Standard ocupațional

SPECIALIST ÎN PROCEDURI ȘI INSTRUMENTE DE SECURITATE A SISTEMELOR INFORMATICE

Cod COR 252913

Inițiator/Autori:

INTERLOG COM SRL

EUROTRAINING SOLUTION SRL

BUSINESS GENERATOR SRL

Marius Florin Sanda

Marie – Jeanne Helene Iordache

Data elaborării:

06.12.2024-21.03.2025

Verificare profesională:

Mihai Daniel Chiroiu

Bogdan Cristian Stanache

Data verificării:

31.03.2025; 07.04.2025

Avizare:

Institutul Național de Cercetare - Dezvoltare în Informatică - ICI București

Data avizării:

20.05.2025

Validare documentație:

Asociația Națională a Comitetelor Sectoriale din România

Comitetul Sectorial pentru Activități de Servicii Administrative și Activități de Servicii Suport

Președinte ANCSR - PUIU Doru

Președinte CSASAASS - BADEA Gabriel

Data validării sectoriale:

07.07.2025

Aprobare:

Autoritatea Națională pentru Calificări

Data aprobării:

Decizia ANC nr.297/08.08.2025

Nr. RS – 13/08.08.2025

STRUCTURA STANDARDULUI OCUPAȚIONAL

SECȚIUNEA A - CERINȚELE PIEȚEI MUNCII

1. Denumirea grupei de baza și a ocupației/codul COR aferent

Grupa de bază COR: 2529 – Specialiști în baze de date și rețele neclasificați în grupele de bază anterioare

Specialist în proceduri şi instrumente de securitate a sistemelor informatice
COD COR 252913

2. Denumirea tradusă a ocupației (En):

INFORMATION SYSTEMS SECURITY PROCEDURES AND TOOLS SPECIALIST

3. Descriere și activități/sarcini specifice grupei de bază

3.1. Descrierea grupei de bază în cadrul căreia este încadrată ocupația, conform COR/ ISCO-08

Această grupă de bază cuprinde specialiștii în baze de date și rețele neclasificați în altă parte în grupa minoră 252 - Specialiști în baze de date și rețele. De exemplu, această grupă de bază include specialiștii în domeniul securității informației şi al tehnologiei comunicațiilor.

3.2. Activități/ sarcini specifice ale grupei de bază conform ISCO-08

a) elaborarea de planuri pentru protejarea fișierelor informatice împotriva modificărilor, distrugerii sau divulgării accidentale sau neautorizate și pentru a satisface nevoile de prelucrare a datelor de urgență;

b) formarea utilizatorilor și promovarea gradului de conștientizare în materie de securitate pentru a asigura securitatea sistemului și pentru a îmbunătăți eficiența serverelor și a rețelei;

c) consultarea utilizatorilor pentru a discuta probleme precum nevoile de acces la datele computerizate, încălcările securității și modificările de programare;

d) monitorizarea rapoartelor actuale privind virușii informatici pentru a stabili când să se actualizeze sistemele de protecție împotriva virușilor;

e) modificarea fișierelor de securitate informatică pentru a încorpora software nou, a corecta erorile sau a schimba starea accesului individual;

f) monitorizarea utilizării fișierelor de date și reglementarea accesului pentru a proteja informațiile din fișierele informatice;

g) efectuarea de evaluări ale riscurilor și efectuarea de teste ale sistemului de prelucrare a datelor pentru a asigura funcționarea activităților de prelucrare a datelor și a măsurilor de securitate;

h) criptarea transmisiilor de date și ridicarea de firewall-uri pentru a ascunde informațiile confidențiale pe măsură ce sunt transmise și pentru a împiedica transferurile digitale viciate;

4. Activități/ sarcini specifice ale ocupației

1. Utilizează competențele digitale în activitatea profesională:
- Utilizează aplicațiile informatice pentru redactarea documentației tehnice.
- Utilizează platformele digitale pentru comunicare și colaborare în cadrul proiectelor IT.
- Utilizează aplicațiile specifice pentru gestionarea sarcinilor și a activităților.
- Accesează și utilizează resursele digitale de specialitate..

2. Aplică principiile de protecție a mediului în utilizarea și gestionarea echipamentelor informatice:
- Selectează echipamentele informatice eficiente energetic.
- Aplică măsurile de reciclare și reutilizare.
- Respectă procedurile privind eliminarea deșeurilor electronice.

3. Gestionează eficient timpul și adaptarea la schimbări în context profesional:
- Organizează activitățile în funcție de priorități și termene.
- Adaptează planul de lucru la modificările din mediu.
- Reevaluează sarcinile în condiții de presiune sau incertitudine.

4. Comunică eficient și colaborează în activitățile profesionale:
- Exprimă clar ideile și soluțiile în cadrul echipei.
- Formulează și recepționează feedbackul constructiv.
- Participă activ la rezolvarea sarcinilor comune..

5. Coordonează echipa implicată în activitatea profesională:
- Planifică activitățile în funcție de obiectivele proiectului.
- Alocă resursele și responsabilitățile membrilor echipei.
- Monitorizează stadiul sarcinilor și ajustează planificarea.
- Sprijină dezvoltarea profesională a colegilor prin mentorat sau feedback.
- Facilitează colaborarea între membrii echipei și alte departamente.
- Asigură respectarea procedurilor interne și a termenelor stabilite.

6. Aplică gândirea critică în procesul de luare a deciziilor tehnice și profesionale:
- Analizează situațiile complexe și formulează concluzii raționale.
- Compară alternativele tehnice și evaluează riscurile asociate.
- Argumentează deciziile luate în fața echipei sau a conducerii.
- Verifică consecințele deciziilor din punct de vedere al securității informației.
- Identifică punctele slabe din soluțiile propuse de alții și propune îmbunătățiri.

7. Aplică prevederile legale referitoare la sănătatea și securitatea în muncă și în domeniul situațiilor de urgență:
- Respectă normele SSM și PSI în toate activitățile desfășurate.
- Utilizează echipamentele în condiții de siguranță.
- Raportează incidentele sau riscurile identificate.
- Participă la instruiri și simulări privind situațiile de urgență.
- Aplică procedurile de evacuare și prim-ajutor în caz de nevoie.

8. Aplică prevederile legislației TIC în activitatea profesională:
- Analizează reglementările legale aplicabile domeniului TIC.
- Aplică prevederile legale în activitățile curente privind protecția datelor, proprietatea intelectuală, licențierea etc.
- Monitorizează actualizările legislative și adaptează procedurile interne.
- Colaborează cu departamentele juridice sau cu alte autorități în cazuri ce implică reglementări TIC.

9. Gestionează conformitatea cu standardele de securitate TIC:
- Verifică alinierea politicilor și procedurilor interne la standarde recunoscute (ISO/IEC 27001, NIST etc.).
- Realizează audituri interne privind securitatea informației.
- Întocmește rapoarte de conformitate.
- Colaborează cu echipele tehnice și manageriale pentru implementarea corectă a cerințelor standardelor.

10. Elaborează și utilizează scripturile pentru automatizarea sarcinilor tehnice:
- Scrie scripturi pentru automatizarea proceselor de rutină (scanări, back-up, alerte etc.).
- Testează și validează scripturile în medii controlate.
- Adaptează scripturile existente în funcție de nevoi specifice.
- Documentează scripturile pentru uz intern.

11. Gestionează și stochează datele în cloud:
- Configurează soluțiile de stocare în cloud în funcție de cerințele de securitate.
- Implementează măsurile de control al accesului la datele stocate în cloud.
- Monitorizează și menține integritatea datelor în medii cloud.
- Aplică politicile de backup și restaurare în cloud.

12. Aplică tehnicile de criptare și procedurile de gestionare a cheilor criptografice pentru protecția datelor:
- Selectează tehnologiile de criptare adecvate tipului de date.
- Implementează procedurile de gestionare a ciclului de viață al cheilor.
- Monitorizează modul de utilizare a criptării în cadrul sistemelor informatice.
- Asigură confidențialitatea și integritatea datelor prin criptare end-to-end.

13. Definește și implementează politicile de securitate a informațiilor în cadrul organizației:
- Identifică cerințele organizaționale privind securitatea informației.
- Redactează politicile și procedurile interne de securitate.
- Validează implementarea politicilor în activitățile operative.
- Revizuiește periodic politicile pentru conformitate și eficiență.

14. Identifică vulnerabilitățile și remediază deficiențele în sistemele TIC:
- Efectuează analize de vulnerabilitate în rețele și sisteme.
- Utilizează instrumentele de scanare automată și testare manuală.
- Aplică patch-urile, actualizările și reconfigurările necesare.
- Documentează deficiențele și măsurile corective.

15. Aplică măsurile de securitate cibernetică pentru protejarea infrastructurii informatice și a sistemelor digitale:
- Implementează mecanismele de protecție la nivel de rețea și stații de lucru.
- Aplică politicile de segmentare a rețelei și control al accesului.
- Configurează și întreține firewall-urile, sistemele de detecție și prevenție a intruziunilor și alte soluții de securitate.
- Aplică actualizările de securitate și patch-urile.

16. Implementează politicile și procedurile pentru asigurare a confidențialității informațiilor:
- Asigură aplicarea politicilor de confidențialitate în cadrul sistemelor IT.
- Controlează accesul la informații în funcție de nivelul de autorizare.
- Informează utilizatorii cu privire la responsabilitățile legate de manipularea datelor sensibile.
- Verifică respectarea procedurilor de confidențialitate.
- Aplică măsuri de protecție adecvate nivelului de sensibilitate al datelor.

17. Monitorizează incidentele de securitate informatică și de intervenție inițială pentru limitarea impactului:
- Supraveghează sistemele de detecție a amenințărilor.
- Analizează alertele și jurnalele de evenimente.
- Aplică procedurile de răspuns rapid în caz de incident.
- Raportează și documentează incidentele de securitate.

18. Elaborează planurile de răspuns la incidentele de securitate:
- Identifică scenariile de incident și impactul potențial.
- Stabilește pașii operaționali și responsabilitățile în caz de incident.
- Redactează procedurile de intervenție, comunicare și recuperare.
- Testează și actualizează periodic planurile.

19. Gestionează drepturile de acces la sistemele informatice în funcție de nivelul de autorizare:
- Configurează permisiunile de acces în funcție de politicile interne.
- Revizuiește periodic drepturile de acces.
- Aplică principiul minimului privilegiu și al separării funcțiilor.
- Implementează soluții de autentificare multifactor.

20. Identifică și remediază vulnerabilitățile aplicațiilor web în fața amenințărilor de securitate cibernetică:
- Efectuează teste de penetrare pentru aplicații web.
- Analizează configurațiile aplicațiilor.
- Identifică vulnerabilitățile cunoscute.
- Propune și implementează măsuri de remediere.

21. Evaluează riscurile asociate infrastructurii informatice și proiectarea de măsuri corective și acțiuni preventive avansate:
- Analizează infrastructura și nivelul de expunere la riscuri.
- Aplică metodele de evaluare a riscurilor (ex: impact, probabilitate).
- Elaborează scenarii de risc și simulări de atacuri.
- Proiectează soluții și controale avansate pentru reducerea riscurilor.

22. Planifică și coordonează exercițiile de recuperare a sistemelor informatice în urma incidentelor sau dezastrelor:
- Elaborează scenarii de testare a planurilor de continuitate.
- Coordonează simulările de recuperare.
- Evaluează capacitatea organizației de a răspunde la incidente majore.
- Revizuiește și îmbunătățește planurile existente pe baza rezultatelor testelor.

23. Aplică tehnicile de investigație digitală în cadrul expertizei criminalistice informatice:
- Colectează și conservă probele digitale conform procedurilor legale.
- Analizează fișierele, log-urile și sistemele compromise.
- Identifică urmele de activitate malițioasă și sursele posibile.
- Redactează rapoarte tehnice de expertiză.

24. Elaborează proceduri de securitate pentru gestionarea dispozitivelor mobile și a muncii la distanță:
- Evaluează riscurile asociate utilizării dispozitivelor mobile și muncii de la distanță.
- Elaborează politici și proceduri privind utilizarea dispozitivelor mobile (BYOD, MDM etc.).
- Stabilește cerințele de criptare, autentificare și control de acces.
- Propune soluții tehnice pentru protejarea comunicațiilor la distanță (VPN, MFA, DLP etc.).
- Elaborează ghiduri de bune practici pentru utilizatorii mobili și lucrul remote.

25. Planifică și implementează măsuri de conștientizare și formare în domeniul securității informației:
- Identifică nevoile de instruire și conștientizare în cadrul organizației.
- Planifică campanii și activități de formare adaptate diferitelor categorii de personal.
- Elaborează materiale de informare și conținut educațional.
- Susține sesiuni de instruire și urmărește participarea angajaților.
- Evaluează nivelul de înțelegere și aplicare a principiilor de securitate de către utilizatori.
- Revizuiește și îmbunătățește periodic măsurile de conștientizare.

5. Competențe

Ponderea competențelor :[1]

Grupa C 1.1 Competențe cheie/educaționale 5%, dintre care competențe digitale minimum 2%
Grupa C 1.2 Competențe transversale/sociale/mediu/ verzi: 5%
Grupa C 1.3 Competențe de bază personale /atitudini: 5%
Grupa C 2.1 Competențe comune la locul de muncă: 5%
Grupa C 2.2 Competențe tehnice generale: 5%
Grupa C 3.1 Competențe fundamentale profesionale: 20 %
Grupa C 3.2 Competențe de domeniu: 25%
Grupa C 3.3 Competențe de specialitate : 15%
Grupa C 3.4 Competențe de specializare: 15%.

