

**Fonaments de Tecnologia de la Informació**

Codi: 102773

Crèdits: 6

Titulació	Tipus	Curs	Semestre
2502441 Enginyeria Informàtica	OB	3	1
2502441 Enginyeria Informàtica	OT	4	1

### Professor/a de contacte

Nom: Jordi Herrera Joancomarti

Correu electrònic: [jordi.herrera@uab.cat](mailto:jordi.herrera@uab.cat)

### Idiomes dels grups

Podeu accedir-hi des d'aquest [enllaç](#). Per consultar l'idioma us caldrà introduir el CODI de l'assignatura. Tingueu en compte que la informació és provisional fins a 30 de novembre de 2023.

### Equip docent

Victor García Font

Maria Merce Villanueva Gay

### Prerequisits

No hi ha prerequisits formals però es recomana haver aprovat l'assignatura "Informació i Seguretat".

### Objectius

L'assignatura "Fonaments de tecnologies de la Informació" forma part de la MATÈRIA 29: TECNOLOGIA DE LA INFORMACIÓ. Alguns temes dels quals s'ocupa són el paper de les TICs en les organitzacions, el tractament de la informació, la criptografia avançada i les seves aplicacions i serveis. D'una banda, aquesta assignatura constitueix una continuació als temes de seguretat vistos a l'assignatura "Informació i Seguretat" i, per altra banda, desenvolupa les bases teòriques que s'apliquen a l'assignatura "Garantia de la Informació i Seguretat".

### Competències

- Enginyeria Informàtica
- Adquirir hàbits de pensament.
- Adquirir hàbits de treball personal.

- Capacitat per a comprendre l'entorn d'una organització i les seves necessitats a l'àmbit de les tecnologies de la informació i les comunicacions.
- Capacitat per a seleccionar, desplegar, integrar i gestionar sistemes d'informació que satisfacin les necessitats de la organització, amb els criteris de cost i qualitat identificats.
- Capacitat per dissenyar, desenvolupar, avaluar i assegurar l'accessibilitat, l'ergonomia, la usabilitat i la seguretat dels sistemes, serveis i aplicacions informàtiques, així com de la informació que gestionen.
- Conèixer i aplicar elements bàsics d'economia, de gestió de recursos humans, d'organització i de planificació de projectes, així com la legislació, la regulació i la normalització en l'àmbit dels projectes informàtics.

## Resultats d'aprenentatge

1. Aplicar les tècniques d'avaluació de costos, gestió del temps, gestió de recursos i planificació en l'entorn de les tecnologies de la informació.
2. Avaluar i operar un sistema d'aplicacions o serveis de comunicació distribuïda.
3. Conèixer els sistemes d'informació i aplicar-los per a satisfer necessitats de les organitzacions.
4. Conèixer i comprendre les necessitats a l'àmbit de les TICs d'una organització.
5. Desenvolupar el pensament científic.
6. Identificar les disposicions normatives aplicables en els desenvolupaments de tecnologies de informació.
7. Incorporar sistemes distribuïts de tractament de la informació a una organització per a incrementar la capacitat operativa.
8. Prevenir i solucionar problemes.
9. Saber protegir l'accés i la seguretat en sistemes de tractament de la informació.
10. Treballar de manera autònoma.

## Continguts

1. Paper de les TICs
  1. TICs a les organitzacions
2. Fonaments
  1. Aritmètica modular
  2. Polinomis sobre  $GF(2)$
3. Tractament de la informació
  1. Codis cíclics
  2. CRC i LFSR
  3. Codis per l'emmagatzematge
4. Criptografia avançada
  1. Criptografia de clau pública
  2. Funcions hash
  3. Protocols criptogràfics
5. Aplicacions i serveis
  1. Tecnologia Blockchain
  2. Criptomonedes: Bitcoins

## Metodologia

Les classes de teoria es basaran en lliçons magistrals, si bé s'intentarà fomentar la participació de l'estudiant en la resolució d'exemples, etc. A les classes de problemes, se seguirà una llista d'exercicis que l'estudiant intentarà resoldre pel seu compte. Es fomentarà l'exposició de la resolució de problemes per part dels estudiants. En les sessions de pràctiques es tractaran en profunditat temes relacionats: plantejament de casos reals, ampliació de determinats temes amb tècniques i algorismes alternatius als ja vistos.

