UNIVERSIDADE DA CORUÑA

Guía Docente				
Datos Identificativos				2023/24
Asignatura (*)	Informática		Código	631G03004
Titulación				
Descriptores				
Ciclo	Período	Curso	Tipo	Créditos
Grao	1º cuadrimestre	Primeiro	Formación básica	6
Idioma	CastelánGalego			
Modalidade docente	Presencial			
Prerrequisitos				
Departamento	Enxeñaría de Computadores			
Coordinación	Vidal Paz, Jose	Correo electrónico	jose.vidal.paz@udc.es	
Profesorado	Andión Fernández, José Manuel Vidal Paz, Jose	Correo electrónico	jose.manuel.andion@udc.es jose.vidal.paz@udc.es	
Web				
Descrición xeral	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 desenrolo da profesión dos futuros egresados en Máquinas Navais, porque posuirán coñecementos sobre o tipo de riscos cibernéticos ós 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 ó 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 Electrónica e Sistemas de Control (codificación da información, hardware, redes), e varias do itinerario ETO, como son Fundamentos de Programación, Electrónica Dixital ou Automatización de Instalacions do Buque. Tamén se considera que está relacionada co Inglés, pois moita da información a manexar (libros, Internet, manuais, videotitoriais, ...) atópase neste idioma.			

Competencias / Resultados do título	
Código	Competencias / Resultados do título

Resultados da aprendizaxe			
Resultados de aprendizaxe	Competencias / Resultados do título		
Coñecer distintos métodos de representación e cifrado da información		B3 B7 B16	C3
Coñecer a estrutura básica dunha computadora e a súas diferentes arquitecturas.	A22 A76	B5	C1 C3

Ser capaz de ensamblar, detectar e reparar fallos hardware nun equipo informático.	A22 A76	B2 B7 B10 B13 B15	
Coñecer o funcionamento e os servizos dun sistema operativo.	A22 A76	B5	C3
Ser capaz de instalar e configurar un sistema operativo, establecendo unha xerarquía de usuarios cos seus correspondentes permisos.	A22 A76	B7 B9 B10 B13 B15 B16	C3
Ser capaz de instalar e configurar unha rede de equipos informáticos, establecendo as medidas de seguridade adecuadas para a mesma.	A22 A76	B7 B9 B10 B13 B15 B16	C3
Coñecer os equipos que forman parte dunha Sala de Control de Máquinas e a súa configuración.		B5	C3
Identificar vulnerabilidades nos sistemas, equipos e datos necesarios para as operacións a bordo dun buque.	A22 A76	B3 B5 B7 B9 B11 B13 B15 B16	C3
Aplicar medidas de protección e detección ante un incidente de ciberseguridade.	A22 A76	B3 B5 B7 B9 B11 B13 B15 B16	C3
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.	A22 A76	B3 B5 B7 B9 B10 B11 B13 B15 B16	C3

Contidos	
Temas	**Subtemas**

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. INTRODUCCIÓN 4.2. MODELOS DE REFERENCIA 4.3. COMPOÑENTES 4.4. PROTOCOLOS 4.5. REDES SEN FIOS
5. SALA DE CONTROL DE MÁQUINAS	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 AIII/2, do Convenio STCW, relacionadas co nivel de xestión de Oficial de Máquinas de Primeira da Mariña Mercante, sen limitación de potencia da planta propulsora e Xefe de Máquinas da Mariña Mercante ata o máximo de 3000 kW.	Cadro A-III/2 del Convenio STCW. Especificación de las normas mínimas de competencia aplicables a los Jefes de máquinas y Primeros Oficiales de máquinas de buques cuya máquina propulsora principal tenga una potencia igual o superior a 3000 kW

Planificación				
Metodoloxías / probas	Competencias / Resultados	Horas lectivas (presenciais e virtuais)	Horas traballo autónomo	Horas totais
Sesión maxistral	B5 C3	28	56	84
Solución de problemas	B7 B9 C3	2	4	6
Proba de resposta múltiple	B3 B5 C3	2	4	6
Prácticas a través de TIC	A22 A76 B9 B10 C3	2	2	4
Traballos tutelados	A22 A76 B9 B10 B16 C1	2	2	4

Estudo de casos	A76 B2 B3 B5 B7 B9 B11 B13 B15 B16 C3	10	10	20
Prácticas de laboratorio	A22 A76 B10 B13 B15 B16 C3	8	8	16
Proba mixta	B7 B13 B16 C3	1	3	4
Atención personalizada		6	0	6
***Os datos que aparecen na táboa de planificación son de carácter orientativo, considerando a heteroxeneidade do alumnado**				

Metodoloxías	
Metodoloxías	**Descrición**
Sesión maxistral	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.
Solución de problemas	As clases maxistrais 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.
Proba de resposta múltiple	Ao final dalgunhas sesións maxistrais o alumnado terá que responder a unha serie de preguntas tipo test relacionadas coa materia tratada na sesión
Prácticas a través de TIC	Levaranse a cabo prácticas sobre a utilización da terminal de comandos do sistema operativo.
Traballos tutelados	Proporase a elaboración dun traballo práctico sobre busca de compoñentes hardware en catálogos web para a instalación e configuración dun equipo informático.
Estudo de casos	Exporanse distintos casos de ciberseguridade que o alumnado debe analizar, estudar como se producen e ver as solucións que se poden adoptar para evitalos.
Prácticas de laboratorio	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).
Proba mixta	A primeira parte da proba consistirá nun cuestionario sobre as competencias teóricas tratadas nas clases maxistrais. A segunda parte da proba consistirá nun exercicio práctico sobre as competencias traballadas ao longo do curso nas clases interactivas e clases de prácticas.

Atención personalizada	
Metodoloxías	**Descrición**
Solución de problemas Prácticas a través de TIC Traballos tutelados Estudo de casos Prácticas de laboratorio Proba mixta	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.

Avaliación			
Metodoloxías	**Competencias / Resultados**	**Descrición**	**Cualificación**

Proba de resposta múltiple	B3 B5 C3	Ó final dalgunhas sesións maxistrais o alumnado terá que responder a unha serie de preguntas tipo test relacionadas coa materia tratada na sesión	10
Solución de problemas	B7 B9 C3	Farase unha proba de resolución de problemas relacionados co primeiro tema da materia.	15
Prácticas a través de TIC	A22 A76 B9 B10 C3	Realizarase unha práctica sobre a utilización da terminal de comandos do sistema operativo.	15
Traballos tutelados	A22 A76 B9 B10 B16 C1	Levarase a cabo unha práctica sobre a busca de compoñentes hardware en catálogos web para a instalación e configuración dun equipo informático.	10
Estudo de casos	A76 B2 B3 B5 B7 B9 B11 B13 B15 B16 C3	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
Prácticas de laboratorio	A22 A76 B10 B13 B15 B16 C3	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

Observacións avaliación

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 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 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 ?suspenso? (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.

Fontes de información

Bibliografía básica	- 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 : Prentice Hall - 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 : McGraw-Hill
Bibliografía complementaria	- 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

Recomendacións
Materias que se recomenda ter cursado previamente
Materias que se recomenda cursar simultaneamente
Inglés Técnico Marítimo/631G03012 Matemáticas I/631G03001
Materias que continúan o temario
Fundamentos de Programación/631G03057 Automatización de Instalacións do Buque/631G03042 Electrónica Dixital/631G03032 Electrónica e Sistemas de Control/631G03016
Observacións