C 1.1

1. Utilizează competențele digitale în activitatea profesională.

C1.2

2. Aplică principiile de protecție a mediului în utilizarea și gestionarea echipamentelor informatice.

C1.3

3. Gestionează eficient timpul și adaptarea la schimbări în context profesional.
4. Comunică eficient și colaborează în activitățile profesionale.

C2.1

5. Coordonează echipa implicată în activitatea profesională.
6. Aplică gândirea critică în procesul de luare a deciziilor tehnice și profesionale.

C2.2

7. Aplică prevederile legale referitoare la sănătatea și securitatea în muncă și în domeniul situațiilor de urgență.

C3.1

8. Aplică prevederile legislației TIC în activitatea profesională.
9. Gestionează conformitatea cu standardele de securitate TIC.
10. Elaborează și utilizează scripturile pentru automatizarea sarcinilor tehnice.
11. Gestionează și stochează datele în cloud.

C3.2

12. Aplică tehnicile de criptare și procedurile de gestionare a cheilor criptografice pentru protecția datelor.
13. Definește și implementează politicile de securitate a informațiilor în cadrul organizației.
14. Identifică vulnerabilitățile și remediază deficiențele în sistemele tehnologiei informației și comunicațiilor (TIC).

C3.3

15. Aplică măsurile de securitate cibernetică pentru protejarea infrastructurii informatice și a sistemelor digitale.
16. Implementează politicile și procedurile pentru asigurarea confidențialității informațiilor.
17. Monitorizează incidentele de securitate informatică și de intervenție inițială pentru limitarea impactului.

[1] Se va stabili în conformitate cu prevederile Hotărârii Guvernului nr. 772/2022 privind aprobarea Metodologiei de acordare a creditelor transferabile pentru formarea profesională a adulților, precum și pentru abrogarea Hotărârii Guvernului nr. 844/2002 privind aprobarea nomenclatoarelor calificărilor profesionale pentru care se asigură pregătirea prin învățământul preuniversitar, precum și durata de școlarizare ; Pentru ocupații de nivel 1-5 de calificare, conform CNC se vor respecta prevederile Ordinului nr.3001/39/2022 privind aprobarea metodologiei de alocare a nivelurilor de calificare pentru calificările de nivel 1-5 din Cadrul național al Calificărilor.

18. Elaborează planurile de răspuns la incidentele de securitate.
19. Gestionează drepturile de acces la sistemele informatice în funcție de nivelul de autorizare.

C3.4

20. Identifică și remediază vulnerabilitățile aplicațiilor web în fața amenințărilor de securitate cibernetică.
21. Evaluează riscurile asociate infrastructurii informatice și proiectarea de contramăsuri avansate.
22. Planifică și coordonează exercițiile de recuperare a sistemelor informatice în urma incidentelor sau dezastrelor .
23. Aplică tehnicile de investigație digitală în cadrul expertizei criminalistice informatice.
24. Elaborează proceduri de securitate pentru gestionarea dispozitivelor mobile și a muncii la distanță.
25. Planifică și implementează măsuri de conștientizare și formare în domeniul securității informației.

6. Niveluri de calificare/ educație:

6.1. Nivelul de calificare conform Cadrului Național al Calificărilor (CNC)	6
6.2. Nivelul de referință conform Cadrului European al Calificărilor (EQF)	6
6.3. Nivelul educațional corespondent, conform ISCED - 2011	6

7. Acces la altă/alte ocupație/ocupații cuprinsă/ cuprinse în COR

Acces la ocupație/ocupații de același nivel de calificare, conform CNC, pe bază de experiență/recunoaștere de competențe din grupele C1 – C3.2

252906 Auditor de securitate cibernetică
252910 Manager de securitate sisteme informatice

8. Informații suplimentare

Nu este cazul;

SECȚIUNEA B - CERINȚE PENTRU EDUCAȚIE ȘI FORMARE PROFESIONALĂ

1. Informații despre programul de educație și formare profesională

1.1. Cerințe specifice de acces la program

1.1.1. Competențe și deprinderi necesare accesului la program:

Nu este cazul

1.1.2. Condiții minime de acces la program, raportate la nivelul de studii:

Niveluri de studii:

- **Învățământ primar** ☐
- **Învățământ gimnazial (secundar inferior)** ☐
- **Învățământ secundar superior : (primii doi ani de liceu)** ☐
- **Învățământ secundar superior:**
  - **Învățământ profesional prin școli profesionale** ☐
  - **Învățământ liceal, fără diplomă de bacalaureat** ☐
  - **Învățământ liceal, cu diplomă de bacalaureat** ☐
- **Învățământ postliceal** ☐
- **Învățământ superior cu diplomă de licență** ■
- **Învățământ superior cu diplomă de master** ☐

1.1.3. Alte studii necesare:

Nu este cazul

1.1.4. Cerințe speciale:

Nu este cazul

2. Descrierea programului de educație și formare profesională

2.1. Durata totală, nr. ore didactice: 180 **din care:**

60 **teorie,**

120 **practică**

Număr de credite: 12 ECTS [2]

2.2. Planul de pregătire (anexa nr. 1 la prezentul standard ocupațional)

[2] Se va stabili în conformitate cu prevederile Hotărârii Guvernului nr. 772/2022 privind aprobarea Metodologiei de acordare a creditelor transferabile pentru formarea profesională a adulților, precum și pentru abrogarea Hotărârii Guvernului nr. 844/2002 privind aprobarea nomenclatoarelor calificărilor profesionale pentru care se asigură pregătirea prin învățământul preuniversitar, precum și durata de școlarizare

2.3. Programa de pregătire teoretică și practică (anexa nr. 2 la prezentul standard ocupațional)

2.4. Echipamente/utilaje/programe software etc. necesare pregătirii teoretice și practice

Pentru pregătirea teoretică sunt necesare următoarele resurse:
- Calculator și echipamente de rețea fizice sau virtuale;
- Conexiune Internet;
- Software specific;
- Platformă de videoconferințe și comunicare online;
- Instrumente/medii de testare și simulare;
- Laboratoare virtuale pentru simulări;
- Legislație și standarde specifice domeniului;
- Resurse digitale online;
- Suport de curs;
- Videoproiector;
- Fișe de practică;
- Consumabile foi flipchart, coli A4, marker, etc

Pentru pregătirea practică sunt necesare următoarele resurse:
- Calculator și echipamente de rețea fizice sau virtuale;
- Conexiune Internet;
- Software specific;
- Platformă de videoconferințe și comunicare online;
- Instrumente/medii de testare și simulare;
- Laboratoare virtuale pentru simulări;
- Legislație și standarde specifice domeniului;
- Resurse digitale online;
- Suport de curs;
- Videoproiector;
- Fișe de practică;
- Consumabile foi flipchart, coli A4, marker, etc.

2.5. Cerințe privind nivelul minim de calificare și experiență profesională pentru formatori și instructori/preparatori formare

Selecția formatorilor cooptați în programul de formare profesională pentru ocupația de "Specialist în proceduri și instrumente de securitate a sistemelor informatice" se realizează din rândul specialiștilor care îndeplinesc cumulativ următoarele condiții:
- Studii superioare cu diplomă de licență;
- Pregătire de specialitate/calificări în domeniu;
- Experiență practică în domeniu de minim 2 ani (dovedită prin contracte, adeverințe)
- Să dețină certificat de absolvire pentru ocupația de formator sau adeverință de atestare a calității de cadru didactic.

2.6. Cerințe privind nivelul minim de calificare și experiență profesională pentru evaluatorii de competențe profesionale

Nu este cazul

SECȚIUNEA C - ASUMAREA STANDARDULUI

1. Informații referitoare la procesul de elaborare, verificare, validare, avizare și aprobare a standardului ocupațional:

1.1. Realizare:
Inițiator/Autori:

MARIUS FLORIN SANDA – *specialist în domeniu*

MARIE – JEANNE HELENE IORDACHE – *specialist în domeniu*

Instituția/instituțiile/persoanele interesate:

SC INTERLOG COM SRL
SIMONA MARIA COJOCĂRESCU - *Administrator*

SC EUROTRAINING SOLUTION SRL
MARIE – JEANNE HELENE IORDACHE – *Administrator*

SC BUSINESS GENERATOR SRL
ELENA CRISTIAN – *Director general*

Data elaborării:06.12.2024-21.03.2025

1.2. Verificare :
Specialist/Instituția de profil:

MIHAI DANIEL CHIROIU- *specialist în domeniu*

BOGDAN CRISTIAN STANACHE - *specialist în domeniu*

Data verificării: 31.03.2025; 07.04.2025

1.3. Avizare:
INSTITUTUL NAȚIONAL DE CERCETARE-DEZVOLTARE ÎN INFORMATICĂ – ICI BUCUREȘTI
Data avizării:20.05.2025

1..4. Validare documentație:
Asociația Națională a Comitetelor Sectoriale, Comitetul Sectorial pentru Activități de Servicii Administrative și Activități de Servicii Suport / Doru Puiu, Gabriel Badea
Data validării: 07.07.2025

1.5. Aprobare:
Autoritatea Națională pentru Calificări conform deciziei nr.297 din data 08.08.2025

Anexa nr. 1 la standardul ocupațional

PLAN DE PREGĂTIRE

Nr. crt.	Competența dobândită	Disciplină/ Modul	Nr. ore teorie	Nr. ore practică	Nr. credite asociate
1.	Utilizează competențele digitale în activitatea profesională	COMPETENȚE DIGITALE ȘI TRANSVERSALE PENTRU EFICIENȚĂ PROFESIONALĂ	3	6	2
2.	Aplică principiile de protecție a mediului în utilizarea și gestionarea echipamentelor informatice		3	6	
3.	Gestionează eficient timpul și adaptarea la schimbări în context profesional		2	4	
4.	Comunică eficient și colaborează în activitățile profesionale		2	4	
5.	Coordonează echipa implicată în activitatea profesională	MANAGEMENT OPERAȚIONAL ȘI CONFORMITATE ÎN SECURITATEA INFORMAȚIEI	2	4	2
6.	Aplică gândirea critică în procesul de luare a deciziilor tehnice și profesionale		1	2	
7.	Aplică prevederile legale referitoare la sănătatea și securitatea în muncă şi în domeniul situațiilor de urgență.		2	4	
8.	Aplică prevederile legislației TIC în activitatea profesională		2	4	
9.	Gestionează conformitatea cu standardele de securitate TIC		3	6	
10.	Elaborează și utilizează scripturile pentru automatizarea sarcinilor tehnice	FUNDAMENTE TEHNICE PENTRU SECURIZAREA SISTEMELOR INFORMATICE	3	6	3
11.	Gestionează și stochează datele în cloud		2	4	
12.	Aplică tehnicile de criptare și procedurile de gestionare a cheilor criptografice pentru protecția datelor.		4	8	

13.	Definește și implementează politicile de securitate a informațiilor în cadrul organizației		3	6	
14.	Identifică vulnerabilitățile și remediază deficiențele în sistemele tehnologiei informației și comunicațiilor (TIC)		3	6	
15.	Aplică măsurile de securitate cibernetică pentru protejarea infrastructurii informatice și a sistemelor digitale	IMPLEMENTAREA MĂSURILOR DE SECURITATE ȘI CONTROL ÎN MEDIUL DIGITAL	2	4	2
16.	Implementează politicile și procedurile pentru asigurarea confidențialității informațiilor		2	4	
17.	Monitorizează incidentele de securitate informatică și de intervenție inițială pentru limitarea impactului		2	4	
18.	Elaborează planurile de răspuns la incidentele de securitate		2	4	
19.	Gestionează drepturile de acces la sistemele informatice în funcție de nivelul de autorizare		2	4	
20.	Identifică și remediază vulnerabilitățile aplicațiilor web în fața amenințărilor de securitate cibernetică	SECURITATE CIBERNETICĂ AVANSATĂ: INVESTIGAȚIE, PREVENȚIE ȘI RECUPERARE	3	6	3
21.	Evaluează riscurile asociate infrastructurii informatice și proiectarea de contramăsuri avansate		3	6	
22.	Planifică și coordonează exercițiile de recuperare a sistemelor informatice în urma incidentelor sau dezastrelor		3	6	
23.	Aplică tehnicile de investigație digitală în cadrul expertizei criminalistice informatice		3	6	
24.	Elaborează proceduri de securitate pentru gestionarea dispozitivelor mobile și a muncii la distanță		2	4	
25.	Planifică și implementează măsuri de conștientizare și formare în domeniul securității informației		1	2	
TOTAL NR ORE			**60**	**120**	**12**
TOTAL NR. CREDITE					

