FIŞA DISCIPLINEI

Securitatea Infrastructurii şi Aplicaţiilor Cloud

Anul universitar 2025-2026

1. Date despre program

1.1. Instituţia de învăţământ superior	Babeş-Bolyai University
1.2. Facultatea	Facultatea de Matematică şi Informatică
1.3. Departamentul	Departamentul de Informatică
1.4. Domeniul de studii	Calculatoare şi Tehnologia Informaţiei
1.5. Ciclul de studii	Master
1.6. Programul de studii / Calificarea	Securitate Cibernetică
1.7. Forma de învăţământ	Cu frecventa

2. Date despre disciplină

2.1. Denumirea disciplinei	**Securitatea infrastructurii şi aplicaţiilor cloud**					Codul disciplinei	**MME8202**
2.2. Titularul activităţilor de curs	C.d.asoc. Ing. Andrei Petru Ştefănie						
2.3. Titularul activităţilor de seminar	C.d.asoc. Ing. Andrei Petru Ştefănie						
2.4. Anul de studiu	2	2.5. Semestrul	3	2.6. Tipul de evaluare	C	2.7. Regimul disciplinei	Obligatoriu

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

3.1. Număr de ore pe săptămână	**4**	din care: 3.2. curs	**2**	3.3. seminar/ laborator/proiect	**2 lab**
3.4. Total ore din planul de învăţământ	**56**	din care: 3.5. curs	**28**	3.6 seminar/laborator/proiect	**28**
Distribuţia fondului de timp pentru studiul individual (SI) şi activităţi de autoinstruire (AI)					**ore**
Studiul după manual, suport de curs, bibliografie şi notiţe (AI)					20
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren					30
Pregătire seminare/ laboratoare/ proiecte, teme, referate, portofolii şi eseuri					30
Tutoriat (consiliere profesională)					6
Examinări					8
3.7. Total ore studiu individual (SI) şi activităţi de autoinstruire (AI)				**94**	
3.8. Total ore pe semestru				**150**	
3.9. Numărul de credite				**6**	

4. Precondiţii (acolo unde este cazul)

4.1. de curriculum	Reţele de calculatoare, baze de date, aplicaţii web, criptare
4.2. de competenţe	Abilităţi de programare în cel puţin un limbaj de programare (Java, JavaScript, C# etc.)

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	Proiector, tabla şi access la internet
5.2. de desfăşurare a seminarului/ laboratorului	Proiector, tabla şi access la internet

6.1. Competenţele specifice acumulate

Competenţe profesionale/esenţiale	• Cunoaşterea şi înţelegerea principalelor paradigme care ţin de protecţia datelor: confidenţialitatea, integritatea şi disponibilitatea datelor; • Capacitatea de a elabora aplicaţii distribuite în Cloud, respectând cerinţe etice şi de securitate;
Competenţe transversale	• Abilităţi de comunicare profesională: descrierea clară, concisă, verbală şi în scris a rezultatelor profesionale; • Spirit de iniţiativă, antreprenorial; operarea cu cunoştinţe economice, învăţarea continuă;

6.2. Rezultatele învăţării

Cunoştinţe	• Studentul/absolventul cunoaşte arhitectura aplicaţiilor cloud şi a modelelor de securitate folosite în cadrul unor asemenea aplicaţii; • Studentul/absolventul cunoaşte mecanismele de bază ce definesc securitatea sistemului şi a mediului software în care se execută o aplicaţie, cum ar fi: permisiunile de acces, politicile de securitate, interacţiunea cu mediul exterior;
Aptitudini	• Studentul/absolventul este capabil să dezvolte sisteme software securizate; • Studentul/absolventul este capabil să utilizeze tehnicile de securitate în dezvoltarea sistemelor software; • Studentul/absolventul este în măsură să evalueze riscul de securitate folosind cel puţin una din metodele consacrate
Responsabilităţi şi autonomie	• Studentul/absolventul îşi asumă responsabilitatea pentru produsul muncii sale, solicită feedback şi îl utilizează constructiv; • Studentul/absolventul demonstrează abilităţi de muncă în echipa şi îşi dezvoltă abilităţile de comunicare;