Al llarg del curs es duran a terme les següents activitats:

- **Classes magistrals:** es presentarà la teoria acompanyada de diversos exercicis d'exemple i s'intentarà fomentar la participació de l'estudiant en la seva resolució.
- **Classes de problemes:** són sessions amb el grup sencer o bé amb grups reduïts amb l'objectiu de poder aplicar la teoria a la resolució de problemes. L'alumne disposarà des de l'inici del curs, d'un llistat de problemes que haurà de resoldre. El professor també pot demanar la resolució d'alguns exercicis abans del seminari i procedir a la discussió de la seva resolució durant aquestes sessions. Aquestes sessions han de servir per promoure, principalment, la capacitat d'anàlisi i síntesi, el raonament crític, la resolució de problemes i el treball en grup.
- **Sessions de pràctiques:** es tractaran en profunditat temes relacionats amb els exposats a teoria. S'incideix en el plantejament de casos reals, l'ampliació de determinats temes amb tècniques i algorismes alternatius.

Competències transversals. En aquesta assignatura es treballaran i avaluaran les següents competències transversals del Grau d'Enginyeria Informàtica:

- **T01.03 - Desenvolupar el pensament científic:** es treballarà de forma més intensa en les sessions de problemes de l'assignatura on els estudiants hauran d'analitzar les problemàtiques presentades i veure quines solucions teòriques són les més adequades i com aquestes es poden aplicar.
- **T02.01 Treballar de forma autònoma:** aquesta es focalitza en aquelles activitats individuals, com ara el lliurament de problemes que es realitza al llarg del curs o les proves individuals de l'assignatura.
- **T02.04 Prevenir i solucionar problemes:** es treballa de forma més extensa en les sessions de pràctiques de l'assignatura.

Nota: es reservaran 15 minuts d'una classe, dins del calendari establert pel centre/titulació, per a la complementació per part de l'alumnat de les enquestes d'avaluació de l'actuació del professorat i d'avaluació de l'assignatura/mòdul.

## Activitats formatives

Títol	Hores	ECTS	Resultats d'aprenentatge
Tipus: Dirigides			
Classes de problemes	12	0,48	1, 3, 4, 5, 6, 9, 10
Classes de teoria	26	1,04	1, 2, 3, 4, 5, 6, 7, 9, 10
Pràctiques obligatòries	12	0,48	3, 8, 9, 10
Tipus: Supervisades			
Tutories i consultes	17	0,68	1, 3, 4, 9, 10
Tipus: Autònomes			
Preparació de problemes i pràctiques	25	1	1, 2, 4, 5, 8, 9, 10
Preparació exàmens parcials i examen final	25	1	1, 2, 4, 9, 10
Treball personal	25	1	1, 2, 4, 9, 10

## Avaluació

Les dates d'avaluació continuada es publicaran al campus virtual i a les transparències de presentació de l'assignatura i poden estar subjectes a canvis de programació per motius d'adaptació a possibles incidències. Sempre s'informarà a través del campus virtual de la UAB sobre aquests canvis, ja que s'entén que aquesta és la plataforma habitual d'intercanvi d'informació entre professors i estudiants.