Anexa nr. 2 la standardul ocupațional

PROGRAMA DE PREGĂTIRE TEORETICĂ ȘI PRACTICĂ

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
1.	COMPETENȚE DIGITALE ȘI TRANSVERSALE PENTRU EFICIENȚĂ PROFESIONALĂ	**Integrarea competențelor digitale în activitatea profesională** **1. Aplicații digitale utilizate în domeniul securității informatice** – Tipuri de aplicații: editoare de texte, foi de calcul tabelar, redactare PDF, aplicații pentru documentare tehnică de produs/cod, aplicații pentru documentație structurată etc. – Platforme pentru comunicare și colaborare (Teams, Zoom, Google Workspace, Slack etc.). **2. Comunicarea și colaborarea în echipe digitale** – Utilizarea platformelor de colaborare pentru gestionarea fluxului de lucru. – Etica și bunele practici în comunicarea profesională digitală. – Creare de documente colaborative și lucrul simultan pe conținut. **3. Gestionarea digitală a sarcinilor profesionale** – Introducere în aplicații de tip project/task management.	Teorie: - Prelegeri interactive; - Prezentări; - Dezbatere; - Studiu de caz; - Discuții libere. Practică: - Demonstrație practică; - Aplicații practice; - Exerciții ghidate; - Simulări virtuale; - Dezbateri; - Învățare prin descoperire ghidată; - Studiu de caz; - Discuții libere în grup; - Lucrul în echipe.	- Calculator și echipamente de rețea fizice sau virtuale; - Conexiune Internet; - Software specific (aplicații de redactare și editare, aplicații de planificare și urmărire a sarcinilor); - Platformă colaborative, de videoconferință și comunicare online; - Instrumente / medii de testare și simulare; - Legislație și standarde specifice domeniului; - Resurse digitale online; - Suport de curs; - Videoproiector; - Fișe de practică; - Consumabile foi flipchart, coli A4, marker, etc.	– Cunoștințe despre tipurile de aplicații digitale relevante pentru redactare, calcul tabelar și documentație tehnică. – Demonstrarea utilizării corecte a aplicațiilor pentru editare PDF, formatare, salvare și partajare de documente. – Abilitatea de a utiliza platforme de colaborare (ex: Teams, Slack, Google Workspace) pentru comunicare eficientă în timp real. – Capacitatea de a crea și edita documente partajate în mod colaborativ. – Demonstrarea abilităților de colaborare prin participarea la activități digitale comune (comentarii, notificări, revizuiri). – Cunoștințe despre aplicații de tip project/task management. – Demonstrarea utilizării task management prin crearea, urmărirea și actualizarea sarcinilor unui proiect.	3	6

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		– Organizarea muncii pe etape, prioritizarea și urmărirea sarcinilor folosind aplicații specifice. – Simularea planificării unui proiect IT (sarcini, termene, responsabilități). **4. Utilizarea resurselor digitale pentru documentare tehnică** – Categorii de resurse utile: baze de date, forumuri, site-uri oficiale. – Criterii de selecție a surselor: actualitate, credibilitate, aplicabilitate. – Căutarea ghidată pentru o temă reală.			– Capacitatea de a organiza sarcinile în funcție de priorități și termene-limită folosind aplicații digitale. – Cunoștințe despre sursele digitale de documentare utilizate în domeniul securității informatice (ghiduri, forumuri, baze de date tehnice). – Demonstrarea căutării ghidate și a filtrării rezultatelor relevante pentru o problemă tehnică.		
		Aplicarea principiilor de protecție a mediului în utilizarea echipamentelor TIC **1. Impactul echipamentelor TIC asupra mediului și soluții sustenabile** – Criterii de eficiență energetică și certificare ecologică pentru echipamentele informatice (consum, certificări de mediu și durabilitate). – Criterii pentru alegerea echipamentelor IT sustenabile (eficiență energetică, certificări ecologice, sustenabilitate, amprentă de carbon, materiale reciclabile).	Teorie: - Prelegeri interactive; - Prezentări interactive; - Dezbatere; - Studiu de caz; - Discuții libere. Practica: - Demonstrație practică; - Exerciții interactive aplicate; - Simulări;	- Calculator și echipamente de rețea fizice sau virtuale; - Conexiune Internet; - Software specific; - Platformă de videoconferințe și comunicare online; - Instrumente/medii de testare și simulare; - Legislație și standarde specifice domeniului; - Resurse digitale online;	– Cunoștințe despre certificările ecologice și criteriile de eficiență energetică aplicabile echipamentelor IT. – Abilitatea de a compara echipamente în funcție de consumul energetic și impactul de mediu. – Capacitatea de a evalua gradul de sustenabilitate al unui echipament TIC. – Abilitatea de a identifica și implementa măsuri pentru economisirea energiei în	3	6

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		– Analiză comparativă între două tipuri de echipamente (laptop, imprimantă) în funcție de consumul energetic și impactul asupra mediului. **2. Reducerea consumului de resurse în activitatea profesională** – Măsuri pentru economisirea energiei (moduri standby, închidere automată, iluminare redusă etc.). – Alternative digitale la consumul de hârtie și transport: documente digitale, semnături electronice, videoconferințe etc. – Studiu de caz privind reorganizarea activităților unui birou pentru reducerea consumului de energie. **3. Reciclarea și eliminarea corectă a echipamentelor electronice** – Noțiuni de bază despre DEEE (deșeuri de echipamente electrice și electronice). – Proceduri de colectare, transport, reciclare și rolul partenerilor autorizați. - Procedură internă pentru eliminarea responsabilă a echipamentelor IT uzate. **4. Criterii de sustenabilitate în procesul de achiziții IT**	- Dezbateri; - Studiu de caz; - Învățare prin rezolvarea de probleme; Discuții libere în grup;	- Suport de curs; - Videoproiector; - Fișe de practică; - Consumabile foi flipchart, coli A4, marker, etc.	utilizarea echipamentelor informatice. – Capacitatea de a propune soluții digitale ca alternativă la consumul de hârtie și transport. – Demonstrarea gândirii critice în reorganizarea activităților unui birou în scopul reducerii consumului de resurse. – Cunoștințe despre funcțiile software sau hardware care contribuie la reducerea consumului (ex. moduri standby, oprire automată). – Cunoștințe despre categoria DEEE și obligațiile legale privind eliminarea acestora. – Abilitatea de a descrie și aplica pașii corecți pentru eliminarea responsabilă a unui echipament IT uzat. – Cunoștințe despre factorii de evaluare sustenabilă a echipamentelor IT (consum, durabilitate, reciclabilitate, mentenanță, trasabilitate). – Abilitatea de a construi o grilă de selecție pentru achiziții IT pe criterii ecologice. – Capacitatea de a argumenta o alegere tehnologică în funcție		

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		– Factori de evaluare: durabilitate, mentenanța, consum, reciclabilitate, transparență furnizori, certificări. – Realizarea unei grile de selecție pentru o viitoare achiziție de echipamente IT sustenabile **5. Promovarea unui comportament eco-responsabil în echipă** – Exemple de practici ecologice aplicabile în activitatea zilnică. – Comunicarea și diseminarea în echipă a mesajelor privind protecția mediului. –Mini-ghid cu 10 reguli eco-responsabile pentru un departament IT.			de impactul asupra mediului și eficiența energetică. – Abilitatea de a identifica și propune practici ecologice aplicabile în activitatea profesională zilnică. – Cunoștințe despre modalități de diseminare eficientă a mesajelor privind sustenabilitatea în cadrul organizației.		
		Gestionarea timpului și adaptarea la schimbări în activitatea profesională **1. Planificarea eficientă a timpului și organizarea activităților** – Stabilirea priorităților în funcție de termene, obiective și resurse. – Utilizarea instrumentelor digitale pentru planificare și urmărire (ex.: Google Calendar). – Crearea unei agende personale/săptămânale într-o aplicație de organizare digitală.	Teorie: - Prelegeri interactive; - Prezentări interactive; - Dezbatere; - Studiu de caz; Discuții libere. Practica: - Demonstrație practică; - Exerciții interactive aplicate;	- Calculator și echipamente de rețea fizice sau virtuale; - Conexiune Internet; - Software specific; - Platformă de videoconferințe și comunicare online; - Instrumente/medii de testare și simulare; - Resurse digitale online; - Suport de curs; - Videoproiector;	– Abilitatea de a își planifica timpul și a-și prioritiza sarcinile în funcție de termene, obiective și resurse. – Abilitatea de a utiliza instrumente digitale de organizare pentru planificarea activităților. – Demonstrarea capacității de a crea și gestiona o agendă de lucru săptămânală în format digital.	2	4

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		2. Gestionarea adaptivă a activităților în contexte dinamice – Tipuri de schimbări: tehnologice, organizaționale, legislative . – Simularea unei reorganizări a planului de lucru (ex: apariția unei sarcini urgente sau modificarea unei proceduri). **3. Luarea deciziilor rapide sub presiune și în condiții de incertitudine** – Metode de reevaluare a sarcinilor: metoda Eisenhower, matrice urgență-importanță. - Tehnici de menținere a controlului în perioade dificile. – Studiu de caz – prioritizarea și restructurarea sarcinilor într-un scenariu neprevăzut (ex: incident de securitate, defecțiune tehnică). **4. Prevenirea blocajelor de timp și ajustarea ritmului de lucru** – Identificarea și eliminarea factorilor perturbatori ai activității, gestionarea multitaskingului și a întreruperilor. – Crearea de „zone tampon” în programul zilnic pentru a absorbi eventualele întârzieri, întreruperi sau sarcini neprevăzute.	- Simulări; - Dezbateri; - Studiu de caz; - Învățare prin rezolvarea de probleme; - Discuții libere în grup.	- Fișe de practică; - Consumabile foi flipchart, coli A4, marker, etc.	– Abilitatea de a reconfigura rapid lista de sarcini în situații neprevăzute. – Demonstrarea cunoașterii metodelor de prioritizare rapidă (ex: matricea Eisenhower). – Capacitatea de a menține controlul asupra activității în condiții de presiune sau incertitudine. – Abilitatea de a identifica „hoții de timp” și factorii perturbatori care afectează productivitatea zilnică. – Capacitatea de a integra zone tampon în programul de lucru, pentru absorbirea întârzierilor sau a sarcinilor urgente. – Demonstrarea implicării active în ajustarea și optimizarea proceselor de lucru în contextul schimbării.		

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		5. Integrarea schimbărilor și îmbunătățirea continuă a rutinei de lucru – Adaptarea la noi instrumente, noi fluxuri sau noi cerințe. – Soluții pentru îmbunătățirea proceselor interne.					
		Comunicarea eficientă și colaborarea în activitățile profesionale **1. Comunicarea clară și profesionistă în contextul echipei IT** – Tipuri de comunicare profesională: verbală, scrisă, digitală. – Adaptarea mesajului în funcție de audiență. – Redactarea unui mesaj tehnic clar. **2. Formularea și recepționarea feedbackului constructiv** – Diferența dintre critică și feedback. – Comportamente în acordarea și primirea feedbackului. – Joc de rol – oferirea și primirea unui feedback după o sarcină de echipă. **3. Participarea activă în activitățile comune ale echipei**	Teorie: - Prelegeri interactive; - Prezentări; - Dezbatere; - Studiu de caz; - Discuții libere. Practica: - Demonstrație practică; - Exerciții aplicate; - Simulări; - Dezbateri; - Studiu de caz; - Învățare prin rezolvarea de probleme; - Discuții libere în grup;	- Calculator și echipamente de rețea fizice sau virtuale; - Conexiune Internet; - Software specific; - Platformă de videoconferințe și comunicare online; - Instrumente/medii de testare și simulare; - Laboratoare virtuale pentru simulări; - Legislație și standarde specifice domeniului; - Resurse digitale online; - Suport de curs; - Videoproiector; - Fișe de practică; - Consumabile foi flipchart, coli A4, marker, etc.	– Cunoștințe despre tipurile de comunicare profesională (verbală, scrisă, digitală). – Abilitatea de a redacta un mesaj tehnic clar și coerent, adaptat contextului profesional. – Capacitatea de a adapta stilul și tonul comunicării în funcție de interlocutor (coleg tehnic, manager, client). – Abilitatea de a formula și transmite feedback constructiv într-un mod respectuos și argumentat. – Capacitatea de a primi feedback și de a-l utiliza pentru îmbunătățirea propriei activități. – Abilitatea de a colabora eficient prin ascultare activă, asumare, clarificare. – Abilitatea de a utiliza platforme digitale (chat, forum, documente colaborative) pentru	2	4

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		– Etica implicării: ascultare activă, disponibilitate, asumare. – Instrumente de colaborare digitală (chat, platforme de lucru în comun). – Exercițiu: rezolvarea în echipă a unei sarcini practice, cu asumarea de roluri diferite. 4. **Gestionarea situațiilor dificile și menținerea unui climat pozitiv** – Strategii de evitare și detensionare a conflictelor minore. –Simulare – medierea unei neînțelegeri într-o echipă mixtă tehnic/non-tehnic.			comunicarea și organizarea echipei. – Capacitatea de a media o neînțelegere profesională minoră într-un mod empatic și orientat spre soluții. – Cunoștințe despre diferența dintre critică și feedback. – Capacitatea de a gestiona situațiile dificile de comunicare fără escaladarea conflictului.		
2	MANAGEMENT OPERAȚIONAL ȘI CONFORMITATE ÎN SECURITATEA INFORMAȚIEI	**Coordonarea echipei implicate în activitatea profesională** **1. Planificarea activităților de echipă în funcție de obiectivele proiectului** – Etapele planificării: stabilirea obiectivelor, identificarea cerințelor, stabilirea resurselor, definirea activităților și a livrabilelor, definirea termenelor, stabilirea bugetului, evaluarea riscurilor. – Rolul coordonatorului în adaptarea planului la ritmul echipei – Elaborarea unui mini-plan de activități pentru o echipă IT implicată într-un proiect.	Teorie: - Expunere; - Dezbatere; - Studiu de caz; - Discuții libere. Practica: - Demonstrație practică; - Exerciții aplicate; - Simulări; - Dezbateri; - Studiu de caz; - Învățare prin rezolvarea de probleme;	- Calculator și echipamente de rețea (fizice sau virtuale); - Conexiune Internet; - Software specific; - Platformă de videoconferințe și comunicare online; - Instrumente/medii de testare și simulare; - Resurse digitale/ online; - Suport de curs; - Fișe de practică; - Videoproiector.	– Capacitatea de a elabora un plan de activități pentru o echipă IT, cu obiective, resurse, termene și evaluarea riscurilor. – Abilitatea de a adapta planificarea activităților la ritmul de lucru și particularitățile echipei. – Demonstrarea abilității de a evalua competențele și disponibilitatea membrilor echipei pentru a aloca eficient sarcinile. – Capacitatea de a delega responsabilitățile într-un mod echilibrat și motivant.	2	4

