



Teaching Guide

Teaching Guide				
Identifying Data				2023/24
Subject (*)	Informatics		Code	631G01110
Study programme	Grao en Náutica e Transporte Marítimo			
Descriptors				
Cycle	Period	Year	Type	Credits
Graduate	2nd four-month period	First	Basic training	6
Language	SpanishGalician			
Teaching method	Face-to-face			
Prerequisites				
Department	Enxeñaría de Computadores			
Coordinador	Vidal Paz, Jose	E-mail	jose.vidal.paz@udc.es	
Lecturers	Andión Fernández, José Manuel	E-mail	jose.manuel.andion@udc.es	
	Vidal Paz, Jose		jose.vidal.paz@udc.es	
Web				
General description	Esta materia encádrase dentro das materias básicas das enxeñarías, e máis concretamente considérase como unha materia transversal porque as competencias adquiridas son importantes para cursar a maioría das materias da titulación. No ano 2017, o Comité de Seguridad Marítima da IMO publica a resolución MSC.428(98) relativa á xestión dos riscos cibernéticos no sector marítimo nos sistemas de xestión da seguridade, a cal entrou en vigor o 1 de xaneiro de 2021. Así mesmo, tamén publica as "Guías sobre gestión del riesgo cibernético?", que proporcionan recomendacións que se deben adoptar a bordo dos buques. Estas novas necesidades xurdidas nestes últimos anos supuxeron un punto de inflexión no sector marítimo, no cal se lle comezou a dar unha maior importancia á seguridade dos seus sistemas IT/OT. As competencias adquiridas nesta materia serán de gran importancia para o desenvolrolo da profesión dos futuros egresados en Náutica, porque posuirán coñecementos sobre o tipo de riscos cibernéticos aos que van a estar expostos, e estarán capacitados para tomar medidas preventivas, analizar rexistros de acceso para detectar incidentes e executar unha política de copias de seguridade para poder recuperar os equipos ao seu estado operativo inicial. Dentro do plan de estudos, aínda que esta materia pódese considerar relacionada con case todas as da titulación, ten a súa continuación coa Informática Aplicada. Ademáis garda unha estreita relación coas Matemáticas (resolución de problemas, representación e interpretación de resultados), así como con Electricidade e Electrónica (codificación da información, hardware, redes). Tamén se considera que está relacionada co Inglés, pois moita da información a manexar (libros, Internet, manuais, videotutoriais, ...) atópase neste idioma.			

Study programme competences / results

Code	Study programme competences / results
A54	RA1C-Write, explain and transmit the theoretical knowledge acquired both orally and in writing using scientific-technical language.
A57	RA4C-Collecting and interpreting relevant data
A58	RA5C-Identify ship components.
A59	RA6C-Identify critical situations and use available means in order to resolve them effectively.
B31	RA9H-Effectively solve practical problems associated with the subject by applying the knowledge acquired.
B32	RA10H-Know, analyse, synthesise and apply the contents, fundamental concepts and applications of the subject.
B33	RA11H-Develop both individual and group work
B34	RA12H-Handle bibliographic material and computer resources.
B35	RA13H-Handle with ease the tools, techniques, equipment and/or material/instrumental of each subject.



B36	RA14H-Use information and communication technology (ICT) tools necessary for the exercise of their profession and for lifelong learning.
B97	RA100H?Recognise protection risks and threats.
B98	RA101H?Conduct regular security inspections of the ship.
C15	RA17X-Communicating effectively in a work environment.

Learning outcomes			
Learning outcomes		Study programme competences / results	
RA1C-Write, explain and transmit the theoretical knowledge acquired both orally and in writing using scientific-technical language.	A54		
RA4C-Collecting and interpreting relevant data	A57		
RA5C-Identify ship components.	A58		
RA6C-Identify critical situations and use available means in order to resolve them effectively.	A59		
RA9H-Effectively solve practical problems associated with the subject by applying the knowledge acquired.		B31	
RA10H-Know, analyse, synthesise and apply the contents, fundamental concepts and applications of the subject.		B32	
RA11H-Develop both individual and group work		B33	
RA12H-Handle bibliographic material and computer resources.		B34	
RA13H-Handle with ease the tools, techniques, equipment and/or material/instrumental of each subject.		B35	
RA14H-Use information and communication technology (ICT) tools necessary for the exercise of their profession and for lifelong learning.		B36	
RA100H-Recognise protection risks and threats.		B97	
RA101H-Conduct regular security inspections of the ship.		B98	
RA17X-Communicating effectively in a work environment.			C15

