



Guía Docente				
Datos Identificativos				2021/22
Asignatura (*)	Informática	Código	631G01110	
Titulación				
Descritores				
Ciclo	Período	Curso	Tipo	Créditos
Grao	2º cuádrimestre	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	Vidal Paz, Jose	Correo electrónico	jose.vidal.paz@udc.es	
Web				
Descrición xeral	<p>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.</p> <p>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 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 comenzou a dar unha maior importancia á seguridade dos seus sistemas IT/OT.</p> <p>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.</p> <p>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).</p> <p>Tamén se considera que está relacionada co Inglés, pois moita da información a manexar (libros, Internet, manuais, videotutoriais, ...) atópase neste idioma.</p>			



Plan de continxencia	<p>1. Modificacións nos contidos</p> <ul style="list-style-type: none"> - Non se realizarán cambios. <p>2. Metodoloxías</p> <p>*Metodoloxías docentes que se manteñen</p> <ul style="list-style-type: none"> - Traballos tutelados (computa na avaliación) <p>*Metodoloxías docentes que se modifican</p> <ul style="list-style-type: none"> - Sesión maxistral (a través de Teams e vídeos en Sharepoint) - Solución de problemas (uso de Teams e Campus Virtual) (computa na avaliación) - Prácticas a través de TIC (uso de Teams, Campus Virtual e escritorios VDI) (computa na avaliación) - Estudo de casos (uso de Teams, Campus Virtual e escritorios VDI) (computa na avaliación) - Prácticas de laboratorio (adoptaranse as medidas sanitarias establecidas polas autoridades, reducíndose o tamaño dos grupos se fose preciso) (computa na avaliación) - Proba mixta (uso do Campus Virtual da UDC e Teams) (computa na avaliación) <p>3. Mecanismos de atención personalizada ao alumnado</p> <ul style="list-style-type: none"> - Correo electrónico: Diariamente. Uso para facer consultas, solicitar encontros virtuais para resolver dúbidas e facer seguimento da resolución de problemas e os traballos tutelados. - Campus Virtual: Diariamente. Segundo a necesidade do alumnado. Dispoñen dos contidos teóricos de todos os temas. Tamén dispoñen dos arquivos para a súa descarga nos que teñen que resolver exercicios prácticos, e vídeos de elaboración propia en Sharepoint para complementar os contidos teóricos. Ademáis, dispoñen de enlaces a páxinas web nas que poderán descargar o software opensource necesario para o seguimento da materia, así como tutoriais e vídeos. Tamén se lles proporcionan enlaces directos á bibliografía dispoñible na UDC. - Teams: 1 sesión semanal de 2 horas en grupo único para avanzar nos contidos teóricos na franxa horaria que ten asignada a materia no calendario de aulas da escola, así como para a presentación oral. Outra sesión semanal de 2 horas en grupos medianos, tamén na franxa horaria que ten asignada a materia, para o seguimento e apoio das prácticas e dos traballos tutelados. Esta dinámica permite facer un seguimento normalizado e axustado as necesidades de aprendizaxe do alumnado para desenvolver o traballo da materia. <p>4. Modificacións na avaliación</p> <ul style="list-style-type: none"> - A proba mixta pasará de ser presencial a ser on-line. <p>5. Modificacións da bibliografía ou webgrafía</p> <ul style="list-style-type: none"> - Non se realizarán cambios. Xa dispoñen de todos os materiais de traballo de maneira dixitalizada no Campus Virtual da UDC.
-----------------------------	---

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			
Coñecer a estrutura 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 operacións a bordo dun buque.	A7	B2 B5 B10 B11 B19	C3 C6 C9 C13
Aplicar medidas de protección e detección ante un incidente de ciberseguridade.	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

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. 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 arqueado 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 arqueado bruto igual ou superior a 500 GT.

Planificación				
Metodoloxías / probas	Competencias / Resultados	Horas lectivas (presenciais e virtuais)	Horas traballo autónomo	Horas totais
Sesión maxistral	B8 B12 C13	28	56	84
Solución de problemas	B2 B5 B19	2	4	6
Prácticas a través de TIC	A7 B5 B6 B19 C3	2	2	4
Traballos tutelados	A7 B5 B6 B12	2	2	4
Estudo de casos	B2 B5 B8 B19 C3 C6 C9 C13	10	10	20
Prácticas de laboratorio	A7 B6 B10 B11 B12 B19 C3	8	8	16
Proba mixta	B2 B10 B19 C3 C6	1	3	4
Atención personalizada		12	0	12

*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. Proporcionaráselle 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 exercicios ou tutoriais 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 maxistras 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.
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 búsqueda 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 cómo se producen y ver as solucións que se poden adoptar para evitalos.
Prácticas de laboratorio	Trátase 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).
Proba mixta	A primeira parte da proba consistirá nun cuestionario sobre as competencias teóricas tratadas nas clases magistras. 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
Estudo de casos	A atención personalizada é imprescindible para dirixir ao alumnado na realización dos problemas propostos e para as prácticas no Aula de Informática.
Solución de problemas	
Prácticas de laboratorio	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.
Prácticas a través de TIC	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.
Traballos tutelados	
Proba mixta	

Avaliación

Metodoloxías	Competencias / Resultados	Descrición	Cualificación
Estudo de casos	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
Solución de problemas	B2 B5 B19	Farase unha proba de resolución de problemas relacionados co primeiro tema da materia.	15
Prácticas de laboratorio	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
Prácticas a través de TIC	A7 B5 B6 B19 C3	Realizarase unha práctica sobre a utilización da terminal de comandos do sistema operativo.	15
Traballos tutelados	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



Observacións avaliación

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 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 puntosNota 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 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 contemplados 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.

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
- 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

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
- Bhajji, 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

Matemáticas I/631G01101

Materias que se recomenda cursar simultaneamente

Matemáticas II/631G01106

Inglés I/631G01108

Materias que continúan o temario

Electricidade e Electrónica/631G01206

Informática Aplicada/631G01501

Observacións

(*A Guía docente é o documento onde se visualiza a proposta académica da UDC. Este documento é público e non se pode modificar, salvo casos excepcionais baixo a revisión do órgano competente dacordo coa normativa vixente que establece o proceso de elaboración de guías