FIŞA DISCIPLINEI

1. Date despre program

1.1 Instituția de învățământ superior	**UNIVERSITATEA DIN ORADEA**
1.2 Facultatea	**FACULTATEA DE INGINERIE ELECTRICĂ ŞI TEHNOLOGIA INFORMAȚIEI**
1.3 Departamentul	**CALCULATOARE si TEHNOLOGIA INFORMATIEI**
1.4 Domeniul de studii	**TEHNOLOGIA INFORMATIEI**
1.5 Ciclul de studii	**LICENȚĂ**
1.6 Programul de studii/Calificarea	**Tehnologia Informației**

2. Date despre disciplină

2.1 Denumirea disciplinei	**Securitatea datelor**						
2.2 Titularul activităților de curs	**Prof.univ.dr.habil. Daniela Elena POPESCU**						
2.3 Titularul activităților de laborator/proiect	**Prof.univ.dr.habil. Daniela Elena POPESCU**						
2.4 Anul de studiu	**III**	2.5 Semestrul	**6**	2.6 Tipul de evaluare	**Ex**	2.7 Regimul disciplinei	**DS**

3. Timpul total estimat (ore pe semestru al activităților didactice)

3.1 Număr de ore pe săptămână	**4**	din care: 3.2 curs	**2**	3.3 laborator /proiect	**1/1**
3.4 Total ore din planul de învățământ	**56**	din care: 3.5 curs	**28**	3.6 laborator /proiect	**28**
Distribuția fondului de timp ore					ore
Studiul după manual, suport de curs, bibliografie și notițe					28
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren					8
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri					**14**
Tutoriat					2
Examinări					4
Alte activități.....					

3.7 Total ore studiu individual	**56**
3.9 Total ore pe semestru	**112**
3.10 Numărul de credite	**4**

4. Precondiții (acolo unde este cazul)

4.1 de curriculum	Sisteme de operare	
4.2 de competențe	Arhitecturi de sisteme de calcul	

5. Condiții (acolo unde este cazul)

5.1. de desfășurare a cursului	- Cursul se poate desfășura față în față sau on-line" - prezență la minim 50% din cursuri	- prezen
5.2. de desfășurare a laboratorului /proiectului	- Seminarul/laboratorul/proiectul se pot desfășura față în față sau on-line - Prezenta obligatorie la toate laboratoarele; - Studenții trebuie să fi parcurs partea teoretică a lucrării; - Se pot recupera pe parcursul semestrului maxim 4 lucrări (30 %); - Frecvența la orele de laborator sub 70% conduce la refacerea disciplinei	- Prezen - Studen - Se pot - Frecve

6.a. Competențele specifice acumulate

Competențe profesionale	• Definirea conceptelor manageriale de baza necesare implementării unui mediu de funcționare cu securitate înaltă la nivelul organizațiilor • Dezvoltarea şi implementarea unor modele de proces ale managementului unui cloud privat. • Fundamentarea științifică a deciziilor de management cu privire la prezervarea si creșterea securității proceselor precum şi implementarea şi urmărirea efectelor acestora în cadrul organizației
Competențe transversale	• Asumarea rolurilor specifice şi a responsabilităților de conducere a unor echipe angajate în activități de dezvoltare infrastructurilor/sistemelor cu securitate înaltă • Creșterea interesului pentru realizarea corectă a unei cercetări științifice şi pentru urmarea unei cariere în cercetare.

6.b. Rezultatele aşteptate ale învățării

Cunoştințe	Studentul/absolventul descrie, identifică, sumarizează concepte și metode elementare privitoare la limbaje de programare, medii de programare, tehnici de programare, baze de date, inteligență artificială și inginerie software și modul lor de aplicare în probleme concrete.
Aptitudini	Studentul/absolventul alege şi explică concepte proprii specifice proiectării algoritmilor, programării orientate pe obiecte, programării logice și funcționale. Studentul/absolventul specifică cerințe, analizează, elaborează, dezvoltă și testează programe în limbaje de programare de uz general (C, etc.) și /sau obiect-orientate (C++, Java, etc.), aplicând elementele specifice ingineriei software. Studentul/absolventul proiectează, implementează, dezvoltă și /sau gestionează aplicații ce includ diverse tipuri de baze de date.
Responsabilitate și autonomie	Studentul/absolventul are o comportare onorabilă, responsabilă, etică, în spiritul legii pentru a asigura reputația profesiei.

