FITXA IDENTIFICATIVA

Dades de l'Assignatura

Codi	34681
Nom	Seguretat informàtica
Cicle	Grau
Crèdits ECTS	6.0
Curs acadèmic	2021 - 2022

Titulació/titulacions

Titulació	Centre	Curs	Període
1400 - Grau Eng.Informàtica	Escola Tècnica Superior d'Enginyeria	3	Segon quadrimestre
1407 - Grau en Enginyeria Multimedia	Escola Tècnica Superior d'Enginyeria	4	Segon quadrimestre

Matèries

Titulació	Matèria	Caràcter
1400 - Grau Eng.Informàtica	14 - Sistemas Operativos, Sistemas Distribuidos y Redes	Obligatòria
1407 - Grau en Enginyeria Multimedia	19 - Optativitat	Optativa

Coordinació

Nom	Departament
PEREZ CONDE, CARLOS	240 - Informàtica
SORIANO GARCIA, FRANCISCO R	240 - Informàtica

RESUM

La seguretat és un atribut essencial dels sistemes informàtics. Fins i tot en una disciplina com la informàtica, en la qual els canvis són continus, els requisits de seguretat canvien a un ritme especialment ràpid. Aquest ritme es deu sobretot a dues raons. La primera és que la dependència de sistemes informàtics és cada vegada major, pel que el nivell d'exigència augmenta. La segona és la contínua aparició de noves tecnologies. Aquestes noves capacitats permeten implantar mecanismes de seguretat més refinats, però al mateix temps també possibiliten la realització d'atacs més sofisticats, el que provoca un canvi continu.

En aquest context, l'assignatura està plantejada per a donar una visió de conjunt dels elements essencials de la seguretat dels sistemes informàtics, intentant que l'alumnat aprenga a seguir aquest procés de canvi continu i siga capaç de mantenir-se al dia i d'utilitzar, a cada moment, les tècniques més apropiades. En aquest sentit, l'assignatura es basa substancialment en els conceptes específics introduïts en les assignatures de xarxes, sistemes operatius, bases de dades i programació, al mateix temps que els complementa amb continguts propis de l'exercici professional de la seguretat, com l'establiment de polítiques de seguretat, l'anàlisi de vulnerabilitats, la detecció d'intrusos o l'anàlisi forense.

L'assignatura “Seguretat informàtica” s'imparteix en el segon quadrimestre de tercer curs com part de la matèria “Sistemes operatius, sistemes distribuïts i xarxes”.

CONEIXEMENTS PREVIS

Relació amb altres assignatures de la mateixa titulació

No heu especificat les restriccions de matrícula amb altres assignatures del pla d'estudis.

Altres tipus de requisits

Es recomana haver cursat les següents assignatures: Programació, Estructures de dades i algorismes, Sistemes operatius i Arquitectura de xarxes de computadors. D'entre elles, són especialment rellevants les dues últimes, per tractar alguns conceptes relacionats amb la seguretat que complementen els continguts estudiats en aquesta assignatura.

COMPETÈNCIES (RD 1393/2007) // RESULTATS DE L'APRENENTATGE (RD 822/2021)

1400 - Grau Eng.Informàtica

- G3 - Capacitat per dissenyar, desenvolupar, avaluar i assegurar l'accessibilitat, l'ergonomia, la usabilitat i la seguretat dels sistemes, dels serveis i de les aplicacions informàtiques, així com de la informació que gestionen.
- G4 - Capacitat per definir, avaluar i seleccionar plataformes maquinari i programari per al desenvolupament i l'execució de sistemes, serveis i aplicacions informàtiques, d'acord amb els coneixements adquirits segons les competències específiques establertes.
- G6 - Capacitat per concebre i desenvolupar sistemes o arquitectures informàtiques centralitzades o distribuïdes integrant maquinari, programari i xarxes d'acord amb els coneixements adquirits segons les competències específiques establertes.

- R1 - Capacitat per dissenyar, desenvolupar, seleccionar i avaluar aplicacions i sistemes informàtics, assegurant-ne la fiabilitat, la seguretat i la qualitat, d'acord amb principis ètics i amb la legislació i la normativa vigents.
- R5 - Coneixement, administració i manteniment sistemes, serveis i aplicacions informàtiques.
- TI2 - Capacitat per seleccionar, dissenyar, desplegar, integrar, avaluar, construir, gestionar, explotar i mantenir les tecnologies de maquinari, programari i xarxes, dins els paràmetres de cost i qualitat adequats.
- TI7 - Capacitat per comprendre, aplicar i gestionar la garantia i la seguretat dels sistemes informàtics.
- SI2 - Capacitat per determinar els requisits dels sistemes d'informació i de comunicació d'una organització atenent aspectes de seguretat i compliment de la normativa i la legislació vigents.

