

Guia docent

Identificació de l'assignatura

Assignatura / Grup	21748 - Seguretat en Sistemes Informàtics / 1
Titulació	Grau d'Enginyeria Informàtica (Pla 2010) - Tercer curs Grau d'Enginyeria Informàtica (Pla 2014) - Tercer curs
Crèdits	6
Període d'impartició	Primer semestre
Idioma d'impartició	Castellà

Professors

Professor/a	Horari d'atenció als alumnes					
	Hora d'inici	Hora de fi	Dia	Data d'inici	Data de fi	Despatx / Edifici
Bartolomé Jaime Serra Cifre						
<i>Responsable</i>						Cal concertar cita prèvia amb el/la professor/a per a fer una tutoria
tomeu.serra@uib.es						
Antonio Sola Venteo						
<i>Responsable</i>						Cal concertar cita prèvia amb el/la professor/a per a fer una tutoria
toni.sola@uib.es						

Contextualització

L'assignatura "Seguretat en Sistemes Informàtics" s'imparteix en el primer semestre del tercer curs.

Objectiu General.L'objectiu general és abastar l'estudi de la seguretat informàtica en les seves diferents facetes, incloent la seva avaluació, la protecció de les xarxes, els protocols i arquitectures de seguretat i la seva implantació en el comerç electrònic.

Objectius Específics. Aconseguir un bon aprofitament dels següents coneixements:

- * Avaluació de la seguretat. Anàlisi de riscos. Gestió de la seguretat.
- * Seguretat bàsica en xarxes. Amenaces, serveis. Infraestructura de clau pública.
- * Protecció a la xarxa. Seguretat perimetral, IDS, antivirus.
- * Seguretat en aplicacions de comerç electrònic.

Requisits



Guia docent

Essencials

L'assignatura requerirà coneixements que s'imparteixen en l'assignatura "Comunicacions de Dades i Xarxes" i "Estructura de Computadors II"

Competències

Específiques

- * CI504 - Capacitat per seleccionar, dissenyar, desplegar, integrar i gestionar xarxes i infraestructures de comunicacions en una organització.
- * CI505 - Capacitat per seleccionar, desplegar, integrar i gestionar sistemes d'informació que satisfacin les necessitats de l'organització, amb els criteris de cost i qualitat identificats.
- * CI506 - Capacitat per concebre sistemes, aplicacions i serveis basats en tecnologies de xarxa, incloent Internet, web, comerç electrònic, multimèdia, serveis interactius i computació mòbil.
- * CI507 - Capacitat per a comprendre, aplicar i gestionar la garantia i la seguretat dels sistemes informàtics.

Genèriques

- * CTR01 - Capacitat d'anàlisi i síntesi, d'organització, de planificació i de presa de decisions.
- * CTR02 - Capacitat d'anàlisi crítica i de proposta i aplicació de noves solucions.
- * CTR03 - Capacitat per adquirir de forma autònoma nous coneixements.
- * CTR04. Capacitat per a la recerca de recursos i de gestió de la informació en l'àmbit de la informàtica.
- * CTR06. Capacitat de lideratge, iniciativa, esperit emprenedor i eficàcia en ambient d'exigència en base a la creativitat, la qualitat i l'adaptació a noves situacions.
- * CTR07 - Capacitat per comunicar conceptes propis de la informàtica de manera oral i escrita en diferents àmbits d'actuació. La competència de es treballarà de forma natural mitjançant el lliurament d'informes escrits i la realització de presentacions.
- * CTR09. Capacitat per desenvolupar habilitats interpersonals, i compromís amb valors socials, ètics, mediambientals i de drets fonamentals, en especial els valors d'igualtat i capacitat.

Bàsiques

- * Podeu consultar les competències bàsiques que l'estudiant ha d'haver assolit en acabar el grau a l'adreça següent: http://estudis.uib.cat/ca/grau/comp_basiques/

Continguts

Els temes següents es desenvoluparan en els corresponents continguts temàtics:

- * Introducció a la criptografia i ala criptoanàlisi
- * Seguretat física: la seguretat del centre de procés de dades
- * Seguretat en els SSOO
- * Seguretat en xarxes
- * Seguretat a nivell d'aplicació
- * Serveis
- * Legislació i seguretat
- * Aspectes avançats de seguretat

Continguts temàtics

Guia docent

1. Visió global de la seguretat en sistemes informàtics.
2. Eines de criptografia
3. Autenticació d'usuaris.
4. Control d'accés.
5. Seguretat en bases de dades.
6. Programari maliciós.
7. Atacs de denegació de servei.
8. Detecció d'intrusions.
9. Tallafocs
10. Desbordament de memòria temporal.
11. Seguretat del programari.
12. Seguretat del sistema operatiu.
13. Computació confiable.
14. Gestió de la seguretat dels sistemes d'informació i avaluació de riscos.
15. Seguretat física,
16. Recursos humans i seguretat.
17. Auditoria de seguretat
18. Criptografia simètrica i confidencialitat de missatges. Criptografia de clau pública i autenticació de missatges.
19. Protocols i estàndars de seguretat a Internet. Aplicacions d'autenticació a Internet.

