Nume: _____ **Data:** _____ **Punctaj:** _____

Protecția datelor și stocarea la nivel de întreprindere Ghid de securitate

Mascarea datelor, tokenizarea, criptarea în repaus vs. în tranzit, copiile de rezervă offline

PREZENTARE GENERALĂ A ÎNVĂȚĂRII: PROTECȚIA DATELOR

SECURIZAT
CRIPTAREA DATELOR
Standardul AES pe 256 de biți

CONFORM
STANDARDE GLOBALE
Cadrele GDPR și CCPA

ZERO-TRUST
POLITICĂ DE ACCES
Autentificare multifactor

Bun venit! Acest pachet de activități te ghidează prin standardele și controalele de protecție a datelor. Vei explora criptarea completă a discului, controalele de acces securizat, copiile de rezervă hardware, postura de securitate în cloud și tehnicile de mascare a datelor.

PUNCTE DE CONTROL ALE FIȘEI DE LUCRU

- [ ] **Partea 1-4: Stăpânește securitatea cibernetică și prevenirea amenințărilor.**
- [ ] **Partea 5-7: Rezolvă puzzle-uri de tip cuvinte încrucișate și căutare de cuvinte.**
- [ ] **Partea 8-9: Rezolvă studii de caz și provocarea cu codul cifrat.**
- [ ] **Partea 10: Parcurge paginile de întrebări frecvente de bază și avansate.**
- [ ] **Partea 11: Explorează 10 fapte interesante din lumea reală.**
- [ ] **Bonus: provocarea Gândește repede.**

Deschide Ghidul VPN.com de securitate cibernetică

URL: https://www.vpn.com/ro/securitate-cibernetica/protectia-datelor/

Harta ta de învățare despre strategia de protecție a datelor

- Diferențiază tehnicile de mascare a datelor de cele de tokenizare.
- Implementează criptarea datelor în repaus pentru unitățile de stocare și criptarea datelor în tranzit folosind TLS.
- Proiectează sisteme de copii de rezervă offline, izolate de rețea, pentru protecția împotriva ransomware.

INSTRUCȚIUNI PENTRU GHIDUL DE PROTECȚIE A DATELOR

Răspunde la întrebările cu alegere multiplă și adevărat/fals, completează propozițiile cu spații libere folosind banca de cuvinte, asociază definițiile și rezolvă cuvintele încrucișate și puzzle-ul de căutare a cuvintelor. Aplică ce ai învățat despre protecția datelor. Încheie cu activitatea bonus Gândește repede.

PROTECȚIA DATELOR ȘI SECURITATEA STOCĂRII ENTERPRISE (INTRODUCERE)

Protecția datelor apără activele de date ale companiei prin mascare, tokenizare, criptarea bazelor de date în repaus și protocoale de transmisie securizate. Proiectarea unor copii de rezervă izolate de rețea poate ajuta la restaurarea bazelor de date esențiale în cazul unei intruziuni active.

CITEȘTE ATENT FIECARE PUNCT DE CONTROL ȘI ALEGE SAU SCRIE RĂSPUNSUL CORECT.

Punct de control 1: Provocare cu alegere multiplă

1. Care este scopul principal al mascării datelor?

- A. Înlocuirea identificatorilor sensibili cu caractere fictive, dar realiste, pentru a proteja confidențialitatea
- B. Comprimarea fișierelor mari de baze de date pentru a economisi spațiu de stocare pe server
- C. Ștergerea e-mailurilor vechi de contact ale clienților din sistemele de copii de rezervă de arhivă
- D. Ascunderea IP-ului public al serverului bazei de date de scanările de pe internet

2. Ce mecanism criptează fișierele stocate pe hard disk-ul unui server de baze de date?

- A. Criptare completă a discului în repaus
- B. Protocoalele de handshake ale sesiunii TLS în tranzit
- C. Reguli de redirecționare a serverelor de nume DNS dinamic
- D. Autentificare multifactor folosind chei hardware

3. Ce reprezintă datele în tranzit?

- A. Pachete de date care se deplasează prin routere și switch-uri de rețea
- B. Jurnale de tranzacții ale bazei de date stocate pe o unitate de rezervă offline
- C. Fișiere de utilizator arhivate, salvate într-un seif cloud izolat
- D. Fișiere statice de configurare a sistemului pe un spațiu de stocare desktop local

4. De ce este esențială o copie de rezervă offline regulată pentru protecția împotriva ransomware?

- A. Oferă o copie curată, offline, pentru restaurarea fișierelor fără a plăti o răscumpărare
- B. Împiedică hackerii să scaneze configurațiile porturilor deschise
- C. Crește vitezele de transmisie pe lățimea de bandă a rețelei locale
- D. Automatizează jurnalele de acceptare a consimțământului pentru cookie-uri din browsere