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		2. Alocarea eficientă a sarcinilor și resurselor – Criterii de evaluare a competențelor membrilor echipei și a gradului de implicare disponibil. – Delegarea echilibrată a responsabilităților. **3. Monitorizarea progresului și ajustarea planificării** – Instrumente digitale pentru urmărirea stadiului sarcinilor. – Identificarea blocajelor și soluții rapide de intervenție **4. Susținerea echipei prin feedback și mentorat** – Tipuri de feedback (constructiv, corectiv, motivant), tehnici de exprimare feedback. – Modalități de mentorat informal în cadrul echipei tehnice. **5. Facilitarea colaborării și comunicării în echipă** – Instrumente digitale pentru colaborare interdepartamentală. – Simularea unei ședințe de echipă cu scop de aliniere a obiectivelor și responsabilităților.	- Lucrul în echipă; - Discuții libere în grup;	- Consumabile foi flipchart, coli A4, marker, etc.	– Cunoștințe despre utilizarea instrumentelor digitale pentru monitorizarea progresului echipei. – Abilitatea de a identifica blocajele în desfășurarea sarcinilor și de a propune soluții prompte pentru rezolvare. – Demonstrarea competențelor de mentorat informal și susținere profesională a colegilor. – Capacitatea de a formula feedback constructiv și motivant, adaptat contextului și nevoilor individuale. – Demonstrarea competenței de a facilita o ședință de echipă clară și orientată spre alinierea obiectivelor. – Capacitatea de a evalua performanțele individuale și de echipă în raport cu obiectivele planificate.		
		Aplicarea gândirii critice în luarea deciziilor tehnice și profesionale	Teorie: - -Expunere; - Dezbatere; - Studiu de caz;	- Calculator și echipamente de rețea (fizice sau virtuale);	– Cunoștințe despre conceptele de bază ale gândirii critice: analiză logică, obiectivitate,	1	2

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		1. Fundamentele gândirii critice în context profesional – Ce înseamnă gândirea critică: analiză logică, obiectivitate, formulare concluzii, argumentare, identificare erori de raționament. – Rolul gândirii critice în luarea deciziilor tehnice (ex: alegerea unei soluții de securitate). **2. Compararea alternativelor și evaluarea riscurilor** – Criterii de analiză tehnică. – Evaluarea riscurilor asociate fiecărei opțiuni. – Analiză comparativă între două soluții IT propuse pentru o sarcină. **3. Argumentarea deciziilor în fața echipei sau a conducerii** – Tehnici de exprimare clară și logică: structurarea mesajului, susținerea cu date, evitarea limbajului ambiguu **4. Analiza critică a soluțiilor propuse de alții și identificarea punctelor slabe** – Tehnici de evaluare constructivă: întrebări exploratorii, testarea ipotezelor. **5. Asumarea responsabilității și urmărirea rezultatelor deciziilor**	- Discuții libere. Practica: - Demonstrație practică; - Exerciții aplicate; - Simulări; - Dezbateri; - Studiu de caz; - -Învățare prin rezolvarea de probleme; - Lucrul în echipă; - Discuții libere în grup;	- Conexiune Internet; - Software specific; - Platformă de videoconferințe și comunicare online; - Instrumente/medii de testare și simulare; - Legislație și standarde specifice domeniului; - Resurse digitale/ online; - Suport de curs; - Fișe de practică; - Videoproiector. - Consumabile foi flipchart, coli A4, marker, etc	identificarea erorilor de raționament. – Abilitatea de a compara opțiuni tehnice alternative pe baza unor criterii prestabilite (cost, securitate, compatibilitate, scalabilitate). – Capacitatea de a evalua riscurile asociate fiecărei opțiuni analizate. – Abilitatea de a structura o decizie profesională într-un mod coerent și clar, susținut de date sau argumente tehnice. – Abilitatea de a analiza critic soluțiile propuse de alți colegi și de a formula întrebări exploratorii sau observații constructive. – Demonstrarea competenței de a identifica incoerențe sau riscuri în soluțiile tehnice existente și de a propune corecturi. – Capacitatea de a propune soluții alternative viabile și de a estima impactul acestora asupra proiectului sau echipei. – Abilitatea de a defini etape de monitorizare și criterii de succes pentru implementarea deciziilor.		

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		– Definirea etapelor de monitorizare a unei sarcini și a criteriilor de evaluare a rezultatelor. – Exemple de lecții învățate.					
		Aplicarea prevederilor legale privind sănătatea și securitatea în muncă și situațiile de urgență **1. Cadrul legal privind sănătatea și securitatea în muncă (SSM) și situațiile de urgență (PSI)** – Prevederi esențiale din Legea 319/2006 (Securitatea și sănătatea în muncă) și legislația PSI. – Obligațiile angajatului și ale angajatorului. – Exemple aplicate în activitatea IT (echipamente electrice, birouri, camere server). – Identificarea riscurilor într-un spațiu de lucru tehnic (simulare). **2. Utilizarea echipamentelor informatice și de protecție în condiții de siguranță** – Norme privind ergonomia postului de lucru. – Utilizarea în siguranță a echipamentelor specifice ocupației. – Configurarea unui post de lucru IT conform normelor de siguranță. **3. Identificarea, raportarea și reducerea riscurilor**	Teorie: - Prelegeri interactive; - -Prezentări interactive; - Dezbatere; - Studiu de caz; - Discuții libere. Practica: Demonstrație practică; - Exerciții interactive aplicate; - -Simulări; - Dezbateri; - Studiu de caz; - Învățare prin rezolvarea de probleme; - Discuții libere în grup;	- Calculator și echipamente de rețea (fizice sau virtuale); - Conexiune Internet; - Software specific; - Platformă de videoconferințe și comunicare online; - Legislație și standarde specifice domeniului; - Resurse digitale/ online; - Suport de curs; - Fișe de practică; - Videoproiector. - Consumabile foi flipchart, coli A4, marker, etc	– Cunoștințe despre prevederile esențiale din Legea 319/2006 și legislația privind prevenirea și stingerea incendiilor (PSI). – Capacitatea de a identifica obligațiile legale ale angajatului și angajatorului în domeniul SSM și PSI. – Demonstrarea înțelegerii riscurilor specifice din activitățile IT (ex: surse de curent, cabluri, camere server, ventilație, ecrane multiple). – Capacitatea de a aplica normele de ergonomie pentru un post de lucru IT. – Abilitatea de a configura un post de lucru în conformitate cu cerințele de siguranță. – Abilitatea de a identifica situații potențial periculoase și de a acționa pentru prevenirea accidentelor. – Participarea activă la instruiri și simulări privind situațiile de urgență și aplicarea corectă a celor învățate.	2	4

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		– Tipuri de riscuri și procedura de raportare. – Comunicarea cu responsabilii SSM/PSI. **4. Participarea la instruiri și simulări privind situațiile de urgență** – Tipuri de situații de urgență (incendiu, cutremur, accident tehnic etc.). – Rolul angajatului în simulări și evacuări. - Simulare de evacuare – stabilirea traseelor, punctelor de adunare, rolurilor **5. Aplicarea procedurilor de prim-ajutor și intervenție** – Intervenții de bază: acordarea primului ajutor (arsuri, leșin, răni etc.).			– Capacitatea de a acționa corect într-o simulare de evacuare. – Cunoștințe despre principalele tipuri de situații de urgență și reacțiile corespunzătoare fiecăreia. – Abilitatea de a aplica măsuri de prim-ajutor în situații comune (leșin, arsuri, răni minore etc.).		
		Aplicarea prevederilor legislației TIC în activitatea profesională **1. Reglementări legale relevante în domeniul tehnologiei informației și comunicațiilor** – Cadrul legislativ aplicabil: GDPR, legea privind securitatea cibernetică, legislație privind licențierea software etc. – Obligații și responsabilități ale utilizatorilor și ale organizației.	Teorie: - Prelegeri interactive; - -Prezentări interactive; - Dezbatere; - Studiu de caz; - Discuții libere. Practica: Demonstrație practică;	- Calculator și echipamente de rețea (fizice sau virtuale); - Conexiune Internet; - Software specific; - Platformă de videoconferințe și comunicare online;	– Cunoștințe despre cadrul legislativ TIC aplicabil. – Capacitatea de a identifica obligațiile legale ale utilizatorilor și organizației în domeniul IT. – Abilitatea de a aplica prevederile privind protecția datelor cu caracter personal în activitățile curente.	2	4

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		2. Aplicarea prevederilor legale în activitatea curentă – Protecția datelor cu caracter personal în activități IT. – Drepturile de proprietate intelectuală în dezvoltarea și utilizarea soluțiilor software. – Politici interne de conformitate legală. **3. Monitorizarea modificărilor legislative și** adaptarea **procedurilor** – Surse oficiale de informare: ANSPDCP, CERT-RO, CE, portaluri de legislație etc. – Adaptarea politicilor și procedurilor interne la schimbările legislative **4. Colaborarea interdepartamentală și relația cu autoritățile competente.** – Când și cum se colaborează cu departamentul juridic. – Exemple de interacțiuni: solicitări ANSPDCP, notificări de incident de securitate.	- Exerciții interactive aplicate; - -Simulări; - Dezbateri; - Studiu de caz; - Învățare prin rezolvarea de probleme; Discuții libere în grup;	- Legislație și standarde specifice domeniului; - Resurse digitale/ online; - Suport de curs; - Fișe de practică; - Videoproiector. - Consumabile foi flipchart, coli A4, marker, etc	– Demonstrarea respectării drepturilor de proprietate intelectuală în utilizarea sau dezvoltarea soluțiilor software. – Capacitatea de a integra cerințele legale în politicile și procedurile interne ale organizației. – Abilitatea de a recunoaște situații care necesită conformitate legală (ex: utilizarea de software nelicențiat, prelucrare neautorizată de date). – Cunoștințe despre tipuri de interacțiuni cu autoritățile competente (ex: răspunsuri la solicitări ANSPDCP, notificări de incidente de securitate). – Capacitatea de a identifica și semnala neconformități juridice sau tehnice în cadrul proceselor informatice. – Abilitatea de a propune de măsuri corective pentru alinierea la cerințele legale.		
		Gestionarea conformității cu standardele de securitate TIC **1. Standardele internaționale în domeniul securității informației**	Teorie: - Expunere; - Dezbatere; - Studiu de caz; - Discuții libere.	- Calculator și echipamente de rețea (fizice sau virtuale); - Conexiune Internet; - Software specific;	– Cunoștințe despre principalele standarde de securitate a informației. – Capacitatea de a identifica cerințele-cheie și aplicabilitatea	3	6

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		– Prezentarea principalelor standarde: ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 27017, ISO/IEC 27018, NIST, ISO/IEC 15408, ISO 31000, CIS Controls etc. – Rolul standardelor în organizații și cerințele de bază. – Identificarea cerințelor-cheie dintr-un standard. **2. Evaluarea conformității politicilor și procedurilor interne** – Metode de analiză și de verificare a implementării cerințelor de standard (analiza documentare, observare directă, chestionare, audituri interne etc.). – Ghiduri de evaluare a alinierii la standarde (ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005 etc.). –**Auditul intern de securitate TIC - generalități** – Etapele unui audit intern: planificare audit, documentare și colectare de date, analiză, realizare audit, raportare, comunicare rezultate, acțiuni corective, îmbunătățire continuă. – Tipuri de constatări: conformități, neconformități, observații.	Practică: - Demonstrație practică; - Exerciții interactive aplicate; - -Simulări; - Dezbateri; - Studiu de caz; - Învățare prin rezolvarea de probleme; - Discuții libere în grup;	- Platformă de videoconferințe și comunicare online; - Instrumente/medii de testare și simulare; - Legislație și standarde specifice domeniului; - Resurse digitale/ online; - Suport de curs; - Fișe de practică; - Videoproiector. - Consumabile foi flipchart, coli A4, marker, etc.	acestora în contextul organizațional. – Abilitatea de a analiza politicile și procedurile interne în raport cu cerințele standardelor relevante. – Cunoștințe despre ghidurile de evaluare a alinierii la standarde (ex: ISO/IEC 27003, 27004, 27005). – Cunoștințe despre etapele unui audit intern de securitate TIC. – Abilitatea de a identifica și clasifica constatări de audit: conformități, neconformități, observații. – Capacitatea de a redacta rapoarte de audit clare, structurate și conforme cu cerințele standardelor. – Capacitatea de a elabora documentația aferentă procesului de audit și pregătirii pentru certificare sau recertificare. – Abilitatea de a propune măsuri corective în cazul constatării neconformităților. – Cunoștințe despre rolul și responsabilitățile echipelor implicate (tehnice,		