Contents	
Topic	Sub-topic
1. REPRESENTACIÓN E CIFRADO DA INFORMACIÓN	1.1. REPRESENTACIÓN DA INFORMACIÓN 1.2. SISTEMAS DE NUMERACIÓN 1.3. CÓDIGOS BINARIOS 1.4. CIFRADO
2. HARDWARE	2.1. INTRODUCCIÓN 2.2. PLACA BASE 2.3. CPU 2.4. MEMORIA 2.5. SISTEMA DE INTERCONEXION: BUSES
3. SISTEMAS OPERATIVOS	3.1. PROCESO DE ARRANQUE 3.2. CONCEPTOS BÁSICOS 3.3. PROCESOS 3.4. MEMORIA 3.5. SISTEMAS DE ARCHIVOS 3.6. XESTIÓN DE USUARIOS
4. REDES E COMUNICACIÓNS	4.1. INTRODUCCIÓN 4.2. MODELOS DE REFERENCIA 4.3. COMPONENTES 4.4. PROTOCOLOS 4.5. REDES SEN FÍOS
5. PONTE INTEGRADA	5.1. EQUIPOS 5.2. INTERCONEXIÓN



6. CIBERSEGURIDADE	6.1. GUIAS DA IMO 6.2. CONCEPTOS BÁSICOS 6.3. BOTNETS 6.4. HACKING DE SISTEMAS 6.5. ESPIONAXE E CIBERVIXIANCIA 6.6. ANALISIS FORENSE EN WINDOWS 6.7. CIBERSEGURIDADE EN DISPOSITIVOS IoT 6.8. MALWARE EN ANDROID
O desenvolvemento e superación destes contidos, xunto cos correspondentes a outras materias que inclúan a adquisición de competencias específicas da titulación, garanten o coñecemento, comprensión e suficiencia das competencias recollidas no cadro AII/2, do Convenio STCW, relacionadas co nivel de xestión de Primeiro Oficial de Ponte da Mariña Mercante, sen limitación de arqueo bruto e Capitán da Mariña Mercante ata o máximo de 3000 GT.	Cadro A-II/2 del Convenio STCW. Especificación de las normas mínimas de competencia aplicables a Capitáns y primeiros oficiais de ponte de buques de arqueo bruto igual ou superior a 500 GT.

Planning				
Methodologies / tests	Competencies / Results	Teaching hours (in-person & virtual)	Student?s personal work hours	Total hours
Guest lecture / keynote speech	A54 A58 B34 B36	28	56	84
Problem solving	B31 B32	2	4	6
Multiple-choice questions	B34 B36	2	4	6
ICT practicals	B31 B34 B35	2	2	4
Supervised projects	A54 B33 B34	2	2	4
Case study	A57 A59 B32 B35 B97 B98 C15	10	10	20
Laboratory practice	A57 B31 B32 B33 B35	8	8	16
Mixed objective/subjective test	B31 B32 B34 B35 B36 B97 B98	1	3	4
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	Realizarase unha explicación introdutoria dos contidos de cada tema. Proporcionaránselle ao alumnado ou ben materiais ou ben indicacións de como consultar fontes adicionais para profundar no estudo do tema. Os conceptos básicos serán traballados individualmente polo alumno no aula contando coa asistencia do profesor e utilizando exercicios ou titoriais que este previamente terá preparados na plataforma de aprendizaxe da universidade. Ademais tamén se lles proporcionarán vídeos que poden visualizar de maneira asíncrona.
Problem solving	As clases maxistras do primeiro tema combinaranse coa resolución de problemas escritos no aula, debatendo as solucións co alumnado para afianzar os coñecementos matemáticos nos que se basea o funcionamento das computadoras.
Multiple-choice questions	Ó final dalgunhas sesións maxistras o alumnado terá que responder a unha serie de preguntas tipo test relacionadas coa materia tratada na sesión
ICT practicals	Levaranse a cabo prácticas sobre a utilización da terminal de comandos do sistema operativo.
Supervised projects	Proporase a elaboración dun traballo práctico sobre busca de compoñentes hardware en catálogos web para a instalación e configuración dun equipo informático.
Case study	Exporanse distintos casos de ciberseguridade que o alumnado debe analizar, estudar como se producen e ver as solucións que se poden adoptar para evitalos.



