



Teaching Guide				
Identifying Data			2024/25	
Subject (*)	Cybersecurity	Code	710G04032	
Study programme	Grao en Xestión Dixital de Información e Documentación			
Descriptors				
Cycle	Period	Year	Type	Credits
Graduate	1st four-month period	Fourth	Optional	6
Language	SpanishGalician			
Teaching method	Face-to-face			
Prerequisites				
Department	Ciencias da Computación e Tecnoloxías da Información			
Coordinador	Vázquez Naya, José Manuel	E-mail	jose.manuel.vazquez.naya@udc.es	
Lecturers	Pérez Jove, Rubén Rivera Dourado, Martiño Vázquez Naya, José Manuel	E-mail	ruben.perez.jove@udc.es martino.rivera.dourado@udc.es jose.manuel.vazquez.naya@udc.es	
Web	http://https://campusvirtual.udc.gal			
General description	A ciberseguridade é un pilar fundamental na sociedade dixital actual, onde a protección da información e dos sistemas informáticos é crucial para garantir a confidencialidade, integridade e dispoñibilidade dos datos. No Grao en Xestión Dixital de Información e Documentación, a asignatura de Ciberseguridade proporciona aos estudantes os coñecementos esenciais para salvagardar a información en contornos dixitais, preparándoos para afrontar os desafíos dun mundo cada vez máis conectado e dependente da tecnoloxía.			

Study programme competences / results	
Code	Study programme competences / results
A14	CE14 - Apply the legal and regulatory provisions and procedures related to the information and documentation activity in general and in the digital environment in particular
A19	CE19 - Determine and apply methods, measures and techniques designed to order, protect, preserve and restore data, information and documents of different nature
A22	CE22 - Acquire computational skills and management of new ICT
B7	CG2 - Capacity for reflection and critical reasoning
B9	CG4 - Capacity for analysis, diagnosis and decision making
B11	CG6 - Ability to understand the importance, value and function of the Digital Information and Documentation Management in the current ICT society
C2	CT2 - Use the basic tools of information and communication technologies (ICT) necessary for the exercise of their profession and for learning throughout their lives

Learning outcomes			
Learning outcomes	Study programme competences / results		
To know and know how to use the basic encryption algorithms	A19 A22	B7 B9 B11	C2
To know and know how to use the concepts of digital signature	A19 A22	B7 B9 B11	C2
To know the basics of network security	A19 A22	B7 B9 B11	C2



To know the different backup, data redundancy and synchronization policies to avoid data loss	A19 A22	B7 B9 B11	C2
To know the legislative environment in relation to the protection of personal data	A14 A19		

Contents	
Topic	Sub-topic
Tema 1: Introducción á Ciberseguridade	<ul style="list-style-type: none"> - Conceptos básicos e principios de ciberseguridade - Vulnerabilidades, ameazas e ataques - Medidas e prácticas de protección
Tema 2: Algoritmos Básicos de Cifrado	<ul style="list-style-type: none"> - Principios de cifrado - Algoritmos de cifrado simétrico - Algoritmos de cifrado asimétrico - Aplicacións prácticas do cifrado
Tema 3: Certificados Dixitais e Sinatura Dixital	<ul style="list-style-type: none"> - Concepto e tipos de certificados dixitais - Autoridades de Certificación (CA) - Sinaturas dixitais: funcionamento e aplicacións
Tema 4: Firewalls e Acceso Seguro a Redes	<ul style="list-style-type: none"> - Fundamentos de firewalls - Redes seguras: VPNs e outras tecnoloxías de acceso seguro
Tema 5: Copias de Seguridade e Redundancia de Datos e Sincronización de Datos	<ul style="list-style-type: none"> - Importancia das copias de seguridade - Tipos de copias de seguridade - Estratexias de backup e plans de recuperación ante desastres - Redundancia de datos: RAID e outras tecnoloxías - Conceptos de sincronización de datos - Tecnoloxías e ferramentas de sincronización
Tema 6: Lexislación de Protección de Datos Persoais	<ul style="list-style-type: none"> - Regulamento Xeral de Protección de Datos (GDPR) - Lei Orgánica de Protección de Datos de Carácter Persoal - Outras normas relevantes no ámbito de protección de datos

Planning				
Methodologies / tests	Competencies / Results	Teaching hours (in-person & virtual)	Student?s personal work hours	Total hours
Guest lecture / keynote speech	A14 A22 B7	21	21	42
ICT practicals	A14 A19 A22 B7 B9 B11 C2	15	30	45
Supervised projects	A19 B7 B9 B11	6	30	36
Objective test	A14 A19 A22 B7 B9 B11	1	20	21
Personalized attention		6	0	6

(*)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	<p>Clases expositivas de presentación dos coñecementos teóricos de cada un dos temas.</p> <p>O material utilizado nestas clases estará dispoñible na plataforma de formación da Universidade da Coruña.</p>
ICT practicals	Realización, por parte do alumno de forma individual ou colectiva, de traballos nos que se requira o emprego de ferramentas ou programas nos que aplicar os conceptos previamente expostos.