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		3. Raportarea și documentarea conformității – Structura unui raport de audit și exemple de anexe.– **4. Colaborarea interdepartamentală pentru menținerea conformității** – Rolul echipelor tehnice, manageriale și de conformitate. – Comunicarea eficientă a cerințelor de îmbunătățire și a modificărilor.			manageriale, de conformitate) în menținerea standardelor. – Capacitatea de a comunica eficient cerințele de îmbunătățire și modificările relevante către actorii implicați.		
3	FUNDAMENTE TEHNICE PENTRU SECURIZAREA SISTEMELOR INFORMATICE	**Elaborarea și utilizarea scripturilor pentru automatizarea sarcinilor tehnice** 1. **Introducere în scripting și automatizare sarcini în IT** – Ce este un script și ce tipuri de sarcini poate automatiza. – Limbaje uzuale: Bash, PowerShell, Python, Batch, JavaScript, C etc. – Domenii de aplicare: backup, scanări, configurări, monitorizare. - Analiza unui script și identificarea funcționalității. 2. **Scrierea scripturilor pentru sarcini repetitive** – Structura de bază a unui script (variabile, condiții, bucle, comenzi). 3. **Testarea și validarea scripturilor în medii controlate**	Teorie: - Expunere; - Dezbatere; - Studiu de caz; - Discuții libere. Practica: - Demonstrație practică; - Exerciții aplicate; - Simulări; - Dezbateri; - Studiu de caz; - Învățare prin rezolvarea de probleme; Discuții libere în grup;	- Calculator și echipamente de rețea fizice sau virtuale; - Conexiune Internet; - Software specific; - Platformă de videoconferințe și comunicare online; - Instrumente/medii de testare și simulare; - Laboratoare virtuale pentru simulări; - Legislație și standarde specifice domeniului; - Resurse digitale online; - Suport de curs; - Videoproiector; - Fișe de practică;	– Cunoștințe despre rolul tipurile de sarcini care pot fi automatizate. – Cunoștințe despre limbajele uzuale de scripting (ex: Bash, PowerShell, Python, Batch, JavaScript, C) și domeniile lor de aplicare. – Capacitatea de a analiza un script existent și de a identifica funcționalitatea fiecărei secțiuni. – Abilitatea de a scrie scripturi simple pentru sarcini repetitive. – Capacitatea de a crea un mediu de testare sigur pentru un script. – Abilitatea de a testa scripturile prin metode adecvate: validare a rezultatelor, debugging, loguri, simulări.	3	6

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		– Crearea unui mediu de testare sigur (Virtual Machines, containere, directoare izolate, laboratoare de testare izolate). - Metode de validare și depanare (debugging, loguri, simulări). 4. **Adaptarea și actualizarea scripturilor existente** – Identificarea punctelor de personalizare într-un script existent. – Actualizarea variabilelor și integrarea în infrastructura reală. 5. **Documentarea și integrarea scripturilor în fluxurile de lucru** – Redactarea documentației de utilizare: scop, cerințe, instrucțiuni de rulare, output.		- Consumabile foi flipchart, coli A4, marker, etc.	– Capacitatea de a adapta scripturi existente prin modificarea variabilelor, a comenzilor sau a fluxului logic. – Cunoștințe despre bune practici în securizarea codului pentru a preveni vulnerabilități (ex: input validat, permisiuni corecte). – Capacitatea de a redacta documentație de utilizare pentru scripturi: scop, cerințe, pași de rulare, rezultate așteptate.		
		Gestionarea și stocarea datelor în cloud **1. Tipuri de soluții de stocare în cloud și criterii de alegere** – Stocare în cloud: publică, privată, hibridă, - Servicii uzuale de stocare publice: public cloud – fișiere, backup arhive, baze de date, aplicații (Amazon S3, Google Cloud Storage, Microsoft Azure Blob). – Cerințe de securitate și conformitate în alegerea platformei cloud.	Teorie: - Expunere; - Dezbatere; - Studiu de caz; - - Discuții libere. Practica: - Demonstrație practică; - Exerciții aplicate; - Simulări; - Dezbateri; - Studiu de caz;	- Calculator și echipamente de rețea fizice sau virtuale; - Conexiune Internet; - Software specific; - Platformă de videoconferințe și comunicare online; - Instrumente/medii de testare și simulare; - Laboratoare virtuale pentru simulări;	- Cunoștințe despre tipurile de stocare în cloud și diferențele funcționale dintre ele. - Capacitatea de a selecta soluții de stocare în cloud în funcție de cerințele de securitate, conformitate și specificul activității IT. - Demonstrarea înțelegerii caracteristicilor serviciilor uzuale de stocare. - Abilitatea de a compara platforme cloud din perspectiva	2	4

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		– Comparație de specificații de securitate între două platforme cloud. **2. Configurarea spațiilor de stocare în funcție de politicile de securitate** - Alegerea furnizorului și a tipului de cloud. – Organizarea conturilor, directoarelor și volumelor logice – Stabilirea politicilor de acces și criptare la nivel de server/client. - Încărcarea datelor în cloud. **3. Controlul accesului la datele stocate în cloud** – Autentificare, autorizare în cloud. – Setarea permisiunilor pentru utilizatori și grupuri. – Simularea unui scenariu de acces diferențiat pentru utilizatori tehnici și non-tehnici **4. Monitorizarea și asigurarea integrității datelor** – Jurnale de acces, audit, alerte și evenimente suspecte. – Instrumente pentru monitorizare și protecție cloud. **5. Politici de backup și restaurare în medii cloud** – Tipuri de backup (automat, incremental, manual); reguli de retenție.	- Învățare prin rezolvarea de probleme; Discuții libere în grup;	- Legislație și standarde specifice domeniului; - Resurse digitale online; - Suport de curs; - Videoproiector; - Fișe de practică; - Consumabile foi flipchart, coli A4, marker, etc.	măsurilor de securitate și a cerințelor de conformitate. - Capacitatea de a configura conturi, directoare și volume logice pentru stocarea datelor. - Abilitatea de a încărca date în cloud și de a stabili reguli clare de acces și criptare. - Capacitatea de a seta permisiuni diferențiate pentru utilizatori și grupuri în funcție de roluri. - Abilitatea de a implementa scenarii de acces diferențiat (ex: tehnic vs. non-tehnic) și de a controla vizibilitatea și modificările asupra datelor. - Cunoștințe despre instrumentele și metodele de monitorizare a accesului și integrității datelor (loguri, alerte, audituri). - Abilitatea de a configura politici de backup: alegerea tipului de backup, programarea, reguli de retenție. - Cunoștințe despre cerințele GDPR privind protecția datelor în cloud.		

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		– Restaurarea datelor și testarea planurilor de recuperare. – Configurarea unui plan de backup și simularea restaurării unei versiuni anterioare. **6. Conformitatea cu legislația privind protecția datelor în cloud** - GDPR: localizarea datelor, criptare, controlul accesului, dreptul de a fi uitat. – Relația cu furnizorii de servicii cloud: contracte, obligații, responsabilități.					
		Aplicarea tehnicilor de criptare și gestionarea cheilor criptografice pentru protecția datelor. 1. **Fundamentele criptării și clasificarea tehnologiilor criptografice** – Tipuri de criptare: - După metoda de criptare: simetrică (AES), asimetrică – cu chei publice sau private (RSA, ECC), hibridă. - După nivelul de aplicare (la nivel de disc, de fișier/folder, de aplicație, în tranzit, în repaus). - După scop (confidențialitate, autentificare și integritate).	Teorie: - Expunere; - Dezbatere; - Studiu de caz; - - Discuții libere. Practica: - Demonstrație practică; - Exerciții aplicate; - Simulări; - Dezbateri; - Studiu de caz; - Învățare prin rezolvarea de probleme;	- Calculator și echipamente de rețea fizice sau virtuale; - Conexiune Internet; - Software specific; - Platformă de videoconferințe și comunicare online; - Instrumente/medii de testare și simulare; - Laboratoare virtuale pentru simulări; - Legislație și standarde specifice domeniului; - Resurse digitale online; - Suport de curs;	- Cunoștințe despre tipurile de criptare: simetrică, asimetrică, hibridă și domeniile lor de aplicare. - Capacitatea de a alege tehnologia de criptare potrivită. - Cunoștințe despre nivelurile de aplicare a criptării. - Abilitatea de a implementa criptarea în aplicații și sisteme conform politicilor de securitate ale organizației. - Capacitatea de a evalua nevoile reale de criptare într-o organizație și de a defini zonele critice care necesită protecție. - Cunoștințe despre ciclul de viață al cheilor criptografice:	4	8

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		– Alegerea tehnologiei de criptare potrivite în funcție de scenariu. 2. **Gestionarea ciclului de viață al cheilor criptografice** – Procese specifice: generare, distribuire, stocare, folosire, rotație/reînnoire, revocare, expirare, arhivare, ștergere/distrugere. – Instrumente pentru gestionare cheilor de criptare și exemple de folosire: HSM (Hardware Security Module), KMS (Key Management Service), PKI (Public Key Infrastructure). – Integrarea instrumentelor în politicile interne de securitate a informației. 3. **Implementarea criptării în aplicații și sisteme** – Criptare la nivel de disc, la nivel de bază de date, aplicație sau transport. – Controlul accesului la cheile de decriptare. 4. **Monitorizarea utilizării criptării și revizuirea periodică** – Instrumente și metode de audit: verificarea logurilor, testarea politicilor de criptare, scanare pentru date necriptate –Exemple de acțiuni corective	- Discuții libere în grup;	- Videoproiector; - Fișe de practică; - Consumabile foi flipchart, coli A4, marker, etc.	generare, distribuire, stocare, folosire, rotație, revocare, arhivare, distrugere. - Abilitatea de a gestiona cheile criptografice cu ajutorul instrumentelor specializate: HSM, KMS, PKI. - Capacitatea de a controla accesul la cheile de decriptare și de a restricționa acest acces doar la personal autorizat. - Cunoștințe despre vulnerabilități comune în criptare și riscurile asociate algoritmilor slabi sau neactualizați. - Capacitatea de a revizui periodic politicile de criptare și de a propune acțiuni corective când sunt identificate deficiențe. - Abilitatea de a colabora cu echipele tehnice pentru integrarea soluțiilor criptografice în infrastructura IT existentă.		

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		5. **Adaptarea la evoluția algoritmilor și standardelor** – Vulnerabilități cunoscute în criptare. – Migrarea la algoritmi recomandați (AES-256, SHA-2, SHA-3, TLS 1.3, RSA 2048+, ECC).					
		Definirea și implementarea politicilor de securitate a informațiilor în cadrul organizației **1. Rolul politicilor de securitate în cadrul organizației** – Tipuri de politici de securitate a informației: - Politica generală de securitate; - Politici privind accesul și autentificarea; - Politici privind criptarea și protecția datelor; - Politici privind securitatea operațională; - Politici privind utilizarea tehnologiei; - Politici privind securitatea angajaților; - Politici privind testarea și evaluarea securității. – Cerințe legislative și de standardizare aplicabile.	Teorie: - Expunere; - Dezbatere; - Studiu de caz; - - Discuții libere. Practica: - Demonstrație practică; - Exerciții aplicate; - Simulări; - Dezbateri; - Studiu de caz; - Învățare prin rezolvarea de probleme; - Discuții libere în grup;	- Calculator și echipamente de rețea fizice sau virtuale; - Conexiune Internet; - Software specific; - Platformă de videoconferințe și comunicare online; - Instrumente/medii de testare și simulare; - Laboratoare virtuale pentru simulări; - Legislație și standarde specifice domeniului; - Resurse digitale online; - Suport de curs; - Videoproiector; - Fișe de practică; - Consumabile foi flipchart, coli A4, marker, etc.	- Cunoștințe despre rolul politicilor de securitate a informației și cerințele lor. - Capacitatea de a face diferența între diverse tipuri de politici (ex: acces, criptare, utilizarea tehnologiei, testare, angajați etc.). - Abilitatea de a identifica politicile de securitate necesare într-un scenariu organizațional specific. - Cunoștințe despre structura standard a unei politici de securitate. - Abilitatea de a redacta politici de securitate adaptate contextului organizațional. - Demonstrarea competenței în aplicarea mecanismelor de implementare: instruiri, proceduri tehnice, controale automate. - Capacitatea de a selecta metode de validare a politicilor	3	6

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		– Identificarea politicilor obligatorii într-un anumit scenariu organizațional **2. Redactarea politicilor și procedurilor de securitate** – Structura unei politici: scop, domeniu de aplicare, termeni și definiții responsabilități, reguli și măsuri de aplicare și excepții, monitorizare, audit și conformitate, referințe legale și standarde aplicabile. – Reguli de redactare (claritate, accesibilitate, aliniere cu terminologia tehnică și juridică). **3. Implementarea și validarea politicilor în activitățile operative** – Mecanisme de implementare: instruire periodică, proceduri tehnice, controale automate. – Metode de validare: checklisturi, interviuri, audituri interne. **4. Monitorizarea aplicării politicilor și intervenția în caz de neconformitate** – Instrumente de urmărire: loguri, alerte, evaluări de performanță, rapoarte. – Pași în gestionarea abaterilor: constatare, avertizare, măsuri corective.			prin checklisturi, interviuri, audituri interne sau evaluări. - Abilitatea de a monitoriza aplicarea politicilor. - Cunoștințe despre pașii de gestionare a neconformităților. - Abilitatea de a contribui la integrarea politicilor de securitate în cultura organizațională și în strategia IT. - Cunoștințe despre importanța sprijinului conducerii în implementarea politicilor.		

