UNIVERSIDADE DA CORUÑA

Teaching Guide				
Identifying Data				2021/22
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	Vidal Paz, Jose	E-mail	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. Asimesmo, tamén publica as "Guías sobre gestión del riesgo cibernético?, que proporcionan recomendacions 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 comenzou a dar unha maior importancia á seguridade dos seus sistemas IT/OT. As competencias adquiridas nesta materia serán de gran importancia para o desenrolo da profesión dos futuros egresados en Náutica, porque poseerán 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, 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.				
Contingency plan	1. Modifications to the contents 2. Methodologies *Teaching methodologies that are maintained *Teaching methodologies that are modified 3. Mechanisms for personalized attention to students 4. Modifications in the evaluation *Evaluation observations: 5. Modifications to the bibliography or webgraphy				

Study programme competences	
Code	**Study programme competences**
A7	Ensamblar e realizar tarefas básicas de mantemento e reparación de equipos informáticos. Instalar e manexar sistemas operativos e aplicacións informáticas. Instalar e realizar as tarefas básicas de xestión de redes de ordenadores.
B2	Resolver problemas de xeito efectivo.
B5	Traballar de forma autónoma con iniciativa.
B6	Traballar de forma colaboradora.
B8	Aprender en ámbitos de teleformación.
B10	Versatilidade.
B11	Capacidade de adaptación a novas situacións.
B12	Uso das novas tecnoloxías TIC, e de Internet como medio de comunicación e como fonte de información.
B19	Utilizar as ferramentas básicas das tecnoloxías da información e as comunicacións (TIC) necesarias para o exercicio da súa profesión e para a aprendizaxe ao longo da súa vida.
C3	Utilizar as ferramentas básicas das tecnoloxías da información e as comunicacións (TIC) necesarias para o exercicio da súa profesión e para a aprendizaxe ao longo da súa vida.
C6	Valorar criticamente o coñecemento, a tecnoloxía e a información dispoñible para resolver os problemas cos que deben enfrontarse.
C9	Posuír e comprender coñecementos que aporten unha base ou oportunidade de ser originais no desenvolvemento e/ou aplicación de ideas, a miúdo nun contexto de investigación
C13	Que os estudantes posúan as habilidades de aprendizaxe que lles permitan continuar estudando dun modo que haberá de ser en grande medida autodirixido ou autónomo.

Learning outcomes			
Learning outcomes	**Study programme competences**		
Coñecer distintos métodos de representación e cifrado da información			
Coñecer a estructura básica dunha computadora e a suas diferentes arquitecturas.	A7	B8 B12	
Ser capaz de ensamblar, detectar e reparar fallos hardware nun equipo informático.	A7	B2 B6 B10 B11	
Coñecer o funcionamento e os servizos dun sistema operativo.	A7	B19	C3
Ser capaz de instalar e configurar un sistema operativo, establecendo unha xerarquía de usuarios cos seus correspondentes permisos.	A7	B2 B5 B6 B10 B11 B19	C3 C6
Ser capaz de instalar e configurar unha rede de equipos informáticos, establecendo as medidas de seguridade adecuadas para a mesma.			
Coñecer os equipos que forman parte dun IBS/INS e a sua configuración.		B12 B19	C3 C6
Identificar vulnerabilidades nos sistemas, equipos e datos necesarios para as operacions a bordo dun buque.	A7	B2 B5 B10 B11 B19	C3 C6 C9 C13

Aplicar medidas de protección e detección ante un incidente de ciberseguridad.	A7	B2 B5 B10 B11 B19	C3 C6 C9 C13
Poñer en práctica plans de continxencia para responder ante un incidente e poder recuperar os sistemas e equipos afectados ao seu estado orixinal de funcionamento.	A7	B2 B5 B6 B10 B11 B19	C3 C6 C9 C13

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 ARQUIVOS 3.6. XESTIÓN DE USUARIOS
4. REDES E COMUNICACIÓNS	4.1. INTRODUCCION 4.2. MODELOS DE REFERENCIA 4.3. COMPOÑENTES 4.4. PROTOCOLOS 4.5. REDES INALÁMBRICAS
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. CIBERSEGURIDADE EN DISPOSITIVOS IoT 6.7. SEGURIDADE WIFI