5. Ce face tokenizarea datelor?

- A. Înlocuiește numerele sensibile ale cardurilor cu token-uri aleatorii nesensibile
- B. Direcționează traficul web prin mai multe noduri onion securizate
- C. Scanează directoarele sistemului în căutarea malware-ului bazat pe semnături
- D. Auditează duratele sesiunilor de autentificare ale administratorilor bazei de date

Punct de control 2: Provocare Adevărat sau Fals

6 Întrebare 6

6. Mascarea datelor modifică permanent înregistrările din baza de date în mediile de producție.

- ○ Adevărat
- ○ Fals

7 Întrebare 7

7. Copiile de rezervă externe trebuie izolate de rețeaua corporativă principală pentru a preveni propagarea ransomware-ului.

- ○ Adevărat
- ○ Fals

8 Întrebare 8

8. Certificatele SSL/TLS securizează bazele de date prin criptarea datelor stocate pe suporturi fizice.

- ○ Adevărat
- ○ Fals

9 Întrebare 9

9. Zero-trust network access (ZTNA) verifică identitatea fiecărui utilizator înainte de a acorda accesul la baza de date.

- ○ Adevărat
- ○ Fals

10 Întrebare 10

10. Tokenizarea bazată pe seif (vault) stochează valorile originale ale cardurilor într-un seif central securizat de token-uri.

- ○ Adevărat
- ○ Fals

Punct de control 3: Inserarea termenilor-cheie

Citește fiecare propoziție de mai jos și completează spațiul liber cu termenul corect din Banca de cuvinte.

1. Înlocuirea numelor personale cu substitute realiste se numește _____ a datelor.

2. Criptarea blocurilor fizice de stocare protejează activele bazei de date _____ .

3. Protocoalele TLS criptează pachetele active de date aflate _____ .

4. Permisiunile bazate pe roluri limitează utilizatorii care pot obține _____ la baza de date.

5. Restaurarea fișierelor corporative curate după o breșă necesită un _____ offline securizat.

6. Auditarea configurărilor cloud evaluează _____ de securitate a unei organizații.

BANCĂ DE CUVINTE DIN VOCABULAR

ACCES BACKUP CRIPTARE ÎN REPAUS ÎN TRANZIT MASCARE MINIMIZARE POSTURĂ

Scrie răspunsurile aici:

1. **2.**

3. **4.**

5. **6.**

Punct de control 4: Asocierea conceptelor despre securitate

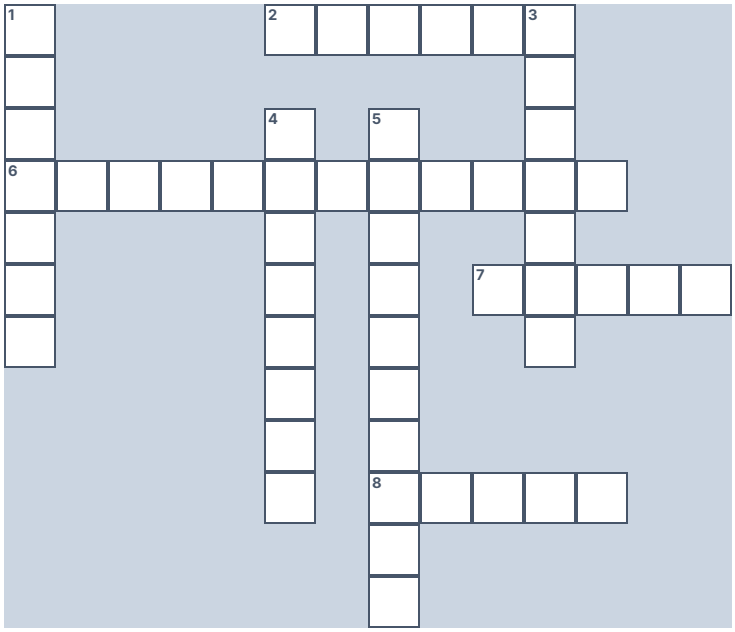
ASOCIEREA DEFINIȚIILOR

Asociază fiecare termen de vocabular din stânga cu definiția corectă din dreapta, scriind litera corespunzătoare (A-H) în câmpul de completare.