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		5. Revizuirea și actualizarea periodică a politicilor – Factori declanșatori: schimbări legislative, tehnologice, organizaționale – Procedura de revizuire: calendar, responsabilități, aprobare **6. Integrarea politicilor în cultura organizațională și în strategia IT** – Importanța sprijinului din partea conducerii. - Modalități de includere a politicilor de securitate in sistemul de management organizațional.					
		Identificarea vulnerabilităților și remedierea deficiențelor în sistemele tehnologiei informației și comunicațiilor (TIC) **1. Identificarea vulnerabilităților** - Tipuri de vulnerabilități (software, de rețea, de configurare). - Surse: CVE, buletine de securitate. - Metode de identificare (audit, inspecție, checklist). **2. Evaluarea riscurilor** - Noțiuni: risc, impact, probabilitate. -- Matrice de risc și scor CVSS. - Prioritizarea remediilor. - Clasificare riscuri pe cazuri concrete.	- Teorie: - - Expunere; - - Dezbatere; - - Studiu de caz; - - Discuții libere. Practica: - Demonstrație practică; - Exerciții aplicate; - Simulări; - Dezbateri; - Studiu de caz; - Învățare prin rezolvarea de probleme;	- Calculator și echipamente de rețea fizice sau virtuale; - Conexiune Internet; - Software specific; - Platformă de videoconferințe și comunicare online; - Instrumente/medii de testare și simulare; - Laboratoare virtuale pentru simulări;	- Cunoștințe despre tipurile de vulnerabilități (software, rețea, configurare) și modul în care acestea afectează sistemele TIC. - Abilitatea de a identifica vulnerabilități folosind surse specializate (CVE, buletine de securitate, alerte CERT). - Demonstrarea aplicării metodelor de identificare a vulnerabilităților: audituri, checklisturi, inspecție manuală. - Abilitatea de a utiliza o matrice de risc pentru a prioritiza remedierea vulnerabilităților. - Capacitatea de a clasifica riscurile identificate pe baza	3	6

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		3. Scanare și testare - Scanere automate (Nmap, OpenVAS, Nessus). - Testare manuală . **4. Remediere** - Gestionarea actualizărilor de securitate și corectare a erorilor pentru sistemele informatice, aplicații, echipamente sau componente software. - Reducerea punctelor slabe (hardening) și controale compensatorii.	- Discuții libere în grup;	- Legislație și standarde specifice domeniului; - Resurse digitale online; - Suport de curs; - Videoproiector; - Fișe de practică; - Consumabile foi flipchart, coli A4, marker, etc.	cazurilor concrete din infrastructura IT. - Abilitatea de a efectua scanări automate de securitate cu instrumente precum Nmap, OpenVAS, Nessus. - Demonstrarea competenței în aplicarea tehnicilor de testare manuală pentru validarea vulnerabilităților identificate. - Capacitatea de a propune soluții adecvate de remediere, în funcție de natura vulnerabilității și nivelul de risc. - Abilitatea de a face actualizări pentru sisteme, aplicații și echipamente. - Cunoștințe despre tehnicile de reducere a suprafeței de atac: hardening, restrângerea serviciilor neutilizate, controale compensatorii. - Capacitatea de a colabora cu echipele IT pentru implementarea eficientă a măsurilor de remediere. - Capacitatea de a monitoriza sistemele post-remediere și de a confirma eficiența măsurilor aplicate. -		

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
4.	IMPLEMENTAREA MĂSURILOR DE SECURITATE ȘI CONTROL ÎN MEDIUL DIGITAL	**Securizarea infrastructurii informatice și a sistemelor digitale** **1. Noțiuni fundamentale despre securitatea infrastructurii** - Suprafața de atac: definiție, tipuri de amenințări, puncte critice din rețea și stații de lucru. - Tipuri de controale: preventive, detective, corective (exemple aplicate). **2. Mecanisme de protecție la nivel de rețea și endpoint** - Firewall-uri, IDS/IPS, EDR – funcții, tipuri, moduri de operare. - Configurarea regulilor de filtrare, restricții de acces și monitorizare. **3. Segmentarea rețelei și controlul accesului** - Principii de segmentare (VLAN, zone DMZ, politici Zero Trust). - Controlul accesului pe bază de roluri (RBAC), reguli de rețea și ACL-uri. **4. Patch management și actualizări de securitate** - Procesul de gestionare a actualizărilor: monitorizare, testare, aplicare. - Importanța patch-urilor pentru reducerea vulnerabilităților. **5. Monitorizare și evaluare a eficienței măsurilor de securitate**	Teorie: - Expunere; - Dezbatere; - Studiu de caz; - Discuții libere. Practică: - Demonstrație practică; - Exerciții aplicate; - Simulări; - Dezbateri; - Studiu de caz; - Învățare prin rezolvarea de probleme; - Discuții libere în grup;	- Calculator și echipamente de rețea fizice sau virtuale; - Conexiune Internet; - Software specific; - Platformă de videoconferințe și comunicare online; - Instrumente/medii de testare și simulare; - Laboratoare virtuale pentru simulări; - Legislație și standarde specifice domeniului; - Resurse digitale online; - Suport de curs; - Videoproiector; - Fișe de practică; - Consumabile foi flipchart, coli A4, marker, etc.	- Cunoștințe despre conceptele de bază legate de securitatea infrastructurii: suprafața de atac, tipuri de amenințări și controale de securitate. - Capacitatea de a identifica punctele critice ale infrastructurii IT (rețea, endpoint, aplicații) care necesită protecție. - Abilitatea de a configura și administra controale de securitate preventive, detective și corective. - Cunoștințe despre funcționarea și tipologia soluțiilor de protecție la nivel de rețea și endpoint (firewall, IDS/IPS, EDR). - Capacitatea de a configura reguli de filtrare, politici de acces și de a monitoriza activitatea prin soluții de securitate. - Demonstrarea utilizării principiilor de segmentare a rețelei pentru limitarea expunerii. - Abilitatea de a aplica politici de control al accesului bazate pe roluri (RBAC) și liste de control al accesului (ACL). - Cunoștințe despre procesul de patch management și importanța actualizărilor pentru reducerea vulnerabilităților.	2	4

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		- Interpretarea log-urilor, alerte de securitate, semnale de atac. - Evaluarea post-audit sau post-incident, îmbunătățirea sistemelor. **6. Colaborarea în proiectarea securizată a infrastructurii** - Rolul colaborativ al specialistului în securitate în proiecte IT. - Integrarea controalelor de securitate în sistemele noi (cloud, aplicații, rețea).			- Demonstrarea implicării în activități de evaluare post-audit sau post-incident pentru validarea eficienței măsurilor. - Capacitatea de a propune și implementa măsuri de îmbunătățire a securității pe baza rezultatelor analizelor și testelor. - Cunoștințe despre metodele de integrare a controalelor de securitate în proiectele IT (rețea, cloud, aplicații).		
		Implementarea politicilor de confidențialitate a informațiilor **1. Politici și reguli privind confidențialitatea informațiilor** - Tipuri de informații confidențiale (ex.: date personale, date financiare, documente interne). - Principii: confidențialitate, necesitatea accesului, proporționalitate, minimizarea riscului. - Politicile interne și reglementări aplicabile (ex.: GDPR). **2. Controlul accesului la date** - Noțiuni despre autorizare și autentificare. - Metode de restricționare a accesului la date: criterii, factori de autentificare, exemple de	Teorie: - Expunere; -Dezbatere; - Studiu de caz; - Discuții libere. Practică: - Demonstrație practică; - Exerciții aplicate; -Simulări; -Dezbateri; - Studiu de caz; - Învățare prin rezolvarea de probleme; - Discuții libere în grup;	- Calculator și echipamente de rețea fizice sau virtuale; - Conexiune Internet; - Software specific; - Platformă de videoconferințe și comunicare online; - Instrumente/medii de testare și simulare; - Laboratoare virtuale pentru simulări;	- Cunoștințe despre tipurile de informații confidențiale (ex: date personale, financiare, documente interne) și riscurile asociate. - Capacitatea de a aplica principiile de confidențialitate: necesitatea accesului, minimizarea riscului, proporționalitatea. - Cunoștințe despre reglementările și politicile interne privind protejarea informațiilor (ex: GDPR). - Abilitatea de a aplica politici de control al accesului în funcție de responsabilitățile utilizatorilor. - Capacitatea de a configura și gestiona metode de restricționare	2	4

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		restricționări (RBAC- Role-Based Access Control, politici ACL, parole, MFA - Multi Factor Authentication). - Studiu de caz: configurarea drepturilor de acces pe foldere sau baze de date într-un scenariu dat. **3. Conștientizarea utilizatorilor și bune practici** - Responsabilitatea utilizatorului în manipularea datelor sensibile. - Reguli de bază pentru protejarea informațiilor (evitarea partajării, folosirea criptării, blocarea stației de lucru etc.). - Redactarea în echipă a unui mini-ghid de manipulare a datelor confidențiale pentru colegii non-tehnici. **4. Monitorizarea și măsuri de protecție tehnică** - Loguri de acces, alerte de securitate, semnalarea incidentelor. - Soluții tehnice de protecție: criptare, DLP (Data Loss Prevention), protecție endpoint. **5. Clasificarea informațiilor și aplicarea măsurilor corespunzătoare**		- Legislație și standarde specifice domeniului; - Resurse digitale online; - Suport de curs; - Videoproiector; - Fișe de practică; - Consumabile foi flipchart, coli A4, marker, etc.	a accesului: RBAC, ACL, MFA, parole, grupuri. - Abilitatea de a clasifica informațiile pe niveluri (intern, confidențial, restricționat) și de a aplica măsurile corespunzătoare. - Cunoștințe despre soluțiile tehnice pentru protecția datelor confidențiale. - Capacitatea de a utiliza loguri, alerte și instrumente de audit pentru a monitoriza accesul și manipularea datelor. - Abilitatea de a participa activ la sesiuni de instruire și conștientizare privind protecția datelor sensibile. - Capacitatea de a identifica și semnala abateri de la politicile de confidențialitate. - Cunoștințe despre responsabilitatea individuală în manipularea datelor sensibile. - Abilitatea de a propune măsuri de corectare în urma unei breșe sau încălcări a confidențialității.		

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		- Niveluri de clasificare: intern, confidențial, restricționat. - Măsuri asociate fiecărui nivel: criptare, trasabilitate, audit. - Studiu de caz: clasificarea documentelor + alegerea măsurilor de protecție aferente.					
		Monitorizarea incidentelor și intervenția inițială în securitatea informatică **1.Noțiuni despre incidente de securitate și semnale de avertizare** - Ce este un incident de securitate. - Tipuri de incidente (sustragerea neautorizată de date, malware, atac DDoS, acces neautorizat). - Semnale precursoare și indicatori de compromitere (IoC). **2. Monitorizarea sistemelor și colectarea datelor** - Surse de date: loguri de sistem, jurnale de acces, fluxuri de date rețea (circulația pachetelor în rețeaa). - Rolul: platformelor SIEM, a sistemelor IDS/IPS, antivirus, supraveghere securitate la nivelul dispozitivelor individuale. - Tipuri de alerte și importanța corelării evenimentelor.	Teorie: - Expunere; -Dezbatere; - Studiu de caz; - Discuții libere. Practică: - Demonstrație practică; - Exerciții aplicate; -Simulări; -Dezbateri; - Studiu de caz; - Învățare prin rezolvarea de probleme; - Discuții libere în grup;	- Calculator și echipamente de rețea fizice sau virtuale; - Conexiune Internet; - Software specific; - Platformă de videoconferințe și comunicare online; - Instrumente/medii de testare și simulare; - Laboratoare virtuale pentru simulări; - Legislație și standarde specifice domeniului; - Resurse digitale online; - Suport de curs;	- Cunoștințe despre ce reprezintă un incident de securitate informatică și tipologia incidentelor. - Capacitatea de a recunoaște semnale precursoare și indicatori de compromitere. - Abilitatea de a utiliza surse relevante pentru monitorizare. - Abilitatea de a analiza fișiere log și de a extrage semnale de alertă relevante. - Cunoștințe despre criteriile de clasificare a incidentelor. - Demonstrarea clasificării incidentelor în funcție de severitate: minor, major, critic. - Capacitatea de a evalua rapid situația și de a prioritiza răspunsul în funcție de riscurile asociate. - Abilitatea de a aplica proceduri de izolare, dezactivare și blocare a accesului în caz de incident.	2	4

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		- Analiza unui fișier log. **3.Analiza și clasificarea incidentelor** - Evaluarea severității și stabilirea priorității răspunsului. - Criterii de clasificare: impact, amploare, timp de detecție. - Exemple de clasificare: minor, major, critic. **4. Răspuns rapid la incidente și comunicare internă** - Proceduri de izolare, dezactivare, blocare acces. - Metode de limitare a propagării atacului. - Notificarea echipelor implicate și metode de păstrare a trasabilității. - Simulare de răspuns la un incident de securitate.		- Videoproiector; - Fișe de practică; - Consumabile foi flipchart, coli A4, marker, etc.	- Cunoștințe despre metodele de limitare a propagării atacurilor informatice. - Abilitatea de a contribui la analiza post-incident și de a formula propuneri pentru îmbunătățirea reacției viitoare. - Cunoștințe despre importanța reacției rapide și coordonate în faza inițială a unui incident.		
		Planuri de răspuns la incidente – concepție, testare și îmbunătățire **1. Tipuri de incidente și impactul lor asupra organizației** - Clasificarea incidentelor: acces neautorizat, malware, ransomware, DDoS, scurgeri de date. - Impact potențial: financiar, reputațional, operațional, legal. - Elemente pentru un scenariu de incident: declanșatorul, evoluția evenimentului, impactul, contextul	Teorie: - Expunere; -Dezbatere; - Studiu de caz; - Discuții libere. Practică: - Demonstrație practică; - Exerciții aplicate; -Simulări; -Dezbateri;	- Calculator și echipamente de rețea fizice sau virtuale; - Conexiune Internet; - Software specific; - Platformă de videoconferințe și comunicare online;	- Cunoștințe despre tipurile de incidente de securitate și impactul acestora asupra organizației. - Abilitatea de a construi un scenariu realist de incident, cu elemente-cheie. - Cunoștințe despre structura standard a unui plan de răspuns la incidente (scop, domeniu, echipă, pași operaționali, comunicare, finalizare).	2	4