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**	**Ordinary class hours**	**Student?s personal work hours**	**Total hours**
Guest lecture / keynote speech	B8 B12 C13	28	56	84
Problem solving	B2 B5 B19	2	4	6
ICT practicals	A7 B5 B6 B19 C3	2	2	4
Supervised projects	A7 B5 B6 B12	2	2	4
Case study	B2 B5 B8 B19 C3 C6 C9 C13	10	10	20
Laboratory practice	A7 B6 B10 B11 B12 B19 C3	8	8	16
Mixed objective/subjective test	B2 B10 B19 C3 C6	1	3	4
Personalized attention		12	0	12
(*)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 profundizar no estudo do tema. Os conceptos básicos serán traballados individualmente polo alumno no aula contando coa asistencia do profesor e utilizando exercícios ou tutoriais que este previamente terá preparados na plataforma de aprendizaxe da universidade. Ademáis tamén se lles proporcionarán vídeos que poden visualizar de maneira asíncrona.
Problem solving	As clases maxistrais do primeiro tema combinaránse coa resolución de problemas escritos no aula, debatindo as solucións co alumnado para afianzar os coñecementos matemáticos nos que se basea o funcionamento das computadoras.
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 búsqueda 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, estudiar cómo se producen y ver as solucions que se poden adoptar para evitalos.
Laboratory practice	Tratase de poñer en práctica os coñecementos teóricos adquiridos, para o cal probarase cómo se ensamblan os equipos informáticos, cómo se instala e configura o S.O., e cómo se conectan entre sí 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 magistrais. 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	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 titorías 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	Description	Qualification
Case study	B2 B5 B8 B19 C3 C6 C9 C13	Exporanse distintos casos de ciberseguridade que o alumnado debe analizar, estudar cómo se producen e ver as solucións que se poden adoptar para evitalos, contestando a un cuestionario final.	25
Problem solving	B2 B5 B19	Farase unha proba de resolución de problemas relacionados co primeiro tema da materia.	15
Laboratory practice	A7 B6 B10 B11 B12 B19 C3	Probarase cómo se ensamblan os equipos informáticos, cómo se instala e configura o S.O., e como se conectan entre sí para formar unha rede de ordenadores, evaluando o traballo desenvolvido por cada alumno no laboratorio.	35
ICT practicals	A7 B5 B6 B19 C3	Realizarase unha práctica sobre a utilización da terminal de comandos do sistema operativo.	15
Supervised projects	A7 B5 B6 B12	Levarase a cabo unha práctica sobre a búsqueda de compoñentes hardware en catálogos web para a instalación e configuración dun equipo informático.	10

Assessment comments

AVALIACIÓN CONTINUA:

Solución de problemas (15%)Prácticas a través de TIC (15%)Traballos tutelados (10%)Estudo de casos (25%)Prácticas de laboratorio (35%)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.PRIMEIRA OPORTUNIDADE:Poderanse recuperar as partes suspensas correspondientes a:Solución de problemas (15%)Prácticas a través de TIC (15%)Estudo de casos (25%)SEGUNDA OPORTUNIDADE:Evaluarase con unha proba mixta, na que se poderá recuperar o 100% da nota, e que consistirá en:Proba mixta sobre as competencias teóricas tratadas nas clases maxistrais (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 puntosNota mínima no exercicio práctico de 20 puntosOBSERVACIONS:

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 con unha proba mixta e un exercicio práctico seguindo os mesmos criterios que se especifican para todo o alumnado na segunda oportunidade.Os criterios de avaliación contemprados no cadro A-II/1 do Código STCW e recollido no Sistema de Garantía de Calidade teránse 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 - Dordoigne, J. (2015). Redes informáticas. Nociones fundamentales. Barcelona: Ediciones ENI - Floyd, T.L. (2006). Fundamentos de Sistemas Digitales. Madrid - Halsall (2006). Redes de computadores e Internet. Madrid: Pearson Educación - Herrerías, 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
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.