

Titulación	Tipo	Curso
Ingeniería Informática	OB	3
Ingeniería Informática	OP	4

Profesor/a de contacto

Nombre : Jordi Herrera Joancomarti

Correo electrónico : jordi.herrera@uab.cat

Equipo docente

Mercè Villanueva Gay

Carlos Garrigues Olivella

Sergi Sánchez Aragón

Idiomas de los grupos

Puede consultar esta información al [final](#) del documento.

Prerrequisitos

No existen prerrequisitos formales pero se recomienda haber aprobado la asignatura de "Información y Seguridad".

Objetivos

La asignatura "Fundamentos de tecnologías de la Información" forma parte de la MATERIA 29: TECNOLOGÍA DE LA INFORMACIÓN. Algunos temas tratados en esta asignatura son el papel de las TICs en las organizaciones, el tratamiento de la información, la criptografía avanzada y sus aplicaciones y servicios. Por un lado, esta asignatura constituye una continuación a los temas de seguridad vistos en la asignatura "Información y Seguridad" y por otra parte, desarrolla las bases teóricas que se aplican en la asignatura "Garantía de la Información y Seguridad".

Resultados de aprendizaje

1. Aplicar las técnicas de evaluación de costes, gestión del tiempo, gestión de recursos y planificación en el entorno de las tecnologías de información.
2. Trabajar de forma autónoma.
3. Saber proteger el acceso y la seguridad en sistemas de tratamiento de la información.
4. Identificar las disposiciones normativas aplicables en los desarrollos de tecnologías de información.

5. Conocer y comprender las necesidades en el ámbito de las TICs de una organización.
6. Evaluar y operar un sistema de aplicaciones o servicios de comunicación distribuida.
7. Conocer los sistemas de información y aplicarlos para satisfacer necesidades de las organizaciones.
8. Incorporar sistemas distribuidos de tratamiento de la información en una organización para incrementar la capacidad operativa.
9. Prevenir y solucionar problemas.
10. Desarrollar el pensamiento científico.

Contenidos

1. El papel de las TICs

- TICs en las organizaciones

2. Fundamentos

- Aritmética modular
- Polinomios sobre GF(2)

3. Tratamiento de la información

Códigos cíclicos

CRC y LFSR

4. Criptografía avanzada

Criptografía de clave pública

Funciones hash

Protocolos criptográficos

5. Aplicaciones y servicios

Tecnología Blockchain

Criptomonedas: Bitcoins

Actividades formativas y Metodología

Título	Horas	ECTS	Resultados de aprendizaje
Clases de teoría	26	1,04	1, 2, 3, 4, 5, 6, 7, 8, 10
Preparación de problemas y prácticas	25	1	1, 2, 3, 5, 6
Tutorías y consultas	17	0,68	1, 2, 3, 5, 7
Clases de problemas	12	0,48	2, 3, 7, 9
Preparación exámenes	25	1	1, 2, 3, 5, 6
Trabajo personal	25	1	1, 2, 3, 5, 6, 9, 10
Prácticas obligatorias	12	0,48	1, 2, 3, 4, 5, 7, 10

Las clases de teoría se basarán en lecciones magistrales, si bien se fomentará la participación del estudiantado en la resolución de ejemplos, etc. En las clases de problemas se seguirá una lista de ejercicios

que el estudiantado intentará resolver por su cuenta. Se fomentará la exposición de la resolución de problemas por parte del estudiantado. 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.

A lo largo del curso se llevarán a cabo las siguientes actividades:

- Clases magistrales: se presentará la teoría acompañada de varios ejercicios de ejemplo y se intentará fomentar la participación del estudiantado en su resolución.
- Clases de problemas: son sesiones con el grupo entero o bien con grupos reducidos con el objetivo de poder aplicar la teoría a la resolución de problemas. El alumnado dispondrá desde el inicio del curso, de un listado de problemas que deberá resolver. El profesorado también puede pedir la resolución de algunos ejercicios (de manera individual) antes del seminario y proceder a la discusión de su resolución durante estas sesiones. Estas sesiones deben servir para promover, principalmente, la capacidad de análisis y síntesis, el razonamiento crítico, la resolución de problemas y el trabajo en grupo.
- Sesiones de prácticas: de asistencia obligatoria, se tratarán en profundidad temas relacionados con los expuestos en teoría. Se incide en el planteamiento de casos reales, la ampliación de determinados temas con técnicas y algoritmos alternativos. Se trabaja en grupos de dos personas.

