

**FITXA IDENTIFICATIVA****Dades de l'Assignatura**

Codi	34896
Nom	Seguretat informàtica
Cicle	Grau
Crèdits ECTS	6.0
Curs acadèmic	2019 - 2020

Titulació/titulacions

Titulació	Centre	Curs	Període
1403 - Grau d'Enginyeria Telemàtica	Escola Tècnica Superior d'Enginyeria	3	Segon quadrimestre

Matèries

Titulació	Matèria	Caràcter
1403 - Grau d'Enginyeria Telemàtica	16 - Administració de Sistemes	Obligatòria

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'alumne 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 "Administració de sistemes".

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: Informàtica, Ampliació d'Informàtica, 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

1403 - Grau d'Enginyeria Telemàtica

- R1 - Capacitat per aprendre de manera autònoma nous coneixements i tècniques adequats per a la concepció, el desenvolupament o l'explotació de sistemes i serveis de telecomunicació.
- G4 - Capacitat per resoldre problemes amb iniciativa, presa de decisions, creativitat, i de comunicar i transmetre coneixements, habilitats i destreses, comprenent la responsabilitat ètica i professional de l'activitat de l'enginyer tècnic de telecomunicació.
- E1 - Capacitat per construir, explotar i gestionar les xarxes, els serveis, els processos i les aplicacions de telecomunicacions, enteses aquestes com a sistemes de captació, transport, representació, processament, emmagatzemament, gestió i presentació d'informació multimèdia, des del punt de vista dels serveis telemàtics.
- E2 - Capacitat per aplicar les tècniques en què es basen les xarxes, els serveis i les aplicacions telemàtiques, com ara sistemes de gestió, senyalització i commutació, encaminament, seguretat (protocols criptogràfics, tunelització, tallafores, mecanismes de cobrament, d'autenticació i de protecció de continguts), enginyeria de tràfic (teoria de grafs, teoria de cues i teletràfic) tarifació i fiabilitat i qualitat de servei, tant en entorns fixos, mòbils, personals, locals o a gran distància, amb diferents amplituds de banda, incloent-hi telefonia i dades.
- E3 - Capacitat per construir, explotar i gestionar serveis telemàtics utilitzant eines analítiques de planificació, de dimensionat i d'anàlisi.



RESULTATS DE L'APRENTATGE

- Dissenyar i avaluar la política de seguretat d'una organització, incloent tant l'anàlisi prèvia com la gestió d'incidents (G-4, E-2).
- Dissenyar, implantar, mantenir i avaluar els mecanismes de seguretat necessaris per a garantir el compliment de la política de seguretat (G-4, R-1, E-2).
- Dissenyar, implantar, mantenir i avaluar els mecanismes necessaris per a detectar incidents i per a poder tractar-los adequadament (G-4, E-2).
- Avaluar nous productes i tecnologies i, si escau, aplicar-los per a mantenir el nivell de seguretat requerit (G-4, R-1, E-2).
- 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 (G-4, E-2).
- 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) (G-4, E-2).
- Explicar tant als usuaris com als directius el perquè de les mesures de seguretat (G-4, E-2).

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:

A- Criptografia

-- Simètrica

-- Asimètrica

-- Hashes

-- Laboratori

B- Seguretat del node

-- Validació i autenticació

-- Control d'accés

-- Programació segura

-- Seguretat del servidor i seguretat del client

-- Laboratori

C- Seguretat perimètrica

-- Tecnologies bàsiques

-- Arquitectures de tallafocs



- Tallafocs d'aplicacions
- Laboratori

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
Laboratori

4. Auditoria i Hacking Ètic

Introducció al procés d'auditoria
El test d'intrusió i els seus tipus
Fases d'un ataqüe/test d'intrusió
Ferramentes per a l'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 visió global i integradora, analitzant amb major detall els aspectes clau i de major complexitat, fomentant, en tot moment, la participació de l'alumnat (E-2).
- Activitats pràctiques. Complementen les activitats teòriques amb l'objectiu d'aplicar els conceptes bàsics i ampliar-los amb el coneixement i l'experiència que vagen adquirint



durant la realització dels treballs 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 per l'alumnat, pràctiques de laboratori, presentacions orals, conferències, tutories programades (individualitzades o en grup) (G-4, E-2)

- Treball personal de l'alumnat. Realització (fora de l'aula) de treballs monogràfics, recerca bibliogràfica dirigida, 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. (G-4, R-1, E-2).

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 (G-4, R-1, E-2).

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. Tots els alumnes tindran 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. Esta part no és recuperable. (G-4, R-1, E-2).