Supervised projects	Realización, por parte do alumno de forma individual ou colectiva de proxectos nos que se poña en práctica o aprendido en cada tema da materia. O profesor tutelar a evolución do traballo.
Objective test	Prueba escrita mediante la que se valorarán los conocimientos y capacidades adquiridos por el alumno.

Personalized attention

Methodologies	Description
ICT practicals Supervised projects	Resolución das dúbidas que xurdan na realización de prácticas e ou traballos. Resolveranse preferentemente no horario asignado para as clases ou nas horas de tutorías establecidas.

Assessment

Methodologies	Competencies / Results	Description	Qualification
ICT practicals	A14 A19 A22 B7 B9 B11 C2	Performance of work with ICT tools in the field of security.	30
Supervised projects	A19 B7 B9 B11	Evaluation of the work proposed by the teacher, or by the student himself, throughout the course.	20
Objective test	A14 A19 A22 B7 B9 B11	Examination test: multiple-choice and/or short essay questions.	50

Assessment comments

Será necesario obter como mínimo o 50% da nota para aprobar a materia. Ademais, para aprobar a materia será preciso (en calquera oportunidade) obter un mínimo dun 40% da nota na proba obxectiva. En caso contrario, a nota máxima que se poderá obter é de 4.5.

A nota da proba obxectiva NON se conserva en ningunha convocatoria. A nota de "prácticas de laboratorio" e de "traballos tutelados" consérvase para o resto de oportunidades do curso académico.

1. PRIMEIRA OPORTUNIDADE

Ó longo do curso realizaranse unha serie de "prácticas de laboratorio" e un "traballo tutelado", coas características e peso indicados no cadro anterior.

Ó finalizar o curso realizarase unha "proba obxectiva", coas características e peso indicados no cadro anterior.

2. SEGUNDA OPORTUNIDADE E OPORTUNIDADE ADIANTADA

Realizarase unha "proba obxectiva", coas características e peso indicados no cadro anterior.

A nota de "prácticas de laboratorio" poderá recuperarse mediante a realización das prácticas que se determinen para a segunda oportunidade (ou oportunidade adiantada). A presentación das prácticas na convocatoria de segunda oportunidade (ou oportunidade adiantada) implica a renuncia á nota obtida previamente, se a houbese.

A nota do "traballo tutelado" poderá recuperarse mediante a realización dun novo traballo, cuxa temática debe ser acordada co coordinador da materia. A presentación do traballo tutelado na convocatoria de segunda oportunidade (ou oportunidade adiantada) implica a renuncia á nota obtida na primeira oportunidade, se a houbese.

Caso de querer recuperar a nota de prácticas de laboratorio ou do traballo tutelado na convocatoria de segunda oportunidade (ou oportunidade adiantada), o alumnado deberá contactar co coordinador da materia, cunha antelación mínima de 20 días naturais antes da data do exame da correspondente convocatoria.

3. CONDICIÓN DE "NON PRESENTADO"

Considerarase como "non presentado" ao alumnado que non se presente a ningunha das actividades avaliadas nunha convocatoria dada.

4. DISPENSA ACADÉMICA, DEDICACIÓN AO ESTUDO, PERMANENCIA E FRAUDE ACADÉMICA

Todos os aspectos relacionados con "dispensa académica", "dedicación ao estudo", "permanencia" e "fraude académica" rexeranse de acordo coa normativa académica vixente da UDC (dispoñible en <https://www.udc.es/es/normativa/academica>).

Sources of information



Basic	<ul style="list-style-type: none">- Stallings, W. (2011). <i>Cryptography and Network Security: Principles and Practice</i> (Fifth ed.). Prentice Hall- Stallings, W., Brown, L. (2018). <i>Computer Security: Principles and Practice</i>. Prentice Hall- Lucena, M. J. (2023). <i>Criptografía y seguridad en Computadores</i>.- Costas, S. J. (2010). <i>Seguridad informática</i>. Madrid: RA-MA Editorial
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 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.