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		tehnic și organizațional afectat, condiții de simulare. - Tipuri de scenarii relevante pentru planificare și estimarea impactului. **2. Structura unui plan de răspuns la incidente de securitate informatică** - Descrierea componentelor planului de răspuns (scop și domeniu de aplicare, tipuri de incidente, echipă de răspuns la incidente, etape operaționale de răspuns, proceduri de răspuns, comunicare, finalizare). - Definirea responsabilităților: CSIRT (Computer Security Incident Response Team), IT, management, comunicații. - Instrumente-suport: liste de verificare, fișe de contact, modele de notificare - Schițe de plan de răspuns pentru un tip de incident (ex: atac ransomware). **3. Proceduri detaliate pentru intervenție și comunicare** - Definirea pașilor operaționali în fazele: detectare, analiză, izolare, eradicare, recuperare. - Fluxul de comunicare internă și externă.	- Studiu de caz; - Învățare prin rezolvarea de probleme; - Discuții libere în grup;	- Instrumente/medii de testare și simulare; - Laboratoare virtuale pentru simulări; - Legislație și standarde specifice domeniului; - Resurse digitale online; - Suport de curs; - Videoproiector; - Fișe de practică; - Consumabile foi flipchart, coli A4, marker, etc.	- Abilitatea de a utiliza instrumente-suport precum liste de verificare, fișe de contact, șabloane de notificare. - Demonstrarea conceperii unui plan de răspuns pentru un incident specific (ex: atac de tip ransomware). - Capacitatea de a detalia etapele intervenției: detectare, analiză, izolare, eradicare, recuperare. - Cunoștințe despre fluxul corect de comunicare internă și externă în timpul unui incident. - Cunoștințe despre obligațiile legale privind notificarea incidentelor (ex: GDPR, CERT-RO). - Capacitatea de a evalua performanța răspunsului: timpi de reacție, calitatea comunicării, completitudinea documentării. - Demonstrarea competenței în actualizarea planurilor de răspuns pe baza lecțiilor învățate, schimbărilor tehnologice sau legislative. - Abilitatea de a propune îmbunătățiri pentru creșterea eficienței și vitezei de reacție a organizației în fața incidentelor.		

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		- Obligații legale de raportare a incidentului. **4. Testarea și actualizarea planurilor** - Tipuri de exerciții: tabletop, simulări tehnice, test complet. - Evaluarea eficienței: timpi de reacție, comunicare, documentare. - Criterii de revizuire a planurilor de răspuns.			- Implicarea activă în procesul de instruire a personalului pentru aplicarea planurilor de răspuns.		
		Administrarea drepturilor de acces în sistemele informatice **1. Principiile accesului controlat la resurse** - Conceptul de drepturi de acces și importanța controlului la resurse. - Principiul minimului privilegiu și al separării funcțiilor. - Riscuri asociate cu drepturi de acces excesive. - Analiza unui caz de acces excesiv și propunerea de reorganizare a permisiunilor. **2. Politici interne și structuri de acces** - Politici de acces: scop, reguli, exemple. - Grupuri de utilizatori, matrici de acces, control acces bazat pe roluri (RBAC).	Teorie: - Expunere; - Dezbatere; - Studiu de caz; - Discuții libere. Practică: - Demonstrație practică; - Exerciții aplicate; - Simulări; - Dezbateri; - Studiu de caz; - Învățare prin rezolvarea de probleme; Discuții libere în grup;	- Calculator și echipamente de rețea fizice sau virtuale; - Conexiune Internet; - Software specific; - Platformă de videoconferințe și comunicare online; - Instrumente/medii de testare și simulare; - Laboratoare virtuale pentru simulări; - Legislație și standarde specifice domeniului;	- Capacitatea de a aplica principiul minimului privilegiu în acordarea drepturilor de acces. - Demonstrarea abilității de a separa atribuțiile între diferite roluri de utilizator. - Capacitatea de a defini și configura roluri de acces, atribuind utilizatorilor permisiuni în funcție de rolurile lor organizaționale. - Aplicarea corectă a unei matrice de acces, mapând utilizatorii/rolurile la resursele sistemului și stabilind ce acțiuni sunt permise fiecărui rol sau utilizator. - Capacitatea de a gestiona conturile utilizatorilor externi.	2	4

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		- Gestionarea conturilor pentru utilizatori temporari, contractori, colaboratori. - Crearea unei matrici de acces pentru un departament într-o aplicație IT **3. Procesul de acordare și retragere a drepturilor** - Cereri formale de acces și validarea acestora. - Activare, modificare, dezactivare conturi. - Trasabilitate și audit. **4. Revizuirea periodică a drepturilor** - Detectarea conturilor inactive, privilegii nejustificate. - Auditul accesului și remedierea anomaliilor. - Raportare și propuneri de corecție. - Studiu de caz: - Examinarea unei liste de conturi fictive și identificarea drepturilor incorecte. **5. Mecanisme de autentificare și MFA** - Metode de autentificare: parolă/PIN/răspuns la o întrebare de securitate, token/cod temporar/aplicație, biometrie (amprentă, recunoaștere facială, vocală, scanare iris).		- Resurse digitale online; - Suport de curs; - Videoproiector; - Fișe de practică; - Consumabile foi flipchart, coli A4, marker, etc.	- Cunoașterea politicilor și procedurilor de gestionare a conturilor utilizatorilor externi. - Abilitatea de a urma un proces standardizat de acordare a accesului, respectând toți pașii necesari. - Capacitatea de a retrage drepturile de acces ale unui utilizator atunci când acesta își schimbă rolul sau părăsește organizația. - Documentarea corectă a acordării și retragerii drepturilor de acces ale unui utilizator. - Capacitatea de a identifica anomalii sau discrepanțe în alocarea drepturilor de acces și de a iniția acțiuni de remediere. - Capacitatea de a efectua un audit periodic al drepturilor de acces ale utilizatorilor. - Aplicarea corectă a procedurilor de raportare a rezultatelor revizuirii drepturilor de acces către factorii de decizie relevanți, formulând recomandări pentru îmbunătățirea politicilor de acces, acolo unde este cazul. - Cunoașterea principalelor metode de autentificare și a		

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		- Autentificare multifactorială (MFA): definiție, beneficii, exemple. - Integrarea autentificării în sistemele organizației. - Configurarea MFA într-un cont demonstrativ (ex. cont Google cu telefon + parolă). - Autentificarea pe bază de certificat digital.			nivelului de protecție oferit de fiecare metodă în parte. - Cunoașterea conceptului de autentificare multi-factor (MFA) și a beneficiilor pe care le aduce. - Cunoașterea modului în care funcționează autentificarea bazată pe certificate digitale și înțelegerea procesului de emitere și gestionare a certificatelor digitale.		
5.	SECURITATE CIBERNETICĂ AVANSATĂ: INVESTIGAȚIE, PREVENȚIE ȘI RECUPERARE	**Securitatea aplicațiilor web – identificarea și remedierea vulnerabilităților** **1. Arhitectura aplicațiilor web și suprafețele de atac** - Componente: front-end, back-end, API, baze de date. - Canale de comunicare și fluxuri de date. - Identificarea zonelor expuse: input-uri, autentificare, permisiuni, marcarea zonelor vulnerabile. - Analiza structurii unei aplicații web demonstrative și marcarea zonelor vulnerabile. **2. Tipuri de vulnerabilități comune aplicațiilor web (OWASP Top 10)**	Teorie: - Expunere; - Dezbatere; - Studiu de caz; - Discuții libere. - Demonstrație practică; - Exerciții aplicate; - Simulări; - Dezbateri; - Studiu de caz; - Învățare prin rezolvarea de probleme; - Discuții libere în grup;	- Calculator și echipamente de rețea fizice sau virtuale; - Conexiune Internet; - Software specific; - Platformă de videoconferințe și comunicare online; - Instrumente/medii de testare și simulare; - Laboratoare virtuale pentru simulări; - Legislație și standarde specifice domeniului;	- Cunoștințe despre arhitectura aplicațiilor web și componentele acesteia. - Capacitatea de a identifica zonele expuse la riscuri în structura unei aplicații web. - Demonstrarea abilităților în analizarea fluxurilor de date și a canalelor de comunicare ale aplicațiilor web. - Cunoștințe despre cele mai frecvente vulnerabilități conform OWASP Top 10. - Capacitatea de a recunoaște tipurile de atacuri cunoscute. - Abilitatea de a utiliza instrumente specializate pentru testarea aplicațiilor web. - Demonstrarea abilității de a efectua teste de penetrare	3	6

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		- SQL Injection, Cross-Site Scripting (XSS), Broken Authentication, CSRF etc. - Riscuri și exploatări posibile pentru fiecare tip de vulnerabilitate. **3. Tehnici și instrumente de testare a securității aplicațiilor** - Teste de penetrare manuale și automate. - Instrumente uzuale de testare automată a aplicațiilor web: Burp Suite, OWASP ZAP, Nikto - Etapele unui test: recunoaștere, scanare, exploatare controlată. **4. Analiza configurațiilor și a codului sursă** - Setări periculoase ale aplicației, serverului sau mediului de rulare, directoare expuse, debug activ. - Cod nesecurizat: lipsa validării, erori de logică - Evaluarea bibliotecilor și componentelor terțe. **5. Remedierea și raportarea vulnerabilităților** - Metode de corectare: validare input, protecție la nivel de server, actualizări. - Redactarea raportului tehnic: descriere, impact, soluție, stare finală.		- Resurse digitale online; - Suport de curs; - Videoproiector; - Fișe de practică; - Consumabile foi flipchart, coli A4, marker, etc.	manuale și automate, respectând etapele de testare. - Cunoștințe despre riscurile asociate setărilor nesigure și a bibliotecilor externe. - Capacitatea de a analiza configurările din mediul de lucru al aplicației. - Capacitatea de a propune soluții tehnice de remediere (. - Demonstrarea abilității de a redacta rapoarte tehnice care descriu vulnerabilitățile, impactul și măsurile luate.		

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		- Monitorizarea vulnerabilităților cunoscute.					
		Evaluarea riscurilor IT și proiectarea măsurilor avansate de securitate **1. Analiza infrastructurii și evaluarea expunerii la risc** - Componentele infrastructurii IT și punctele critice (rețea, aplicații, baze de date, servicii). - Tipuri de riscuri: tehnice, umane, organizaționale, externe. - Metode de identificare a riscurilor: audit intern, inspecție, interviuri, analiza istorică a incidentelor. - Estimarea nivelului de expunere la amenințări. **2. Metodologii de evaluare a riscurilor** - Modele de analiză a riscurilor: impact x probabilitate, scoruri de risc, matricea de risc. - Termeni-cheie: risc, amenințare, vulnerabilitate, risc rezidual, risc acceptat. - Utilizarea standardelor și metodologiilor: ISO/IEC 27005, NIST, ENISA Risk Management.	Teorie: - Expunere; - Dezbatere; - Studiu de caz; - Discuții libere. Practică: - Demonstrație practică; - Exerciții aplicate; - Simulări; - Dezbateri; - Studiu de caz; - Învățare prin rezolvarea de probleme; Discuții libere în grup;	- Calculator și echipamente de rețea fizice sau virtuale; - Conexiune Internet; - Software specific; - Platformă de videoconferințe și comunicare online; - Instrumente/medii de testare și simulare; - Laboratoare virtuale pentru simulări; - Legislație și standarde specifice domeniului; - Resurse digitale online; - Suport de curs; - Videoproiector; - Fișe de practică; - Consumabile foi flipchart, coli A4, marker, etc.	- Cunoștințe despre componentele infrastructurii IT. - Abilități despre identificarea punctelor critice în rețea, aplicații, baze de date și servicii. - Cunoștințe despre conceptele fundamentale: risc, vulnerabilitate, amenințare, impact, probabilitate, risc rezidual. - Capacitatea de a identifica tipuri de riscuri relevante pentru infrastructura IT. - Aplicarea corectă a metodelor de identificare a riscurilor: audit, inspecție, interviu, analiză istorică. - Aplicarea corectă a metodelor de analiză a riscurilor (scor, matrice de risc, formule de evaluare). - Capacitatea de a utiliza metodologii și standarde internaționale de evaluare a riscurilor (ex. ISO/IEC 27005, NIST, ENISA). - Abilitatea de a elabora o matrice de risc și de a clasifica	3	6

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		- Elaborarea unei matrice de risc pentru un scenariu dat (serviciu IT esențial). **3. Scenarii de risc și simulări** - Tehnici de construire a scenariilor: modelarea actorilor, vectorilor de atac și a efectelor. - Simulări de atacuri: DDoS, ransomware, acces neautorizat, pierdere de date. - Analiza consecințelor asupra continuității activității și protecției datelor sensibile. - Elaborarea unui scenariu de atac asupra infrastructurii și analiza răspunsului. **4. Proiectarea și integrarea măsurilor avansate de securitate** - Tipuri de controale: preventive, de detectare, corective și compensatorii. - Măsuri tehnice avansate: segmentare rețea, Zero Trust, EDR, DLP, microsegmentare. **5. Monitorizare, evaluare și îmbunătățire continuă** - Testarea eficienței măsurilor: simulări, audituri, atacuri controlate (red teaming). - Evaluarea riscurilor reziduale și actualizarea planurilor de securitate.			riscurile într-un scenariu real sau simulat. - Demonstrarea capacității de a construi scenarii de risc pornind de la amenințări și vectori de atac. - Cunoștințe despre măsuri avansate de securitate. - Capacitatea de a proiecta soluții adaptate structurii IT și nivelului de risc acceptat. - Abilitatea de a testa și evalua eficiența măsurilor implementate, în urma simulărilor sau auditului.		