☐	1. CRIPTARE	A	Crearea de copii externe securizate ale datelor, pentru restaurare în caz de defecțiuni ale sistemului.
☐	2. COPIE DE REZERVĂ	B	Transformarea textului simplu în text cifrat ilizibil, astfel încât datele interceptate să rămână private.
☐	3. MINIMIZARE	C	Starea colectivă de securitate și pregătirea de apărare a cloudului unei organizații.
☐	4. ACCES	D	Respectarea standardelor de reglementare precum GDPR sau CCPA pentru gestionarea informațiilor private ale utilizatorilor.
☐	5. POSTURĂ	E	Incident de securitate în care datele protejate sunt accesate sau divulgate fără autorizare.
☐	6. BRESĂ	F	Restricționarea permisiunilor de citire și scriere în baza de date la rolurile de utilizator autentificate.
☐	7. CONFORMITATE	G	Înlocuirea caracterelor sensibile din câmpurile bazei de date pentru a proteja identitățile personale.
☐	8. MASCARE	H	Limitarea colectării datelor personale la minimul absolut necesar pentru operare.

Punct de control 5: Careu de cuvinte încrucișate

Rezolvă careul de cuvinte încrucișate tastând litere în căsuțele albe active. Numerele corespund indiciilor de mai jos.



ORIZONTAL

2. Crearea de copii securizate ale datelor în afara sediului, pentru restaurare în caz de defecțiuni de sistem (6)

6. Respectarea standardelor de reglementare, precum GDPR sau CCPA, pentru gestionarea informațiilor private ale utilizatorilor (12)

7. Incident de securitate în care datele protejate sunt accesate sau dezvăluite fără autorizare (5)

8. Restricționarea permisiunilor de citire și scriere în baza de date la rolurile de utilizator autentificate (5)

VERTICAL

1. Înlocuirea caracterelor sensibile din câmpurile bazei de date pentru a proteja identitățile personale (7)

3. Starea colectivă de securitate și pregătirea de apărare a cloudului unei organizații (7)

4. Transformarea textului simplu în text cifrat ilizibil, astfel încât datele interceptate să rămână private (8)

5. Limitarea colectării datelor personale la minimul absolut necesar pentru operațiuni (10)

Punct de control 5, variantă alternativă: Indicii accesibile pentru cuvinte încrucișate

Utilizatorii de cititoare de ecran și de tastatură pot introduce răspunsurile la cuvintele încrucișate direct în câmpurile de text de mai jos.

ORIZONTAL

2 orizontal: Crearea de copii securizate ale datelor în afara sediului, pentru restaurare în caz de defecțiuni de sistem (6 litere):

6 orizontal: Respectarea standardelor de reglementare, precum GDPR sau CCPA, pentru gestionarea informațiilor private ale utilizatorilor (12 litere):

7 orizontal: Incident de securitate în care datele protejate sunt accesate sau dezvăluite fără autorizare (5 litere):

8 orizontal: Restricționarea permisiunilor de citire și scriere în baza de date la rolurile de utilizator autentificate (5 litere):

VERTICAL

1 vertical: Înlocuirea caracterelor sensibile din câmpurile bazei de date pentru a proteja identitățile personale (7 litere):

3 vertical: Starea colectivă de securitate și pregătirea de apărare a cloudului unei organizații (7 litere):

4 vertical: Transformarea textului simplu în text cifrat ilizibil, astfel încât datele interceptate să rămână private (8 litere):

5 vertical: Limitarea colectării datelor personale la minimul absolut necesar pentru operațiuni (10 litere):

Punct de control 6: Căutarea cuvintelor ascunse

Găsește în grila de mai jos cei 8 termeni cheie de vocabular ascunși. Cuvintele pot fi orizontale, verticale sau diagonale.

B S I F N R L M Ă P W Q O B Ț
Ș Ș S D K Î Â A R A B Ă Â O X
E K E Î X J X S U T A J C R M
R Î C C I M M C T J C Q P G M
A M C Q R S T A S T K F Â C Ș
Z Q A O H S Â R O V U C Ș R Y
I U Â Z V F J E P G P Z C I M
M C R W P Â Ț Ă A Z N C J P A
I C O C E G I C R Q L D I T S
N Z Ș E R U B D A A R O M A P
I C O N F O R M I T A T E R T
M X Q Î S T E S B M Y Ă F E S
W W Î A R Z Ș Y Y K F I M R Î
L L T O G Q Ă Q G Z A O U F Ț
Â Y S Y Ă G L Z F Î N P N W Â

LISTĂ DE CUVINTE DIN VOCABULAR

CRIPTARE BACKUP MINIMIZARE ACCES POSTURĂ BREȘĂ
CONFORMITATE MASCARE

Punct de control 6, variantă alternativă: Asocierea accesibilă a vocabularului

Asociază fiecare dintre cei 8 termeni de vocabular din Căutarea de cuvinte cu definiția corectă, scriind litera (A-H) în spațiul liber.