L'avaluació de l'assignatura, sobre 10 punts, es farà de la forma següent:

- Part teòrica (7 punts): Per poder superar l'assignatura, cal obtenir almenys 3,5 dels 7 punts de nota de la part teòrica perquè pugui fer mitjana amb la part pràctica. L'avaluació de la part teòrica del curs es divideix en dos apartats:

Exàmens (6 punts): Dues proves parcials individuals per un total de 6 punts (3 punts cadascuna). Com a part de l'avaluació continuada, aquestes proves es realitzaran durant les sessions de teoria. Cada prova avaluarà de forma separada una part del temari i la nota final serà la mitjana aritmètica de les dues proves. Cada prova només podrà fer mitjana en cas que sigui qualificada amb una nota superior a 4 sobre 10. En cas que alguna de les proves no tingui una nota superior a 4, les proves parcials es consideraran suspeses.

Exercicis (1 punt): Com a part de l'avaluació continuada, es lliurarà la resolució d'activitats o exercicis proposats al llarg del curs.

- Pràctiques obligatòries (3 punts): Com a part de l'avaluació continuada, s'hauran de resoldre algunes pràctiques en el Laboratori Integrat. Cal obtenir almenys 1,5 punts en la valoració de les pràctiques, dels 3 sobre els que es valoren les pràctiques, per poder superar l'assignatura.

Els estudiants que hagin suspès la part de teòrica de l'assignatura tindran l'opció de presentar-se a l'examen final, on s'examinaran de TOT el temari del curs, independentment de les notes obtingudes en les proves parcials. La nota d'aquest examen de recuperació serà la que es considerarà com a nota d'exàmens per al càlcul final de la nota de l'assignatura, és a dir, tindrà un 60% del pes sobre la nota final de l'assignatura. Per superar l'assignatura cal que la nota de l'examen de recuperació més la nota dels exercicis sigui superior a 5 sobre 10.

Els estudiants que vulguin millorar la nota obtinguda en les proves parcials, es poden presentar a l'examen final per millorar la nota. En aquest cas, el fet de lliurar l'examen i que el professor el corregeixi implicarà sobreescriure les notes de les proves prèvies.

El lliurament dels exercicis i la realització de les pràctiques no serà possible recuperar-les.

Per a cada activitat d'avaluació, s'indicarà un lloc, data i hora de revisió en la qual l'estudiant podrà revisar l'activitat amb el professor. En aquest context, es podran fer reclamacions sobre la nota de l'activitat, que seran avaluades pel professorat responsable de l'assignatura. Si l'estudiant no es presenta a aquesta revisió, no es revisarà posteriorment aquesta activitat.

Aquesta assignatura no preveu el sistema d'avaluació única.

-----

Aquells alumnes que ja hagin cursat prèviament l'assignatura i que tinguin les pràctiques superades, se'ls mantindrà la nota de pràctiques. És important, però, que es posin en contacte amb el professor de pràctiques de l'assignatura a l'inici del curs (quan es realitzen els grups de pràctiques) per informar-lo d'aquest fet. En cap cas no es mantindran ni les notes dels exàmens de teoria ni les dels lliuraments dels problemes que es realitzen al llarg del curs.

Sense perjudici d'altres mesures disciplinàries que s'estimin oportunes, i d'acord amb la normativa acadèmicavigent, les irregularitats comeses per un estudiant que puguin conduir a una variació de la qualificació es qualificaran amb un zero (0). Les activitats d'avaluació qualificades d'aquesta forma i per aquest

procediment no seran recuperables. Si és necessari superar qualsevol d'aquestes activitats d'avaluació per aprovar l'assignatura, aquesta assignatura quedarà suspesa directament, sense oportunitat de recuperar-la en el mateix curs. Aquestes irregularitats inclouen, entre d'altres:

- la còpia total o parcial d'una pràctica, informe, o qualsevol altra activitat d'avaluació;
- deixar copiar;
- presentar un treball de grup no fet íntegrament pels membres del grup ús no autoritzat de la IA (p. ex, Copilot, ChatGPT o equivalents) per a resoldre exercicis, pràctiques i/o qualsevol altra activitat avaluable;
- presentar com a propis materials elaborats per un tercer, encara que siguin traduccions o adaptacions, i en general treballs amb elements no originals i exclusius de l'estudiant;
- tenir dispositius de comunicació (com telèfons mòbils, smart watches, etc.) accessibles durant les proves d'avaluació teòric-pràctiques individuals (exàmens);
- parlar amb companys durant les proves d'avaluació teòric-pràctiques individuals (exàmens);
- copiar o intentar copiar d'altres alumnes durant les proves d'avaluació teòric-pràctiques (exàmens);
- usar o intentar usar escrits relacionats amb la matèria durant la realització de les proves d'avaluació teòric-pràctiques (exàmens), quan aquests no hagin estat explícitament permesos.