7. Obiectivele disciplinei (rezulta din grila competențelor specifice acumulate)

7.1 Obiectivul general al disciplinei	Familiarizarea studenților cu elementele definitorii pentru implementarea si creșterea nivelului de securitate a informațiilor la nivel organizațional precum si identificarea strategiilor sănătoase de dezvoltare instituțională sub acest aspect
7.2 Obiectivele specifice	• Disciplina are ca obiectiv familiarizarea studenților cu problemele de securitate a informației, cu ceea ce reprezintă vulnerabilitățile datelor, cu modul in care se pune problema protecției sistemelor atât neconectate in rețea cat si a celor conectate in rețea. • Cursul isi propune prezentarea caracteristicilor de baza ale problemelor de securizare a informației, având ca scop dezvoltarea capabilităților de dezvoltare a politici de securitate in ansamblu in vederea protejării informației • Laboratoarele sunt orientate spre prezentarea in prima faza a problemelor de Securitate la nivelul sistemelor de calcul, după care accentual cade asupra dezvoltării abilitaților de utilizarea a tool-urilor utile pentru scanarea si identificarea

	vulnerabilităților, pe prezentarea etapelor si a modului in care se realizează testele de penetrării a sisteme, precum si protecțiilor ce se pot lua in acest sens .

8. Conținuturi

8.1.Curs	Metode de predare	Observații
1. **Introducere în securitatea datelor** o Definiții și concepte de bază o Importanța securității datelor 2. **Principii fundamentale ale securității informațiilor** o Confidențialitate, integritate și disponibilitate o Managementul riscurilor 3. **Reglementări și standarde de securitate** o GDPR, HIPAA, ISO/IEC 27001 o Alte reglementări relevante 4. **Amenințări și vulnerabilități** o Tipuri de amenințări (malware, phishing, etc.) o Identificarea și analiza vulnerabilităților 5. **Măsuri de protecție a datelor** o Controlul accesului și autentificarea o Criptografie și protecția datelor în tranzit și în repaus 6. **Politici și proceduri de securitate** o Crearea și implementarea politicilor de securitate o Proceduri de gestionare a incidentelor 7. **Securitatea rețelelor** o Protecția rețelelor locale și globale o Firewall-uri, IDS/IPS 8. **Securitatea aplicațiilor** o Securitatea dezvoltării software-ului o Testarea și evaluarea securității aplicațiilor 9. **Backup și recuperare în caz de dezastru** o Strategii de backup o Planuri de recuperare și continuitate 10. **Audit și monitorizare** o Tehnici de auditare a securității o Monitorizarea activităților și detectarea anomaliilor 11. **Securitatea fizică și a infrastructurii** o Protecția echipamentelor fizice o Măsuri de securitate a infrastructurii IT 12. **Aspecte legale și etice în securitatea datelor** o Drepturile și responsabilitățile legale o Dilemele etice și gestionarea acestora	• Expunere libera curs cu videoproiector/ retroproiector si tabla într-o maniera interactiva: punctate din când in când întrebări pentru studenți in scopul creșterii gradului de interactivitate • Indicarea unor teme pentru documentare si studiu individual	28 ore