Metodologia docent

Per treballar les competències assignades, es preveuen les activitats formatives presencials que s'enumeren a continuació:

- Classes teòriques - grup gran
- Classes pràctiques - grup gran
- Ampliació de continguts i treballs - grups mitjans
- Tutories - grups petits

Els continguts teòrics de l'assignatura s'exposaran a través de classes de teoria, en què s'explicaran les diferents tècniques i eines de seguretat. Aquests continguts s'il·lustraran mitjançant problemes senzills, i pràctiques en què es podrà practicar amb eines de seguretat d'ús freqüent per a la protecció de xarxes i sistemes informàtics i que, a més, tractaran d'estimular la capacitat d'anàlisi i síntesi de l'estudiant. Les activitats pràctiques es realitzaran, en la mesura del possible i en funció de la seva adequació, fomentant el treball en grup i amb el suport d'eines informàtiques. Així mateix, es complementarà la formació mitjançant tutories presencials i tutories electròniques.

A més de les classes presencials, l'estudiant haurà de desenvolupar part de l'adquisició i posada en pràctica de coneixements per si mateix. En particular, és previst afavorir l'aprofundiment i ampliació de coneixements mitjançant l'ús dels llibres de text de referència, reforçant així la capacitat d'autoaprenentatge de l'estudiant. Aquest esforç de l'alumne en solitari serà avaluat, en funció de la seva idoneïtat, en forma de treballs, problemes, o exposicions a classe.

Guia docent

Activitats de treball presencial (2,4 crèdits, 60 hores)

Modalitat	Nom	Tip. agr.	Descripció	Hores
Classes teòriques	Teoria	Grup gran (G)	Se presentan los conceptos, resultados y procedimientos principales de la asignatura por medio de la exposición magistral.	30
Classes pràctiques	Problemes i casos pràctics	Grup mitjà (M)	* Il·lustrar els continguts teòrics mitjançant problemes senzills i exemples pràctics. * La metodologia consistirà en la realització d'exercicis a classe iamb la familiarització amb eines de seguretat d'ús freqüent per a la protecció de xarxes i sistemes informàtics.	17
Tutories ECTS	Tutories	Grup petit (P)	La finalitat de les tutories serà tractar de resoldre els dubtes dels alumnes en general i d'ajudar en la realització dels treballs.	6
Avaluació	Examen. Part pràctica	Grup gran (G)	* La finalitat és avaluar el coneixement per part de l'alumne del contingut pràctic de l'assignatura. * S'efectuarà durant el període d'examens finals.	3
Avaluació	Examen	Grup gran (G)	Comprovar l'assoliment dels coneixements i competències treballades durant tot el període d'aprenentatge. S'efectuarà durant el període d'examens finals	2
Avaluació	Validació 1	Grup gran (G)	Comprovar l'assoliment dels coneixements i competències treballades durant el primer període del quadrimestre. Constarà de diverses preguntes de resposta curta.	1
Avaluació	Validació 2	Grup gran (G)	Comprovar l'assoliment dels coneixements i competències treballades durant el segon període del quadrimestre. Constarà de diverses preguntes de resposta curta.	1

A començament del semestre hi haurà a disposició dels estudiants el cronograma de l'assignatura a través de la plataforma UIBdigital. Aquest cronograma inclourà almenys les dates en què es faran les proves d'avaluació contínua i les dates de lliurament dels treballs. A més, el professor o la professora informará els estudiants si el pla de treball de l'assignatura es durà a terme a través del cronograma o per una altra via, inclosa la plataforma Aula digital.

Activitats de treball no presencial (3,6 crèdits, 90 hores)

Modalitat	Nom	Descripció	Hores
Estudi i treball autònom individual	Estudi de continguts	* Estudi individual del que s'ha explicat en les classes magistrals o de la tasca encomanada per esser treballada de forma autònoma.	40

Guia docent

Modalitat	Nom	Descripció	Hores
Estudi i treball autònom individual o en grup	Realització de treballs teòrics i pràctics	Preparar i realitzar els treballs/pràctiques proposats.	50

Riscs específics i mesures de protecció

Les activitats d'aprenentatge d'aquesta assignatura no comporten riscos específics per a la seguretat i salut dels alumnes i, per tant, no cal adoptar mesures de protecció especials.

