

Titulación	Tipo	Curso
2502441 Ingeniería Informática	OB	3
2502441 Ingeniería Informática	OT	4

Contacto

Nombre: Cristina Perez Sola

Correo electrónico: cristina.perez@uab.cat

Equipo docente

Maria Merce Villanueva Gay

(Externo) Carles Garrigues Olivella

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 y contextualización

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".

Competencias

- Ingeniería Informática
- Adquirir hábitos de pensamiento.
- Adquirir hábitos de trabajo personal.

- Capacidad para comprender el entorno de una organización y sus necesidades en el ámbito de las tecnologías de la información y las comunicaciones.
- Capacidad para diseñar, desarrollar, evaluar y asegurar la accesibilidad, ergonomía, usabilidad y seguridad de los sistemas, servicios y aplicaciones informáticas, así como de la información que gestionan.
- Capacidad para seleccionar, desplegar, integrar y gestionar sistemas de información que satisfagan las necesidades de la organización, con los criterios de coste y calidad identificados.
- Conocimiento y aplicación de elementos básicos de economía y de gestión de recursos humanos, organización y planificación de proyectos, así como la legislación, regulación y normalización en el ámbito de los proyectos informáticos.

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. Conocer los sistemas de información y aplicarlos para satisfacer necesidades de las organizaciones.
3. Conocer y comprender las necesidades en el ámbito de las TICs de una organización.
4. Desarrollar el pensamiento científico.
5. Evaluar y operar un sistema de aplicaciones o servicios de comunicación distribuida.
6. Identificar las disposiciones normativas aplicables en los desarrollos de tecnologías de información.
7. Incorporar sistemas distribuidos de tratamiento de la información en una organización para incrementar la capacidad operativa.
8. Prevenir y solucionar problemas.
9. Saber proteger el acceso y la seguridad en sistemas de tratamiento de la información.
10. Trabajar de forma autónoma.

Contenido

1. El papel de las TICs
 1. TICs en las organizaciones
2. Fundamentos
 1. Aritmética modular
 2. Polinomios sobre GF(2)
3. Tratamiento de la información
 1. Códigos cíclicos
 2. CRC y LFSR
4. Criptografía avanzada
 1. Criptografía de clave pública
 2. Funciones hash
 3. Protocolos criptográficos
5. Aplicaciones y servicios
 1. Tecnología Blockchain
 2. Criptomonedas: Bitcoins

Actividades formativas y Metodología

Título	Horas	ECTS	Resultados de aprendizaje
Tipo: Dirigidas			
Clases de problemas	12	0,48	2, 8, 9, 10

Clases de teoría	26	1,04	1, 5, 2, 3, 4, 6, 7, 9, 10
Prácticas obligatorias	12	0,48	1, 2, 3, 4, 6, 9, 10
Tipo: Supervisadas			
Tutorías y consultas	17	0,68	1, 2, 3, 9, 10
Tipo: Autónomas			
Preparación de problemas y prácticas	25	1	1, 5, 3, 9, 10
Preparación exámenes	25	1	1, 5, 3, 9, 10
Trabajo personal	25	1	1, 5, 3, 4, 8, 9, 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.

Competencias transversales. En esta asignatura se trabajarán y evaluarán las siguientes competencias transversales del Grado de Ingeniería Informática:

- T01.03 - Desarrollar el pensamiento científico: se trabajará de forma más intensa en las sesiones de problemas de la asignatura donde el estudiantado deberá analizar las problemáticas presentadas y ver qué soluciones teóricas son las más adecuadas y cómo éstas se pueden aplicar.
- T02.01 - Trabajar de forma autónoma: ésta se focaliza en aquellas actividades individuales, tales como la entrega de problemas que se realiza a lo largo del curso o las pruebas individuales de la asignatura.
- T02.04 - Prevenir y solucionar problemas: se trabaja de forma más extensa en las sesiones de prácticas de la asignatura.

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

Las fechas de evaluación continua 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 a través del campus virtual de la UAB sobre estos cambios, ya que se entiende que es la plataforma habitual de intercambio de información entre profesorado y estudiantado.

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

- Parte teórica (7 puntos): Para poder superar la asignatura, es necesario superar la parte teórica de forma individual para que pueda promediar, es decir, hay que obtener al menos 3,5 puntos en la valoración total de la parte teórica. 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 separada una parte del temario y la nota final será la media aritmética de ambas pruebas. Cada prueba sólo podrá promediar en caso de que sea calificada con una nota superior a 4 sobre 10. En caso de que alguna de las pruebas no tenga una nota superior a 4, las pruebas parciales se considerarán suspendidas.
 - Ejercicios (1 punto): Como parte de la evaluación continua, se entregará la resolución de actividades o ejercicios propuestos a lo largo del curso.
- Prácticas obligatorias (3 puntos): Como parte de la evaluación continua, se tendrán que resolver algunas prácticas en el Laboratorio Integrado. Es necesario obtener al menos 1,5 puntos en la valoración de las prácticas, de los 3 sobre los que se valoran las prácticas, para poder superar la asignatura.