TERMENI DE VOCABULAR

- **A. CRIPTARE**
- **B. BACKUP**
- **C. MINIMIZARE**
- **D. ACCES**
- **E. POSTURĂ**
- **F. BREȘĂ**
- **G. CONFORMITATE**
- **H. MASCARE**

DEFINIȚII ȘI CÂMPURI DE ASOCIERE

1. Incident de securitate în care datele protejate sunt accesate sau dezvăluite fără autorizare.
2. Înlocuirea caracterelor sensibile din câmpurile bazei de date pentru a proteja identitățile personale.
3. Restricționarea permisiunilor de citire și scriere în baza de date la rolurile de utilizator autentificate.
4. Starea colectivă de securitate și pregătirea de apărare a cloudului unei organizații.
5. Respectarea standardelor de reglementare, precum GDPR sau CCPA, pentru gestionarea informațiilor private ale utilizatorilor.
6. Limitarea colectării datelor personale la minimul absolut necesar pentru operațiuni.
7. Transformarea textului simplu în text cifrat ilizibil, astfel încât datele interceptate să rămână private.
8. Crearea de copii securizate ale datelor în afara sediului, pentru restaurare în caz de defecțiuni de sistem.

Punct de control 7: Provocare cu cuvinte amestecate

Descifrează literele de mai jos pentru a dezvălui conceptele și termenii-cheie de securitate cibernetică. Scrie răspunsurile în casetele de introducere furnizate.

1. **RPTCAREI** _____
2. **RIMIMEZAIN** _____
3. **TPUĂSRO** _____
4. **TIONMERATC OF** _____
5. **KCPBUA** _____
6. **EACSC** _____
7. **ȘĂBER** _____
8. **ACEMRAS** _____

Activitate bonus: Gândește repede

3 RĂSPUNSURI PE CATEGORIE. CÂȘTIGĂ CINE COMPLETEAZĂ PRIMUL LISTA.

1	Lucruri pe care le salvezi într-o copie de rezervă			
2	Cuvinte legate de securitatea cibernetică			
3	Persoane care au voie să vadă date sensibile			
4	Moduri de a șterge datele în siguranță			
5	Locuri în care sunt stocate datele			
6	Lucruri care ar trebui criptate			
7	Date pe care un spital trebuie să le protejeze			
8	Tipuri de copii de rezervă			
9	Informații pe care nu ar trebui să le dai niciodată			
10	Semnale de avertizare într-un e-mail			
11	Obiceiuri sigure pe care le poți începe de azi			
12	Persoane pe care le poți întreba pentru ajutor IT			
13	Dispozitive care pot fi sparte			
14	Moduri de a proteja datele			
15	Lucruri care pot distruge datele			

Punct de control 8: Studii de caz despre securitatea cibernetică

Aplică conceptele pe care le-ai învățat pentru a rezolva scenariile reale de mai jos.

STUDIU DE CAZ 1: ACTUALIZAREA CRIPTĂRII BAZEI DE DATE ENTERPRISE LA REPAUS



Scenariu: Un retailer online stochează bazele de date ale tranzacțiilor în stocare cloud, fără criptare completă a discului. Un audit recent de conformitate a semnalat acest lucru drept un risc serios de securitate a datelor conform CCPA. Proiectează o arhitectură de recuperare.

Întrebare de discuție: Analizează riscurile de conformitate cu CCPA și propune o strategie de criptare a datelor stocate (at rest).

STUDIU DE CAZ 2: LIMITAREA RANSOMWARE-ULUI ȘI RESTAURAREA DATELOR



Scenariu: Un atac ransomware activ criptează unitățile de rețea dintr-o rețea locală corporativă. Administratorul a detectat infecția devreme. Planifică pașii de izolare și de recuperare.

Întrebare de discuție: Detaliază acțiunile imediate de izolare și planifică un proces securizat de restaurare.

Punct de control 9: Descifrează codul

Un profesionist în securitate cibernetică protejează activele rețelei de actorii amenințărilor online. Folosește cheia literă–număr de mai jos pentru a descifra mesajul, scriind literele corespunzătoare în spațiile libere.

CHEIE DE CRIPTARE LITERĂ-NUMĂR

A=1 Ă=2 Â=3 B=4 C=5 D=6 E=7 F=8 G=9 H=10 I=11

Î=12 J=13 K=14 L=15 M=16 N=17 O=18 P=19 Q=20 R=21 S=22

Ș=23 T=24 Ț=25 U=26 V=27 W=28 X=29 Y=30 Z=31

19 21 18 24 7 13 7 1 31 2 6 1 24 7 15 7

19 21 11 27 1 24 7 19 21 11 17

5 18 17 24 21 18 1 15 7 22 11 9 26 21 7

Mesaj descifrat:

SFAT: FIECARE NUMĂR REPREZINTĂ POZIȚIA ACELEI LITERE ÎN ALFABET (DE EX. 1 = A, 2 = B, 31 = Z).