Avaluació de l'aprenentatge dels estudiants

En funció de les competències pròpies i transversals que es treballen en aquesta assignatura, es proveeixen els procediments d'avaluació enumerats a continuació:

- Proves objectives.
- Proves de resposta breu i proves de desenvolupament.
- Treballs i projectes.
- Informes / memòries de pràctiques
- Proves orals (exposició de treballs).
- Proves d'execució de tasques reals o simulades.

El sistema de qualificacions s'expressarà mitjançant qualificació numèrica.

Frau en elements d'avaluació

D'acord amb l'article 33 del Reglament acadèmic, "amb independència del procediment disciplinari que es pugui seguir contra l'estudiant infractor, la realització demostradorament fraudulenta d'alguns dels elements d'avaluació inclosos en guies docents de les assignatures comportarà, a criteri del professor, una menysvaloració en la seva qualificació que pot suposar la qualificació de «suspens 0» a l'avaluació anual de l'assignatura".

Teoria

Modalitat	Classes teòriques
Tècnica	Proves objectives (no recuperable)
Descripció	Se presentan los conceptos, resultados y procedimientos principales de la asignatura por medio de la exposición magistral.
Criteris d'avaluació	Control d'assistència a classe.

Percentatge de la qualificació final: 5%

Guia docent

Problemes i casos pràctics

Modalitat	Classes pràctiques
Tècnica	Proves objectives (no recuperable)
Descripció	*Il·lustrar els continguts teòrics mitjançant problemes senzills i exemples pràctics.*La metodologia consistirà en la realització d'exercicis a classe i amb la familiarització amb eines de seguretat d'ús freqüent per a la protecció de xarxes i sistemes informàtics.

Criteris d'avaluació

Percentatge de la qualificació final: 5%

Examen. Part pràctica

Modalitat	Avaluació
Tècnica	Proves objectives (recuperable)
Descripció	*La finalitat és avaluar el coneixement per part de l'alumne del contingut pràctic de l'assignatura.* S'efectuarà durant el període d'exàmens finals.

Criteris d'avaluació

Percentatge de la qualificació final: 35%

Examen

Modalitat	Avaluació
Tècnica	Proves objectives (recuperable)
Descripció	Comprovar l'assoliment dels coneixements i competències treballades durant tot el període d'aprenentatge. S'efectuarà durant el període d'exàmens finals .

Criteris d'avaluació

Percentatge de la qualificació final: 20%

Validació 1

Modalitat	Avaluació
Tècnica	Proves de resposta breu (no recuperable)
Descripció	Comprovar l'assoliment dels coneixements i competències treballades durant el primer període del quadrimestre. Constarà de diverses preguntes de resposta curta.

Criteris d'avaluació

Percentatge de la qualificació final: 10%

Validació 2

Modalitat	Avaluació
Tècnica	Proves de resposta breu (no recuperable)
Descripció	Comprovar l'assoliment dels coneixements i competències treballades durant el segon període del quadrimestre. Constarà de diverses preguntes de resposta curta.

Criteris d'avaluació

Percentatge de la qualificació final: 10%



Guia docent

Realització de treballs teòrics i pràctics

Modalitat	Estudi i treball autònom individual o en grup
Tècnica	Informes o memòries de pràctiques (recuperable)
Descripció	Preparar i realitzar els treballs/pràctiques proposats.
Criteris d'avaluació	
Percentatge de la qualificació final:	15%

Recursos, bibliografia i documentació complementària

Bibliografia bàsica

- * W. Stallings, L. Brown, *Computer Security*, Pearson, 2nd Ed. 2008
- * W. Stallings, *Cryptography and Network Security*. Fifth Edition, Pearson, 2010.

Bibliografia complementària

- * M. J. Lucena López, *Criptografia y seguridad en computadores*, 2003.
- * C. Adams, S. Lloyd, *Understanding PKI : concepts, standards, and deployment considerations*, Addison-Wesley, 2003.
- * S. Garfinkel, G. Spafford, *Web security, privacy & commerce*, O'Reilly & Associates, 2002.
- * S. Northcutt et al., *Intrusion signatures and analysis*, New Riders, 2001.
- * R. Oppliger, *Secure messaging with PGP and S/MIME*, Artech House, 2001.
- * E. D. Zwicky, S. Cooper, D. B. Chapman, *Building Internet Firewalls*, O'Reilly & Associates, 2000.
- * P. Fites, M. P. J. Kratz, *Information Systems Security, A Practitioner's Reference*. Van Nostrand Reinhold, N.Y. 1993.

Altres recursos

- * Plana a Campus Extens:
 - Presentacions
 - Enllaços d'interès

