



| Guía docente | | | | |
|-----------------------|---|--------------------|--|----------|
| Datos Identificativos | | | | 2022/23 |
| Asignatura (*) | Informática | Código | 631G03004 | |
| Titulación | Grao en Máquinas Navais | | | |
| Descritores | | | | |
| Ciclo | Periodo | Curso | Tipo | Créditos |
| Grado | 1º cuatrimestre | Primero | Formación básica | 6 |
| Idioma | CastellanoGallego | | | |
| Modalidad docente | Presencial | | | |
| Prerrequisitos | | | | |
| Departamento | Enxeñaría de Computadores | | | |
| Coordinador/a | 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 | | | | |
| Descripción general | <p>Esta materia se encuadra dentro de las materias básicas de las ingenierías, y más concretamente se considera como una materia transversal porque las competencias adquiridas son importantes para cursar la mayoría de las materias de la titulación.</p> <p>En el año 2017, el Comité de Seguridad Marítima de la IMO publica la resolución MSC.428(98) relativa a la gestión de los riesgos cibernéticos en el sector marítimo en los sistemas de gestión de seguridad, la cual ha entrado en vigor el 1 de enero de 2021. Asimismo, también publica las "Guías sobre gestión del riesgo cibernético?", que proporcionan recomendaciones que se deben adoptar a bordo de los buques. Estas nuevas necesidades surgidas en estos últimos años ha supuesto un punto de inflexión en el sector marítimo, en el cual se le ha comenzado a dar una mayor importancia a la seguridad de sus sistemas IT/OT.</p> <p>Las competencias adquiridas en esta materia serán de gran importancia para el desarrollo de la profesión de los futuros egresados en Máquinas Navales, porque poseerán conocimientos sobre el tipo de riesgos cibernéticos a los que van a estar expuestos, y serán capaces de tomar medidas preventivas, analizar registros de acceso para detectar incidentes y ejecutar una política de copias de seguridad para poder recuperar los equipos a su estado operativo inicial.</p> <p>Dentro del plan de estudios, aunque esta materia se puede considerar relacionada con casi todas las de la titulación, guarda una estrecha relación con las Matemáticas (resolución de problemas, representación e interpretación de resultados), así como con la Electricidad y Electrónica (codificación de la información, hardware, redes), y varias del itinerario ETO, como son Fundamentos de Programación, Electrónica Digital o Automatización de Instalaciones del Buque.</p> <p>También se considera que está relacionada con el Inglés, porque mucha de la información que se tiene que manejar (libros, Internet, manuales, videotutoriales, ...) se encuentran en este idioma.</p> | | | |

| Competencias del título | |
|-------------------------|--|
| Código | Competencias del título |
| A22 | CE22 - Hacer funcionar los ordenadores y redes informáticas a bordo de los buques. |
| A76 | CE76 - Ensamblar y realizar tareas básicas de mantenimiento y reparación de equipos informáticos. Instalar, manejar y restaurar un sistema operativo, gestionando una jerarquía de usuarios y realizando auditorías del mismo. Instalar y configurar una red de equipos informáticos, estableciendo distintos mecanismos de seguridad. |
| B2 | CB2 - Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio |
| B3 | CB3 - Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética |



| | |
|-----|--|
| B5 | CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía |
| B7 | CG02 - Resolver problemas de forma efectiva. |
| B9 | CG04 - Trabajar de forma autónoma con iniciativa. |
| B10 | CG05 - Trabajar de forma colaborativa. |
| B11 | CG06 - Comportarse con ética y responsabilidad social como ciudadano y como profesional. |
| B13 | CG08 - Capacidad para el aprendizaje de nuevos métodos y teorías, que le doten de una gran versatilidad para adaptarse a nuevas situaciones. |
| B15 | CG10 - Capacidad para resolver problemas con iniciativa, toma de decisiones, creatividad, razonamiento crítico y de comunicar y transmitir conocimientos habilidades y destrezas. |
| B16 | CG11 - Valorar críticamente el conocimiento, la tecnología y la información disponible para resolver los problemas con los que deben enfrentarse. |
| C1 | CT01 - Expresarse correctamente, tanto de forma oral como escrita, en las lenguas oficiales de la comunidad autónoma. |
| C3 | CT03 - Utilizar las herramientas básicas de las tecnologías de la información y las comunicaciones (TIC) necesarias para el ejercicio de su profesión y para el aprendizaje a lo largo de su vida. |