RESULTATS D'APRENENTATGE (RD 1393/2007) // SENSE CONTINGUT (RD 822/2021)

- Dissenyar i avaluar la política de seguretat d'una organització, incloent tant l'anàlisi prèvia com la gestió d'incidents.
- Dissenyar, implantar, mantenir i avaluar els mecanismes de seguretat necessaris per a garantir el compliment de la política de seguretat.
- Dissenyar, implantar, mantenir i avaluar els mecanismes necessaris per a detectar incidents i per a poder tractar-los adequadament.
- Avaluar nous productes i tecnologies i, si escau, aplicar-los per a mantenir el nivell de seguretat requerit.
- Coordinar-se amb altres professionals tècnics (administradors de sistemes, de xarxes, de bases de dades, d'aplicacions...) per a assolir un correcte funcionament dels sistemes informàtics.
- Informar adequadament de les incidències de seguretat, així com interpretar de forma adequada els avisos de seguretat llançats per uns altres, especialment els dels centres de resposta (CERTs).
- Explicar tant als usuaris com als directius el perquè de les mesures de seguretat.

DESCRIPCIÓ DE CONTINGUTS

1. Introducció

Concepte de seguretat
Què volem protegir i per què? Política de seguretat
Enfront de què? Riscos i vulnerabilitats
El procés de la seguretat
Normatives (ètica, legislació i estàndards, ISACA, ISO 27000, IS2)

2. Mecanismes de seguretat

Aquesta unitat temàtica està formada per tres temes:
- Criptografia (3 hores TP)
Simètrica
Asimètrica
Hashes
- Seguretat del node
Validació i autenticació
Control d'accés
Programació segura
Seguretat del servidor i seguretat del client
- Seguretat perimètrica
Tecnologies bàsiques
Arquitectures de tallafocs
Tallafocs d'aplicacions

3. Detecció i tractament d'intrusions

Detecció d'intrusos basada en el host (HIDS)
Detecció d'intrusos basada en la xarxa (NIDS)
Honeypots i honeynets
Anàlisi forense

4. Auditoria i hacking ètic

Introducció al procés d'auditoria
El test d'intrusió i els seus tipus
Fases d'un atac/test d'intrusió
Eines per al hacking ètic

VOLUM DE TREBALL

ACTIVITAT	Hores	% Presencial
Classes de teoria	30,00	100
Pràctiques en laboratori	20,00	100
Pràctiques en aula	10,00	100
Elaboració de treballs en grup	10,00	0
Estudi i treball autònom	20,00	0
Lectures de material complementari	10,00	0
Preparació d'activitats d'avaluació	20,00	0
Preparació de classes de teoria	20,00	0
Preparació de classes pràctiques i de problemes	10,00	0
TOTAL	**150,00**	

METODOLOGIA DOCENT

Les activitats formatives es desenvoluparan d'acord amb la següent distribució:

•Activitats teòriques. En les classes teòriques es desenvoluparan els temes proporcionant una visióglobal i integradora, analitzant amb major detall els aspectes clau i de major complexitat, fomentant,en tot moment, la participació de l'alumnat.

•Activitats pràctiques. Complementen les activitats teòriques amb l'objectiu d'aplicar els conceptesbàsics i ampliar-los amb el coneixement i l'experiència que vagen adquirint durant la realització delstreballs proposats. Comprenen els següents tipus d'activitats presencials: classes de problemes i qüestions en aula, sessions de discussió i resolució de problemes i exercicis prèviament treballats perl'alumnat, pràctiques de laboratori , presentacions orals, conferències, tutories programades(individualitzades o en grup)

•Treball personal de l'alumnat. Realització (fora de l'aula) de treballs monogràfics, recerca bibliogràficadirigida, qüestions i problemes, així com la preparació de classes i exàmens (estudi). Aquesta tasca es realitzarà de manera individual i intenta potenciar el treball autònom.

•Treball en menuts grups. Realització, per part de menuts grups d'estudiants (2-4) de treballs,qüestions, problemes fora de l'aula. Aquesta tasca complementa el treball individual i fomenta la capacitat d'integració en grups de treball.

AVALUACIÓ

L'assignatura podrà ser avaluada de dues formes distintes, una donant major pes a les activitats presencials i altra amb major pes per a l'examen final. Cada estudiant tindrà com nota final la més alta de les dues.

L'avaluació de l'assignatura es portarà a terme en la primera convocatòria mitjançant:

- Avaluació de la teoria i els problemes (TP).

Aquesta part tindrà un pes del 75 % de la nota final i serà necessari arribar a un 4,5 sobre 10 per a fer la mitjana.

Avaluació contínua (EC), basada en la participació i grau d'implicació en el procés d'ensenyament-aprenentatge, tenint en compte l'assistència regular a les activitats presencials previstes i la resolució de qüestions i problemes proposats. Aquesta part no és recuperable.

