Universitat Autònoma de Barcelona

2023/2024

Información y Seguridad

Código: 102769
Créditos ECTS: 6

Titulación	Tipo	Curso	Semestre
2502441 Ingeniería Informática	OB	2	2

Contacto

Nombre: Cristina Fernandez Cordoba

Correo electrónico: cristina.fernandez@uab.cat

Idiomas de los grupos

Puede consutarlo a través de este enlace. Para consultar el idioma necesitará introducir el CÓDIGO de la asignatura. Tenga en cuenta que la información es provisional hasta el 30 de noviembre del 2023.

Equipo docente

Cristina Perez Sola

Victor García Font

Adrià Figuerola Torrell

Prerrequisitos

No hay prerequisitos. Sí que es aconsejable que el/la estudiante domine las cuestiones más básicas de algorítmica y programación. También es conveniente que el/la estudiante tenga nociones de álgebae lineal, análisis matemática y probabilidades.

Objetivos y contextualización

La asignatura "Información y Seguridad" forma parte de la MATERIA 9 : ALGORÍTMICA Y INFORMACIÓN. Algunos de los temas de los que se ocupa son: medida de la información; codificación de la fuente y del canal; criptografía; privacidad, autenticidad y accesibilidad; infraestructura de llave pública (PKI), etc.

Competencias

- Actitud personal.
- Adquirir hábitos de pensamiento.
- Capacidad para concebir, redactar, organizar, planificar, desarrollar y firmar proyectos en el ámbito de la ingeniería en informática que tengan por objeto la concepción, el desarrollo o la explotación de sistemas, servicios y aplicaciones informáticas.

- Capacidad para diseñar, desarrollar, seleccionar y evaluar aplicaciones y sistemas informáticos, asegurando su fiabilidad, seguridad y calidad, conforme a principios éticos y a la legislación y normativa vigente.
- Conocimiento y aplicación de los procedimientos algorítmicos básicos de las tecnologías informáticas para diseñar soluciones a problemas, analizando la idoneidad y complejidad de los algoritmos propuestos.

Resultados de aprendizaje

1. Desarrollar el pensamiento sistémico.
2. Desarrollar la curiosidad y la creatividad.
3. Diseñar, desarrollar, seleccionar y evaluar aplicaciones asegurando su fiabilidad y seguridad.
4. Gestionar la información incorporando de forma crítica las innovaciones del propio campo profesional, y analizar las tendencias de futuro.
5. Identificar la complejidad computacional de un algoritmo en términos de recursos de memoria y tiempo de ejecución.
6. Identificar los principales ataques que puede recibir un sistema informático, así como los posibles métodos de protección, detección y aplicación de políticas de seguridad que permitan evitar el daño al sistema o minimizar su repercusión.

Contenido

1. Motivación. Planteo de los problemas de la comunicación (1 horas)
    1. Esquema de comunicación. Elementos.
    2. Ruido, errores de transmisión.
    3. Espias: privacidad y autenticidad.
3. Conceptos básicos de teoría de la información (4 horas)
    1. Medida de la información.
    2. Modelo de Shannon de fuente discreta sin memoria.
    3. Entropía de una variable aleatoria discreta.
    4. Información mutua entre dos v.a. discretas. Capacidad de un canal.
5. Codificación de la fuente (3 horas)
    1. Códigos de longitud fixa, variable, a descodificación única e instantáneos.
    2. Primer teorema de Shannon. Existencia de códigos óptimos.
    3. Construcción de códigos óptimos: método de Huffman.
7. Compresión de datos (3 horas)
    1. Tipos de compresión.
    2. Métodos estadísticos y técnicas de diccionario.
9. Codificación del canal (3 horas)
    1. Modelos importantes de canales discretos sin memoria.
    2. Reglas de descodificación.
    3. Segundo teorema de Shannon.
11. Códigos detectores y correctores de errores (4 horas)
    1. Codificación. Códigos bloque. Errores.
    2. Códigos binarios lineales. Parámetros.
    3. Matrices generadoras y de control.
    4. Descodificación.
    5. Algunos códigos importantes.
13. Criptografía y seguridad (8 horas)
    1. Conceptos básicos. Seguridad y autenticidad.
    2. Criptografía de llave simétrica.
    3. Criptografía de llave pública.
    4. Certificadoss digitales e infrastructuras de llave pública.

