Standard ocupațional

MANAGER SECURITATEA INFORMAȚIEI (CHIEF INFORMATION SECURITY OFFICER -CISO)

Cod COR 133048

Inițiator/Autori:
Marius Florin Sanda
Marie – Jeanne Helene Iordache

Data elaborării:
06.11.2024-29.11.2024; 04.04.2025-03.09.2025; 18.02.-20.02.2026

Verificare profesională:
Mihai Daniel Chiroiu
Bogdan Cristian Stanache

Data verificării:
10.09.2025; 17.09.2025; 24.02-25.02.2026

Avizare:
Institutul Național de Cercetare - Dezvoltare în Informatică - ICI București

Data avizării:
03.10.2025; 03.03.2026

Validare documentație:
Asociația Națională a Comitetelor Sectoriale din România
Comitetul Sectorial Activități Financiare, Bancare, de Asigurări
Președinte ANCSR - PUIU Doru
Președinte CS AFBA- SAVU Emanuela Mihaela

Data validării sectoriale:
06.11.2025; 03.03.2026

Aprobare:
Autoritatea Națională pentru Calificări

Data aprobării:
Decizia ANC nr.84/18.03.2026

Nr. RNS – 4/ 18.03.2026

STRUCTURA STANDARDULUI OCUPAȚIONAL

SECȚIUNEA A - CERINȚELE PIEȚEI MUNCII

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

Grupa de bază COR: 1330 – Conducători în servicii de tehnologia informației și comunicațiilor
MANAGER SECURITATEA INFORMAȚIEI (CHIEF INFORMATION SECURITY OFFICER – CISO)
COD COR 133048

2. Denumirea tradusă a ocupației (En):

INFORMATION SECURITY MANAGER (CHIEF INFORMATION SECURITY OFFICER – CISO)

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

Conducătorii din serviciile de tehnologia informației și comunicațiilor planifică, conduc și coordonează activitatea de achiziții, de dezvolltare, de întreținere și utilizare a calculatorului si a sistemelor de comunicații.

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

a) consultarea cu utilizatorii, conducerea, furnizorii și tehnicienii pentru a evalua nevoile de calcul și cerințele sistemelor, precum și specificarea tehnologiei necesare pentru satisfacerea acestor nevoi;

b) formularea și coordonarea strategiilor, politicilor și planurilor privind tehnologia informației și comunicațiilor (TIC);

c) coordonarea selecției și instalării resurselor TIC și organizarea instruirii utilizatorilor;

d) conducerea operațiunilor TIC, analizarea fluxurilor de lucru, stabilirea priorităților, dezvoltarea standardelor și definirea termenelor-limită;

e) supravegherea securității sistemelor TIC;

f) repartizarea, revizuirea, gestionarea și coordonarea activității analiștilor de sisteme, programatorilor și a altor specialiști din domeniul informatic;

g) evaluarea utilizării tehnologiei în cadrul organizației și a nevoilor aferente, precum și formularea de recomandări pentru îmbunătățiri, cum ar fi actualizări de hardware și software;

h) stabilirea și gestionarea bugetelor, controlul cheltuielilor și asigurarea utilizării eficiente a resurselor;

i) stabilirea și coordonarea procedurilor operaționale și administrative;

j) supravegherea procesului de selecție, formare și evaluare a performanței personalului;

k) reprezentarea întreprinderii sau organizației la convenții, seminare și conferințe din domeniul TIC.

4. Activități/sarcini specifice ale ocupației

1. Utilizează instrumente digitale pentru analiza și interpretarea datelor, în scopul comunicării, colaborării și deciziilor:

- Selectează și folosește instrumente digitale pentru comunicare și colaborare în echipă.
- Colectează și centralizează date din surse multiple.
- Aplică formule și indicatori simpli pentru analiza datelor.
- Creează vizualizări de date și tablouri de bord pentru monitorizarea progresului.
- Interpretează rapoarte și fundamentează decizii pe baza datelor obținute.

2. Promovează practici sustenabile și eficiente energetic în activitățile IT&C:

- Identifică și sprijină decizii tehnologice care reduc amprenta de carbon.
- Participă la selecția echipamentelor și infrastructurii cu consum redus de energie.
- Coordonează dezvoltarea politicilor sustenabile pentru IT&C.
- Supraveghează implementarea politicilor sustenabile pentru IT&C.

3. Coordonează activitățile echipelor, respectă legislația muncii și asigură gestionarea conflictelor în organizație:

- Planifică, organizează și monitorizează activitățile echipei.
- Coordonează activitatea echipelor în medii fizice, hibride și virtuale.
- Utilizează platforme digitale pentru colaborare și gestionarea documentelor de lucru.
- Deleagă sarcini pe baza competențelor, experienței și obiectivelor echipei.
- Comunică strategic în organizație și adaptează mesajele în funcție de audiență.
- Participă la ședințe și forumuri de decizie.
- Aplică regulamente interne, proceduri organizaționale și prevederi ale legislației muncii.
- Asigură respectarea normelor de securitate și sănătate în muncă.
- Gestionează conflictele în echipă prin tehnici constructive de soluționare.

4. Evaluează infrastructura IT&C și asigură conformitatea cu standardele și calitatea sistemelor:

- Identifică principalele componente hardware, software și de rețea ale infrastructurii IT&C.
- Analizează arhitectura infrastructurii și modul de integrare cu procesele și utilizatorii organizației.
- Evaluează compatibilitatea infrastructurii IT&C cu soluțiile și tehnologiile existente și cu cele propuse.
- Aplică standarde și bune practici relevante pentru evaluarea și monitorizarea infrastructurii.
- Utilizează indicatori și instrumente de monitorizare pentru aprecierea performanței, conformității, disponibilității și a calității sistemelor și infrastructurii IT&C.
- Analizează rapoartele de monitorizare și identifică neconformități față de standarde sau parametrii de referință.
- Documentează evaluările efectuate și formulează recomandări pentru decizii manageriale.
- Colaborează cu echipele tehnice pentru implementarea măsurilor de corecție și îmbunătățire.

5. Gestionează achizițiile, bugetele și resursele umane IT&C, coordonând relațiile cu furnizorii și partenerii:

- Planifică achizițiile și bugetele IT&C pe baza obiectivelor și resurselor disponibile.
- Coordonează definirea specificațiilor tehnice și a cerințelor funcționale pentru bunuri și servicii IT&C.
- Selectează și evaluează furnizorii și partenerii pe baza criteriilor stabilite.
- Negociază și administrează contractele IT&C și acordurile privind nivelul serviciilor.
- Monitorizează execuția bugetară, analizează abaterile și dispune ajustările necesare.
- Evaluează investițiile IT&C prin analize cost–beneficiu și indicatori de eficiență.
- Planifică, coordonează și dezvoltă resursele umane IT&C, inclusiv recrutarea și evaluarea performanței.

- Coordonează și menține relații de colaborare eficientă cu furnizorii, partenerii și alte departamente implicate.

6. Monitorizează și evaluează performanța sistemelor, a proceselor și a serviciilor IT&C cu asigurarea respectării cadrului legal aplicabil IT&C:

- Identifică procesele, sistemele și serviciile IT&C care fac obiectul monitorizării și evaluării.
- Stabilește indicatori de performanță și criterii de evaluare, aliniate la obiectivele organizației.
- Utilizează soluții și platforme pentru monitorizarea performanței și conformității sistemelor IT&C.
- Colectează și analizează date relevante pentru evaluarea performanței (loguri, alerte, rapoarte).
- Verifică conformitatea sistemelor, proceselor și serviciilor IT&C cu legislația și reglementările aplicabile.
- Evaluează impactul incidentelor asupra performanței și conformității sistemelor IT&C.
- Elaborează rapoarte de performanță și documente de conformitate, incluzând constatări, concluzii și măsuri corective.
- Propune și sprijină implementarea măsurilor de optimizare a performanței și respectării cadrului legal.