Laboratory practice	Tratase de poñer en práctica os coñecementos teóricos adquiridos, para o cal probarase como se ensamblan os equipos informáticos, como se instala e configura o S.O., e como se conectan entre si para formar unha rede de ordenadores. Estas prácticas levaranse a cabo nun laboratorio (taller de montaxe).
Mixed objective/subjective test	A primeira parte da proba consistirá nun cuestionario sobre as competencias teóricas tratadas nas clases maxistras. A segunda parte da proba consistirá nun exercicio práctico sobre as competencias traballadas ao longo do curso nas clases interactivas e clases de prácticas.

Personalized attention	
Methodologies	Description
Case study Problem solving Laboratory practice ICT practicals Supervised projects Mixed objective/subjective test Multiple-choice questions	A atención personalizada é imprescindible para dirixir ao alumnado na realización dos problemas propostos e para as prácticas no Aula de Informática. Realizarase no despacho do profesorado nos horarios de tutorías establecido a comezo de curso e posto en coñecemento do alumnado polos medios apropiados no centro e na plataforma de teleaprendizaxe da universidade. Ademais o profesorado tamén poderá resolver as dúbidas recibidas por medios electrónicos como correo electrónico ou foros creados a tal efecto na plataforma de teleaprendizaxe da universidade, ou videoconferencias a través de Teams.

Assessment			
Methodologies	Competencies / Results	Description	Qualification
Case study	A57 A59 B32 B35 B97 B98 C15	Exporanse distintos casos de ciberseguridade que o alumnado debe analizar, estudar como se producen e ver as solucións que se poden adoptar para evitalos, contestando a un cuestionario final.	25
Problem solving	B31 B32	Farase unha proba de resolución de problemas relacionados co primeiro tema da materia.	15
Laboratory practice	A57 B31 B32 B33 B35	Probarase como se ensamblan os equipos informáticos, como se instala e configura o S.O., e como se conectan entre si para formar unha rede de ordenadores, avaliando o traballo desenvolvido por cada alumno no laboratorio.	25
ICT practicals	B31 B34 B35	Realizarase unha práctica sobre a utilización da terminal de comandos do sistema operativo.	15
Supervised projects	A54 B33 B34	Levarase a cabo unha práctica sobre a busca de compoñentes hardware en catálogos web para a instalación e configuración dun equipo informático.	10
Multiple-choice questions	B34 B36	Ó final dalgunhas sesións maxistras o alumnado terá que responder a unha serie de preguntas tipo test relacionadas coa materia tratada na sesión	10

Assessment comments



PRIMEIRA OPORTUNIDADE: Avaliarase mediante Avaliación Continua tal e como se especifica a continuación: Solución de problemas (15%) Cuestionarios tipo test (10%) Prácticas a través de TIC (15%) Traballos tutelados (10%) Estudo de casos (25%) Prácticas de laboratorio (25%) Para superar a materia por avaliación continua será preciso obter:

Nota mínima final de 50 puntos
 Nota mínima nos casos de estudo de 10 puntos
 Nota mínima nas prácticas de laboratorio de 15 puntos.
 Na data do exame final poderanse recuperar as partes suspensas correspondentes a: Solución de problemas (15%) Prácticas a través de TIC (15%) Estudo de casos (25%) Prácticas de laboratorio (5%)
SEGUNDA OPORTUNIDADE: Avaliarase cunha proba mixta, na que se poderá recuperar o 100% da nota, e que consistirá en: Proba mixta sobre as competencias teóricas tratadas nas clases maxistras (50%). Exercicio práctico sobre as competencias traballadas ao longo do curso nas clases interactivas e clases prácticas (50%). Para superar a materia na segunda oportunidade será preciso obter: Nota mínima na proba mixta de 20 puntos
 Nota mínima no exercicio práctico de 20 puntos

OBSERVACIONES:

