the previous minima (laboratory practices and supervised project) and to get a minimum of 5 points out of 10 in the final weighted grade.In case of not reaching the minimum required to pass any of the parts (laboratory practices and/or supervised project), the students will have a second opportunity in which they will only deliver the items that were not passed.In case of passing part of the evaluated items, but not reaching the minimum required to pass the whole subjet, the grade to be included in the official qualification sheet will be calculated as the minimum between the weighted average of the parts passed and 4.9.The condition of "Presented" will be provided to those students who submit all the compulsory practicals and assignments or takes the objective test during the official evaluation period.The delivery of practices and assignments must be carried out within the established term, and will follow the specifications indicated in the proposal both for the presentation and for the defense.The professors will facilitate, to the best possible option and within the schedules established for the subject, attendance to the theory and practice groups that best fit the needs of the students who are enrolled part-time, for whom the form of evaluation established here also applies. Students with academic waiver of attendance exemption must attend all the assessment tests.In case of fraudulent performance of exercises or tests, once it is demonstrated, will imply a failing grade (numerical grade 0) in the call in which it is committed, whether the commission of the fault occurs in the first opportunity or in the second one.The subject will be taught in English. The theory lectures will be given by UVigo and broadcasted to all students. There will be a specific face-to-face interactive teaching group at each university (USC-UDC-UVigo).

Sources of information	
Basic	- William Stallings (2018). Effective Cybersecurity: A Guide to Using Best Practices and Standards. Addison-Wesley Professional
Complementary	- Alessandro Parisi (2019). Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies. Packt Publishing

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
In order to make the most of the subject, students are recommended to actively follow the classes and to participate in the different activities and use the personalized attention to solve any doubts or questions that may arise.As stated in the different regulations applicable to university teaching regarding gender perspective, in this subject non-sexist language will be used, the intervention of male and female students in class will be encouraged, etc. Likewise, we will work to identify and modify sexist prejudices and attitudes, promoting values of respect and equality. In general, we will try to detect situations of discrimination, for example, for reasons of gender, and we will propose actions and measures to correct them.