Punct de control 10: Întrebări frecvente de bază despre securitatea cibernetică (Partea A)

Parcurge întrebările și răspunsurile frecvente despre atenuarea amenințărilor online.

Q1: Ce este protecția datelor?

Este procesul de securizare a datelor personale și de afaceri împotriva accesului neautorizat, pierderii sau corupției, prin controale tehnice.

Q2: De ce este importantă criptarea integrală a discului?

Securizează blocurile de date stocate pe unitățile fizice, împiedicând pe oricine să citească datele dacă fură fizic hard disk-ul.

Q3: Care este diferența dintre criptarea datelor stocate și cea a datelor în tranzit?

Criptarea în repaus protejează fișierele stocate pe unități, în timp ce criptarea în tranzit protejează pachetele de rețea active care circulă prin routere.

Q4: Ce este mascarea datelor?

Înlocuiește detaliile sensibile (precum numerele cardurilor de credit) cu date fictive, dar realiste, pentru testare, fără a expune înregistrări reale.

Q5: De ce este importantă copia de siguranță offline?

Păstrează o copie curată a fișierelor tale izolată de rețea, ceea ce ajută la protejarea copiilor tale de rezervă împotriva criptării de către ransomware.

Punct de control 10: Întrebări frecvente de bază despre securitatea cibernetică (Partea B)

Parcurge întrebările și răspunsurile frecvente despre atenuarea amenințărilor online.

Q6: Ce este un seif de tokenizare a datelor?

O bază de date securizată și izolată care asociază token-uri aleatorii cu valorile sensibile originale (precum numerele principale ale cardurilor de credit).

Q7: Ce înseamnă accesul zero-trust la baza de date?

Înseamnă verificarea identității fiecărui utilizator și a stării dispozitivului la fiecare autentificare, în loc să ai încredere în oricine se află în interiorul rețelei.

Q8: Cum protejează TLS datele în tranzit?

TLS criptează conținutul sesiunii TCP, împiedicând actorii rău intenționați din rețelele publice să intercepteze sau să modifice pachetele în tranzit.

Q9: Ce este auditarea accesului la baza de date?

Înregistrarea continuă a interogărilor din baza de date și a autentificărilor pentru a detecta tipare de acces neautorizat sau anomalii de securitate.

Q10: Ce este un audit al posturii de securitate în cloud?

Un proces care analizează configurațiile cloud pentru a identifica porturile deschise, regulile de acces configurate greșit și lacunele de conformitate în securitate.

Punct de control 10: Întrebări frecvente avansate despre securitate (Partea C)

Explorează aspecte tehnice avansate ale cadrelor de securitate, ale analizei software-ului rău intenționat și ale conformității datelor.

Q1: Cum funcționează criptarea envelope?

Criptează datele cu o cheie de date, apoi criptează acea cheie de date cu o cheie principală, simplificând stocarea și rotirea cheilor.

Q2: Ce este criptarea omomorfă?

O metodă avansată de criptare care permite efectuarea operațiilor direct pe datele criptate, fără a le decripta mai întâi.

Q3: De ce se folosește criptarea la nivel de coloană în baza de date?

Criptează individual anumite coloane sensibile (precum CNP-uri/SSN), protejându-le chiar dacă administratorii obțin acces general de citire la tabel.

Q4: Ce este prevenirea pierderii datelor (DLP)?

Software care monitorizează punctele de ieșire din rețea pentru a detecta și bloca transferurile de ieșire neautorizate de fișiere sensibile.

Q5: Cum protejează copiile de siguranță write-once-read-many (WORM) împotriva ransomware-ului?

Copiile de rezervă WORM împiedică ștergerea sau modificarea fișierelor pentru o durată stabilită, oprind ransomware-ul să cripteze copiile de rezervă existente.

Punct de control 10: Întrebări frecvente avansate despre securitate (Partea D)

Explorează aspecte tehnice avansate ale cadrelor de securitate, ale analizei software-ului rău intenționat și ale conformității datelor.

Q6: Care este riscul refolosirii cheilor?

Reutilizarea aceleiași chei criptografice pe baze de date diferite înseamnă că o singură cheie compromisă expune toate bazele de date.

Q7: Cum îmbunătățește tokenizarea bazei de date conformitatea cu CCPA?