7. Evaluează nevoile IT&C ale organizației și coordonează guvernanța și strategiile de digitalizare și dezvoltare tehnologică:

- Analizează cerințele și identifică nevoile organizației în domeniu.
- Integrează standarde și cadre de guvernanță în evaluarea și planificarea IT&C.
- Coordonează procesele de audit managerial IT&C și alte instrumente de guvernanță, utilizând rezultatele pentru ajustarea strategiei și îmbunătățirea proceselor.
- Integrează obiectivele de digitalizare și dezvoltare tehnologică în strategia generală a organizației.
- Elaborează propuneri și strategii IT&C privind digitalizarea și dezvoltarea tehnologică, incluzând obiective, direcții de acțiune, resurse și indicatori.
- Monitorizează implementarea strategiei IT&C și a mecanismelor de guvernanță prin indicatori de performanță.
- Identifică neconformitățile și dispune măsuri corective și preventive în cadrul guvernanței IT&C.
- Asigură gestionarea documentației și a rapoartelor manageriale aferente proiectelor IT&C ca parte a mecanismelor de guvernanță organizațională.

8. Definește, implementează și actualizează politicile de securitate a informației, monitorizând informațiile și gestionând incidentele:

- Identifică domeniile organizaționale care necesită politici de securitate a informațiilor.
- Elaborează și validează politici și proceduri de securitate adaptate riscurilor și cadrului legal.
- Coordonează procesul de aprobare, publicare și implementare a politicilor de securitate.
- Supraveghează fluxurile și accesul la informații pentru identificarea abaterilor și riscurilor.
- Coordonează gestionarea incidentelor de securitate a informațiilor prin măsuri de limitare, raportare și prevenire.
- Revizuiește și actualizează periodic politicile de securitate a informațiilor pe baza auditurilor și incidentelor.

9. Coordonează implementarea politicilor de control al accesului, autentificare și gestionare a identității:

- Coordonează stabilirea și aplicarea politicilor de control al accesului și drepturilor utilizatorilor.
- Coordonează integrarea și utilizarea soluțiilor de management al identității (IAM).
- Stabilește metode și niveluri de autentificare adecvate riscurilor identificate.
- Monitorizează și documentează accesul la resursele organizației.
- Gestionează ciclul de viață al identităților digitale și al drepturilor de acces.
- Verifică periodic trasabilitatea și corectitudinea drepturilor acordate.

- Organizează sesiuni de instruire și conștientizare privind politicile de acces și autentificare.

10. Evaluează riscurile de securitate informatică și stabilește măsuri de protecție:

- Analizează contextul organizațional și stabilește domeniul de aplicare al analizei de risc în securitatea informatică.
- Identifică și corelează activele informatice cu procesele critice din organizație.
- Identifică vulnerabilitățile și amenințările asociate activelor informatice.
- Evaluează probabilitatea și impactul riscurilor utilizând metode cantitative, calitative sau mixte.
- Prioritizează riscurile în funcție de scorul rezultat și de nivelul de toleranță al organizației.
- Propune măsuri de protecție tehnice și organizaționale adecvate pentru reducerea riscurilor.
- Elaborează analiza de risc și planul de atenuare și control al riscurilor.
- Monitorizează implementarea măsurilor și actualizează periodic analiza de risc.
- Asigură documentarea și arhivarea analizei de risc și a măsurilor de protecție.

11. Coordonează securitatea informatică pentru infrastructura critică, echipamentele mobile și munca la distanță:

- Identifică riscurile asociate mobilității și muncii la distanță.
- Elaborează și coordonează implementarea politicilor privind utilizarea și securizarea dispozitivelor mobile.
- Stabilește și monitorizează măsuri de acces securizat la distanță, incluzând criptarea și controalele de acces.
- Coordonează gestionarea ciclului de viață al dispozitivelor mobile și monitorizarea activităților asociate.
- Supraveghează aplicarea politicilor și măsurilor de securitate pentru activitățile desfășurate la distanță.
- Integrează cerințele de securitate fizică în protecția infrastructurii digitale critice.
- Definește reguli și proceduri pentru accesul fizic în zonele sensibile.
- Coordonează răspunsul la incidente fizice cu impact asupra securității IT.
- Organizează auditul măsurilor de securitate fizică și colaborează cu alte departamente pentru îmbunătățiri.

12. Elaborează și testează planuri de continuitate și de recuperare în caz de dezastru și colaborează cu autoritățile competente:

- Evaluează impactul potențial al incidentelor majore asupra proceselor critice și resurselor organizației.
- Elaborează planuri de continuitate a activității și planuri de recuperare în caz de dezastru, adaptate tipurilor de riscuri identificate.
- Integrează cerințele legale și standardele aplicabile în planurile de continuitate și recuperare.
- Testează planurile prin simulări și exerciții practice, documentând rezultatele și lecțiile învățate.
- Colaborează cu autoritățile relevante în domeniul securității informației și respectă procedurile oficiale de raportare.
- Asigură documentația și evidențele necesare pentru audituri, controale și evaluări externe.
- Actualizează periodic planurile pe baza rezultatelor testelor, a modificărilor organizaționale și a feedbackului din partea autorităților.

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 instrumente digitale pentru analiza și interpretarea datelor, în scopul comunicării, colaborării și deciziilor.

C 1.2

2. Promovează practici sustenabile și eficiente energetic în activitățile IT&C.

C2.1

3. Coordonează activitățile echipelor, respectă legislația muncii și asigură gestionarea conflictelor în organizație.

C 3.1

4. Evaluează infrastructura IT&C și asigură conformitatea cu standardele și calitatea sistemelor.
5. Gestionează achizițiile, bugetele și resursele umane IT&C, coordonând relațiile cu furnizorii și partenerii.

C3.2

6. Monitorizează și evaluează performanța sistemelor, a proceselor și a serviciilor IT&C cu asigurarea respectării cadrului legal aplicabil IT&C.
7. Evaluează nevoile IT&C ale organizației și coordonează guvernanța și strategiile de digitalizare și dezvoltare tehnologică.

C3.3

8. Definește, implementează și actualizează politicile de securitate a informației, monitorizând informațiile și gestionând incidentele.
9. Coordonează implementarea politicilor de control al accesului, autentificare și gestionare a identității.

C 3.4

10. Evaluează riscurile de securitate informatică și stabilește măsuri de protecție.
11. Coordonează securitatea informatică pentru infrastructura critică, echipamentele mobile și munca la distanță.
12. Elaborează și testează planuri de continuitate și de recuperare în caz de dezastru și colaborează cu autoritățile competente.

[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.

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

Ocupațiile avute în vedere în stabilirea accesului la ocupații de același nivel de calificare conform CNC, pe bază de experiență/recunoaștere de competențe din grupele C1 – C3.2. sunt:

Ocupația	**Cod COR**
Manager tehnologia informațiilor și comunicațiilor	133007

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

Pentru accesul la instruire se recomandă ca participanții la curs să aibă o experiență profesională relevantă de minimum un an în domeniul IT/digital sau în funcții ori domenii de activitate care implică utilizarea, administrarea ori gestionarea sistemelor informatice și a informațiilor în format electronic

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)

2.3. 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:
- Servere, unități de stocare dedicate;
- Echipamente de rețea (fizice sau virtuale);
- Firewall-uri;
- Sisteme de prevenire/detectare a intruziunilor;
- Token de autentificare multifactor;
- Sisteme de acces biometric;
- Conexiune Internet;
- Platforme/instrumente software de testare/simulare a vulnerabilităților/penetrare;
- Platformă de management riscuri;
- Soluții de criptare;
- Dashboard-uri de raportare;
- Platformă de videoconferință, comunicare și colaborare online;
- Legislație, protocoale, standarde specifice;
- Resurse digitale online;
- Fișe de practică;
- Suport de curs;
- Videoproiector;
- Ecran de proiecție/monitor;
- Coli flipchart, coli A4, markere, etc.