| Resultados de aprendizaje | | | |
|---|-------------------------|--------------------------------------|----------|
| Resultados de aprendizaje | Competencias del título | | |
| Conocer distintos métodos de representación y cifrado de la información | | B3 B7 B16 | C3 |
| Conocer la estructura básica de un computador y sus diferentes arquitecturas. | A22 A76 | B5 | C1 C3 |
| Ser capaz de ensamblar, detectar y reparar fallos hardware en un equipo informático. | A22 A76 | B2 B7 B10 B13 B15 | |
| Conocer el funcionamiento y los servicios de un sistema operativo. | A22 A76 | B5 | C3 |
| Ser capaz de instalar y configurar un sistema operativo, estableciendo una jerarquía de usuarios con sus correspondientes permisos. | A22 A76 | B7 B9 B10 B13 B15 B16 | C3 |
| Ser capaz de instalar y configurar una red de equipos informáticos, estableciendo las medidas de seguridad adecuadas para la misma | A22 A76 | B7 B9 B10 B13 B15 B16 | C3 |
| Conocer los equipos que forman parte de una Sala de Control de Máquinas y su configuración. | | B5 | C3 |



| | | | |
|--|------------|---|----|
| Identificar vulnerabilidades en los sistemas, equipos y datos necesarios para las operaciones a bordo de un buque. | A22 A76 | B3 B5 B7 B9 B11 B13 B15 B16 | C3 |
| Aplicar medidas de protección y detección ante un incidente de ciberseguridad. | A22 A76 | B3 B5 B7 B9 B11 B13 B15 B16 | C3 |
| Poner en práctica planes de contingencia para responder ante un incidente y poder recuperar los sistemas y equipos afectados a su estado original de funcionamiento. | A22 A76 | B3 B5 B7 B9 B10 B11 B13 B15 B16 | C3 |

| Contenidos | |
|---|--|
| Tema | Subtema |
| 1. REPRESENTACIÓN Y CIFRADO DE LA INFORMACIÓN | 1.1. REPRESENTACIÓN DE LA 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. GESTIÓN DE USUARIOS |
| 4. REDES Y COMUNICACIONES | 4.1. INTRODUCCION 4.2. MODELOS DE REFERENCIA 4.3. COMPONENTES 4.4. PROTOCOLOS 4.5. REDES INALÁMBRICAS |
| 5. SALA DE CONTROL DE MÁQUINAS | 5.1. EQUIPOS 5.2. INTERCONEXIÓN |



| | |
|---|--|
| 6. CIBERSEGURIDAD | 6.1. GUIAS DE LA IMO 6.2. CONCEPTOS BÁSICOS 6.3. BOTNETS 6.4. HACKING DE SISTEMAS 6.5. ESPIONAJE Y CIBERVIGILANCIA 6.6. ANALISIS FORENSE EN WINDOWS 6.7. CIBERSEGURIDAD EN DISPOSITIVOS IoT 6.8. MALWARE EN ANDROID |
| El desarrollo y superación de estos contenidos, junto con los correspondientes a otras materias que incluyan la adquisición de competencias específicas de la titulación, garantizan el conocimiento, comprensión y suficiencia de las competencias recogidas en el cuadro AIII/2, del Convenio STCW, relacionadas con el nivel de gestión de Oficial de Máquinas de Primera de la Marina Mercante, sin limitación de potencia de la planta propulsora y Jefe de Máquinas de la Marina Mercante hasta un máximo de 3000 kW. | Cuadro 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 | | | | |
|------------------------------|--|--------------------|--|---------------|
| Metodologías / pruebas | Competencias | Horas presenciales | Horas no presenciales / trabajo autónomo | Horas totales |
| Sesión magistral | B5 C3 | 28 | 56 | 84 |
| Solución de problemas | B7 B9 C3 | 2 | 4 | 6 |
| Prueba de respuesta múltiple | B3 B5 C3 | 2 | 4 | 6 |
| Prácticas a través de TIC | A22 A76 B9 B10 C3 | 2 | 2 | 4 |
| Trabajos tutelados | A22 A76 B9 B10 B16 C1 | 2 | 2 | 4 |
| Estudio 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 |
| Prueba mixta | B7 B13 B16 C3 | 1 | 3 | 4 |
| Atención personalizada | | 6 | 0 | 6 |