Metodología

Las clases de teoría se basarán en lecciones magistrales, intentando fomentar la participación del alumnado en la resolución de problemas, ejemplos, etc. En las clases de problemas, se seguirá una lista de ejercicios que el/la estudiante intentará resolver por su cuenta. Se fomentará la exposición de la resolución de problemas por parte del alumnado. En las sesiones de prácticas se tratarán en profundidad temas relacionados: planteamiento de casos reales, ampliación de determinados temas con técnicas y algoritmos alternativos a los ya vistos. Se utilizará el Campus Virtual como medio de comunicación del profesorado y el alumnado (publicación de material, noticias, etc.).

Competencias transversales. Serán trebajadas y evaluadas en diversos momentos a lo largo del curso. Concretamente:

- T01.04 - Desarrollar el pensament sistémico: A lo largo de todo el curso, consideramos las diferentes partes que intervienen en un sistema de transmisión de la información y veremos como están relacionadas entre ellas. La evaluación de esta competencia está incluida en la evaluación de la resolución de ejercicios y en las pruebas parciales y final.

- T06.02 - Desarrollar la curiosidad y la creatividad: Especialmente, tanto en la resolución de retos que se pueden presentar a lo largo del curso como en la resolución de problemas, se pretende desarrollar la curiosidad y es
necesaria la creatividad para llevar a cabo la resolución.

- T06.04- Gestionar la información incorporando de manera crítica las innovaciones del propio campo profesional, y analizar las tendencias de futuro: En la realización de las prácticas es necesario hacer uso de técnicas quese están usando hoy en día. En esta parte valoramos cuáles son las tendencias de futuro y cómo se utilizan en la resolución de la prácticas.

Nota: se reservarán 15 minutos de una clase dentro del calendario establecido por el centro o por la titulación para que el alumnado rellene las encuestas de evaluación de la actuación del profesorado y de evaluación de la asignatura o módulo.

Actividades

Título	Horas	ECTS	Resultados de aprendizaje
Tipo: Dirigidas			
Clases de problemas	12	0,48	1, 3, 6, 5
Clases de teoría	26	1,04	1, 3, 6, 5
Prácticas obligatorias	12	0,48	1, 2, 3, 4, 6, 5
Tipo: Supervisadas			
Tutorías y consultas	17	0,68	1, 3, 6, 5
Tipo: Autónomas			
Preparación de problemas y prácticas	25	1	1, 3, 6, 5
Preparación del examen final	25	1	1, 3, 6, 5
Trabajo personal	25	1	1, 3, 6, 5

Evaluación

Las fechas de evaluación continuada se publicarán en el Campus Virtual y en las transparencias de presentación de la asignatura y pueden estar sujetas a cambios de programación por motivos de adaptación a posibles incidencias. Siempre se informará en el Campus Virtual sobre estos cambios ya que se entiende que ésta es la plataforma de intercambio de información entre profesorado y alumnado.

La evaluación de la asignatura, sobre 10 puntos, se hará de la forma siguiente:

- Dospruebas parciales individuales, 6 puntos (3 puntos cada una). Como parte de la evaluación continuada la primera prueba se hará en horas de teoría y la segunda en la fecha especificada por la coordinación. La primera prueba parcial se realizará al finalizar los primeros cinco capítulos del curso, y la segunda prueba parcial al finalizar todos los capítulos del curso. Hay que obtener como mínimo3 (de los 6) puntos para poder superar la asignatura.
- Resolución de ejercicios, 1.5 puntos. Como parte de la evaluación continuada, se tendrán que realizar activitades o bien resolver ejercicios vía cuestionarios en línea. En algún caso se podría programar alguna otra actividad de evaluación y se pondrá en conocimiento del alumnado a través del Campus Virtual.
- Prácticas obligatorias,2.5 puntos. Como parte de la evaluación continuada, se tendrán que resolver algunas prácticas en el Laboratorio. Se realizará un examen final para obtener la nota de prácticas. Hay que obtener almenos 1 punto (de los 2.5 puntos) para poder superar la asignatura.
- Examen final, 6 puntos. Quien no haya superado la asignatura a partir de las pruebas paciales individuales, y tenga un mínimo de 2.5 sobre 10 puntos de nota final de la asignatura, tendrá la opción de presentarse al examen final de la asignatura para recuperar toda la materia de la asignatura. Por lo tanto, no hay recuperación de los parciales por separado sino que el examen es de todo el curso. Hay que obtener al menos 3 puntos sobre 6 para poder superar la asignatura.