El estudiantado que haya suspendido la parte de teórica de la asignatura tendrá la opción de presentarse al examen final, donde se examinarán de TODO el temario del curso, independientemente de las notas obtenidas en los exámenes parciales.

El estudiantado que quiera mejorar la nota obtenida en los exámenes parciales, pueden presentarse en el examen final para mejorar la nota. En este caso, el hecho de entregar el examen y que el profesor lo corrija implicará sobrecribir las notas de los exámenes previos.

La entrega de los ejercicios y la realización de las prácticas no será posible recuperarlas.

Para cada actividad de evaluación, se indicará un lugar, fecha y hora de revisión en la que el estudiante podrá revisar la actividad con el profesorado. En este contexto, se podrán realizar reclamaciones sobre la nota de la actividad, que serán evaluadas por el profesorado responsable de la asignatura. Si el estudiantado no se presenta a esta revisión, no se revisará posteriormente esta actividad.

Esta asignatura no prevé el sistema de evaluación única.

Aquel alumnado que ya haya cursado previamente la asignatura y que tenga las prácticas superadas, se les mantendrá la nota de prácticas. Sin embargo, es importante que se pongan en contacto con el profesor de prácticas de la asignatura al inicio del curso (cuando se realizan los grupos de prácticas) para informarle de este hecho. En ningún caso se mantendrán ni las notas de los exámenes de teoría ni las de las entregas de los problemas que se realizan a lo largo del curso.

Sin perjuicio de otras medidas disciplinarias que se estimen oportunas, y de acuerdo con la normativa académica vigente, las irregularidades cometidas por un estudiante que puedan conducir a una variación de la calificación se calificarán 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, esta asignatura 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 de evaluación;
- dejar copiar;
- uso no autorizado de la IA (p. ej, Copiloto, ChatGPT o equivalentes) para resolver ejercicios, prácticas y/o cualquier otra actividad evaluable;
- presentar un trabajo de grupo no realizado íntegramente por los miembros del grupo;
- presentar como propios materiales elaborados por un tercero, aunque sean traducciones o adaptaciones, y por lo general trabajos con elementos no originales y exclusivos del estudiante;
- tener dispositivos de comunicación (como teléfonos móviles, smart watches, etc.) accesibles durante las pruebas de evaluación teórico-prácticas individuales (exámenes);
- hablar con compañeros durante las pruebas de evaluación teórico-prácticas individuales (exámenes);
- copiar o intentar copiar de otros alumnos durante las pruebas de evaluación teórico-prácticas (exámenes);
- usar o intentar usar escritos relacionados con la materia durante la realización de las pruebas de evaluación teórico-prácticas (exámenes), cuando éstos no hayan sido explícitamente permitidos.

En futuras ediciones de esta asignatura, al estudiante 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 el intento de) en cualquiera de las actividades de evaluación equivale a un SUSPENSO, no compensable y sin convalidaciones de partes de la asignatura en cursos posteriores.

El alumnado que logre el número mínimo de puntos para aprobar la asignatura, pero no haya alcanzado la nota mínima en alguna de las actividades de evaluación, será evaluado con una nota final de 4.5. En caso de que no se haya aprobado la asignatura por la calificación de un cero de una actividad por motivo de copia, la nota final de la asignatura será un 3, hecho que no permitirá compensar esta asignatura.

Por último, obtendrán la calificación de "No Evaluable" aquel estudiantado que no se presente a ninguna de las pruebas individuales (pruebas parciales y el examen final). La participación en alguna de estas actividades de evaluación supondrá recibir una calificación distinta de "No Evaluable".

No se hará ninguna actividad de evaluación a ningún alumno en un horario diferente al establecido a menos que exista una causa justificada, se ha avisado con anterioridad a la actividad y el profesor ha dado su consentimiento. En otro caso, si un alumno no ha asistido a una actividad, ésta no se puede recuperar.

En cuanto a las matrículas de honor, éstas 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 estudiantado matriculado, se concederán a las personas con notas más altas. En caso de empate, se tendrá en cuenta las soluciones propuestas en cada una de las actividades de evaluación realizadas a lo largo del curso.

Bibliografía

- Josep M. Basart, Josep Rifà y Mercè Villanueva: Fonaments de matemàtica discreta. Materials de la UAB. (1999).
- Josep Rifà y Llorenç Huguet: Comunicació Digital. Masson Ed. (1991).
- Victor Shoup: A computational Introduction to number theory and Algebra. (2008). <http://shoup.net/ntb/>
- Cristina Pérez Solà y Jordi Herrera Joancomartí, La criptografia que et cal saber. (2023) Disponible on-line: <https://criptografia.cat/>
- Nigel P. Smart: Cryptography Made Simple. Springer. (2016)
- Christof Paar y Jan Pelzl: Understanding Cryptography: A Textbook for Students and Practitioners. Springer. (2010).
- Ross Anderson: Security Engineering: A Guide to Building Dependable Distributed System, Wiley (2001).
- Charles P. Pfleeger: Security in Computing. Prentice Hall (1997).
- Andreas M. Antonopoulos: Mastering Bitcoin. Programming the Open Blockchain. O'Reilly Media (2017) 3rd Edition. <https://github.com/aantonop/bitcoinbook>

Software

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

Lista de idiomas

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