Proves objectives individuals, consistents en diversos exàmens o proves de coneixement, que constaran tant de qüestions teòric-pràctiques com de problemes. Les proves es realitzaran cap a la primera meitat del quadrimestre (denominada T1), durant la segona meitat del quadrimestre (T2) i fora de l'horari lectiu en el període d'exàmens (denominada T3). Cadascuna d'aquestes proves abordarà tots els continguts de l'assignatura impartits fins al moment de la seua realització.

La nota de TP es calcularà de la següent forma:

TP = 0,15 * EC + 0,15 * T1 + 0,25 * T2 + 0,45 * T3

- Avaluació de les activitats pràctiques de laboratori (L) a partir de la consecució d'objectius en les sessions de laboratori.

Aquestes activitats es realitzaran per parelles, el seu pes serà del 25 % sobre la nota final i serà necessari arribar a un 4,5 sobre 10 per a fer la mitjana. Totes les sessions de laboratori tindran el mateix pes sobre la nota final. En cas de no poder assistir a una sessió, l'estudiant podrà lliurar el treball corresponent al seu professor o professora de laboratori. El lliurament haurà de ser en persona, en horari de tutories i l'estudiant haurà d'estar preparat per a respondre qüestions sobre la realització de la pràctica i per a realitzar parts de la mateixa en el moment (amb menuts canvis). Aquest tipus de lliurament ha de ser realitzat abans que cap grup de laboratori haja realitzat la pràctica i tindrà una penalització del 20 %.

La nota de l'assignatura es conformarà en el cas de seguir l'avaluació contínua com la suma

de les parts anteriors de la següent manera:

Si TP < 4,5 o L < 4,5

NotaFinal = Mínim(TP, TL)

En altre cas:

Notafinal = 0,75 * TP + 0,25 * L

En cas de no haver superat l'assignatura seguint l'avaluació contínua (o en cas que la nota calculada d'aquesta segona forma resultara més favorable per a l'estudiant), la prova d'avaluació T3 serà l'examen final de l'assignatura i TP es calcularà de la següent forma:

TP = 0,15 * EC + 0,85 * T3

La nota final es calcularà de la mateixa forma que amb l'avaluació contínua.

En la segona convocatòria l'assignatura s'avaluarà de la mateixa forma que en la primera

convocatòria, amb les següents excepcions:

- S'obrirà un termini de lliurament de pràctiques amb les mateixes condicions que en la primera convocatòria (lògicament no es realitzaran en el laboratori), llevat que la penalització serà del 30 % i que el lliurament haurà de realitzar-se abans de l'examen de la segona convocatòria.
- L'examen de la segona convocatòria substituirà a la prova T3.
- En EC es mantindrà la nota de l'estudiant.

Per a poder sol·licitar avançament de convocatòria, serà necessari haver cursat prèviament l'assignatura i haver obtingut la nota mínima exigida en l'avaluació de les activitats pràctiques de laboratori (L). D'aquesta forma es tracta de conciliar el dret de l'estudiantat a aquest avançament amb la metodologia docent i el mecanisme d'avaluació de l'assignatura.

REFERÈNCIES

Bàsiques

- Charles P. Pfleeger; Shari Lawrence Pfleeger; Jonathan Margulies. Security in Computing, Fifth Edition. Prentice Hall, 2015. ISBN-13: 978-0-13-408504-3.
- Stephen Northcutt et altres, Inside Network Perimeter Security. Sams; 2005, ISBN-13: 978-0672327377.

Complementàries

- Elizabeth D. Zwicky et altres, Building Internet Firewalls, O'Reilly Media, Inc 2nd edition;2000, ISBN-13: 978-1-56592-871-8
- C. Pogue et altres, Unix and Linux Forensic Analysis DVD Toolkit. Syngress; 2008, ISBN-13: 978-1597492690
- John Vacca, Computer and Information Security Handbook, 2nd Edition, Morgan Kaufmann, 2012, ISBN-13: 978-0-12-394397-2
- B. Carrier, File system forensic analisys, Addison-Wesley Professional; 2005, ISBN-13: 978-0321268174
- Lance Spitzner, Honeypots: tracking hackers, Addison-Wesley Professional, 2002, ISBN-13: 978-0321108951
- D. Farmer, W. Venema, Forensic Discovery, Addison-Wesley Professional; 2005, ISBN-13: 978-0201634976
- Bruce Schneier. Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition. John Wiley & Sons, 1996. ISBN: 978-0-471-11709-4

ADDENDA COVID-19

Aquesta addenda només s'activarà si la situació sanitària ho requereix i previ acord del Consell de Govern

Si la situació sanitària ho requereix, la Comissió Acadèmica de la Titulació aprovarà un Model Docent de la Titulació i la seua adaptació a cada assignatura, establint-se en aquest model les condicions concretes en les quals es desenvoluparà la docència de l'assignatura, tenint en compte les dades reals de matrícula i la disponibilitat d'espais.