Token-urile pseudonimizează înregistrările din sistemele non-producție și limitează expunerea în caz de breșă, dar datele tokenizate pot fi totuși informații cu caracter personal.

Q8: De ce este esențială clasificarea datelor?

Clasifică fișierele după nivelul de sensibilitate, ajutând organizațiile să aplice cele mai puternice controale de criptare și acces datelor cu risc ridicat.

Q9: Care este rolul rotirii cheilor?

Actualizarea periodică a cheilor de criptare limitează cantitatea de date istorice expuse dacă o singură cheie este spartă în cele din urmă.

Q10: Cum protejează enclavele securizate interogările bazei de date din memorie?

Enclavele securizate izolează operațiile de interogare în blocuri de memorie protejate de procesor, împiedicând administratorii gazdei să vadă textul necriptat din RAM.

Partea 11: 10 fapte și perspective din lumea reală despre securitatea cibernetică

Parcurge fapte din lumea reală despre breșele de securitate, mecanismele de apărare și standardele de conformitate.

1. INFORMAȚII DESPRE SECURITATE

Reglementările GDPR au intrat în vigoare în mai 2018 și au schimbat modul în care site-urile globale gestionează consimțământul pentru cookie-uri și registrele de date personale.

2. INFORMAȚII DESPRE SECURITATE

O amendă pentru încălcarea GDPR poate ajunge la 20 de milioane de euro sau la 4% din cifra de afaceri globală, ceea ce reprezintă o expunere juridică substanțială. [4]

3. INFORMAȚII DESPRE SECURITATE

CCPA a intrat în vigoare în ianuarie 2020, stabilind drepturi pionierat pentru consumatori în materie de confidențialitate digitală în Statele Unite.

4. INFORMAȚII DESPRE SECURITATE

Minimizarea datelor reduce spațiul ocupat de baza de date, scăzând costurile de operare ale serverelor și diminuând amploarea impactului unei încălcări a securității.

5. INFORMAȚII DESPRE SECURITATE

Distrugerea criptografică rezolvă dificultatea ștergerii copiilor de rezervă prin eliminarea cheilor, în loc să editeze fișierele istorice de pe benzile de backup.

6. INFORMAȚII DESPRE SECURITATE

Majoritatea țărilor din lume au adoptat acum legi de protecție a datelor personale pentru a proteja drepturile la confidențialitate ale consumatorilor.

7. PERSPECTIVĂ ASUPRA SECURITĂȚII

Formularele de consimțământ opt-in cu căsuțe bifate în prealabil sunt interzise în mod explicit conform definițiilor europene de reglementare a confidențialității datelor.

8. PERSPECTIVĂ ASUPRA SECURITĂȚII

GDPR impune raportarea încălcărilor securității datelor cu caracter personal către autoritatea de supraveghere în termen de 72 de ore de la luarea la cunoștință, atunci când este posibil. [3]

9. PERSPECTIVĂ ASUPRA SECURITĂȚII

Hashing-ul parolelor cu algoritmi lenți, precum bcrypt sau Argon2, face mult mai dificilă spargerea offline a hash-urilor furate. [6]

10. INFORMAȚII DESPRE SECURITATE

Datele în repaus reprezintă fișierele de baze de date salvate, în timp ce datele în tranzit acoperă pachetele aflate în mișcare prin routerele de rețea.

Referințe tehnice și surse

Ghidul de studiu și puzzle-urile interactive sunt alcătuite pe baza standardelor globale NIST, OWASP și de conformitate privind confidențialitatea datelor.

REFERINȚE ACADEMICE ȘI DIN INDUSTRIE

[1] NIST. (2025). SP 800-88 Rev. 2, Guidelines for Media Sanitization.

https://csrc.nist.gov/pubs/sp/800/88/r2/final

[2] CISA. (2023). #StopRansomware Guide.

https://www.cisa.gov/stopransomware/ransomware-guide

[3] Intersoft Consulting. (n.d.). Art. 33 GDPR – Notification of a personal data breach to the supervisory authority.

https://gdpr-info.eu/art-33-gdpr/

[4] Intersoft Consulting. (n.d.). Art. 83 GDPR – General conditions for imposing administrative fines.

https://gdpr-info.eu/art-83-gdpr/

[5] California Privacy Protection Agency. (n.d.). Frequently Asked Questions (FAQs).

https://cppa.ca.gov/faq.html

[6] OWASP. (n.d.). Password Storage Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

Barem: Punct de control 1 – Alegere multiplă

1 Întrebarea 1 — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Care este scopul principal al mascării datelor? → Înlocuirea identificatorilor sensibili cu caractere fictive, dar realiste, pentru a proteja confidențialitatea