Pentru pregătirea practică sunt necesare următoarele resurse:
- Servere, unități de stocare dedicate;
- Echipamente de rețea (fizice sau virtuale);
- Firewall-uri;
- Sisteme de prevenire/detectare a intruziunilor;
- Token de autentificare multifactor;
- Sisteme de acces biometric;
- Conexiune Internet;
- Platforme/instrumente software de testare/simulare a vulnerabilităților/penetrare;
- Platformă de management riscuri;
- Soluții de criptare;
- Dashboard-uri de raportare;
- Platformă de videoconferință, comunicare și colaborare online;
- Legislație, protocoale, standarde specifice;
- Resurse digitale online;
- Fișe de practică;
- Suport de curs;
- Videoproiector;
- Ecran de proiecție/monitor;
- Coli flipchart, coli A4, markere, 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 ”MANAGER SECURITATEA INFORMAȚIEI (CHIEF INFORMATION SECURITY OFFICER – CISO)” 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 1 an;
- 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:

Inițiator/Autori:

MARIUS FLORIN SANDA – *specialist în domeniu*

IORDACHE MARIE – JEANNE HELENE – *specialist în domeniu*

Instituția/instituțiile/persoanele interesate:

S.C. INTERLOG COM SRL
SIMONA MARIA COJOCĂRESCU - *Administrator*

S.C. EUROTRAINING SOLUTION SRL

IORDACHE MARIE – JEANNE HELENE – *Administrator*

S.C. BUSINESS GENERATOR SRL

CRISTIAN ELENA – *Director general*

Data elaborării: 06.11.2024-29.11.2024;04.04.2025-03.09.2025; 18.02.-20.02.2026

1.2. Verificare :
MIHAI DANIEL CHIROIU- *specialist în domeniu*
BOGDAN CRISTIAN STANACHE - *specialist în domeniu*
Data verificării: 10.09.2025; 17.09.2025; 24.02-25.02.2026

1.3. Avizare:
INSTITUTUL NAȚIONAL DE CERCETARE-DEZVOLTARE ÎN INFORMATICĂ – ICI BUCUREȘTI
Data avizării: 03.10.2025; 03.03.2026

1..4. Validare documentație:
Comitet sectorial/semnatari:
ANCSR-Presedinte PUIU Doru; CS AFBA-Presedinte SAVU Emanuela Mihaela
Data validării:06.11.2025; 03.03.2026

1.5. Aprobare:
Autoritatea Națională pentru Calificări conform deciziei nr.84 din data 18.03.2026

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 instrumente digitale pentru analiza și interpretarea datelor, în scopul comunicării, colaborării și deciziilor.	Fundamente digitale, sustenabilitate și coordonare organizațională	5	10	3
2.	Promovează practici sustenabile și eficiente energetic în activitățile IT&C.		5	10	
3.	Coordonează activitățile echipelor, respectă legislația muncii și asigură gestionarea conflictelor în organizație.		5	10	
4.	Evaluează infrastructura IT&C și asigură conformitatea cu standardele și calitatea sistemelor.	Managementul infrastructurii și resurselor IT&C	5	10	2
5.	Gestionează achizițiile, bugetele și resursele umane IT&C, coordonând relațiile cu furnizorii și partenerii.		5	10	
6.	Monitorizează și evaluează performanța sistemelor, a proceselor și a serviciilor IT&C cu asigurarea respectării cadrului legal aplicabil IT&C.	Performanță, conformitate și strategie în IT&C	5	10	2
7.	Evaluează nevoile IT&C ale organizației și coordonează guvernanța și strategiile de digitalizare și dezvoltare tehnologică.		5	10	
8.	Definește, implementează și actualizează politicile de securitate a informației, monitorizând informațiile și gestionând incidentele.	Politici și controlul accesului în securitatea informației	5	10	2
9.	Coordonează implementarea politicilor de control al accesului, autentificare și gestionare a identității		5	10	
10.	Evaluează riscurile de securitate informatică și stabilește măsuri de protecție.	Riscuri, infrastructuri critice și continuitate în securitatea informației	5	10	3
11.	Coordonează securitatea informatică pentru infrastructura critică, echipamentele mobile și munca la distanță.		5	10	
12.	Elaborează și testează planuri de continuitate și de recuperare în caz de dezastru și colaborează cu autoritățile competente.		5	10	
	TOTAL NR ORE		**60**	**120**	**12**
	TOTAL NR. CREDITE				

Anexa nr. 2 la standardul ocupațional

PROGRAMA DE PREGĂTIRE TEORETICĂ ȘI PRACTICĂ

Nr. crt.	DICIPLINĂ/ MODUL	CONȚINUT TEMATIC	METODE/ FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	4	5	6	7	8	9
1	**Fundamente digitale, sustenabilitate și coordonare organizațională**	**Utilizarea instrumentelor digitale pentru analiza și interpretarea datelor, în scopul comunicării, colaborării și deciziilor:** *1. Colaborare digitală și management de sarcini* – Selectarea și utilizarea aplicațiilor profesionale pentru gestionarea proiectelor și echipelor, cu suport pentru colaborare în timp real. – Planificarea și urmărirea digitală a sarcinilor: creare, alocare responsabilități, stabilire termene, monitorizare progres. – Organizarea activității în echipe distribuite geografic; reguli de comunicare digitală și bune practici pentru menținerea coeziunii și productivității. *2. Colectarea și centralizarea datelor* – Identificarea și structurarea datelor relevante pentru luarea deciziilor. – Utilizarea instrumentelor care permit centralizarea datelor din surse multiple și actualizarea lor în timp real. *3. Calculul indicatorilor de performanță folosind aplicații informatice și analiza datelor* – Aplicarea formulelor uzuale (sume, medii, variații procentuale, ponderări). – Calculul și interpretarea indicatorilor descriptivi: medie, mediană, mod, dispersie.	*Teorie*: - Expunere; - Prezentare statică și interactivă; - Dezbaterea dirijată; - Studiu de caz; -Demonstrație practică; - Discuții libere; *Practică*: - Studiu de caz aplicativ; - Exerciții aplicate; - Simulare; - Dezbateri; - Discuții libere în grup	- Servere, unități de stocare dedicate; - Echipamente de rețea (fizice sau virtuale); - Firewall-uri; - Sisteme de prevenire/detectare a intruziunilor; - Token de autentificare multifactor; - Sisteme de acces biometric; - Conexiune Internet; - Platforme/instrumente software de testare/simulare a vulnerabilităților/penetrare; - Platformă de management riscuri; - Soluții de criptare; - Dashboard-uri de raportare; - Platformă de videoconferință, comunicare și colaborare online;	– Demonstrarea cunoașterii aplicațiilor digitale utilizate pentru colaborare și gestionarea proiectelor/echipelor. – Abilitatea de a colecta, centraliza și structura corect datele relevante din surse digitale multiple. – Abilitatea de a aplica formule și de a calcula cu acuratețe indicatori statistici simpli. – Capacitatea de a selecta și utiliza indicatori relevanți pentru evaluarea performanței unui proces sau proiect. – Abilitatea de a crea rapoarte vizuale și tablouri de bord clare, relevante și ușor de interpretat. – Capacitatea de a interpreta corect rapoarte digitale de activitate, identificând puncte critice și oportunități de îmbunătățire. – Justificarea corectă a deciziilor operaționale sau investiționale pe baza datelor analizate, prin compararea alternativelor.	**5**	**10**

