Guia docent
270123 - SI - Seguretat Informàtica

Última modificació: 10/02/2025

Unitat responsable: Facultat d'Informàtica de Barcelona
Unitat que imparteix: 701 - DAC - Departament d'Arquitectura de Computadors.

Titulació: GRAU EN ENGINYERIA INFORMÀTICA (Pla 2010). (Assignatura optativa).

Curs: 2024 **Crèdits ECTS:** 6.0 **Idiomes:** Català, Castellà

PROFESSORAT

Professorat responsable: RENÉ SERRAL GRACIÀ

Altres:

Primer quadrimestre:
ROBERTO BARREDA ORENGA - 11, 13
MARC CATRISSE I PÉREZ - 12
RENÉ SERRAL GRACIÀ - 11, 12, 13

Segon quadrimestre:
ROBERTO BARREDA ORENGA - 11, 12
MARC CATRISSE I PÉREZ - 11, 12

CAPACITATS PRÈVIES

Les obtingudes a les assignatures Sistemes Operatius i Xarxes de Computadors.

Coneixements d'anglès tècnic.

REQUISITS

- Pre-Corequisit SO
- Pre-Corequisit XC

COMPETÈNCIES DE LA TITULACIÓ A LES QUALS CONTRIBUEIX L'ASSIGNATURA

Específiques:
CT6.4. Demostrar coneixement i capacitat d'aplicació de les característiques, de les funcionalitats i de l'estructura dels Sistemes Distribuïts i de les Xarxes de Computadors i d'Internet que en garanteixi l'ús i l'administració, així com el disseny i la implementació d'aplicacions basades en elles.
CT7.1. Demostrar coneixement de les mètriques de qualitat i saber-les utilitzar.
CT7.2. Avaluar sistemes hardware/software en funció d'un criteri de qualitat determinat.
CT7.3. Determinar els factors que incideixen negativament en la seguretat i la fiabilitat d'un sistema hardware/software, i minimitzar-ne els efectes.
CT8.1. Identificar tecnologies actuals i emergents i avaluar si són aplicables, i en quina mesura, per a satisfer les necessitats dels usuaris.
CTI1.1. Demostrar comprensió de l'entorn d'una organització i de les seves necessitats en l'àmbit de les tecnologies de la informació i les comunicacions.
CTI1.2. Seleccionar, dissenyar, desplegar, integrar gestionar xarxes i infraestructures de comunicacions en una organització.
CTI1.3. Seleccionar, desplegar, integrar i gestionar sistemes d'informació que satisfacin les necessitats de l'organització amb els criteris de cost i qualitat identificats.
CTI2.3. Demostrar comprensió, aplicar i gestionar la garantia i la seguretat dels sistemes informàtics (CEIC6).
CTI3.1. Concebre sistemes, aplicacions i serveis basats en tecnologies de xarxa, tenint en compte Internet, web, comerç electrònic, multimèdia, serveis interactius i computació ubiqua.

Genèriques:
G6. Gestionar l'adquisició, l'estructuració, l'anàlisi i la visualització de dades i d'informació de l'àmbit de l'enginyeria informàtica, i valorar de forma crítica els resultats d'aquesta gestió.

METODOLOGIES DOCENTS

Aquesta assignatura ha de donar una visió global i el més tècnica possible dels problemes i solucions de seguretat als sistemes informàtics i a les xarxes. Per aquesta raó, cobreix molts temes i ha de tenir una component descriptiva gran.

Tanmateix, la metodologia docent farà servir exemples i problemes per anar introduint els conceptes per a que els estudiants assoleixin les competències necessàries. A més, s'intentarà fomentar la interactivitat amb els estudiants plantejant a classe situacions reals per discutir les solucions possibles.

Per altra banda, les pràctiques al laboratori aniran completant les capacitats i els coneixements adquirits a classe de teoria/problemes.