2 Întrebarea 2 — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Ce mecanism criptează fișierele stocate pe hard disk-ul unui server de baze de date? → Criptare completă a discului în repaus

3 Întrebarea 3 — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Ce reprezintă datele în tranzit? → Pachete de date care se deplasează prin routere și switch-uri de rețea

4 Întrebarea 4 — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

De ce este esențială o copie de rezervă offline regulată pentru protecția împotriva ransomware? → Oferă o copie curată, offline, pentru restaurarea fișierelor fără a plăti o răscumpărare

5 Întrebarea 5 — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Ce face tokenizarea datelor? → Înlocuiește numerele sensibile ale cardurilor cu token-uri aleatorii nesensibile

Barem: Punct de control 2 – Adevărat sau fals

6 Întrebarea 6

Răspuns corect: Fals

NOTĂ PENTRU PROFESOR

Mascarea modifică copiile de test sau ascunde valorile la momentul interogării; înregistrările din producție rămân neschimbate.

7 Întrebarea 7

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Copiile de rezervă externe trebuie izolate de rețeaua corporativă principală pentru a preveni propagarea ransomware-ului.

8 Întrebarea 8

Răspuns corect: Fals

NOTĂ PENTRU PROFESOR

Certificatele TLS protejează datele în tranzit; datele stocate (at rest) necesită criptare la nivel de disc, fișier sau bază de date.

9 Întrebarea 9

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Zero-trust network access (ZTNA) verifică identitatea fiecărui utilizator înainte de a acorda accesul la baza de date.

10 Întrebarea 10

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Tokenizarea bazată pe seif păstrează valorile originale într-un seif securizat de token-uri, care asociază fiecare token cu datele sale.

Chei de vocabular și grilă de notare

Barem de notare pentru profesor: Acordă 1 punct pentru fiecare asociere corectă (8 puncte în total) și pentru fiecare termen din context (6 puncte în total).

PUNCT DE CONTROL 4: BAREM – ASOCIEREA CONCEPTELOR

B 1. CRIPTARE	A 2. COPIE DE REZERVĂ	H 3. MINIMIZARE	F 4. ACCES
C 5. POSTURĂ	E 6. BRESĂ	D 7. CONFORMITATE	G 8. MASCARE

PUNCT DE CONTROL 3: BAREM – TERMENI-CHEIE

1 MASCARE	2 ÎN REPAUS	3 ÎN TRANZIT	4 ACCES
5 BACKUP	6 POSTURĂ		

PUNCT DE CONTROL 6, VARIANTĂ ALTERNATIVĂ: BAREM – ASOCIEREA CUVINTELOR

1 F – BREȘĂ	2 H – MASCARE	3 D – ACCES	4 E – POSTURĂ
5 G – CONFORMITATE	6 C – MINIMIZARE	7 A – CRIPTARE	8 B – BACKUP

NOTE DE DISCUȚIE PENTRU PROFESORI

Termeni-cheie:
Verifică dacă elevii pot explica CRIPTARE, COPIE DE REZERVĂ și MINIMIZARE cu propriile cuvinte și pot da câte un exemplu pentru fiecare.

Studii de caz:
Cere elevilor să își susțină recomandările cu fapte din fișă, nu cu presupuneri.

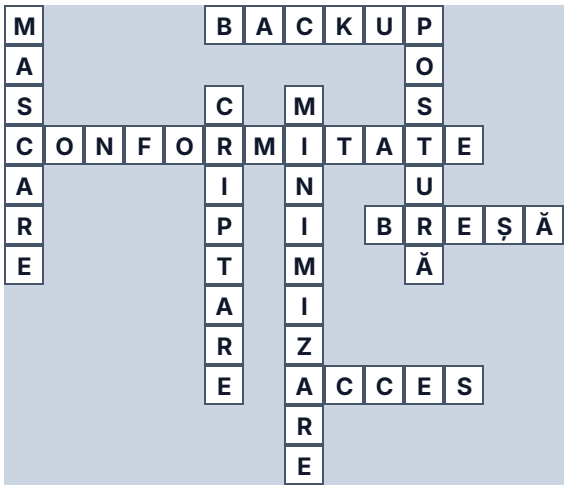
Evaluarea surselor:
Cere elevilor să verifice cel puțin o afirmație în sursele fișei și discutați de ce cifrele, prețurile și regulile se pot schimba în timp.