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. (G-4, E-2)

La nota de TP es calcularà de la següent forma:

$$TP = 0,20 * EC + 0,15 * T1 + 0,25 * T2 + 0,4 * T3$$

- Avaluació de les activitats pràctiques de laboratori (L) a partir de la consecució d'objectius en les sessions de laboratori. (G-4, E-2)

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'alumne podrà lliurar el treball corresponent al seu professor de laboratori. El lliurament haurà de ser en persona, en horari de tutories i l'alumne 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 $L < 4,5$

$NotaFinal = \text{Mínim}(*TP, *TL)$

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'alumne), la prova d'avaluació T3 serà l'examen final de l'assignatura i TP es calcularà de la següent forma:

$TP = 0,20 * EC + 0,80 * T3$

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 la part EC es mantindrà la nota de l'alumne.

Avançament de convocatòria

Per a poder sol·licitar avançament de convocatòria, els estudiants hauran d'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 dels estudiants a aquest avançament amb la metodologia docent i el mecanisme d'avaluació de l'assignatura.

En qualsevol cas, el sistema d'avaluació es regirà per l'establert en el Reglament d'Avaluació i Qualificació de la Universitat de València per a Graus i Màsters. (

http://www.uv.es/graus/normatives/2017_108_Reglament_avaluacio_qualificacio.pdf).



REFERÈNCIES

Bàsiques

- Referencia b1: Charles P. Pfleeger et altres, Security in Computing, Fifth Edition, Prentice Hall, 2015, ISBN-13: 978-0-13-408507-4
- Referencia b2: Stephen Northcutt et altres, Inside Network Perimeter Security. Sams; 2005, ISBN-13: 978-0672327377
- Bruce Schneier. Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition. John Wiley & Sons, 1996. ISBN: 978-0-471-11709-4

Complementàries

- Referencia c1: Elizabeth D. Zwicky et altres, Building Internet Firewalls, O'Reilly Media, Inc 2nd edition; 2000, ISBN-13: 978-1-56592-871-8
- Referencia c2: C. Pogue et altres, Unix and Linux Forensic Analysis DVD Toolkit. Syngress; 2008, ISBN-13: 978-1597492690
- Referencia c3: John Vacca, Computer and Information Security Handbook, 2nd Edition, Morgan Kaufmann, 2012, ISBN-13: 978-0-12-394397-2
- Referencia c4: B. Carrier, File system forensic analysis, Addison-Wesley Professional; 2005, ISBN-13: 978-0321268174
- Referencia c5: Lance Spitzner, Honeypots: tracking hackers, Addison-Wesley Professional, 2002, ISBN-13: 978-0321108951
- Referencia c6: D. Farmer, W. Venema, Forensic Discovery, Addison-Wesley Professional; 2005, ISBN-13: 978-0201634976

ADDENDA COVID-19

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

1. Contenidos

Se mantienen los contenidos inicialmente recogidos en la guía docente

2. Volumen de trabajo y planificación temporal de la docencia

Mantenimiento del peso de las distintas actividades que suman las horas de dedicación en créditos ECTS marcadas en la guía docente original



3. Metodología docente

A principios de la semana se proponen las transparencias que deben ser revisadas por los alumnos. Se pone posteriormente en un foro unas cuantas preguntas o problemas para comprobar si se han entendido los conceptos principales. Al finalizar la semana el profesor indica la respuesta correcta y los errores cometidos.

Además, se cuelga un video locutado de algunas transparencias y se realizan algunas pruebas de examen online con carácter no puntuable.

Todas las prácticas de laboratorio se pueden hacer desde casa usando la máquina virtual NETinVM.

Para tutorías, vía e-mail a cualquier hora, uso de aula virtual y foros.

Todas las tareas de cada semana están puestas el lunes a primera hora y deben ser realizadas hasta sábado a última hora.

4. Evaluación

Criterio de evaluación único:

$$02EC + 0,15T1 + 0,2T3 + 0,45Lab$$

Se ha pasado peso de examen T3 a Lab. Los otros apartados ya estaban hechos antes de la interrupción de clases presenciales.

Además, alternativamente el examen T3 puede ser sustituido por Trabajo individual para alumnos que indiquen problemas de recursos de hardware o de red. Si una persona no dispone de los medios para establecer esta conexión y acceder al aula

virtual, deberá contactar con el profesorado por correo electrónico en el momento de publicación de este anexo a la guía docente

No hay nota mínima en ningún apartado.

Para segunda convocatoria:

Se pueden volver a entregar todos o algunos laboratorios (Lab) y realizar un nuevo examen (T3) o trabajo y desaparece el T1 siendo el nuevo criterio de evaluación:



02EC + 0,2T3 + 0,6Lab

5. Bibliografia

La bibliografia recomendada se mantiene

