

**FITXA IDENTIFICATIVA****DADES DE L'ASSIGNATURA**

Codi: 34681
Nom: Seguretat informàtica
Cicle: Grau
Crèdits ECTS: 6
Curs acadèmic: 2025-26

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	Sistemas Operativos, Sistemas Distribuidos y Redes	OBLIGATÒRIA
1407 - Grau en Enginyeria Multimedia	Optativitat	OPTATIVA

COORDINACIÓ

SORIANO GARCIA FRANCISCO R

PEREZ CONDE CARLOS

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".

"Sistemes operatius, sistemes distribuïts i xarxes".

CONEIXEMENTS PREVIS

RELACIÓ AMB ALTRES ASSIGNATURES DE LA MATEIXA TITULACIÓ

No s'ha especificat 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 / RESULTATS D' APRENENTATGE

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.

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.



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.

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. Criptografia**
 - Criptografia simètrica
 - Criptografia asimètrica
 - Funcions de dispersió (hashes)
 - Comunicació i emmagatzematge segurs
 - Integritat
 - Signatura digital
 - Gestió de claus públiques
 - Autenticació i intercanvi de claus de sessió
 - Privacitat
 - Laboratori
- 3. Seguretat del node**
 - Validació i autenticació
 - Control d'accés
 - Seguretat dels programes
 - Seguretat de servidors i clients
 - Laboratori
- 4. Seguretat perimètrica**
 - Concepte de tallafocs
 - Filtrat de paquets
 - Proxies
 - Disseny de tallafocs
 - Integració de VPNs
 - Laboratori
- 5. 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
- 6. 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 (HORES)

ACTIVITATS PRESENCIALS

Activitat	Hores
Teoria	30,00
Pràctiques a l'aula	10,00
Laboratori	20,00
Total hores	60,00

ACTIVITATS NO PRESENCIALS

Activitat	Hores
Assistència a altres activitats	0,00
Elaboració de treballs individuals o en grup	10,00
Estudi i treball autònom	30,00
Preparació de classes	30,00
Preparació d'activitats d'avaluació	20,00
Resolució de casos pràctics	0,00
Total hores	90,00

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.

- 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)

- 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.

- Treball en petits grups. Realització, per part de petits 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.

S'utilitzarà la plataforma d'e-learning (Aula Virtual) de la Universitat de València com suport de comunicació amb l'alumnat. A través d'ella es tindrà accés al material didàctic utilitzat en classe, així com els problemes i exercicis a resoldre.

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 70 % 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 30 % 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 menor que 4,5 o L menor que 4,5

NotaFinal = Mínim(TP, TL)

En altre cas:

Notafinal = 0,7 * TP + 0,3 * 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.

En qualsevol cas, l'avaluació de l'assignatura es farà d'acord amb el Reglament d'avaluació i qualificació de la Universitat de València per a títols de grau i de màster, aprovat en la sessió del Consell de Govern de 30 de maig de 2017 (ACGUV 108/2017). Així mateix, la còpia o plagi manifest de qualsevol activitat que forma part de l'avaluació suposarà la impossibilitat de superar l'assignatura, sotmetent-se seguidament als procediments disciplinaris oportuns indicats en el [PROTOCOL D'ACTUACIÓ DAVANT PRÀCTIQUES FRAUDULENTES A LA UNIVERSITAT DE VALÈNCIA \(ACGUV 123/2020\)](#).

**BIBLIOGRAFIA**

- Pfleeger, Charles P., et al. Security in Computing. Sixth edition., Addison Wesley Professional, 2024.
- Kizza, Joseph Migga. Guide to Computer Network Security. 6th ed. 2024., Springer International Publishing, 2024, <https://doi.org/10.1007/978-3-031-47549-8>.
- Vacca, John R., editor. Computer and Information Security Handbook. Volume 1. Fourth edition., Morgan Kaufmann, 2025.
- Pfleeger, Charles P., and Shari Lawrence Pfleeger. Analyzing Computer Security: A Threat/Vulnerability/Countermeasure Approach. 1st edition, Prentice Hall, 2012.
- Tanenbaum, Andrew S., and David J. Wetherall. Computer Networks. 5th ed., Pearson, 2014.
- Schneier, Bruce. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 20th anniversary edition., Wiley, 2015.
- Zwicky, Elizabeth D., et al. Building Internet Firewalls. 2nd ed., O'Reilly, 2000.
- Northcutt, Stephen. Inside Network Perimeter Security. 2nd ed., Sams, 2005.
- Khan, Umer. Cisco PIX Firewalls: Configure / Manage / Troubleshoot. 1st ed., Elsevier Science & Technology Books, 2005, <https://doi.org/10.1016/B978-1-59749-004-7.X5000-6>.
- Sammons, John. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. Second edition., Syngress, 2015.
- Nikkel, Bruce. Practical Linux Forensics. No Starch Press, 2021.
- Carrier, Brian. File System Forensic Analysis. Addison-Wesley, 2005.
- Farmer, Dan, and Wietse Venema. Forensic Discovery. Addison-Wesley, 2004.
- Shiva V. N. Parasram. Digital Forensics with Kali Linux - Second Edition. Packt Publishing, 2020.
- Cannon, David, et al. CISA: Certified Information Systems Auditor Study Guide. 4th ed., Sybex, a Wiley brand, 2016.
- Engebretson, Patrick. The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy. Second edition, Elsevier Science, 2013.
- Graham, Daniel. Ethical Hacking. No Starch Press, 2021.
- Sheikh, Ahmed. Certified Ethical Hacker (CEH) Preparation Guide: Lesson-Based Review of Ethical Hacking and Penetration Testing. 1st ed., Apress, 2021, <https://doi.org/10.1007/978-1-4842-7258-9>.
- Velu, Vijay Kumar. Mastering Kali Linux for Advanced Penetration Testing: Become a Cybersecurity Ethical Hacking Expert Using Metasploit, Nmap, Wireshark, and Burp Suite. Fourth edition., Packt Publishing, Limited, 2022.