



FIȘA DISCIPLINEI SECURITATEA BAZELOR DE DATE

1. Date despre program

1.1 Instituția de învățământ superior	UNIVERSITATEA „OVIDIUS” DIN CONSTANȚA
1.2 Facultatea	Matematică și Informatică
1.3 Departamentul	Matematică și Informatică
1.4 Domeniul de studii	Informatică
1.5 Ciclul de studii	Licență
1.6 Programul de studii	Securitate cibernetică și învățare automată / Cyber Security and Machine Learning
1.7 Anul universitar	2025-2026

2. Date despre disciplină

2.1 Denumirea disciplinei	Securitatea bazelor de date					
2.2 Cod disciplină	CSML.1.1.01					
2.3 Titularul activităților de curs	Conf. dr. Elena BĂUTU					
2.4 Titularul activităților aplicative	Conf. dr. Elena BĂUTU					
2.5 Anul de studii	1	2.6 Semestrul	1	2.7 Tipul de evaluare	E	2.8 Regimul disciplinei */**
						DF/DOB

* DF – disciplină fundamentală, DS – disciplină de specializare, DC – disciplină complementară

** DOB – disciplină obligatorie; DOP – disciplină opțională; DFA – Disciplină facultativă

3. Timpul total (ore pe semestru)

3.1 Număr de ore activități directe pe săptămână	4	din care: 3.2 curs	2	3.3 aplicații***	2
3.4 Total ore activități directe pe semestru	56	din care: 3.5 curs	28	3.6 aplicații	28
3.7 Total ore de studiu individual					69
Distribuția fondului de timp					[ore]
Studiul cărților, manualelor, suportului de curs,, notițelor, bibliografie minimală recomandată					20
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					10
Pregătire seminar / laborator / proiect, teme, referate, portofolii și eseuri					25
Pregătire pentru prezentări sau verificări					5
Pregătire pentru examinarea finală					7
Alte activități: consultații					2
3.8 Total ore pe semestru	125 (3.4. + 3.7)				
3.9 Numărul de credite	5				

*** S - seminar; L - laborator; P - proiect

4. Precondiții

4.1 de curriculum	Sisteme de operare, baze de date, sisteme de gestionare a bazelor de date
-------------------	---



4.2 de rezultate ale învățării	Înțelegerea conceptelor de bază ale bazelor de date relaționale, modelarea conceptuală, conceptele de gestionare a bazelor de date, limbajul SQL pentru interogarea, actualizarea și gestionarea bazelor de date relaționale.
--------------------------------	---

5. Condiții necesare pentru desfășurarea optimă a activităților didactice

5.1. de desfășurare a cursului	Sală de clasă dotată cu videoproiector disponibil Moodle/Webex/Microsoft Teams
5.2. de desfășurare a laboratorului*	Sală de laborator cu calculatoare disponibile Moodle/Webex/Microsoft Teams

*Se alege tipul de aplicație aferent disciplinei

6. Obiectivele disciplinei

6.1 Obiectivul general al disciplinei	Înțelegerea problemelor legate de securitatea bazelor de date și amenințările la adresa acestora. Înțelegerea tehnologiilor de securitate de ultimă generație. Identificarea soluțiilor pentru asigurarea securității bazelor de date.
6.2 Obiectivele specifice	Înțelegerea noțiunilor fundamentale de securitate a sistemelor de baze de date. Identificarea riscurilor și vulnerabilităților sistemului de operare din perspectiva bazelor de date. Înțelegerea modelelor de securitate a bazelor de date. Identificarea și utilizarea mecanismelor specifice de securitate a bazelor de date.