Nr. crt.	DICIPLINĂ/ MODUL	CONȚINUT TEMATIC	METODE/ FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	4	5	6	7	8	9
		– Definirea și utilizarea indicatorilor de performanță relevanți (KPI). *4. Vizualizarea datelor și realizarea unui tablou de bord* – Crearea tabelelor pivot, a graficelor relevante și a rapoartelor vizuale. – Construirea unui tablou de bord pentru monitorizarea progresului și a indicatorilor. *5. Interpretarea rapoartelor pentru fundamentarea deciziilor* – Citirea și înțelegerea rapoartelor de digitale de activitate. – Fundamentarea deciziilor operaționale și a investițiilor tehnologice pe baza datelor.		- Legislație, protocoale, standarde specifice; - Resurse digitale online; - Fișe de practică; - Suport de curs; - Videoproiector; - Ecran de proiecție/monitor; - Coli flipchart, coli A4, markere, etc.			
		Practici sustenabile și eficiente energetic în activitățile IT&C: *1. Introducere în sustenabilitatea digitală* – Definirea sustenabilității în contextul IT&C (reducere consum energetic, gestionare deșeuri electronice, tehnologii cloud și virtualizare, achiziții verzi, munca remote). – Principii ESG (mediu, social, guvernanță) aplicabile în domeniul IT&C. – Reglementări și directive relevante. – Fundamentarea deciziilor tehnologice prin aplicarea principiilor ESG și respectarea reglementărilor relevante. *2. Impactul mediului digital asupra amprentei de carbon și a consumului de resurse* – Amprenta de carbon a activităților IT&C (hardware, software, cloud).	*Teorie*: - Expunere; - Prezentare statică și interactivă; - Dezbaterea dirijată; - Studiu de caz; -Demonstrație practică; - Discuții libere; *Practică*: - Studiu de caz aplicativ; - Exerciții aplicate; - Simulare;	- Servere, unități de stocare dedicate; - Echipamente de rețea (fizice sau virtuale); - Firewall-uri; - Sisteme de prevenire/detectare a intruziunilor; - Token de autentificare multifactor; - Sisteme de acces biometric; - Conexiune Internet; - Platforme/instrumente software de testare/simulare a	– Demonstrarea înțelegerii conceptului de sustenabilitate aplicat în domeniul IT&C. – Capacitatea de a identifica soluții tehnologice eficiente energetic și cu impact redus asupra mediului. – Abilitatea de a selecta echipamente în funcție de criterii de eficiență și certificări ecologice. – Manifestarea interesului pentru integrarea principiilor verzi în politicile IT ale organizației. – Capacitatea de a justifica decizii de investiții în tehnologii sustenabile.	**5**	**10**

Nr. crt.	DICIPLINĂ/ MODUL	CONȚINUT TEMATIC	METODE/ FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	4	5	6	7	8	9
		– Impactul ciclului de viață al echipamentelor: producție, utilizare, eliminare – Reciclare și recuperare în IT&C. *3. Tehnologii și soluții pentru eficiență energetică în IT* – Criterii pentru selecția echipamentelor cu consum redus de energie. – Utilizarea infrastructurilor cloud eficiente energetic. – Optimizarea software-ului pentru reducerea resurselor utilizate. *4. Politici și bune practici pentru un IT&C sustenabil în organizații* – Achizițiile verzi in domeniul IT&C. – Crearea și aplicarea politicilor sustenabile privind IT&C pentru asigurarea tranziției verzi. – Promovarea comportamentelor ecologice în utilizarea tehnologiei digitală (power saving, imprimare responsabilă, reutilizare etc.).	- Dezbateri; - Discuții libere în grup	vulnerabilităților/penetrare; - Platformă de management riscuri; - Soluții de criptare; - Dashboard-uri de raportare; - Platformă de videoconferință, comunicare și colaborare online; - Legislație, protocoale, standarde specifice; - Resurse digitale online; - Fișe de practică; - Suport de curs; - Videoproiector; - Ecran de proiecție/monitor; - Coli flipchart, coli A4, markere, etc.	– Capacitatea de a propune măsuri concrete pentru reducerea amprentei digitale. – Cunoașterea reglementărilor europene și naționale privind responsabilitatea ecologică în domeniul IT – Capacitatea de a colabora pentru a defini și aplica politici interne privind sustenabilitatea în domeniul IT&C.		
		Coordonarea activității echipelor, respectarea legislației muncii și gestionarea conflictelor în organizație: *1. Planificarea, organizarea și monitorizarea activităților echipei* – Definirea obiectivelor și a rezultatelor așteptate. – Distribuirea sarcinilor pe roluri și responsabilități. – Stabilirea priorităților și a termenelor realiste.	*Teorie*: - Expunere; - Prezentare statică și interactivă; - Dezbaterea dirijată; - Studiu de caz; -Demonstrație practică; - Discuții libere;	- Servere, unități de stocare dedicate; - Echipamente de rețea (fizice sau virtuale); - Firewall-uri; - Sisteme de prevenire/detectare a intruziunilor; - Token de autentificare multifactor;	– Demonstrarea cunoașterii metodelor de planificare și organizare a activităților în echipă. – Capacitatea de a stabili obiective, termene și resurse adecvate pentru proiecte și activități. – Capacitatea de a aplica metode de prioritizare și de	**5**	**10**

Nr. crt.	DICIPLINĂ/ MODUL	CONȚINUT TEMATIC	METODE/ FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	4	5	6	7	8	9
		– Adaptarea planificării la contexte imprevizibile (ex. schimbări de resurse, urgențe). – Monitorizarea progresului: urmărirea rezultatelor, feedback, ajustări. *2. Coordonarea echipelor și utilizarea platformelor digitale* – Coordonarea echipelor în medii fizice, hibride și virtuale. – Stiluri de leadership adaptate contextului de lucru distribuit. – Provocări legate de comunicarea asincronă, lipsa contactului direct, adaptabilitatea echipelor. – Gestionarea colaborativă a documentelor și a fluxurilor de lucru digitale. *3. Delegarea sarcinilor* – Criterii pentru delegare: competențe, experiență, interese profesionale. – Obiectivele delegării: eficientizare, optimizare, creșterea responsabilității. *4. Regulamente interne, legislația muncii și securitatea și sănătatea în muncă* – Politici și proceduri interne aplicabile în organizație. – Regulamente de ordine interioară și coduri de conduită profesională. – Drepturile și obligațiile angajaților în munca de echipă.	*Practică*: - Studiu de caz aplicativ; - Exerciții aplicate; - Simulare; - Dezbateri; - Discuții libere în grup	- Sisteme de acces biometric; - Conexiune Internet; - Platforme/instrumente software de testare/simulare a vulnerabilităților/penetrare; - Platformă de management riscuri; - Soluții de criptare; - Dashboard-uri de raportare; - Platformă de videoconferință, comunicare și colaborare online; - Legislație, protocoale, standarde specifice; - Resurse digitale online; - Fișe de practică; - Suport de curs; - Videoproiector; - Ecran de proiecție/monitor; - Coli flipchart, coli A4, markere, etc.	adaptare a planificării la schimbări și situații neprevăzute. – Abilitatea de a monitoriza progresul echipei utilizând indicatori și tehnici adecvate de urmărire și ajustare. – Capacitatea de a coordona echipe în medii fizice, hibride și virtuale, utilizând stiluri de leadership adecvate. – Abilitatea de a utiliza platforme digitale pentru colaborare, gestionarea sarcinilor și documentelor de lucru. – Capacitatea de a delega sarcini în funcție de competențe, experiență și obiectivele echipei. – Demonstrarea cunoașterii și aplicării regulamentelor interne și a prevederilor legislației muncii relevante. – Abilitatea de a identifica riscurile specifice muncii în domeniul IT&C și de a aplica măsuri de securitate și sănătate în muncă adecvate. – Capacitatea de a comunica strategic în organizație și de a adapta mesajele la diferite categorii de public.		