(*) Los datos que aparecen en la tabla de planificación són de carácter orientativo, considerando la heterogeneidad de los alumnos

| Metodologías | |
|------------------------------|---|
| Metodologías | Descripción |
| Sesión magistral | Se realizará una explicación introductoria de los contenidos de cada tema. Se le proporcionará al alumnado o bien materiales o bien indicaciones de cómo consultar fuentes adicionales para profundizar en el estudio del tema. Los conceptos básicos serán trabajados individualmente por el alumno en el aula contando con la asistencia del profesor y utilizando ejercicios o tutoriales que éste previamente tendrá preparados en la plataforma de aprendizaje de la universidad. Además también se les proporcionarán videos que pueden visualizar en modo asincrónico. |
| Solución de problemas | Las clases magistrales del primer tema se combinarán con la resolución de problemas escritos en el aula, debatiendo las soluciones con el alumnado para afianzar los conocimientos matemáticos en los que se basa el funcionamiento de los ordenadores. |
| Prueba de respuesta múltiple | Al inicio de cada sesión magistral el alumnado tendrá que responder a una serie de preguntas tipo test relacionadas con la materia tratada en la sesión anterior. |
| Prácticas a través de TIC | Se llevarán a cabo prácticas sobre la utilización de la terminal de comandos del sistema operativo. |



| | |
|--------------------------|---|
| Trabajos tutelados | Se propondrá la elaboración de un trabajo práctico sobre la búsqueda de componentes hardware en catálogos web para la instalación y configuración de un equipo informático. |
| Estudio de casos | Se expondrán distintos casos de ciberseguridad que el alumnado debe analizar, estudiar cómo se producen y ver las soluciones que se pueden adoptar para evitarlos. |
| Prácticas de laboratorio | Se trata de poner en práctica los conocimientos teóricos adquiridos, para lo cual se probará cómo se ensamblan los equipos informáticos, cómo se instala y configura el S.O., y cómo se conectan entre sí para formar una red de ordenadores. Estas prácticas se llevarán a cabo en un laboratorio (taller de montaje). |
| Prueba mixta | La primera parte de la prueba consistirá en un cuestionario sobre las competencias teóricas tratadas en las clases magistrales. La segunda parte de la prueba consistirá en un ejercicio práctico sobre las competencias trabajadas a lo largo del curso en las clases interactivas y clases prácticas. |

Atención personalizada

| Metodologías | Descripción |
|--|---|
| Solución de problemas Prácticas a través de TIC Trabajos tutelados Estudio de casos Prácticas de laboratorio Prueba mixta | La atención personalizada es imprescindible para dirigir al alumnado en la realización de los problemas propuestos y para las prácticas del Aula de Informática. Se realizarán en el despacho del profesorado en los horarios de tutorías establecido al inicio del curso y puesto en conocimiento del alumnado por los medios apropiados en el centro y en la plataforma de teleaprendizaje de la universidad. Además el profesorado también podrá resolver las dudas recibidas por medios electrónicos como correo electrónico, foros creados a tal efecto en la plataforma de teleaprendizaje de la universidad, o videoconferencias a través de Teams |