OBJECTIUS D'APRENENTATGE DE L'ASSIGNATURA

1.Ser capaç d'entendre les amenaces i riscos de seguretat dels sistemes informàtics.
2.Ser capaç d'analitzar codi maliciós, com ara virus, troians, etc.
3.Ser capaç d'entendre i identificar mecanismes de control d'accés d'un sistema operatiu.
4.Conèixer les problemàtiques de seguretat a les xarxes de computadors i ser capaç de trobar solucions per protegir-les.
5.Ser capaç de dissenyar mecanismes de protecció per a les aplicacions distribuïdes.
6.Ser capaç d'entendre la necessitat i funcionament de mecanismes forenses a la seguretat informàtica.
7.Ser capaç de fer servir mecanismes criptogràfics per a la protecció de recursos informàtics.
8.Ser capaç d'entendre, aplicar i dissenyar infraestructures de clau pública (PKI).
10.Ser capaç d'entendre els mecanismes de protecció i les polítiques de seguretat.
11.Ser capaz de gestionar l'adquisició, l'estructuració, l'anàlisi i la visualització de dades i d'informació de l'àmbit de l'enginyeria informàtica, valorant de manera crítica els resultats d'aquesta gestió.

HORES TOTALS DE DEDICACIÓ DE L'ESTUDIANTAT

Tipus	Hores	Percentatge
Hores grup petit	15,0	10.00
Hores aprenentatge autònom	84,0	56.00
Hores activitats dirigides	6,0	4.00

Tipus	Hores	Percentatge
Hores grup gran	45,0	30.00

Dedicació total: 150 h

CONTINGUTS

Introducció

Descripció:
Amenaces, anàlisi de riscos, mecanismes de protecció, seguretat a les comunicacions, seguretat forense , polítiques, recuperació, aspectes legals, ...

Criptografia

Descripció:
Conceptes bàsics de criptografia. Clau pública. Signatura electrònica.

Infraestructura PKI

Descripció:
Certificats. Directoris. Protocols.

Seguretat a les aplicacions

Descripció:
Seguretat a la web. Protocols segurs d'aplicació.

Seguretat en els sistemes operatius

Descripció:
Anàlisi de les amenaces. Funcionament dels codis maliciosos. Virus i worms. Protecció. Antivirus. Estructura d'un SO.

Anàlisi forense

Descripció:
Recopilació d'evidències. Anàlisi.

ACTIVITATS

Desenvolupament del tema 1. Introducció.

Descripció:
Aprenentatge dels conceptes i objectius associats a aquest tema.

Objectius específics:
1, 10

Dedicació: 5h
Aprenentatge autònom: 4h
Grup gran/Teoria: 1h

Desenvolupament del tema 2. Criptografia.

Descripció:
Aprenentatge dels conceptes i objectius associats a aquest tema.

Objectius específics:
7

Dedicació: 18h
Aprenentatge autònom: 8h
Grup gran/Teoria: 6h
Grup mitjà/Pràctiques: 4h

Desenvolupament del tema 3. Infraestructura PKI.

Descripció:
Aprenentatge dels conceptes i objectius associats a aquest tema.

Objectius específics:
8

Dedicació: 9h
Aprenentatge autònom: 5h
Grup gran/Teoria: 3h
Grup mitjà/Pràctiques: 1h

Lab 1. Ús de certificats digitals i apache (HTTPS)

Descripció:
Ser capaç de crear un certificat X.509 amb openssl i instal·lar-lo a un servidor web apache per a configurar el protocol HTTPS

Objectius específics:
8

Dedicació: 6h
Aprenentatge autònom: 4h
Grup petit/Laboratori: 2h

Primer examen de teoria

Descripció:
Examen de teoria dels primers temes de l'assignatura: Introducció, Criptografia, Infrastructura PKI i seguretat en xarxes

Objectius específics:
1, 4, 7, 8, 10

Dedicació: 7h 30m
Aprenentatge autònom: 6h
Activitats dirigides: 1h 30m

Desenvolupament del tema 4. Seguretat a les aplicacions.

Descripció:
Aprenentatge dels conceptes i objectius associats a aquest tema.

Objectius específics:
5

Competències relacionades:
G6. Gestionar l'adquisició, l'estructuració, l'anàlisi i la visualització de dades i d'informació de l'àmbit de l'enginyeria informàtica, i valorar de forma crítica els resultats d'aquesta gestió.