7. Obiectivele disciplinei (reieşind din grila competenţelor acumulate)

7.1 Obiectivul general al disciplinei	• Să ofere studenţilor o înţelegere cuprinzătoare a principiilor de securitate, a riscurilor şi a controalelor asociate cu cloud computing-ul. • Să dezvolte capacitatea de a proiecta, implementa şi securiza aplicaţii şi infrastructuri cloud în diferite modele de servicii (IaaS, PaaS, SaaS). • Să conştientizeze modelele de responsabilitate partajată şi modul în care acestea influenţează proiectarea securităţii şi răspunsul la incidente în cloud. • Să promoveze o perspectivă critică asupra modului în care adoptarea cloud-ului afectează conformitatea, guvernanţa şi expunerea la ameninţări.

7.2 Obiectivele specifice	• Să dobândească experienţă practică în securizarea sarcinilor de lucru pe principalele platforme de cloud public (de exemplu, AWS, Azure, GCP). • Să înţeleagă şi să aplice servicii cheie de securitate în cloud, cum ar fi gestionarea identităţii şi a accesului, criptarea, monitorizarea şi gestionarea vulnerabilităţilor. • Să analizeze incidente de securitate şi configurări greşite din lumea reală pentru a deriva cele mai bune practici de prevenire şi remediere. • Evaluarea cadrelor de conformitate cloud (CIS Benchmarks, NIST 800-53, ISO 27017 etc.) şi modelarea acestora utilizând politici şi controale native cloud. • Integrarea securităţii în ciclul de viaţă complet al aplicaţiilor native cloud utilizând automatizarea şi serviciile gestionate.

8. Conţinuturi

8.1 Curs	Metode de predare	Observaţii
1. Introducere în securitatea cloud • Modele de cloud computing (IaaS, PaaS, SaaS) • Modelul responsabilităţii partajate • Peisajul ameninţărilor cloud şi vectori de atac comuni • Beneficiile şi riscurile adoptării cloudului • Prezentare generală a cadrelor de conformitate (CIS, NIST, ISO 27017, FedRAMP)	Expunere: descriere, explicaţie, exemple, dezbatere	
2. Arhitectura de securitate în cloud • Principii de securitate native în cloud • Apărare în profunzime şi Zero Trust • Responsabilităţi de securitate la toate nivelurile (aplicaţii, reţea, date, identitate) • Modele de proiectare sigure în aplicaţiile cloud	Expunere: descriere, explicaţie, exemple, dezbatere	
3. Gestionarea identităţii şi accesului (IAM) Partea I • Principii de autentificare şi autorizare • Utilizatori, roluri şi politici • Federaţie şi SSO • IAM în AWS, Azure şi GCP	Expunere: descriere, explicaţie, exemple, dezbatere	
4. Gestionarea identităţii şi accesului (IAM) Partea II • Gestionarea privilegiilor şi privilegiul minim • Lanţuri de roluri şi acces între conturi • Configurări greşite comune ale IAM şi căi de atac • Detectarea şi remedierea riscurilor IAM	Expunere: descriere, explicaţie, exemple, dezbatere	
5. Reţele cloud şi securitate perimetrală Partea I • Reţele virtuale, subreţele, tabele de rutare • Grupuri de securitate şi ACL-uri de reţea • Controlul intrărilor/ieşirilor • Conectivitate privată vs. publică	Expunere: descriere, explicaţie, exemple, dezbatere	
6. Reţele cloud şi securitate perimetrală Partea I • Conectivitate hibridă (VPN-uri, Direct Connect, ExpressRoute) • Segmentarea reţelei • Reţele Zero Trust • Monitorizarea reţelei şi analiza accesibilităţii	Expunere: descriere, explicaţie, exemple, dezbatere	
7. Securitatea datelor - Protecţie şi criptare • Clasificarea datelor şi ciclul de viaţă al acestora • Criptarea datelor stocate şi în tranzit • Sisteme de gestionare a cheilor (AWS KMS, Azure Key Vault, GCP KMS)	Expunere: descriere, explicaţie, exemple, dezbatere	