Evaluación

| Metodologías | Competencias | Descripción | Calificación |
|------------------------------|---------------------------------------|--|--------------|
| Prueba de respuesta múltiple | B3 B5 C3 | Al inicio de cada sesión magistral el alumnado tendrá que responder a una serie de preguntas tipo test relacionadas con la materia tratada en la sesión anterior. | 10 |
| Solución de problemas | B7 B9 C3 | Se hará una prueba de resolución de problemas relacionados con el primer tema de la materia. | 15 |
| Prácticas a través de TIC | A22 A76 B9 B10 C3 | Se realizará una práctica sobre la utilización de la terminal de comandos del sistema operativo. | 15 |
| Trabajos tutelados | A22 A76 B9 B10 B16 C1 | Se realizará una práctica sobre búsqueda de componentes hardware en catálogos web para la instalación y configuración de un equipo informático. | 10 |
| Estudio de casos | A76 B2 B3 B5 B7 B9 B11 B13 B15 B16 C3 | Se expondrán distintos casos de ciberseguridad que el alumnado debe analizar, estudiar cómo se producen y ver las soluciones que se pueden adoptar para evitarlos, contestando a un cuestionario final. | 25 |
| Prácticas de laboratorio | A22 A76 B10 B13 B15 B16 C3 | Se probará cómo se ensamblan los equipos informáticos, cómo se instala y configura el S.O., y cómo se conectan entre sí para formar una red de ordenadores, evaluando el trabajo desarrollado por cada alumno en el laboratorio. | 25 |

Observaciones evaluación



EVALUACIÓN CONTINUA:

Solución de problemas (15%) Cuestionarios tipo test (10%) Prácticas a través de TIC (15%) Trabajos tutelados (10%) Estudio de casos (25%) Prácticas de laboratorio (25%) Para superar la materia por evaluación continua será necesario obtener: Nota mínima final de 50 puntos Nota mínima en los casos de estudio de 10 puntos Nota mínima en las prácticas de laboratorio de 15 puntos. PRIMERA OPORTUNIDAD: Se podrán recuperar las partes suspensas correspondientes a: Solución de problemas (15%) Prácticas a través de TIC (15%) Estudio de casos (25%) SEGUNDA OPORTUNIDAD: Se evaluará con una prueba mixta, en la que se podrá recuperar el 100% de la nota, y que consistirá en: Prueba mixta sobre las competencias teóricas tratadas en las clases magistrales (50%). Ejercicio práctico sobre las competencias trabajadas a lo largo del curso en las clases interactivas y clases prácticas (50%). Para superar la materia en la segunda oportunidad será necesario obtener: Nota mínima en la prueba mixta de 20 puntos Nota mínima en el ejercicio práctico de 20 puntos OBSERVACIONES:

Para el alumnado con reconocimiento de dedicación a tiempo parcial y dispensa académica de exención de asistencia, según establece la "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):

En la primera oportunidad se les evaluará con una prueba mixta y un ejercicio práctico siguiendo los mismos criterios que se especifican para todo el alumnado en la segunda oportunidad. La realización fraudulenta de las pruebas o actividades de evaluación, una vez comprobada, implicará directamente la calificación de suspenso "0" en la materia en la oportunidad correspondiente, invalidando así cualquier calificación obtenida en todas las actividades de evaluación de cara a la segunda oportunidad y a la oportunidad adelantada.

Los criterios de evaluación contemplados en el cuadro A-II/1 del Código STCW, y recogido en el Sistema de Garantía de Calidad, se tendrán en cuenta a la hora de diseñar y realizar la evaluación.

Fuentes de información

| Fuentes de información | |
|------------------------|---|
| Básica | <ul style="list-style-type: none">- 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 |



| | |
|-----------------------|---|
| Complementaría | <ul style="list-style-type: none">- 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 |
|-----------------------|---|

Recomendaciones

Asignaturas que se recomienda haber cursado previamente

Asignaturas que se recomienda cursar simultáneamente

Inglés Técnico Marítimo/631G03012

Matemáticas I/631G03001

Asignaturas que continúan el temario

Fundamentos de Programación/631G03057

Automatización de Instalaciones del Buque/631G03042

Electrónica Digital/631G03032

Electrónica y Sistemas de Control/631G03016

Otros comentarios

(*) La Guía Docente es el documento donde se visualiza la propuesta académica de la UDC. Este documento es público y no se puede modificar, salvo cosas excepcionales bajo la revisión del órgano competente de acuerdo a la normativa vigente que establece el proceso de elaboración de guías