Chei de rezolvare ale puzzle-urilor și note pentru profesor

SOLUȚIA JOCULUI DE CĂUTARE DE CUVINTE

B	S	I	F	N	R	L	M	Ă	P	W	Q	O	B	Ț
Ș	Ș	S	D	K	Î	Â	A	R	A	B	Ă	Â	O	X
E	K	E	Î	X	J	X	S	U	T	A	J	C	R	M
R	Î	C	C	I	M	M	C	T	J	C	Q	P	G	M
A	M	C	Q	R	S	T	A	S	T	K	F	Â	C	Ș
Z	Q	A	O	H	S	Â	R	O	V	U	C	Ș	R	Y
I	U	Â	Z	V	F	J	E	P	G	P	Z	C	I	M
M	C	R	W	P	Â	Ț	Ă	A	Z	N	C	J	P	A
I	C	O	C	E	G	I	C	R	Q	L	D	I	T	S
N	Z	Ș	E	R	U	B	D	A	A	R	O	M	A	P
I	C	O	N	F	O	R	M	I	T	A	T	E	R	T
M	X	Q	Î	S	T	E	S	B	M	Y	Ă	F	E	S
W	W	Î	A	R	Z	Ș	Y	Y	K	F	I	M	R	Î
L	L	T	O	G	Q	Ă	Q	G	Z	A	O	U	F	Ț
Â	Y	S	Y	Ă	G	L	Z	F	Î	N	P	N	W	Â

SOLUȚIA CUVINTELOR ÎNCRUCIȘATE



GHID PENTRU PROFESOR: SOLUȚIILE LA CUVINTELE ÎNCRUCIȘATE

ORIZONTAL

2 orizontal: BACKUP Crearea de copii securizate ale datelor în afara sediului, pentru restaurare în caz de defecțiuni de sistem (6 litere)

6 orizontal: CONFORMITATE Respectarea standardelor de reglementare, precum GDPR sau CCPA, pentru gestionarea informațiilor private ale utilizatorilor (12 litere)

7 orizontal: BREȘĂ Incident de securitate în care datele protejate sunt accesate sau dezvăluite fără autorizare (5 litere)

8 orizontal: ACCES Restricționarea permisiunilor de citire și scriere în baza de date la rolurile de utilizator autentificate (5 litere)

VERTICAL

1 vertical: MASCARE Înlocuirea caracterelor sensibile din câmpurile bazei de date pentru a proteja identitățile personale (7 litere)

3 vertical: POSTURĂ Starea colectivă de securitate și pregătirea de apărare a cloudului unei organizații (7 litere)

4 vertical: CRIPTARE Transformarea textului simplu în text cifrat ilizibil, astfel încât datele interceptate să rămână private (8 litere)

5 vertical: MINIMIZARE Limitarea colectării datelor personale la minimul absolut necesar pentru operațiuni (10 litere)

Cuvinte amestecate și barem pentru codul cifrat

Barem pentru activitatea de descifrare a cuvintelor de vocabular și pentru provocarea Codul secret.

BAREMUL PENTRU DESCIFRAREA CUVINTELOR

1. RPTCAREI — **CRIPTARE**
2. RIMIMEZAIN — **MINIMIZARE**
3. TPUĂSRO — **POSTURĂ**
4. TIONMERATCOF — **CONFORMITATE**
5. KCPBUA — **BACKUP**
6. EACSC — **ACCES**
7. ȘĂBER — **BREȘĂ**
8. ACEMRAS — **MASCARE**

BAREMUL PROVOCĂRII CU CODUL SECRET

"PROTEJEAZĂ DATELE PRIVATE PRIN CONTROALE SIGURE"

Barem pentru studiile de caz

A Studiu de caz 1: Actualizarea criptării bazei de date Enterprise la repaus

Soluția profesorului

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- Analiza scenariului: Un retailer online stochează bazele de date ale tranzacțiilor în stocare cloud fără criptarea întregului disc. Un audit recent de conformitate a semnalat acest lucru ca pe un risc serios de securitate a datelor conform CCPA. Proiectează o arhitectură de recuperare.
- Strategie și soluție recomandată: Implementează criptarea completă a discului AES-256 pentru datele stocate, pe toate sistemele de fișiere. Folosește un serviciu centralizat de gestionare a cheilor (KMS) cu rotație automată și aplică politici IAM stricte pentru a controla accesul la decriptare.

B Studiu de caz 2: Limitarea ransomware-ului și restaurarea datelor

Soluția profesorului

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- Analiza scenariului: Un atac ransomware activ criptează unitățile de rețea dintr-o rețea locală corporativă. Administratorul a detectat infecția devreme. Planifică pașii de izolare și recuperare.
- Strategie și soluție recomandată: Izolează imediat segmentul compromis. Formatează punctele finale afectate și restaurează din cea mai recentă copie de rezervă offline write-once-read-many (WORM). Verifică integritatea copiei de rezervă înainte de a reconecta sistemele.