Nr. crt.	DICIPLINĂ/ MODUL	CONȚINUT TEMATIC	METODE/ FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	4	5	6	7	8	9
		– Noțiuni esențiale din Codul muncii: timp de muncă și repaus, munca la distanță, ore suplimentare. – Identificarea riscurilor specifice muncii la birou și telemuncii. – Măsuri de protecție fizică și digitală în mediul profesional. – Instruirea și informarea angajaților privind securitatea și sănătatea în muncă. *5. Comunicarea strategică și gestionarea conflictelor* – Diferențele dintre comunicarea operațională, tactică și strategică; obiectivele comunicării în decizie. – Analiza audienței și adaptarea mesajelor (top management vs. echipe operaționale). – Redactarea documentelor argumentate: structură, analiză, opțiuni, recomandări. – Pregătirea și exprimarea punctelor de vedere în ședințe și forumuri de decizie. – Utilizarea canalelor și formelor de comunicare (formale, informale, digitale). – Simplificarea limbajului tehnic pentru public non-tehnic. – Tehnici constructive de abordare a conflictelor.			– Abilitatea de a redacta documente argumentate pentru susținerea deciziilor organizaționale. – Capacitatea de a participa activ și constructiv la ședințe și forumuri de decizie. – Abilitatea de a utiliza canale și forme de comunicare adecvate. – Capacitatea de a simplifica limbajul tehnic pentru a-l face inteligibil persoanelor non-tehnice. – Abilitatea de a gestiona conflicte în echipă prin aplicarea tehnicilor constructive de soluționare.		
2	**Managementul infrastructurii și resurselor IT&C**	**Evaluarea infrastructurii IT&C și asigurarea conformității cu standardele și calitatea sistemelor:** *1. Arhitectura generală a infrastructurii IT&C*	*Teorie*: - Expunere; - Prezentare statică și interactivă;	- Servere, unități de stocare dedicate; - Echipamente de rețea (fizice sau virtuale); - Firewall-uri;	– Demonstrarea cunoașterii componentelor hardware, software și de rețea dintr-o infrastructură IT&C.	**5**	**10**

Nr. crt.	DICIPLINĂ/ MODUL	CONȚINUT TEMATIC	METODE/ FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	4	5	6	7	8	9
		– Definirea infrastructurii IT&C. – Componentele esențiale: stații de lucru, servere, dispozitive de stocare, sisteme de operare, aplicații. – Tipuri de arhitectură (centralizată, distribuită, cloud etc.). *2. Rețele de comunicații în organizații* – Clasificarea tipurilor de rețele (LAN, WAN, VPN), explicarea topologiilor și a protocoalelor de comunicații esențiale pentru conectivitate și funcționare eficientă. *3. Compatibilitatea infrastructurii cu soluțiile IT&C existente și cu cele propuse* – Identificarea limitărilor hardware și software (resurse, incompatibilități). – Evaluarea gradului de interoperabilitate între sisteme existente și tehnologii noi. – Factorii care influențează scalabilitatea și reziliența infrastructurii. *4. Colaborarea cu echipele tehnice* – Terminologie de bază pentru comunicarea eficientă între roluri tehnice și non-tehnice. – Traducerea cerințelor de business în specificații tehnice (și invers). *5. Standardele și bunele practici pentru monitorizarea calității* – Introducerea în conceptul de calitate IT&C: diferențierea între calitatea infrastructurii, a serviciilor și a proceselor IT. – Prezentarea principalelor standarde internaționale relevante, de exemplu: ISO	- Dezbaterea dirijată; - Studiu de caz; -Demonstrație practică; - Discuții libere; *Practică*: - Studiu de caz aplicativ; - Exerciții aplicate; - Simulare; - Dezbateri; - Discuții libere în grup	- Sisteme de prevenire/detectare a intruziunilor; - Token de autentificare multifactor; - Sisteme de acces biometric; - Conexiune Internet; - Platforme/instrumente software de testare/simulare a vulnerabilităților/penetrare; - Platformă de management riscuri; - Soluții de criptare; - Dashboard-uri de raportare; - Platformă de videoconferință, comunicare și colaborare online; - Legislație, protocoale, standarde specifice; - Resurse digitale online; - Fișe de practică; - Suport de curs; - Videoproiector;	– Capacitatea de a analiza arhitectura infrastructurii și interacțiunea dintre sisteme și utilizatori. – Demonstrarea cunoașterii tipurilor de rețele și topologiilor implementate în organizație. – Capacitatea de a verifica compatibilitatea infrastructurii existente cu noile soluții IT&C propuse. – Identificarea limitărilor tehnice, problemelor de interoperabilitate și a factorilor care influențează scalabilitatea și reziliența. – Capacitatea de a evalua rețelele din punct de vedere al performanței și securității. – Cunoașterea terminologiei tehnice de bază din domeniul IT&C: – Demonstrarea cunoașterii standardelor importante din domeniu și a bunelor practici aplicabile monitorizării calității sistemelor IT&C. – Abilitatea de a utiliza indicatori de performanță, disponibilitate și securitate în evaluarea sistemelor.		

Nr. crt.	DICIPLINĂ/ MODUL	CONȚINUT TEMATIC	METODE/ FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	4	5	6	7	8	9
		9001:2015 (managementul calității în organizații, aplicabil și în IT), ISO/IEC 25010:2023 (caracteristicile de calitate pentru produsele și sistemele software), ITIL – Information Technology Infrastructure Library (bune practici pentru managementul serviciilor IT). – Indicatori utilizați în evaluarea calității (disponibilitate, timpi de răspuns, rate de eroare, reziliență etc.). – Metodologii de audit și evaluare a calității infrastructurii IT&C. *6. Instrumente și metode de monitorizare* – Exemple de soluții software și hardware de monitorizare a performanței. – Exemple de folosire a rezultatelor obținute prin monitorizare în procesul decizional. *7. Raportarea și îmbunătățirea continuă* – Structura unui raport de evaluare a infrastructurii și a calității sistemelor. – Identificarea ariilor ce necesită îmbunătățiri și formularea de recomandări manageriale, în colaborare cu echipele tehnice. – Colaborarea cu echipele tehnice pentru implementarea soluțiilor.		- Ecran de proiecție/monitor; - Coli flipchart, coli A4, markere, etc.	– Capacitatea de a aplica metodologii de audit și evaluare a calității infrastructurii. – Abilitatea de a utiliza instrumente software și hardware de monitorizare a performanței și securității. – Capacitatea de a interpreta datele colectate din sistemele de monitorizare și de a detecta abateri față de parametrii de referință. – Abilitatea de a elabora rapoarte de evaluare a infrastructurii și de a identifica ariile ce necesită îmbunătățire. – Capacitatea de a colabora cu echipele tehnice pentru implementarea măsurilor corective și preventive.		
		Gestionarea achizițiilor, bugetelor și resurselor umane IT&C, coordonarea relațiilor cu furnizorii și partenerii: *1. Planificarea achizițiilor și bugetelor IT&C* – Etapele procesului de achiziție: planificare, selecție, contractare, monitorizare.	*Teorie*: - Expunere; - Prezentare statică și interactivă;	- Servere, unități de stocare dedicate; - Echipamente de rețea (fizice sau virtuale); - Firewall-uri;	– Demonstrarea cunoașterii etapelor procesului de achiziție IT&C și a tipurilor de achiziții aplicabile. – Capacitatea de a elabora specificații tehnice și funcționale	**5**	**10**