En las pruebas parciales, el examen final, la resoluciónde ejercicios y las prácticas se valorarántantolos conocimientos adquiridos así como el pensamiento lógico y sistémico en la resolución de ejercicios utilizando dichos conocimientos.

Actividades que no se pueden recuperar:

De acuerdo con la coordinación del Grado y la dirección de la Escuela de Ingeniería, las actividades siguientes no se pueden recuperar:

- Resolución de ejercicios.
- Prácticas obligatorias.

Alumnado repetidor:

En el caso de estudiantes repetidores, se podrá validar la nota de las prácticas del curso anterior, siempre que ésta sea superior o igual a 1.25 (sobre 2.5).

Integridad académica:

Sin perjuicio de otras medidas disciplinarias que se estimen oportunas, y de acuerdo con la normativa académica vigente, las actividades de evaluación (prácticas, problemas o exámenes) com irregularidades cometidas por un/a estudiante que puedan conducir a una variación de la calificación se calificarán intégramente con un cero (0). Las actividades de evaluación calificadas de esta forma y por este procedimiento no serán recuperables. Si es necesario superar cualquiera de estas actividades de evaluación para aprobar la asignatura, ésta quedará suspendida directamente, sin oportunidad de recuperarla en el mismo curso. Estas irregularidades incluyen, entre otras:

- la copia total o parcial de una práctica, informe, o cualquier otra actividad deevaluación;
- dejar copiar;
- presentar un trabajo de grupo no realizado íntegramente por los miembros del grupo;
- presentarcomo propios materiales elaborados por un tercero, aunque sean traducciones o adaptaciones, y en general trabajos con elementos no originales y exclusivos del/de la estudiante;
- uso no autorizado de IA (p. ex. Copilot, ChatGPT o equivalente);

- tener dispositivos de comunicación (como teléfonos móviles, smart watches, etc.) accesibles durante las pruebas de evaluación teórico-prácticas individuales (exámenes).

Para aprobar es necesario que la evaluación de cada una de las partes supere el mínimo exigido y que la evaluacióntotalsupere los 5 puntos. En caso de no superar la asignatura devido a que alguna deles actividades de evaluació no llegue a la nota mínima requerida, la nota numérica del expediente será el valor menor entre 4.5 y la media ponderada de las notas. Con las excepciones de que se otorgará la calificación de "no avaluable" a quien no participe en ninguna de las actividades de evaluación, y de que la nota numérica del expediente será el valor menor entre 3.0 i la media ponderada de las notas en caso que se hayan cometido irregularidades en un acto de evaluación (y por lo tanto no será posible el aprobado por compensación).

Matrícula de honor:

Para poder obtener una MH la nota final tiene que ser igual o superior a los 9 puntos. Como el número de MH no puede superar el 5% del número de estudiantes matriculados, se concederán a quien tenga las notas finales más altas. En caso de empate, se tendrán en cuenta las resoluciones de las pruebas parciales. Es importante tener en cuenta que no se hará ninguna actividad de evaluación a ningún alumno/a en un horario diferente del establecido si no existe una causa justificada, se ha avisado con anterioridad a la actividad y el profesorado hadado su consentimiento. En cualquier otro caso, si el estudiante no ha asistido a una actividad, ésta no se puede recuperar.

Realización y revisión de las actividades de evaluación:

En el caso de evaluaciones en línea de cuestionarios, se podrá pedir una revisión posteriormente a la fecha de cierre del cuestionario. Para el resto de actividades de evaluación, se indicará un lugar, fecha y hora de revisión en la que el estudiante podrá revisar la actividad con el/la profesor/a. En estecontexto, se podrán hacer reclamacionessobre la nota de la actividad, que serán evaluadas por el profesorado responsable dela asignatura. Si el estudiante no se presenta a esta revisión, no se revisará posteriormente esta actividad.