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		- Optimizarea procesului de management al riscurilor.					
		Exerciții de recuperare IT și continuitate operațională **1. Scenarii de testare a planurilor de continuitate IT** - Tipuri de incidente majore și dezastre relevante: atac cibernetic, cădere de sistem, catastrofe naturale, erori umane critice. - Elemente-cheie într-un scenariu de recuperare: declanșator, infrastructură afectată, starea inițială a sistemelor, obiectivele testului. **2. Organizarea și coordonarea exercițiilor de recuperare** - Stabilirea obiectivelor exercițiului: RTO (Recovery Time Objective), RPO (Recovery Point Objective). - Planificarea etapelor unui exercițiu: pregătire, simulare, reacție, restaurare, raportare. - Comunicarea responsabilităților în cadrul echipelor implicate. **3. Evaluarea capacității organizaționale de răspuns** - Metode de urmărire și măsurare a capacității de răspuns: timpi de reacție, acuratețea execuției, coordonarea între echipe.	Teorie: - Expunere; - Dezbatere; - Studiu de caz; - Discuții libere. Practică: - Demonstrație practică; - Exerciții aplicate; - Simulări; - Dezbateri; - Studiu de caz; - Învățare prin rezolvarea de probleme; Discuții libere în grup;	- Calculator și echipamente de rețea fizice sau virtuale; - Conexiune Internet; - Software specific; - Platformă de videoconferințe și comunicare online; - Instrumente/medii de testare și simulare; - Laboratoare virtuale pentru simulări; - Legislație și standarde specifice domeniului; - Resurse digitale online; - Suport de curs; - Videoproiector; - Fișe de practică; - Consumabile foi flipchart, coli A4, marker, etc.	- Cunoștințe despre tipologiile de incidente critice și impactul acestora asupra sistemelor informatice. - Capacitatea de a construi scenarii de simulare adaptate infrastructurii IT a organizației. - Abilitatea de a defini obiective clare pentru exercițiile de recuperare (RTO, RPO). - Demonstrarea competenței în planificarea etapelor unui exercițiu de recuperare. - Cunoștințe privind rolurile și responsabilitățile dintr-un plan de răspuns și recuperare . - Abilitatea de a comunica eficient pașii de urmat în timpul simulărilor. - Demonstrarea capacității de a supraveghea desfășurarea unui exercițiu de recuperare și de a interveni în cazul apariției unor obstacole. - Cunoștințe despre metodele de evaluare a performanței în timpul exercițiilor. - Abilitatea de a redacta un raport detaliat post-exercițiu.	3	6

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		- Instrumente de monitorizare și logare a acțiunilor în timpul exercițiului. - Criterii de succes și identificarea punctelor critice. **4. Revizuirea și îmbunătățirea planurilor de recuperare** - Interpretarea datelor rezultate din exercițiu: rapoarte de incident simulare, feedback din echipe, observații critice. - Adaptarea planurilor de continuitate pe baza constatărilor: documentație, resurse, procese. - Propuneri de optimizare: achiziții, actualizări software, training pentru echipe. **5. Comunicarea cu conducerea și raportarea rezultatelor** - Structura raportului de exercițiu: scop, desfășurare, rezultate, dificultăți, recomandări. - Comunicarea rezultatelor testului și a capacității reale de recuperare. - Prezentarea recomandărilor în funcție de performanțele obținute.			- Capacitatea de a formula propuneri de îmbunătățire a planurilor de continuitate pe baza rezultatelor obținute în timpul simulărilor. - Cunoștințe despre criteriile de evaluare a capacității organizaționale de răspuns la incidente majore.		
		Tehnicile de investigație digitală în cadrul expertizei criminalistice informatice **1. Introducere în investigația digitală și cadrul legal**	Teorie: - Expunere; - Dezbatere; - Studiu de caz; - Discuții libere.	- Calculator și echipamente de rețea fizice sau virtuale;	- Cunoștințe privind etapele și cerințele legale ale unei investigații digitale.	3	6

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		- Noțiuni fundamentale: ce este investigația digitală, diferența față de alte tipuri de investigații IT. - Tipuri de incidente care impun investigație digitală. - Cadrul legal național și internațional privind criminalistica digitală. - Drepturi, responsabilități și limitări ale investigatorului. **2. Colectarea și conservarea probelor digitale** - Tipuri de probe digitale: fișiere, loguri, metadate, memorie RAM, trafic de rețea, dispozitive de stocare. - Etapele procesului de colectare a probelor (identificare, izolare, achiziție, verificare). - Reguli de conservare a integrității: hash-uri (MD5, SHA), imaging forensic (ex: FTK Imager, Autopsy, EnCase). - Instrumente utilizate pentru duplicarea și protejarea probelor - Documentarea procesului: lanțul custodie, înregistrarea operațiunilor. **3. Analiza probelor digitale și identificarea urmelor** - Analiza fișierelor: timpi de acces/modificare/creare, extensii ascunse, fișiere șterse.	Practică: - Demonstrație practică; - Exerciții aplicate; - Simulări; - Dezbateri; - Studiu de caz; - Învățare prin rezolvarea de probleme; Discuții libere în grup;	- Conexiune Internet; - Software specific; - Platformă de videoconferințe și comunicare online; - Instrumente/medii de testare și simulare; - Laboratoare virtuale pentru simulări; - Legislație și standarde specifice domeniului; - Resurse digitale online; - Suport de curs; - Videoproiector; - Fișe de practică; - Consumabile foi flipchart, coli A4, marker, etc.	- Cunoștințe despre principiile lanțului de custodie și admisibilitatea probelor digitale. - Capacitatea de a completa corect documentația de colectare și custodie a probelor. - Capacitatea de a examina loguri, fișiere și alte date digitale pentru identificarea indiciilor de activitate malițioasă. - Demonstrarea abilității de a corela datele extrase din diverse surse (loguri, fișiere, rețea). - Capacitatea de a construi o cronologie coerentă a incidentului pe baza dovezilor. - Demonstrarea capacității de a formula concluzii tehnice clare, fără interpretări speculative. - Capacitatea de a redacta un raport structurat, clar și argumentat (inclusiv scop, metodologie, constatări, concluzii). - Capacitatea de a integra corect anexe și dovezi digitale în raport. - Capacitatea de a păstra confidențialitatea și de a evita accesul la informații nerelevante pentru investigație. - Cunoștințe despre cadrul instituțional relevant pentru		

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		- Investigarea jurnalelor/log-urilor de sistem: Windows Event Viewer, Linux logs, firewall logs. - Monitorizarea conexiunilor de rețea: porturi, IP-uri suspecte, sesiuni anormale. - Analiza activității utilizatorilor: conturi, permisiuni, parole, acces neautorizat. - Tehnici de detectare a activităților malițioase: malware, exfiltrare de date, escaladare de privilegii. **4. Interpretarea rezultatelor și formularea concluziilor tehnice** - Reconstrucția cronologică a unui incident. - Corelarea între acțiuni suspecte și surse. - Evitarea interpretărilor subiective – delimitarea clară între fapt și opinie. - Structura concluziilor: dovezi , analiză, constatări, recomandări. **5. Redactarea raportului de expertiză digitală** - Structura unui raport tehnic (introducere, metodologie, constatări, concluzii, anexe). - Claritate și obiectivitate pentru cititori non-tehnici (juriști, magistrați, manageri).			investigațiile digitale (autorități, atribuții).		

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		- Exemple de formulări acceptabile în raportare. - Elemente-cheie pentru admisibilitatea probelor. **6. Confidențialitate, etică și relația cu autoritățile** - Norme de etică profesională în investigarea digitală. - Obligații privind păstrarea confidențialității. - Comunicare cu instituțiile abilitate (ex: Poliție, DIICOT, CERT-RO). - Prezența ca expert în investigații sau în instanță.					
		Elaborarea procedurilor de securitate pentru gestionarea dispozitivelor mobile și a muncii la distanță. **1. Evaluarea riscurilor asociate utilizării dispozitivelor mobile și a muncii remote** - Categorii de riscuri (pierdere/dispozitiv furat, acces neautorizat, aplicații nesigure etc.) - Evaluarea nivelului de expunere în funcție de tipul de activitate, date accesate și medii de lucru. - Diferențe între riscurile echipamentelor personale vs. corporative.	Teorie: - Expunere; - Dezbatere; - Studiu de caz; - Discuții libere.	-	- Capacitatea de a evalua riscurile asociate dispozitivelor mobile și muncii la distanță, în funcție de tipul de dispozitiv, utilizator și date accesate. - Capacitatea de a defini cerințe de securitate pentru autentificare, criptare și control de acces. - Abilitatea de a selecta și justifica soluții tehnice adecvate în funcție de contextul organizațional și nivelul de risc. - Demonstrarea înțelegerii principiilor BYOD și MDM, precum și a modului de aplicare a	2	4

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		2. Politici și proceduri privind utilizarea dispozitivelor mobile - Ce înseamnă Bring Your Own Device și Mobile Device Management: avantaje, riscuri, cerințe minime de securitate. - Politici de utilizare a dispozitivelor mobile: structură, reguli, interdicții, consecințe. - Proceduri de integrare și control: înrolare dispozitive, audit periodic, separare profiluri. **3. Cerințe de criptare, autentificare și control de acces** - Criptare la nivel de disc și aplicație (BitLocker, FileVault, aplicații mobile). - Autentificare: parole puternice, MFA, biometrie, SSO. - Controlul accesului în funcție de roluri și niveluri de autorizare (RBAC, ACL). **4. Soluții tehnice pentru protecția comunicațiilor la distanță** - VPN: rol, funcționare, tipuri. - MFA – autentificare multifactor: metode și integrare. - DLP (Data Loss Prevention. - Securizarea sesiunilor remote și utilizarea aplicațiilor cloud în siguranță.			acestora în cadrul politicilor organizaționale de securitate. - Demonstrarea competenței în monitorizarea și revizuirea procedurilor de securitate, inclusiv în integrarea feedback-ului și în formularea măsurilor de corectare.		

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		5. Ghiduri de bune practici și instruirea utilizatorilor - Comportamente recomandate în mobilitate (blocare ecran, evitarea rețelelor publice, backup). Mini-ghid pentru utilizatori: reguli, exemple, situații de evitat.					
		Planifică și implementează formarea și conștientizarea utilizatorilor în securitatea informatică **1. Identificarea nevoilor de instruire și conștientizare în organizație** - Categorii de angajați și niveluri de risc (tehnici, non-tehnici, manageri). - Surse de informații pentru analiza nevoilor: incidente, audituri, feedback intern. **2. Planificarea activităților de instruire** - Tipuri de activități: sesiuni, campanii, mesaje periodice, simulări de atac. - Conturarea unui mini-plan de formare pentru un departament **3. Elaborarea conținutului educațional** - Tipuri de materiale: afișe, pliante, tutoriale, chestionare, simulări, newslettere.	Practică: - Demonstrație practică; - Exerciții aplicate; - Simulări; - Dezbateri; - Studiu de caz; - Învățare prin rezolvarea de probleme; - Discuții libere în grup; Practică: - Demonstrație practică; - Exerciții - aplicate; - Simulări; - Dezbateri; - Studiu de caz;	- Calculator și echipamente de rețea (fizice sau virtuale); - Conexiune Internet; - Software specific; - Platformă de videoconferințe și comunicare online; - Instrumente/medii de testare și simulare; - Legislație și standarde specifice domeniului; - Resurse digitale/ online; - Suport de curs; - Fișe de practică; - Videoproiector.	- Capacitatea de a identifica și structura nevoile de instruire în domeniul securității informației pentru diferite categorii de personal. - Planificarea corectă a unei activități de conștientizare, adaptată unui public-țintă și unui context organizațional specific. - Cunoștințe privind conceperea de materiale de formare eficiente, conforme cu principiile educației pentru adulți și securității informației. - Abilitatea de a evalua impactul unei sesiuni de instruire prin metode adecvate (chestionare, simulări, feedback) și de a propune ajustări pe baza rezultatelor.	1	2

Nr. crt.	DISCIPLINĂ / MODUL	CONȚINUT TEMATIC	METODE / FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	3	4	5	6	7	8
		- Principii de redactare: claritate, relevanță, accesibilitate. **4. Organizarea sesiunilor de instruire și monitorizarea participării** - Canale: online, fizic, auto-formare ghidată, LMS. - Metode de stimulare a participării (certificare internă, recunoaștere, premii simbolice). **5. Evaluarea eficienței și revizuirea campaniilor** - Chestionare, teste, feedback etc. - Ajustarea mesajelor, formatelor și frecvenței.	- Învățare prin rezolvarea de probleme; - Discuții libere în grup;	- Consumabile foi flipchart, coli A4, marker, etc.			