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.

Evaluación

Actividades de evaluación continuada

Título	Peso	Horas	ECTS	Resultados de aprendizaje
Resolución de ejercicios	1	1	0,04	1, 2, 3, 4, 5, 6, 7, 8
Pruebas individuales. Evaluación continua	6	3	0,12	1, 3, 4, 5, 6, 7, 8
Prácticas obligatorias	3	2	0,08	3, 5, 7, 9, 10
Examen final	6	2	0,08	1, 2, 3, 4, 5, 6, 7, 8

Las fechas de evaluación continua se publicarán en el campus virtual y en las transparencias de presentación de la asignatura, y podrán estar sujetas a cambios de programación por motivos de adaptación a posibles incidencias. Estos cambios se comunicarán siempre a través del campus virtual de la UAB, ya que se entiende que esta es la plataforma habitual de intercambio de información entre el profesorado y el estudiantado.

La evaluación de la asignatura, sobre 10 puntos, se realizará de la siguiente manera:

- Parte teórica (7 puntos): Para superar la asignatura será necesario obtener al menos 3,5 de los 7 puntos correspondientes a la parte teórica para que esta pueda hacer media con la parte práctica. La evaluación de la parte teórica del curso se divide en dos apartados:
- Exámenes (6 puntos): Dos pruebas parciales individuales por un total de 6 puntos (3 puntos cada una). Como parte de la evaluación continua, estas pruebas se realizarán durante las sesiones de teoría. Cada prueba evaluará de forma independiente una parte del temario y la nota final será la media aritmética de ambas. Cada prueba solo podrá hacer media si obtiene una calificación superior a 4 sobre 10. En caso de que alguna de las pruebas no alcance una nota superior a 4, las pruebas parciales se considerarán suspendidas.
- Ejercicios (1 punto): Como parte de la evaluación continua, se realizarán actividades y ejercicios en el aula y/o en línea, que deberán entregarse según las indicaciones proporcionadas. Estos ejercicios no serán recuperables.

- Prácticas obligatorias (3 puntos): Como parte de la evaluación continua, deberán resolverse diversas prácticas en el Laboratorio Integrado. Las prácticas deberán entregarse en las fechas indicadas en el campus virtual, pero su evaluación se realizará única y exclusivamente mediante un examen que tendrá lugar durante la sesión de prácticas posterior a aquella en la que se haya realizado cada práctica (en el caso de la última práctica, esta evaluación se llevará a cabo el mismo día del segundo examen parcial del curso). En estas pruebas se evaluará la asimilación tanto de los conceptos teóricos como de los prácticos asociados a cada actividad. Será necesario obtener al menos 1,5 puntos de los 3 correspondientes a las prácticas para poder superar la asignatura.

El estudiantado que haya suspendido la parte teórica de la asignatura tendrá la opción de presentarse al examen final, en el que se evaluará TODO el temario del curso, independientemente de las calificaciones obtenidas en las pruebas parciales. La nota de este examen de recuperación será la que se tendrá en cuenta como nota de exámenes para el cálculo de la calificación final de la asignatura; es decir, tendrá un peso del 60 % sobre la nota final. Para superar la asignatura será necesario que la nota del examen de recuperación, sumada a la nota de los ejercicios, sea superior a 5 sobre 10.

El estudiantado que desee mejorar la nota obtenida en las pruebas parciales podrá presentarse al examen final. En este caso, el simple hecho de entregar el examen y que el profesorado lo corrija implicará la sustitución de las calificaciones obtenidas previamente en las pruebas parciales.

La recuperación de las prácticas se realizará mediante un único examen de recuperación que incluirá los contenidos de todas las prácticas del curso. En este examen, la nota máxima que podrá obtenerse será de 7,5 sobre 10.

La entrega de los ejercicios no podrá recuperarse.

Para cada actividad de evaluación se indicará un lugar, una fecha y una hora de revisión en la que el estudiantado podrá revisar la actividad junto con el profesorado. En este contexto, podrán presentarse reclamaciones sobre la calificación de la actividad, que serán evaluadas por el profesorado responsable de la asignatura. Si el estudiante no asiste a esta revisión, la actividad no será revisada posteriormente.