En edicions futures d'aquesta assignatura, a l'estudiant que hagi comès irregularitats en un acte d'avaluació no se li convalidarà cap de les activitats d'avaluació realitzades.

En resum: copiar, deixar copiar o plagiar (o l'intent de) en qualsevol de les activitats d'avaluació equival a un SUSPENS, no compensable i sense convalidacions de parts de l'assignatura en cursos posteriors.

Els alumnes que aconseguixin el nombre mínim de punts per aprovar l'assignatura, però no hagin assolit la nota mínima en alguna de les activitats d'avaluació, seran avaluats amb una nota final de 4.5. En el cas que no s'hagi aprovat l'assignatura per la qualificació d'un zero d'una activitat per motiu de còpia, la nota final de l'assignatura serà un 3, fet que no permetrà compensar aquesta assignatura.

Finalment, obtindran la qualificació de "No Avaluable" aquells estudiants que no es presentin a cap de les proves individuals (proves parcials i l'examen final). La participació en alguna d'aquestes activitats d'avaluació suposarà rebre una qualificació diferent de "No Avaluable".

No es farà cap activitat d'avaluació a cap alumne en un horari diferent de l'establert si no és que existeix una causa justificada, s'ha avisat amb anterioritat a l'activitat i el professor ha donat el seu consentiment. En qualsevol altre cas, si un alumne no ha assistit a una activitat, aquesta no es pot recuperar.

Pel que fa a les matrícules d'honor, aquestes es podran concedir a aquells estudiants que hagin superat l'assignatura amb una nota final igual o superior a 9. Donat que el nombre de matrícules d'honor no pot superar el 5% dels estudiants matriculats, es concediran als estudiants amb les notes més altes. En cas d'empat, es tindrà en compte les solucions proposades en cada una de les activitats d'avaluació que s'han realitzat al llarg del curs.

## Activitats d'avaluació continuada

Títol	Pes	Hores	ECTS	Resultats d'aprenentatge
Examen final	6	2	0,08	1, 2, 3, 4, 6, 7, 9, 10
Proves individuals. Avaluació continuada	6	3	0,12	1, 2, 3, 4, 6, 7, 9
Pràctiques obligatòries	3	2	0,08	3, 4, 5, 8, 9

## Bibliografia

- J.M. Basart, J. Rifà i M. Villanueva: Fonaments de matemàtica discreta. Materials de la UAB. (1999).
- J. Rifà i L. Huguet: Comunicación Digital. Masson Ed. (1991).
- V. Shoup: A computational Introduction to number theory and Algebra. (2008). <http://shoup.net/ntb/>
- C. Pérez Solà i J. Herrera Joancomartí, La criptografia que et cal saber. (2023) Disponible on-line: <https://criptografia.cat/>
- N. P. Smart: Cryptography Made Simple. Springer. (2016)
- C. Paar, J. Pelzl: Understanding Cryptography: A Textbook for Students and Practitioners. Springer. (2010).
- R. Anderson: Security Engineering: A Guide to Building Dependable Distributed System, Wiley (2001).
- C.P. Pfleeger: Security in Computing. Prentice Hall (1997).
- A. M. Antonopoulos: Mastering Bitcoins. Unlocking digital cryptocurrencies. O'Reilly Media (2017) 2nd Edition. <https://github.com/aantonop/bitcoinbook>

## Programari

Les practiques de l'assignatura es faran en Python utilitzant el Jupyter Notebook.