7. Rezultatele învățării

Cunoștințe	Studentul/absolventul - identifică și argumentează concepte fundamentale ale securității datelor și bazelor de date relaționale. - înțelege principiile securității bazelor de date, inclusiv autentificarea utilizatorilor, modelele de control al accesului și proiectarea securizată a bazelor de date.
Aptitudini	Studentul - proiectează, dezvoltă și demonstrează soluții software utilizând diverse tehnici și politici de securitate specifice bazelor de date relaționale. - implementează și configurează politici de securitate în sistemele de baze de date relaționale, monitorizează jurnalele de securitate și efectuează evaluări ale vulnerabilităților.
Responsabilitate și autonomie	Studentul/absolventul - efectuează acțiuni pentru dezvoltarea sistemelor software care utilizează baze de date și gestionează acțiunile necesare pentru a asigura securitatea maximă a bazelor de date relaționale. - asigură integritatea, confidențialitatea și disponibilitatea sistemelor de baze de date, asumându-și responsabilitatea pentru deciziile de securitate și respectarea standardelor etice și organizaționale.



8. Conținuturi

8.1 Curs	Metode de predare	Număr ore alocate
Fundamentele bazelor de date și securitate: Scurtă prezentare generală a sistemelor de gestionare a bazelor de date (SGBD) și a SGBD relaționale (SGBDR). Modelarea conceptuală a datelor: Modelul de date entitate-relație. Prezentare generală a modelului de date relațional și a bazelor de date relaționale. Constrângeri de integritate a datelor, forme normale. Tranzacții și proprietăți ACID. Baze de date distribuite și modele de date semi-structurate. Prezentare generală a securității bazelor de date: probleme generale de securitate, politici de securitate	Metode de predare interactive Dialog	6
Gestionarea utilizatorilor și controlul accesului Gestionarea utilizatorilor în bazele de date: Profiluri, politici de parolă, studii de caz în Oracle și PostgreSQL. Modele de control al accesului la date pentru baze de date relaționale. Proprietățile modelelor de control al accesului. Controlul accesului discreționar, matricea de acces. Controlul accesului obligatoriu. Controlul accesului bazat pe roluri, politici administrative. Baze de date relaționale securizate pe mai multe niveluri (Bell-LaPadula etc.)	Problemă Conversație euristică Studiu de caz Metode care contribuie la dezvoltarea gândirii critice.	4
Mecanisme de control al accesului în practică Grafic de privilegii și autorizații. Controlul accesului bazat pe roluri: studii de caz în Oracle (Privilegii și roluri) și PostgreSQL (Roluri, privilegii, securitate la nivel de rând). Securitate bazată pe conținut: PostgreSQL (securitate la nivel de coloană, vizualizări, partiționare, criptare a coloanelor), Oracle (securitate la nivel de rând, vizualizări, baze de date private virtuale). Criptarea datelor, gestionarea ciclului de viață al cheilor.	Învățare independentă Învățare cooperativă Sinteză / esențializare a informațiilor	10
Backup, recuperare și auditare Copiere de rezervă și recuperare în PostgreSQL: copie de rezervă/restaurare a sistemului de fișiere, dump SQL. Copiere de rezervă și recuperare în Oracle: copie de rezervă fizică și logică, instrumente specifice Oracle. Auditarea bazelor de date: studii de caz în Oracle și PostgreSQL	Lucru în echipă	6
Confidențialitatea și protecția datelor Mascarea și anonimizarea datelor. GDPR și reglementările privind confidențialitatea datelor. Implementări		2



Bibliografie

- [1]. Faragallah, Osama S., El-Sayed M. El-Rabaie, Fathi E. Abd El-Samie, Ahmed I. Sallam, and Hala S. El-Sayed. Multilevel security for relational databases. CRC Press, 2014.
- [2]. Michael Gertz and Sushil Jajodia (Editors), Handbook of Database Security: Applications and Trends , ISBN-10: 0387485325. Springer, 2007
- [3]. Stavroulakis, Peter, and Mark Stamp, eds. Handbook of information and communication security. Springer Science & Business Media, 2010.
- [4]. Afyouni, Hassan A. Database security and auditing: Protecting data integrity and accessibility. Nelson Education, 2005.
- [5]. Coronel, Carlos, and Steven Morris. Database systems: design, implementation, & management. Cengage Learning, 2016.
- [6]. Peter Ping Liu, Database Security, School of Technology, College of Business & Applied Sciences, Eastern Illinois University
- [7]. T. Ozsu and P. Valduriez, Principles of Distributed Database Systems, Springer; 3rd Edition. edition (March 2, 2011), ISBN-10: 1441988335
- [8]. Pfleeger, C.P., Pfleeger, S.L. and Margulies, M., "Security in Computing", 2006, Prentice Hall. Boston—MA, USA.
- [9]. Christian Mancias, "Conceptual Data Modeling and Database Design. A Fully Algorithmic Approach, Apple Academic Press, 2016