Esta asignatura no contempla el sistema de evaluación única.

El alumnado que ya haya cursado previamente la asignatura y tenga las prácticas superadas conservará la nota de prácticas. No obstante, es importante que se ponga en contacto con el profesorado responsable de prácticas al inicio del curso (cuando se organizan los grupos de prácticas) para informar de esta circunstancia. En ningún caso se conservarán las calificaciones de los exámenes de teoría ni las de las entregas de problemas realizadas durante el curso.

Sin perjuicio de otras medidas disciplinarias que puedan considerarse oportunas y de acuerdo con la normativa académica vigente, las irregularidades cometidas por un estudiante que puedan dar lugar a una alteración de la calificación serán calificadas con un cero (0). Las actividades de evaluación calificadas de esta forma y por este procedimiento no serán recuperables. Si fuera necesario superar alguna de estas actividades para aprobar la asignatura, esta quedará suspendida directamente, sin posibilidad de recuperación en el mismo curso. Entre estas irregularidades se incluyen, entre otras:

- La copia total o parcial de una práctica, informe o cualquier otra actividad de evaluación.
- Permitir que otro estudiante copie.
- Presentar un trabajo en grupo que no haya sido realizado íntegramente por los miembros del grupo.
- El uso no autorizado de herramientas de Inteligencia Artificial (por ejemplo, Copilot, ChatGPT o equivalentes) para resolver ejercicios, prácticas o cualquier otra actividad evaluable.
- Presentar como propios materiales elaborados por terceros, aunque sean traducciones o adaptaciones, y, en general, trabajos con elementos que no sean originales y exclusivos del estudiante.
- Tener dispositivos de comunicación (como teléfonos móviles, relojes inteligentes, etc.) accesibles durante las pruebas individuales de evaluación teórico-práctica (exámenes).
- Hablar con compañeros durante las pruebas individuales de evaluación teórico-práctica (exámenes).
- Copiar o intentar copiar de otros estudiantes durante las pruebas teórico-prácticas (exámenes).
- Utilizar o intentar utilizar escritos relacionados con la materia durante la realización de las pruebas

teórico-prácticas (exámenes), cuando estos no hayan sido autorizados expresamente.

En futuras ediciones de esta asignatura, al estudiantado que haya cometido irregularidades en un acto de evaluación no se le convalidará ninguna de las actividades de evaluación realizadas.

En resumen: copiar, dejar copiar o plagiar (o intentarlo) en cualquiera de las actividades de evaluación equivale a un SUSPENSO, no compensable y sin convalidación de partes de la asignatura en cursos posteriores.

- El alumnado que alcance el número mínimo de puntos para aprobar la asignatura, pero no haya obtenido la nota mínima exigida en alguna de las actividades de evaluación, recibirá una calificación final de 4,5. En el caso de no haber aprobado la asignatura debido a la obtención de un cero en una actividad por motivo de copia, la nota final será de 3, lo que impedirá compensar esta asignatura.
- Finalmente, obtendrán la calificación de «No evaluable» aquellos estudiantes que no se presenten a ninguna de las pruebas individuales (pruebas parciales y examen final). La participación en cualquiera de estas actividades de evaluación supondrá recibir una calificación distinta de «No evaluable».
- No se realizará ninguna actividad de evaluación en un horario distinto del establecido, salvo que exista una causa justificada, se haya comunicado con antelación a la actividad y el profesorado haya dado su consentimiento. En cualquier otro caso, si un estudiante no ha asistido a una actividad, esta no podrá recuperarse. El protocolo de «solicitud de reprogramación de actividades de evaluación» está disponible en la página web de la Escuela de Ingeniería y es de aplicación en los casos descritos en los criterios e instrucciones de evaluación del centro.
- En cuanto a las matrículas de honor, podrán concederse al estudiantado que haya superado la asignatura con una nota final igual o superior a 9. Dado que el número de matrículas de honor no puede superar el 5 % del alumnado matriculado, estas se concederán a quienes hayan obtenido las calificaciones más altas. En caso de empate, se tendrán en cuenta las soluciones propuestas en cada una de las actividades de evaluación realizadas a lo largo del curso.
- En esta asignatura se permite el uso de tecnologías de Inteligencia Artificial (IA) exclusivamente en tareas de apoyo al aprendizaje, como la búsqueda bibliográfica o de información, la corrección de textos o el estudio personal. No se permite el uso de tecnologías de IA para la resolución de actividades evaluables entregables (es decir, las prácticas, los ejercicios entregables o los exámenes). Cualquier trabajo que incluya fragmentos generados mediante IA será considerado una falta de honestidad académica y podrá conllevar una penalización parcial o total en la calificación de la actividad, o sanciones de mayor gravedad en los casos que así lo requieran.