Para o alumnado con recoñecemento de dedicación a tempo parcial e dispensa académica de exención de asistencia, segundo establece a "NORMA QUE REGULA O RÉXIME DE DEDICACIÓN AO ESTUDO DOS ESTUDANTES DE GRAO E MÁSTER UNIVERSITARIO NA UDC (Arts. 2.3; 3.b; 4.3 e 7.5) (04/05/2017):

Na primeira oportunidade se lles avaliará cunha proba mixta e un exercicio práctico seguindo os mesmos criterios que se especifican para todo o alumnado na segunda oportunidade. A realización fraudulenta das probas ou actividades de avaliación, unha vez comprobada, implicará directamente a cualificación de ?suspense? (nota numérica 0) na convocatoria correspondente do curso académico, tanto se a comisión da falta se produce na primeira oportunidade como na segunda. Para isto, procederase a modificar a súa cualificación na acta de primeira oportunidade, se fose necesario. Os criterios de avaliación contemplados no cadro A-II/1 do Código STCW e recollido no Sistema de Garantía de Calidade teranse en conta á hora de deseñar e realizar a avaliación.

Sources of information

Basic	- Beekman, G (2005). Introducción a la informática. Madrid: Pearson Educación - Bigelow, S.J. (2003). Localización de averías, reparación, mantenimiento y optimización de redes. Madrid: McGraw Hill - BIMCO (2019). Cyber Security Workbook for On Board Ship Use. Livingston, Scotland: Witherby Publishing - Davis, C (2005). Hacking exposed. Computer forensics secrets & solutions. Emeryville, USA: 2005 - Delgado, J.M. (2016). Windows 10. Madrid: ANAYA - Derfler, F.J. (1993). Así funcionan las comunicaciones. Madrid: ANAYA - Díaz, J.M. (2004). Fundamentos de redes inalámbricas. Madrid: Pearson Educación - Dordogne, J. (2015). Redes informáticas. Nociones fundamentales. Barcelona: Ediciones ENI - Floyd, T.L. (2006). Fundamentos de Sistemas Digitales. Madrid: Prentice Hall - Halsall (2006). Redes de computadores e Internet. Madrid: Pearson Educación - Herreras, J.E. (2012). El PC. Hardware y componentes. Madrid: ANAYA - Oncins, A. (2015). Seguridad informática. Hacking ético. Barcelona: Ediciones ENI - Prieto, A. (2005). Conceptos de informática. Madrid: McGraw-Hill
--------------	--



Complementary	- Abelar, G. (2005). Securing your business with Cisco ASA and PIX firewalls. Indianapolis: Cisco Press - Aziz, Z (2002). Troubleshooting IP Routing Protocols. Indianapolis: Cisco Press - Bardot, Y; Gaumé, S (2018). Mantenimiento y reparación de un PC en red. Barcelona: Ediciones ENI - Benjamin, H (2005). CCIE Security exam certification guide. Indianapolis: Cisco Press - Bhaiji, Y (2004). CCIE Security Practice Labs. Indianapolis: Cisco Press - Dhanjani, N (2003). Claves hackers en Linux y Unix. Madrid: McGraw Hill - Dunham, K. (2009). Mobile malware attacks and defense. Burlington, USA: Elsevier, Inc - Dwivedi, H. (2010). Mobile application security. USA: McGraw Hill - Fernández, J.A. (2019). Internet segur@. Madrid: ANAYA - Hoda, M. (2005). Cisco Network Security Troubleshooting Handbook. Indianapolis: Cisco Press - Lewis, M. (2004). Troubleshooting Virtual Private Networks. Indianapolis: Cisco Press - Lucas, M.W. (2010). Network flow analysis. San Francisco, USA: William Pollock - Odom, W (2014). Cisco CCNA Routing and Switching. Madrid: Pearson Educación - Provos, N.; Holz, T. (2008). Virtual Honeypots. From botnet tracking to intrusion detection. Boston, USA: Pearson Education - Sportack, M.A. (1999). Fundamentos de enrutamiento IP. Madrid: Pearson Educación - Ujaldón, M. (2001). Arquitectura del PC. Madrid: Editorial Ciencia-3
----------------------	--

Recommendations

Subjects that it is recommended to have taken before

Mathematics I/631G01101

Subjects that are recommended to be taken simultaneously

Mathematics II/631G01106

English I/631G01108

Subjects that continue the syllabus

Electricity and Electronics/631G01206

Applied Informatics/631G01501

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.