• Gestionarea secretelor şi accesul bazat pe token-uri		
8. Securitatea datelor – Backup şi recuperare • Strategii de backup şi snapshot • Backup-uri continue vs. recuperare la un moment dat • Recuperare în caz de dezastru (conceptele RPO/RTO) • Imuabilitate şi stocare WORM	Expunere: descriere, explicaţie, exemple, dezbatere	
9. Guvernanţă şi gestionarea conturilor multiple Partea I • Structura conturilor multiple şi cele mai bune practici • Politici de control al serviciilor (SCP) • Facturare şi audit centralizate • Gestionarea poziţiei de securitate a organizaţiei	Expunere: descriere, explicaţie, exemple, dezbatere	
10. Guvernanţă şi gestionarea conturilor multiple, partea a II-a • Grupuri de gestionare Azure şi planuri • Dosare GCP şi politici de organizare • Aplicarea politicilor între cloud-uri • Gestionarea conformităţii la scară largă	Expunere: descriere, explicaţie, exemple, dezbatere	
11. Monitorizare şi logging Partea I • Importanţa observabilităţii pentru securitate • Servicii de logging native în cloud (CloudTrail, CloudWatch, Azure Monitor, GCP Cloud Logging) • Stocarea şi păstrarea centralizată a log-urilor • Detectarea anomaliilor în log-uri	Expunere: descriere, explicaţie, exemple, dezbatere	
12. Monitorizare şi logging Partea II • Integrare cu instrumentele SIEM/SOAR • Corelarea log-urilor şi alertelor • Studii de caz privind investigarea incidentelor • Monitorizarea continuă a conformităţii	Expunere: descriere, explicaţie, exemple, dezbatere	
13. Instrumente şi platforme de securitate în cloud • Prezentare generală a CNAPP, CSPM, CWPP, CIEM, KSPM • Abordări bazate pe agenţi vs. abordări fără agenţi • Benchmarking şi automatizarea conformităţii (CIS, STIG) • Protecţie în timpul rulării şi tendinţe emergente	Expunere: descriere, explicaţie, exemple, dezbatere	
14. Recapitulare şi evaluare finală • Revizuirea subiectelor cheie • Discuţii integrative • Evaluare finală şi prezentări ale studenţilor	Expunere: descriere, explicaţie, exemple, dezbatere	

Bibliografie

1. Chris Dotson - Practical Cloud Native Security, O'Reilly Media, 2nd edition, 2023
2. Ross Anderson – Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley, 3rd edition, 2020
3. Yuri Diogenes, Nicholas DiCola, Jonathan Trull – Azure Security Handbook: A Comprehensive Guide for Defending Your Enterprise Environment, Microsoft Press, 1st edition, 2021
4. Center for Internet Security (CIS) – CIS Benchmarks for AWS, Azure, and GCP, latest online edition

NIST Special Publication 800-144 – Guidelines on Security and Privacy in Public Cloud Computing, U.S. Department of Commerce, 2011

8.2 Seminar / laborator	Metode de predare	Observaţii
1. Introducere în fundamentele securităţii în cloud • Prezentare generală a platformei AWS Academy şi a structurii cursului • Accesul şi navigarea în mediul AWS Academy Learner Lab • Revizuirea modelului de responsabilitate partajată şi a infrastructurii globale AWS	Demonstraţie, configurare ghidată, Q&A	