Bibliografía

- Josep M. Basart, Josep Rifà i Mercè Villanueva: Fonaments de matemàtica discreta. Materials de la UAB. (1999). Biblioteca UAB: https://bibcercador.uab.cat/permalink/34CSUC_UAB/1eqfv2p/alma991004816599706709
- Josep Rifà i Llorenç Huguet: Comunicació Digital. Masson Ed. (1991). Biblioteca UAB: https://bibcercador.uab.cat/permalink/34CSUC_UAB/1eqfv2p/alma991002495519706709
- Victor Shoup: A computational Introduction to number theory and Algebra. (2008). <http://shoup.net/ntb/>. Biblioteca UAB: https://bibcercador.uab.cat/permalink/34CSUC_UAB/avjcib/alma991010755053206709
- Cristina Pérez Solà i Jordi Herrera Joancomartí, La criptografia que et cal saber. (2023) Disponible on-line: <https://criptografia.cat/>
- Nigel P. Smart: Cryptography Made Simple. Springer. (2016). <https://doi.org/10.1007/978-3-319-21936-3>. Biblioteca UAB: https://bibcercador.uab.cat/permalink/34CSUC_UAB/1eqfv2p/alma991006792939706709
- Christof Paar i Jan Pelzl: Understanding Cryptography: A Textbook for Students and Practitioners. Springer. (2010). <https://doi.org/10.1007/978-3-642-04101-3>. Biblioteca UAB: https://bibcercador.uab.cat/permalink/34CSUC_UAB/1eqfv2p/alma991010489805006709
- Ross Anderson: Security Engineering: A Guide to Building Dependable Distributed System, Wiley (2001). Biblioteca UAB: https://bibcercador.uab.cat/permalink/34CSUC_UAB/1c3utr0/cdi_proquest_ebookcentral_EBC6412239
- Charles P. Pfleeger: Security in Computing. Prentice Hall (1997). Biblioteca UAB: https://bibcercador.uab.cat/permalink/34CSUC_UAB/avjcib/alma991005937479706709
- Andreas M. Antonopoulos: Mastering Bitcoin. Programming the Open Blockchain. O'Reilly Media (2017)

Software

Las prácticas de la asignatura se realizarán en Python utilizando el Jupyter Notebook.

Grupos e idiomas de la asignatura

La información proporcionada es provisional hasta el 30 de noviembre. A partir de esta fecha, podrá consultar el idioma de cada grupo a través de este [enlace](#). Para acceder a la información, será necesario introducir el CÓDIGO de la asignatura

Tipo de docencia	Grupo	Idioma	Semestre	Turno
(TE) Teoría	450	Catalán	primer cuatrimestre	mañana-mixto
(PAUL) Prácticas de aula	451	Catalán	primer cuatrimestre	mañana-mixto
(PLAB) Prácticas de laboratorio	451	Catalán	primer cuatrimestre	mañana-mixto
(PAUL) Prácticas de aula	452	Catalán	primer cuatrimestre	mañana-mixto
(PLAB) Prácticas de laboratorio	452	Catalán	primer cuatrimestre	mañana-mixto
(PAUL) Prácticas de aula	453	Catalán	primer cuatrimestre	mañana-mixto
(PLAB) Prácticas de laboratorio	453	Catalán	primer cuatrimestre	mañana-mixto
(PLAB) Prácticas de laboratorio	454	Catalán	primer cuatrimestre	mañana-mixto
(PLAB) Prácticas de laboratorio	455	Catalán	primer cuatrimestre	mañana-mixto