Dedicació: 25h
Aprenentatge autònom: 15h
Grup gran/Teoria: 6h
Grup mitjà/Pràctiques: 4h

Lab 2. Anàlisis de Vulnerabilitats web

Descripció:
Comprensió de les tècniques de programació segures descrites a la sessió. Ús de les aplicacions webscarab i webgoat de la distribució de linux OWASP

Objectius específics:
1, 5

Competències relacionades:
G6. Gestionar l'adquisició, l'estructuració, l'anàlisi i la visualització de dades i d'informació de l'àmbit de l'enginyeria informàtica, i valorar de forma crítica els resultats d'aquesta gestió.

Dedicació: 8h
Aprenentatge autònom: 4h
Grup petit/Laboratori: 4h

Desenvolupament del tema 5. Seguretat als sistemes operatius.

Descripció:
Aprenentatge dels conceptes i objectius associats a aquest tema.

Objectius específics:
2, 3

Competències relacionades:
G6. Gestionar l'adquisició, l'estructuració, l'anàlisi i la visualització de dades i d'informació de l'àmbit de l'enginyeria informàtica, i valorar de forma crítica els resultats d'aquesta gestió.

Dedicació: 23h
Aprenentatge autònom: 13h
Grup gran/Teoria: 6h
Grup mitjà/Pràctiques: 4h

Lab 5. Anàlisis de codi maliciós

Descripció:
Comprendre les diferents formes d'anàlisis de codi maliciós. Ser capaç d'utilitzar correctament l'eina d'anàlisis IDAPro

Objectius específics:
1, 2

Competències relacionades:
G6. Gestionar l'adquisició, l'estructuració, l'anàlisi i la visualització de dades i d'informació de l'àmbit de l'enginyeria informàtica, i valorar de forma crítica els resultats d'aquesta gestió.

Dedicació: 8h
Aprenentatge autònom: 4h
Grup petit/Laboratori: 4h

Desenvolupament tema 7. Seguretat forense.

Descripció:
Aprenentatge dels conceptes i objectius associats a aquest tema.

Objectius específics:
6

Competències relacionades:
G6. Gestionar l'adquisició, l'estructuració, l'anàlisi i la visualització de dades i d'informació de l'àmbit de l'enginyeria informàtica, i valorar de forma crítica els resultats d'aquesta gestió.

Dedicació: 8h
Aprenentatge autònom: 3h
Grup gran/Teoria: 3h
Grup mitjà/Pràctiques: 2h

Lab 6. Investigació d'un cas forense

Descripció:
Els estudiants aprendran els procediments i metodologies bàsiques que s'han de tenir en compte a l'hora de realitzar una anàlisi forense. També s'espera que, després del laboratori, augmenti la seva comprensió de les eines i aplicacions forenses necessàries per resoldre la majoria dels incidents de seguretat en què hi ha proves digitals.

Objectius específics:
6

Competències relacionades:
G6. Gestionar l'adquisició, l'estructuració, l'anàlisi i la visualització de dades i d'informació de l'àmbit de l'enginyeria informàtica, i valorar de forma crítica els resultats d'aquesta gestió.

Dedicació: 6h
Aprenentatge autònom: 4h
Grup petit/Laboratori: 2h

Lab CT. Ús solvent dels recursos bibliogràfics

Descripció:
Gestionar l'adquisició, l'estructuració, l'anàlisi i la visualització de dades i d'informació de l'àmbit de l'enginyeria informàtica, valorant de manera crítica els resultats d'aquesta gestió.
- Planificar i utilitzar la informació necessària per a un treball acadèmic (per exemple, per al treball de fi de grau) a partir duna reflexió crítica sobre els recursos dinformació utilitzats.
- Gestionar la informació de manera competent, independent i autònoma.
- Avaluar la informació trobada i identificar-ne les llacunes.

Objectius específics:
11

Competències relacionades:
G6. Gestionar l'adquisició, l'estructuració, l'anàlisi i la visualització de dades i d'informació de l'àmbit de l'enginyeria informàtica, i valorar de forma crítica els resultats d'aquesta gestió.

Dedicació: 4h
Aprenentatge autònom: 2h
Grup petit/Laboratori: 2h

Qüestionari sobre l'ús solvent dels recursos bibliogràfics

Descripció:
Qüestionari sobre l'ús solvent dels recursos bibliogràfics

Objectius específics:
11

Competències relacionades:
G6. Gestionar l'adquisició, l'estructuració, l'anàlisi i la visualització de dades i d'informació de l'àmbit de l'enginyeria informàtica, i valorar de forma crítica els resultats d'aquesta gestió.