Evaluación única:

Esta asignatura no prevee evaluación única.

Podéis consultar la normativa académica de la UAB aprobada por el Consejo de Gobierno de la UAB: http://webs2002.uab.es/afers_academics/info_ac/0041.htm

Actividades de evaluación continuada

Título	Peso	Horas	ECTS	Resultados de aprendizaje
Exament final	6	2	0,08	1, 3, 4, 6, 5
Pruebas individuales de evaluación continuada	6	3	0,12	1, 3, 5
Prácticas obligatorias	2.5	2	0,08	1, 2, 3, 4, 6, 5
Resolución de ejercicios	1.5	1	0,04	1, 3, 6, 5

Bibliografía

Bibliografía básica

- L. Huguet i J. Rifà. Comunicación Digital. Ed. Masson, 1991.
- D. Salomon: Data compression - The Complete Reference, 4th Edition. Springer 2007.
- R.B. Ash. Information Theory. John Wiley and Sons Inc, 1965.
- G. Alvarez. Teoría matemática de la información. Ediciones ICE, 1981.
- T.C. Bell, J.G. Cleary i I.H. Witten. Text Compression. Prentice Hall, 1990.
- J. Domingo i Ferrer and J. Herrera i Joancomartí, Criptografia per als Serveis Telemàtics i el Comerç Electrònic, Col·lecció Manuals no. 31, Barcelona: Editorial UOC, 1999. ISBN 84-8429-007-7.

- A. Menezes, P. van Oorschot and S.Vanstone.: Handbook of Applied Cryptography, CRC Press. (1996). Available at http://www.cacr.math.uwaterloo.ca/hac .

Bibliografía complementaria

- C.E. Shannon, "A mathematical theory of communications," Bell Syst. Tech. J., 27, 379-423, 1948.
- B. McMillan, "The basic theorems of Information Theory," Ann. Math. Stat., 24, 196-219, 1953.
- A.I. Khinchin. Mathematical foundations of Information Theory. Dover Publications, Inc., 1957.
- R. W. Hamming. Coding and Information Theory. Prentice Hall, Inc., 1980.
- M. Mansuripur. Introduction to Information Theory. Prentice Hall, Inc., 1987.
- G.J. Chaitin. Algorithmic Information Theory. Cambridge University Press., 1987.
- An Introduction to Computer Security: The NIST Handbook. Special Publication 800-12. NIST(1995). http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf
- D. E. Robling Denning. Cryptography and Data Security. Addison-Wesley Publishing Company (1988).
- B. Schneier. Applied Criptography, John Wiley and Sons, Inc. 1996.
- G.S. Simmons. Contemporary Criptology. The Science of Information Integrity, IEEEPress (1991).
- R. Anderson. Security Engineering: A Guide to Building Dependable Distributed System,Wiley (2001).
- C.P. Pfleeger. Security in Computing. , Prentice Hall (1997).
- V. Shoup. A computational Introduction tonumber theory and Algebra. http://shoup.net/ntb/

Software

Las actividades prácticas se realizarán en un entorno dockertzado, con contenedores de Jupyter Notebook que contendrán como kernel una de las últimas versiones de SageMath.

SageMath es un sistema de software matemático de código abierto con licencia GPL. Se basa en muchos paquetes de código abierto existentes: NumPy, SciPy, matplotlib, Sympy, Maxima, GAP, FLINT, R y muchos más. Acceda a su poder combinado a través de un lenguaje común basado en Python o directamente a través de interfaces o envoltorios. Desde la versión 9.0 lanzada en enero de 2020, SageMath está usando Python 3. . (https://www.sagemath.org/)

Jupyter Notebook es un proyecto dirigido por la comunidad con el objetivo de "desarrollar un programario de código abierto, estándares abiertos y servicions para la informática interactiva de docenas de lesnguages de programación". (https://jupyter.org/)
Docker es un proyecto de código abierto que automatiza el despliegue de aplicaciones dentro de contenedores de programario, proporcionando así una capa adicional de abstracción y automatización de virtualización de aplicaciones en diferentes sistemas operativos.(https://www.docker.com/resources/what-container/)