13. **Tendințe emergente și viitorul securității datelor** o Tehnologii emergente (blockchain, AI, etc.) o Provocări și oportunități viitoare 14. **Managementul securității informației – privire globala, suita de protocoale ISO 27000, GDPR**		
Bibliografie 1. Notițe de curs (slide-uri) puse la dispoziție studenților in format electronic pe platforma Office 365 2. Stallings W, Cryptography and Network Security Principles and Practice, Third Edition, Prentice Hall, 2003, 3. D.E.Popescu, Managementul securității informației, Editura Universității din Oradea, 2012 4. Computer Hacking, Security testing, Penetration testing and basic Security, Author: Cary hall & Erin Watson, Kindle edition, free, https://www.amazon.com/Hacking-Computer-Security-Testing-Penetration-ebook/dp/B01N1UPX8D 5. ITIL 6. 6 https://portswigger.net		
8.2. Laborator	Metode de predare	Observații
1. 1. Prezentarea activitatilor de laborator, laboratoare, reguli de protectia muncii si semne conventionale specifice domeniului sistemelor informatice - informatii generale, generale privind protectia si monitorizarea datelor 2. Anonimat și confidențialitate, Darknet, darkweb. Studii de caz 4. Comparație între instrumentele de scanare în rețea și instrumentele de scanare a vulnerabilităților. 5. Utilizarea NMAP pentru scanarea porturilor și scanarea vulnerabilităților (sau alternativă Nessus). Case de studiu 6-7. Utilizarea facilităților Metaspoit. Case de studiu 8 programe SetUid. Exemple 9-13 Utilizarea platformei Portswigger pentru exploatarea vulnerabilităților aplicațiilor web. Cazuri selectate 14. Laboratorul didactic lucrează cu verificarea cunoştinţelor	Discuții si recomandări legate de temele primite spre rezolvare prin temele de proiect abordate	Se alocă 2 ore pentru fiecare dintre cele 14 puncte detaliate ale activității de laborator.
Bibliografie 1. D.E.Popescu, Managementul securității informației, Editura Universitatii din Oradea, 2012 2. Modulul Moodle cu lucrările de laborator 3. Webografie recomandata in cadrul orelor de proiect 4. Platforma Portswigger - https://portswigger.net 5. Metasploit: The Penetration Tester's Guide, Authors: David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni, https://www.amazon.com/Metasploit-Penetration-Testers-David-Kennedy/dp/159327288X		

9. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatori reprezentativi din domeniul aferent programului

- Conținutul disciplinei se regăsește în curricula specializărilor de Calculatoare si Tehnologia Informației și din alte centre universitare care au acreditate aceste specializări, iar cunoașterea problemelor legate de Cloud Computing precum și a modului de funcționare și proiectare a acestora este o cerință stringentă a angajatorilor din domeniu (Rds&Rcs, Plexus, Neologic, Celestica, Keysys etc).

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	- pentru nota 5 este necesară cunoașterea noțiunilor fundamentale cerute în subiecte, fără a	Evaluarea se poate face față în față sau on-line in funcție de situația impusa	70 %

	prezenta detalii asupra acestora - pentru nota 10, este necesară cunoașterea amănunțită a tuturor subiectelor		
10.5 Laborator	- pentru nota 5, cunoașterea in linii mari a alternativelor de soluționare a temei de proiect primita Concret: Pentru nota 5: răspuns corect la minim 1/3 din întrebările primite legate de tema proiectului - pentru nota 10, cunoașterea detaliata a soluției propuse cu prezentarea unor analize comparative pentru demonstrarea eficientei acesteia. Concret: Pentru nota 10: răspuns corect la toate întrebările legate	**Test + aplicație practică** La fiecare laborator studenții primesc un test și o notă. De asemenea, fiecare student primește o notă pentru activitatea la laborator în timpul semestrului și pentru dosarul cu lucrările de laborator. Astfel rezultă o medie pentru laborator. Întrebările sunt puse pe baza referatelor întocmite la lucrările de laborator.	30%
10.7 Standard minim de performanţă			
Asimilarea unor cunoștințe detaliate despre vulnerabilități, riscuri si soluții de securitate in gestionarea si vehicularea informației într-o companie Soluționarea la termen, în activități individuale și activități desfășurate în grup, în condiții de asistență calificată, a problemelor care necesită aplicarea de principii și reguli respectând normele deontologiei profesionale. Asumarea responsabilă de sarcini specifice în echipe pluri-specializate și comunicarea eficientă la nivel instituțional. • Dezvoltare a spiritului de echipă, spiritului de ajutorare reciprocă, conștientizarea importanței pregătirii pe parcursul semestrului pentru obținerea rezultatelor bune și durabile, conștientizarea importanței căutării, cercetării proprie legate de învățare (bibliotecă, internet), cultivarea unei discipline a muncii, efectuate corect și la timp			

Data completării
08.09.2025

Semnătura titularului de curs
Prof.dr.habil.D.E.Popescu

e-mail : depopescu@uoradea.ro

Semnătura titularului de laborator
Prof.dr.habil.D.E.Popescu

e-mail : depopescu@uoradea.ro

Data avizării în departament
___.09.2025

Semnătura directorului de departament,
Conf.univ.dr.ing.Elisa Valentina Moisi
emoisi@uoradea.ro

Data avizării în Consiliul Facultății
___.09.2025

Semnătură Decan
Prof. dr.habil. Eugen Gergely
egergely@uoradea.ro