• Introducere în procesul de trimitere şi evaluare a lucrărilor de laborator		
2. Utilizarea politicilor bazate pe resurse pentru securizarea unui bucket S3 • Crearea şi configurarea bucket-urilor S3 cu politici de acces diferite • Utilizarea politicilor bucket şi a politicilor IAM pentru gestionarea accesului • Implementarea principiilor privilegiului minim	Demonstraţie, configurare ghidată, Q&A	
3. Securizarea resurselor VPC utilizând grupuri de securitate • Configurarea unui VPC cu subreţele publice şi private • Crearea şi aplicarea grupurilor de securitate pentru controlul traficului de intrare/ieşire • Testarea scenariilor de conectivitate şi verificarea izolării reţelei • Revizuirea celor mai bune practici pentru segmentarea reţelei	Demonstraţie, configurare ghidată, Q&A	
4. Criptarea datelor în repaus utilizând AWS KMS • Crearea şi gestionarea cheilor de criptare în AWS KMS • Criptarea şi decriptarea obiectelor S3 şi a volumelor EBS • Înţelegerea rotaţiei cheilor şi a gestionării politicilor	Demonstraţie, configurare ghidată, Q&A	
5. Monitorizare şi alertare cu CloudTrail şi CloudWatch • Activarea şi configurarea AWS CloudTrail pentru monitorizarea activităţii contului • Configurarea alarmelor şi logging CloudWatch • Crearea de filtre metrice pentru detectarea evenimentelor relevante pentru securitate	Demonstraţie, configurare ghidată, Q&A	
6. Remedierea unui incident utilizând AWS Config şi Lambda • Utilizaţi AWS Config pentru a detecta resursele neconforme. • Dezvoltaţi o funcţie Lambda pentru remedierea automată.	Demonstraţie, configurare ghidată, Q&A	
7. Evaluarea finală şi recapitulare	Demonstraţie, configurare ghidată, Q&A	

Bibliografie

1. AWS Academy Cloud Security Foundations – Learner Lab Manual, AWS Academy, latest edition
2. AWS Documentation – Identity and Access Management (IAM), Amazon S3 Security, AWS KMS, AWS Config, CloudTrail, CloudWatch, available at https://docs.aws.amazon.com/
3. Center for Internet Security (CIS) – CIS Amazon Web Services Foundations Benchmark, latest online edition

9. Coroborarea conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi angajatori reprezentativi din domeniul aferent programului

- Disciplina este în concordanţă cu tendinţele actuale din programele academice privind securitatea cloud şi arhitectura cloud securizată, oferite de universităţi de renume din Europa şi din întreaga lume.
- Conţinutul cursului este în concordanţă cu cadrele şi liniile directoare internaţionale promovate de organisme profesionale şi de standardizare, precum NIST, ENISA şi Centrul pentru Securitate Internet (CIS).
- Componenta practică, oferită prin programul AWS Academy Cloud Security Foundations, asigură alinierea la cele mai bune practici şi certificări recunoscute în industrie (de exemplu, AWS Certified Security - Specialty, Azure Security Engineer Associate).
- Organizaţiile de software recunosc importanţa conceptelor discutate în cadrul acestui curs.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Cercetare individuală şi prezentare pe o temă legată de ceea ce s-a predat la curs.	Colocviu	70%
10.5 Seminar/laborator	Capacitatea de a pune în practică conceptele cursului şi tehnologiile prezentate	Test	30%
10.6 Standard minim de performanţă			
• Cel puţin nota 5 (pe o scară de la 1 la 10) atât la prezentare, cât şi la proiectul de laborator.			

11. Etichete ODD (Obiective de Dezvoltare Durabilă / Sustainable Development Goals)[1]

Nu se aplică.

Data completării:	Semnătura titularului de curs	Semnătura titularului de seminar
15.04.2025	**C.d.asoc. Ing. Andrei Petru Ştefănie**	**C.d.asoc. Ing. Andrei Petru Ştefănie**

Data avizării în departament:
...

Semnătura directorului de departament

Conf.dr. Adrian STERCA