Dedicació: 3h
Aprenentatge autònom: 2h
Activitats dirigides: 1h

Segon examen de teoría

Descripció:
Examen de teoria dels temes de l'assignatura: Seguretat a les aplicacions, seguretat als sistemes operatius i anàlisi forense.

Objectius específics:
2, 3, 5, 6

Competències relacionades:
G6. Gestionar l'adquisició, l'estructuració, l'anàlisi i la visualització de dades i d'informació de l'àmbit de l'enginyeria informàtica, i valorar de forma crítica els resultats d'aquesta gestió.

Dedicació: 7h 30m
Aprenentatge autònom: 6h
Activitats dirigides: 1h 30m

Examen final de laboratori

Descripció:
Examen sobre totes les pràctiques de laboratori fetes al llarg del curs.

Objectius específics:
2, 3, 4, 5, 7, 8

Competències relacionades:
G6. Gestionar l'adquisició, l'estructuració, l'anàlisi i la visualització de dades i d'informació de l'àmbit de l'enginyeria informàtica, i valorar de forma crítica els resultats d'aquesta gestió.

Dedicació: 5h
Aprenentatge autònom: 4h
Activitats dirigides: 1h

Examen final

Descripció:
Examen exclusiu per als alumnes que s'han presentat a tots dos controls però no han aprovat l'assignatura. L'examen és sobretot el temari.

Objectius específics:
1, 2, 3, 4, 5, 6, 7, 8, 10

Competències relacionades:
G6. Gestionar l'adquisició, l'estructuració, l'anàlisi i la visualització de dades i d'informació de l'àmbit de l'enginyeria informàtica, i valorar de forma crítica els resultats d'aquesta gestió.

Dedicació: 7h
Aprenentatge autònom: 6h
Activitats dirigides: 1h

SISTEMA DE QUALIFICACIÓ

1. Realització d'un control (C1) a meitat del quadrimestre i d'un segon control al final (C2) sobre la matèria exposada a les classes de teoria.
Teoria = 0,5 x C1 + 0,5 x C2

2. Realització de les pràctiques:
2.1 S'avaluarà a través de lliuraments i/o qüestionaris individuals per Atenea (NQ)
2.2 Es realitzarà un examen final de laboratori (EL).
La nota del laboratori serà: Lab = 0,5 * NQ + 0,5 EL

3. Realització d'una activitat individual dedicada a la competència transversal (CT) proposada pels professors de teoria i/o laboratori relacionada amb "Ús solvent de recursos bibliogràfics"

La nota final (NF) de l'assignatura es calcularà de la manera següent:
NF = 0,7 x Teoria + 0,25 x Lab + 0,05 x CT

No hi haurà examen final, hi ha la possibilitat de repetir el primer parcial durant el segon parcial (que es farà en l'horari d'examens a final de curs)

El nivell d'assoliment de la competència transversal s'avalua a partir de la CT i es calcula de la manera següent:
A si CT >= 8.5; B si CT >=7; C si CT >= 5; D si CT < 5

BIBLIOGRAFIA

Bàsica:
- Stallings, W. Network security essentials: applications and standards. 6th ed. Pearson Education, 2017. ISBN 9781292154916.
- Stallings, W. Cryptography and network security: principles and practice. 8th edition Global Edition. Boston: Person, 2023. ISBN 9781292437484.
- Stallings, W. Computer Security: Principles and Practice. 4th ed. Prentice Hall, 2018. ISBN 9781292220611.
- Menezes, A.J.; Van Oorschot, P.C.; Vanstone, S.A. Handbook of applied cryptography. CRC Press, 1997. ISBN 0-8493-8523-7.
- Adams, C.; Lloyd, S. Understanding PKI: concepts, standards, and deployment considerations. 2nd ed. Addison-Wesley, 2003. ISBN 0-672-32391-5.

Complementària:
- Medina, M.; Molist, M. Cibercrimen : ¡protégete del Bit-Bang!, los ataques en el Ciberespacio a : tu ordenador, tu móvil, tu empresa... aprende de víctimas, expertos y CiberVigilantes. Barcelona: Tibidabo, 2015. ISBN 9788416204823.