Nr. crt.	DICIPLINĂ/ MODUL	CONȚINUT TEMATIC	METODE/ FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	4	5	6	7	8	9
		– Tipuri de achiziții: echipamente hardware, licențe software, servicii cloud, consultanță. – Tipuri de bugete: operațional, investițional, pe proiecte (alocate pentru inițiative specifice). – Categorii de cheltuieli IT&C și tehnici de estimare bugetară (categorii pe bază de istoric, obiective, tehnici top-down / bottom-up). *2. Selecția și managementul furnizorilor și partenerilor IT&C* – Stabilirea criteriilor de selecție a furnizorilo: competență tehnică, sustenabilitate, reputație, conformitate legală. – Analiza ofertelor și evaluarea tehnico-financiară (grile de scor, comparații). – Negocierea și administrarea contractelor IT&C și a acordurilor SLA (Service Level Agreement). – Monitorizarea și evaluarea performanței furnizorilor: respectarea livrabilelor, timpi de răspuns, calitatea suportului. – Mecanisme de colaborare eficientă și de comunicare continuă cu furnizorii și partenerii strategici. *3. Integrarea cerințelor de securitate și sustenabilitate în achiziții* – Cerințe minime de securitate informatică care se impun prin documentația de achiziție. – Principii de achiziție verde: eficiență energetică, reducerea impactului asupra mediului.	- Dezbaterea dirijată; - Studiu de caz; -Demonstrație practică; - Discuții libere; *Practică*: - Studiu de caz aplicativ; - Exerciții aplicate; - Simulare; - Dezbateri; - Discuții libere în grup	- Sisteme de prevenire/detectare a intruziunilor; - Token de autentificare multifactor; - Sisteme de acces biometric; - Conexiune Internet; - Platforme/instrumente software de testare/simulare a vulnerabilităților/penetrare; - Platformă de management riscuri; - Soluții de criptare; - Dashboard-uri de raportare; - Platformă de videoconferință, comunicare și colaborare online; - Legislație, protocoale, standarde specifice; - Resurse digitale online; - Fișe de practică; - Suport de curs; - Videoproiector; - Ecran de proiecție/monitor; - Coli flipchart, coli A4, markere, etc.	clare, aliniate la obiectivele organizației și la standardele în vigoare. – Capacitatea de a selecta și evalua furnizorii și partenerii în funcție de criterii tehnice, economice, legale și de sustenabilitate. – Abilitatea de a negocia și gestiona contracte IT&C, asigurând respectarea termenilor și condițiilor. – Enumerarea corectă a cerințelor privind achizițiile verzi și a celor care se referă la securitatea informatică. – Capacitatea de a monitoriza execuția bugetară, de a identifica abaterile și de a propune ajustări corespunzătoare. – Abilitatea de a efectua analize cost–beneficiu pentru investițiile IT&C, utilizând indicatori financiari și de eficiență. – Capacitatea de a organiza și coordona resursele umane IT&C, inclusiv procesele de recrutare, integrare, evaluare și dezvoltare profesională. – Abilitatea de a menține relații de colaborare eficiente cu		

Nr. crt.	DICIPLINĂ/ MODUL	CONȚINUT TEMATIC	METODE/ FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	4	5	6	7	8	9
		– Referințe la standarde și criterii aplicabile (ex.: ISO 20400, criterii UE de achiziții verzi). *4. Monitorizarea execuției bugetare și analiza cost–beneficiu* – Principiile execuției bugetare: angajamente, plăți, abateri. – Instrumente de monitorizare: tabele de control, rapoarte periodice, indicatori financiari etc. – Ajustarea bugetului. – Elemente ale analizei cost–beneficiu pentru investiții IT&C; indicatori de eficiență financiară. *5. Managementul resurselor umane IT&C* – Organizarea echipelor IT&C: roluri, responsabilități, structuri ierarhice și matriciale. – Procesul de recrutare și integrare a personalului în colaborare cu HR. – Evaluarea performanței: obiective, criterii, instrumente de evaluare. – Identificarea nevoilor de formare profesională și planificarea dezvoltării continue. *6. Colaborarea interdepartamentală și documentația de suport* – Relația cu departamentele de achiziții, IT&C, juridic și audit. – Asigurarea trasabilității, documentației și arhivării.			furnizorii, partenerii și departamentele interne, asigurând comunicare clară și trasabilitate documentară.		

Nr. crt.	DICIPLINĂ/ MODUL	CONȚINUT TEMATIC	METODE/ FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	4	5	6	7	8	9
		– Raportarea periodică privind achizițiile, bugetele și resursele umane IT&C.					
3	**Performanță, conformitate și strategie în IT&C**	**Monitorizarea și evaluarea performanței sistemelor, a proceselor și a serviciilor IT&C cu asigurarea respectării cadrului legal aplicabil IT&C:** *1. Obiectivele manageriale ale monitorizării sistemelor și serviciilor IT&C* – Rolul strategic al monitorizării în atingerea obiectivelor organizației: prevenție, alertare, optimizare. – Contextul de afaceri și riscurile asociate serviciilor și proceselor IT&C. – Diferența între monitorizarea operațională, cea de securitate și cea managerială. – Prioritățile manageriale: disponibilitate, fiabilitate sistemelor, calitatea serviciilor IT și proceselor IT. *2. Soluții pentru monitorizarea securității și performanței în scopul prevenirii incidentelor, alertării și reacției eficiente* – Tipuri de platforme și soluții de monitorizare a performanței și securității; diferențiere în funcție de scop și capabilități.. – Criterii manageriale de selecție a soluțiilor de monitorizare: scalabilitate, costuri, integrare cu sistemele existente. – Tipuri de date colectate: jurnale (logs), metadate, telemetrie, fluxuri de trafic. – Cerințe privind tablourile de bord și raportările automate.	*Teorie*: - Expunere; - Prezentare statică și interactivă; - Dezbaterea dirijată; - Studiu de caz; -Demonstrație practică; - Discuții libere; *Practică*: - Studiu de caz aplicativ; - Exerciții aplicate; - Simulare; - Dezbateri; - Discuții libere în grup	- Servere, unități de stocare dedicate; - Echipamente de rețea (fizice sau virtuale); - Firewall-uri; - Sisteme de prevenire/detectare a intruziunilor; - Token de autentificare multifactor; - Sisteme de acces biometric; - Conexiune Internet; - Platforme/instrumente software de testare/simulare a vulnerabilităților/penetrare; - Platformă de management riscuri; - Soluții de criptare; - Dashboard-uri de raportare; - Platformă de videoconferință, comunicare și colaborare online; - Legislație, protocoale, standarde specifice;	– Capacitatea de a stabili obiectivele de monitorizare în funcție de riscuri și vectori de atac. – Înțelegerea corectă a relației dintre tipul de infrastructură și necesitatea de monitorizare specifică. – Capacitatea de a recunoaște tipurile de soluții de monitorizare și sursele de date relevante pentru decizii manageriale. – Descrierea funcționalității tablourilor de bord și a indicatorilor de alertă. – Interpretarea corectă a datelor în analiza performanței și a securității informatice. – Capacitatea de a descrie corect etapele unui incident și rolul managerial în coordonarea răspunsului. – Evaluarea capacității de a analiza rapoarte post-incident și de a extrage lecții relevante pentru îmbunătățirea proceselor. – Demonstrarea înțelegerii cerințelor legale specifice incidentelor ce implică date personale (ex. notificări GDPR).	**5**	**10**

Nr. crt.	DICIPLINĂ/ MODUL	CONȚINUT TEMATIC	METODE/ FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	4	5	6	7	8	9
		3. *Evaluarea impactului incidentelor asupra performanței și conformității sistemelor IT&C.* – Etapele răspunsului la incidente, din perspectiva impactului asupra performanței și conformității sistemelor. – Tipuri de incidente cu impact asupra performanței și serviciilor: indisponibilitate, degradare performanță sistem, erori de sistem, incidente GDPR. – Evaluarea impactului incidentelor și escaladarea corespunzătoare în organizație. – Raport post-incident: constatări, impact, acțiuni corective. – Particularități ale incidentelor care implică date cu caracter personal și obligațiile de notificare conform GDPR. *4. Evaluarea performanței proceselor și serviciilor IT&C folosind indicatori și praguri critice* – Indicatori pentru sisteme: disponibilitate, timp de răspuns, rate de eroare. – Indicatori pentru procese: durată de execuție, fiabilitate, eficiență. – Indicatori pentru servicii: respectarea acordurilor privind nivelul serviciilor, satisfacția utilizatorilor, timpi de rezolvare. – Praguri critice și alerte automate. *5. Raportarea rezultatelor și colaborarea interdepartamentală* – Structura raportului de performanță destinat managementului: obiective, indicatori,		- Resurse digitale online; - Fișe de practică; - Suport de curs; - Videoproiector; - Ecran de proiecție/monitor; - Coli flipchart, coli A4, markere, etc.	– Capacitatea de a selecta și explica indicatori relevanți pentru evaluarea performanței IT&C la nivel organizațional. – Capacitatea de a stabili praguri critice și de a înțelege semnificația alertelor automate. – Corelarea corectă a performanța sistemelor și a proceselor cu obiectivele de afaceri. – Capacitatea de a redacta și prezenta rapoarte de performanță destinate managementului și auditului. – Capacitatea de a descrie incidentele care implică date cu caracter personal. – Identificarea corectă a obligațiilor legale aplicabile (ex: GDPR, Legea nr. 58/2023, Legea nr. 124/2025) în activitățile de management IT&C. – Analiza gradului de aliniere între politicile interne și legislația actuală privind securitatea cibernetică și protecția datelor.		

