Universitat Autònoma de Barcelona

Fonaments de Tecnologia de la Informació

2016/2017

Codi: 102773
Crèdits: 6

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

Professor de contacte

Nom: Jordi Herrera Joancomarti
Correu electrònic: Jordi.Herrera@uab.cat

Utilització d'idiomes a l'assignatura

Llengua vehicular majoritària: català (cat)
Grup íntegre en anglès: No
Grup íntegre en català: Sí
Grup íntegre en espanyol: No

Equip docent

Josep Rifà Coma
Roger Ten Valls

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
- Treballar en equip

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 distribuida.
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 la capacitat d'anàlisi, síntesi i prospectiva.
6. Identificar les disposicions normatives aplicables en els desenvolupaments de tecnologies de informació.
7. Incorporar sistemes distribuits de tractament de la informació a una organització per a incrementar la capacitat operativa.
8. Saber protegir l'accés i la seguretat en sistemes de tractament de la informació.
9. Treballar cooperativament.
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
4. Criptografia avançada
    1. Criptografia de clau pública
    2. Funcions hash
    3. Protocols criptogràfics
    4. Variants de signatures digitals
5. Aplicacions i serveis
    1. Criptomonedes: Bitcoins
    2. La xarxa TOR

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 activitat:

- 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.

Activitats formatives

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

- Dues proves parcials individuals, 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. La superació de cada prova implicarà la superació de la part del temari a la que fa referència.
- Resolució d'exercicis, 1 punt. Com a part de l'avaluació continuada, es lliurarà la resolució d'activitats o exercicis a classe.
- 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 punt per poder superar l'assignatura.

En cas de no superar alguna de les proves parcials, es podran recuperar de la següent manera:

- Examen final, fins a 6 punts. Aquells estudiants que no hagin superat alguna (o cap) de les dues proves parcials de l'assignatura, tindran l'opció de presentar-se a l'examen final, on s'examinaran de la part de l'assignatura que tinguin suspesa o de les dues parts, en cas de tenir les dues parts suspeses. Caldrà superar cada una de les parts per separat per superar l'assignatura. Els estudiants que vulguin millorar la nota obtinguda en els exàmens parcials, es poden presentar a l'examen final per millorar la nota.

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

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 acadèmica vigent, 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;
- 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 teorico-pràctiques individuals (exàmens).

Els alumnes que aconsegueixin 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'asignatura 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.

Activitats d'avaluació

Títol	Pes	Hores	ECTS	Resultats d'aprenentatge
Examen final	6	2	0,08	1, 2, 3, 4, 5, 6, 7, 8
Pràctiques obligatòries	3	2	0,08	3, 4, 5, 8, 9
Proves individuals. Avaluació continuada	6	3	0,12	1, 2, 3, 4, 5, 6, 7, 8
Resolució Exercicis	1	1	0,04	1, 2, 3, 5, 6, 7, 8, 9, 10

Bibliografia

- J. Domingo i J. Herrera, 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 i S.Vanstone.: Handbook of Applied Cryptography, CRC Press. (1996). http://www.cacr.math.uwaterloo.ca/hac.
- 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).

- 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 (2014). https://github.com/aantonop/bitcoinbook
- K. Peng: Anonymous Communication Networks: Protecting Privacy on the Web. CRC Press. (2014)
- V. Shoup: A computational Introduction to number theory and Algebra. (2008). http://shoup.net/ntb/