8.2 Aplicații (laborator)*

**Se alege tipul de aplicație aferent disciplinei*

	Metode de predare	Număr ore alocate
Construirea unei baze de date relaționale. Exerciții privind identificarea și implementarea constrângerilor de integritate și a formelor normale. Aplicații ale instrucțiunilor SQL DDL și DML.	Dialog	6
Gestionarea utilizatorilor și a rolurilor. Exerciții despre crearea utilizatorilor, atribuirea privilegiilor, gestionarea parolelor și definirea rolurilor. Aplicații în Oracle și PostgreSQL.	Problemă	4
Politici de control al accesului. Exerciții privind implementarea DAC, MAC și RBAC. Aplicații ale regulilor de control al accesului în bazele de date relaționale.	Conversație euristică	4
Mecanisme de control al accesului în practică. Exerciții privind configurarea privilegiilor, rolurilor și securității la nivel de rând sau coloană. Aplicații în Oracle și PostgreSQL.	Studiu de caz	4
Baze de date private virtuale (VPD). Exerciții privind crearea și gestionarea unui VPD. Studiu de caz cu aplicații în Oracle.	Învățare independentă și cooperativă	2



Backup și recuperare. Exerciții privind efectuarea de copii de rezervă fizice și logice și restaurarea datelor. Aplicații care utilizează instrumente PostgreSQL și Oracle.	Sinteză / esențializare a informațiilor	4
Auditarea bazelor de date. Exerciții privind configurarea auditării și înregistrarea activității utilizatorilor. Aplicații care generează rapoarte de audit în Oracle și PostgreSQL.		2
Prezentări de proiecte. Aplicații ale tehnicilor de securitate învățate în proiectele de semestru.		2

Bibliografie

[1]. Yang, Li. "Teaching database security and auditing." Proceedings of the 40th ACM technical symposium on Computer science education. 2009.

[2]. Afyouni, Hassan A. Database security and auditing: Protecting data integrity and accessibility. Nelson Education, 2005.

[3]. Coronel, Carlos, and Steven Morris. Database systems: design, implementation, & management. Cengage Learning, 2016.

[4]. Oracle Database Security Guide, <https://docs.oracle.com/en/database/oracle/oracle-database/21/dbseg/index.html>

[5]. Postgres documentation, <https://www.postgresql.org/docs/>

9. Evaluare

Tip activitate	9.1 Criterii de evaluare	9.2 Metode de evaluare	9.3 Pondere din nota finală
9.4 Curs	Participare activa	Evaluare orală continuă pe parcursul semestrului	10%
9.5 Aplicații* <i>*Se alege tipul de aplicație aferent disciplinei</i>	Interes și capacitate de lucru pentru studiu individual și în echipă	Teme de casa prezentate pe parcursul semestrului	10%
		Prezentarea unui proiect cu aplicarea mecanismelor de securitate discutate în cadrul cursurilor	30%
	Cunoașterea și înțelegerea noțiunilor discutate	Examen în sesiune	40%
Din oficiu			10%



9.6 Standard minim de performanță / Condiții de promovare: Nota 5 din 10

Restricții de integritate în Modelul de Date Relațional. Mecanisme de Control al Accesului bazate pe roluri (crearea și gestionarea utilizatorilor, rolurilor și privilegiilor) implementate în Oracle/Postgres. Fundamentele backup-ului și recuperării.

Nota finală se calculează ca medie ponderată (vezi 9.4, 9.5). Examenul este promovat dacă nota finală este mai mare sau egală cu 5.

Data completării,

Titular activităților de curs,
Conf. dr. Elena BĂUTU

Titular aplicații,
Conf. dr. Elena BĂUTU

15.09.2025

Data avizării în Departament,

Director de Departament,
Conf. dr. Elena PELICAN

19.09.2025

Decan,
Conf. dr. Aurelian NICOLA