Nr. crt.	DICIPLINĂ/ MODUL	CONȚINUT TEMATIC	METODE/ FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	4	5	6	7	8	9
		evoluții, riscuri, interpretare, concluzii, recomandări. – Raportarea periodică către management, audit și, în cazul GDPR, către autoritățile de supraveghere. *6. Cadrul legal și conformitatea cu reglementările privind protecția datelor și securitatea cibernetică* – Legislația aplicabilă în contextul performanței IT&C: Regulamentul General privind Protecția Datelor (GDPR), Legea securității cibernetice, Legea nr. 124/2025, reglementări sectoriale. – Obligațiile managerului în cazul prelucrării datelor personale în incidente de securitate. – Notificarea incidentelor de securitate către autoritățile competente (ANSPDCP, DNSC). – Monitorizarea respectării cerințelor legale prin audituri, rapoarte și politici interne.					
		Evaluarea nevoilor IT&C ale organizației, coordonarea guvernanței și a strategiilor de digitalizare și dezvoltare tehnologică: *1. Analiza cerințelor IT&C, evaluarea nevoilor organizației și guvernanța:* – Noțiuni fundamentale de guvernanță IT și diferența față de managementul operațional IT. – Rolul managerului în formularea cerințelor IT pornind de la obiectivele organizației. – Metode de identificare a nevoilor IT&C ale organizației (analiza infrastructurii, interviuri, sondaje interne etc.).	Teorie: - Expunere; - Prezentare statică și interactivă; - Dezbaterea dirijată; - Studiu de caz; -Demonstrație practică; - Discuții libere; Practică:	- Servere, unități de stocare dedicate; - Echipamente de rețea (fizice sau virtuale); - Firewall-uri; - Sisteme de prevenire/detectare a intruziunilor; - Token de autentificare multifactor; - Sisteme de acces biometric;	– Cunoașterea diferenței dintre guvernanța IT și managementul operațional. – Identificarea și formularea coerentă a nevoilor IT&C pornind de la obiectivele și procesele organizației. – Argumentarea corelării dintre nevoile identificate și direcțiile strategice ale organizației. – Capacitatea de a elabora o strategie de digitalizare care	**5**	**10**

Nr. crt.	DICIPLINĂ/ MODUL	CONȚINUT TEMATIC	METODE/ FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	4	5	6	7	8	9
		– Cadre de referință pentru guvernanța IT și standarde aplicabile (COBIT, ITIL, ISO/IEC). – Corelarea nevoilor IT cu misiunea, strategia și prioritățile organizaționale. *2. Elaborarea strategiei de digitalizare și definirea indicatorilor de performanță în IT&C* – Structura unei strategii IT: analiză de context intern și extern, viziune, obiective, direcții de acțiune, resurse, indicatori de performanță. – Corelarea strategiei IT cu obiectivele generale ale organizației. – Tipuri de indicatori de performanță (KPI): pentru infrastructură, servicii, aplicații, suport IT. – Colectarea și interpretarea valorilor indicatorilor. – Utilizarea KPI-urilor pentru urmărirea implementării strategiei și luarea deciziilor. *3. Audit managerial și asigurarea conformității IT* – Tipuri de audit relevante în domeniul IT și al securității informației. – Etapele unui audit managerial: obiective, criterii, colectare de date, constatări, plan de acțiune. – Identificarea neconformităților și elaborarea planurilor de măsuri corective și preventive. – Încadrarea în cerințele legale și de standardizare din domeniu.	- Studiu de caz aplicativ; - Exerciții aplicate; - Simulare; - Dezbateri; - Discuții libere în grup	- Conexiune Internet; - Platforme/instrumente software de testare/simulare a vulnerabilităților/penetrare; - Platformă de management riscuri; - Soluții de criptare; - Dashboard-uri de raportare; - Platformă de videoconferință, comunicare și colaborare online; - Legislație, protocoale, standarde specifice; - Resurse digitale online; - Fișe de practică; - Suport de curs; - Videoproiector; - Ecran de proiecție/monitor; - Coli flipchart, coli A4, markere, etc.	include: analiza contextului, viziunea, obiectivele, direcțiile de acțiune și calendarul de implementare. – Identificarea și selectarea unor indicatori de performanță adecvați pentru monitorizarea implementării strategiei. – Capacitatea de a interpreta valorile indicatorilor și de a propune ajustări sau acțiuni corective în funcție de abaterile de la obiective. – Demonstrarea modului în care indicatorii sunt integrați în procesul decizional și în revizuirea periodică a strategiei. – Înțelegerea rolului auditului în asigurarea performanței și conformității proceselor IT&C. – Capacitatea de a identifica neconformități relevante și de a propune măsuri corective aliniate cu cadrul legislativ și de guvernanță. – Capacitatea de a documenta deciziile și procesele IT&C. – Capacitatea de a coordona procesul de raportare strategică (indicatori, obstacole, raporări).		

Nr. crt.	DICIPLINĂ/ MODUL	CONȚINUT TEMATIC	METODE/ FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	4	5	6	7	8	9
		– Auditul ca instrument de guvernanță și îmbunătățire a proceselor. *4. Managementul documentării și raportării* – Structura și organizarea documentației în proiectele IT. – Documentarea deciziilor strategice și a rezultatelor proiectelor IT. – Structura rapoartelor manageriale: indicatori, obstacole, soluții propuse. – Utilizarea rapoartelor în procesele de audit și pentru ajustarea strategiilor.			– Demonstrarea utilizării corecte a raportărilor în luarea deciziilor manageriale și în corelare cu auditul.		
4	**Politici și controlul accesului în securitatea informației**	**Definirea, implementarea și actualizarea politicilor de securitate a informației, monitorizând informațiile și gestionând incidentele:** *1. Rolul politicilor de securitate a informației în organizație* – Diferențierea dintre politică și strategie. – Identificarea domeniilor esențiale ce necesită politici de securitate. – Definirea tipurilor de documente: politică / procedură / instrucțiune de lucru. – Obiectivele politicilor de securitate: prevenție, control, responsabilizare. – Corelarea politicilor de securitate cu strategia și riscurile organizației. *2. Tipuri de politici de securitate și conținutul acestora* – Tipuri de politici pentru: acces și drepturi, parole, utilizarea echipamentelor, protecția	*Teorie*: - Expunere; - Prezentare statică și interactivă; - Dezbaterea dirijată; - Studiu de caz; -Demonstrație practică; - Discuții libere; *Practică*: - Studiu de caz aplicativ; - Exerciții aplicate; - Simulare; - Dezbateri; - Discuții libere în grup	- Servere, unități de stocare dedicate; - Echipamente de rețea (fizice sau virtuale); - Firewall-uri; - Sisteme de prevenire/detectare a intruziunilor; - Token de autentificare multifactor; - Sisteme de acces biometric; - Conexiune Internet; - Platforme/instrumente software de testare/simulare a vulnerabilităților/penetrare; - Platformă de management riscuri;	– Înțelegerea diferenței dintre politică, procedură, instrucțiune și strategie în domeniul securității informației. – Identificarea corectă a domeniilor care necesită politici de securitate în cadrul unei organizații. – Capacitatea de a corela politicile de securitate cu riscurile identificate și cu obiectivele strategice ale organizației. – Redactarea clară și structurată a unei politici de securitate, respectând elementele standard (scop, aplicabilitate, reguli, responsabilități etc.). – Formularea unui proces intern de consultare și aprobare a	**5**	**10**

