

Fonaments de Tecnologia de la Informació

2013/2014

Codi: 102773

Crèdits: 6

Titulació	Tipus	Curs	Semestre
2502441 Enginyeria Informàtica	OT	4	1

Professor de contacte

Nom: Jaume Pujol Capdevila

Correu electrònic: Jaume.Pujol@uab.cat

Utilització d'idiomes

Llengua vehicular majoritària: català (cat)

Algun grup íntegre en anglès: No

Algun grup íntegre en català: Sí

Algun grup íntegre en espanyol: No

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, aplicacions i serveis i criptografia avançada. Per una part, hi ha continuació al temes de seguretat vistos a l'assignatura "Informació i Seguretat". Per altra part, hi ha una introducció a l'assignatura "Sistemes d'Informació" i 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 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 la capacitat d'anàlisi, síntesi i prospectiva.
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. 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. Intercanvi de claus de Diffie-Hellman
 2. Protocols de tres passes de Shamir
 3. Protocols d'autenticació
 4. Estratègies d'atac i vulnerabilitats clàssiques dels protocols
 5. Esquemes de compartició de secrets
 6. Diners digitals utilitzant signatures digitals
5. Seguretat en aplicacions i serveis
 1. Certificats digitals
 2. SSL
6. Sistemes de gestió de la seguretat de la informació
 1. Introducció als ISMS i normativa
 2. Família ISO27000
 3. Implicacions econòmiques
 4. Legislació

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.

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. Cal obtenir almenys 2.4 punts per poder superar l'assignatura.
- Resolució d'exercicis, 1.5 punts. Com a part de l'avaluació continuada, es lliurarà la resolució d'activitats o exercicis a classe.
- Pràctiques obligatòries, 2.5 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.
- Examen final, 6 punts. Aquells estudiants que no hagin superat l'assignatura arran de les proves parcials individuals tindran l'opció de presentar-se a l'examen final. Cal obtenir almenys 2.4 punts per poder superar l'assignatura.

Sense perjudici d'altres mesures disciplinàries que s'estimin oportunes, i d'acord amb la normativa acadèmica vigent, es qualificaran amb un zero les irregularitats comeses per l'estudiant que puguin conduir a una variació de la qualificació d'un acte d'avaluació. Per tant, copiar o deixar copiar una pràctica o qualsevol altra activitat d'avaluació implicarà suspendre-la amb un zero, i si és necessària superar-la per aprovar, tota l'assignatura quedarà suspesa. No seran recuperables les activitats d'avaluació qualificades d'aquesta forma i per aquest procediment, i per tant l'assignatura serà suspesa directament sense oportunitat de recuperar-la en el mateix curs.

Finalment, obtindran la qualificació de "No Presentat" 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 Presentat".

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
Proves individuals. Avaluació continuada	6	3	0,12	1, 2, 3, 4, 5, 6, 7, 8
Pràctiques obligatòries	2.5	2	0,08	3, 4, 5, 8, 9
Resolució Exercicis	1.5	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. Rifà i L. Huguet: Comunicación Digital. Masson Ed. (1991).
- D.E. Robling Denning: Cryptography and Data Security. Addison-Wesley Publishing Company (1988).
- B. Schneier: Applied Cryptography, John Wiley and Sons, Inc. 1996.
- G.S. Simmons: Contemporary Cryptology. The Science of Information Integrity, IEEE Press (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 to number theory and Algebra. <http://shoup.net/ntb/>
- A. Jaquith: Security Metrics Replacing Fear, Uncertainty, and Doubt Addison-Wesley Professional (2007). ISBN:0321349989