Nr. crt.	DICIPLINĂ/ MODUL	CONȚINUT TEMATIC	METODE/ FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	4	5	6	7	8	9
		datelor, mobilitate, backup, utilizarea e-mailului și internetului, lucru la distanță. – Structura standard a unei politici: scop, domeniu de aplicabilitate, termeni și definiții, principii și responsabilități, reguli și cerințe , excepții, sancțiuni. – Corelarea fiecărei politici cu riscurile specifice și obiectivele organizației *3. Procesul de redactare și aprobare a politicilor* – Identificarea nevoilor și consultarea părților interesate. – Redactarea clară și accesibilă a politicii. – Procedura de aprobare internă și publicare oficială. *4. Coordonarea implementării politicilor* – Mecanisme de comunicare internă. – Integrarea politicilor în procesele organizaționale și corelarea cu auditul intern. – Instrumente de control pentru politicile aplicate. – Corelarea politicilor de securitate cu mecanismele de gestionare a incidentelor și fluxurilor de informații. *5. Revizuirea și actualizarea politicilor* – Criterii de actualizare: audituri, incidente, schimbări legislative sau organizaționale. – Revizuire periodică și aprobare a versiunilor actualizate. – Arhivarea și trasabilitatea documentelor.		- Soluții de criptare; - Dashboard-uri de raportare; - Platformă de videoconferință, comunicare și colaborare online; - Legislație, protocoale, standarde specifice; - Resurse digitale online; - Fișe de practică; - Suport de curs; - Videoproiector; - Ecran de proiecție/monitor; - Coli flipchart, coli A4, markere, etc.	politicilor, cu implicarea părților interesate relevante. – Demonstrarea modului în care politicile pot fi integrate în procesele operaționale existente și cum pot fi comunicate eficient în cadrul organizației. – Capacitatea de a corela politicile de securitate cu mecanismele de monitorizare a informațiilor și gestionarea incidentelor. – Stabilirea criteriilor și a frecvenței de revizuire a politicilor, în funcție de schimbările legislative, organizaționale sau de securitate.		

Nr. crt.	DICIPLINĂ/ MODUL	CONȚINUT TEMATIC	METODE/ FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	4	5	6	7	8	9
		Coordonarea implementării politicilor de control al accesului, autentificare și gestionare a identității *1. Fundamente ale controlului accesului* – Tipuri de acces: fizic, virtual, la aplicații, la date. – Modele de control al accesului. – Principiile „need to know” și „least privilege” – aplicare practică. – Răspunderea managerială privind limitarea accesului și drepturile de utilizator. *2. Politici organizaționale privind accesul utilizatorilor și identitatea digitală* – Definirea obiectivelor unei politici de acces în context organizațional. – Structura unei politici de acces: scop, aplicabilitate, reguli, responsabilități, excepții, sancțiuni. – Coordonarea procesului de atribuire, modificare și revocare a drepturilor de acces – implicarea managementului, IT-ului și HR-ului. – Gestionarea accesului și al identității virtuale pentru un angajat: ciclul de viață al accesului (onboarding, mutări interne, offboarding). – Revizuirea periodică a politicilor și adaptarea acestora la modificările organizaționale, riscuri emergente și cerințe legale.	*Teorie*: - Expunere; - Prezentare statică și interactivă; - Dezbaterea dirijată; - Studiu de caz; -Demonstrație practică; - Discuții libere; *Practică*: - Studiu de caz aplicativ; - Exerciții aplicate; - Simulare; - Dezbateri; - Discuții libere în grup	- Servere, unități de stocare dedicate; - Echipamente de rețea (fizice sau virtuale); - Firewall-uri; - Sisteme de prevenire/detectare a intruziunilor; - Token de autentificare multifactor; - Sisteme de acces biometric; - Conexiune Internet; - Platforme/instrumente software de testare/simulare a vulnerabilităților/penetrare; - Platformă de management riscuri; - Soluții de criptare; - Dashboard-uri de raportare; - Platformă de videoconferință, comunicare și colaborare online; - Legislație, protocoale, standarde specifice; - Resurse digitale online; - Fișe de practică; - Suport de curs;	– Cunoașterea clară a tipurilor de acces și de gestionare a identității utilizatorilor. – Identificarea corectă a modelelor de control al accesului. – Explicarea responsabilității manageriale în limitarea și supravegherea accesului utilizatorilor. – Enumerarea obiectivelor unei politici de acces, adaptată specificului unei organizații. – Structurarea corectă a unei politici de acces: scop, reguli, excepții, responsabilități și sancțiuni. – Redactarea unei politici de acces. – Descrierea completă a ciclului de viață al accesului unui angajat: la angajare, în timpul activității și la plecarea din organizație. – Cunoașterea motivelor de revocare a drepturilor în funcție de roluri și modificări organizaționale. – Coordonarea reviziei periodice a drepturilor de acces. – Capacitatea de a explica rolul și funcționalitățile soluțiilor IAM	**5**	**10**

Nr. crt.	DICIPLINĂ/ MODUL	CONȚINUT TEMATIC	METODE/ FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	4	5	6	7	8	9
		– Instruirea personalului privind drepturile de acces și utilizarea identității virtuale. *3. Managementul identității accesului (IAM)* – Funcționalități ale unui sistem IAM: gestionarea conturilor utilizatorilor (creare, modificare, ștergere), Single Sign-On, Multi-Factor Authentication, audit. – Exemple de soluții IAM folosite în organizații. – Rolul managerial în selectarea și integrarea soluțiilor IAM în infrastructura IT&C a organizației. *4. Autentificarea, trasabilitatea accesului și verificări periodice* – Tipuri de autentificare: bazată pe parolă, OTP, biometrie, certificate digitale – criterii de alegere managerială.. – Autentificarea multifactor (MFA): definiție, implementare, situații în care este obligatorie. – Trasabilitatea accesului: loguri, sesiuni active, verificare periodică a drepturilor. – Organizarea auditului periodic de acces: obiective, metode, colaborarea cu echipele IT și de securitate. – Identificarea deficiențelor în controlul accesului și aplicarea măsurilor corective.		- Videoproiector; - Ecran de proiecție/monitor; - Coli flipchart, coli A4, markere, etc.	și integrarea lor în infrastructura organizației. – Alegerea tipurilor adecvate de autentificare în funcție de riscuri și nivel de acces. – Justificarea corectă a implementării MFA în scenarii specifice (ex. acces la date sensibile). – Descrierea corectă a modului în care se face trasabilitatea accesului.		
5	**Riscuri, infrastructuri critice și**	**Evaluarea riscurilor de securitate informatică și stabilirea de măsuri de protecție:**	*Teorie*: - Expunere;	- Servere, unități de stocare dedicate; - Echipamente de rețea (fizice sau virtuale);	– Cunoașterea diferenței dintre conceptele: amenințare, vulnerabilitate, activ și risc informatic.	**5**	**10**

Nr. crt.	DICIPLINĂ/ MODUL	CONȚINUT TEMATIC	METODE/ FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	4	5	6	7	8	9
	continuitate în securitatea informației	*1. Fundamente ale managementului riscurilor de securitate IT* – Definirea riscului informatic: componentele riscului (activ, vulnerabilitate, amenințare, impact). – Rolul managementului riscurilor în guvernanța securității informației. – Cadre și standarde de referință.. *2. Identificarea și clasificarea activelor informatice* – Clasificarea activelor (hardware, software, aplicații, date, personal, infrastructuri). – Metode de identificare a riscurilor: interviuri, audituri, analiza evenimentelor anterioare. – Corelarea activelor cu procesele critice și scenariile de risc. *3. Analiza vulnerabilităților și amenințărilor* – Surse tipice de vulnerabilități: tehnice, organizaționale, umane. – Amenințări interne vs. externe, deliberate vs. accidentale. – Colectarea datelor și utilizarea listelor de control/standarde pentru identificare. *4. Evaluarea și prioritizarea riscurilor* – Metode de evaluare: cantitative (formule), calitativă (matrice de risc), mixte. – Stabilirea pragurilor de acceptabilitate a riscurilor. – Estimarea probabilității și a impactului asupra activelor.	- Prezentare statică și interactivă; - Dezbaterea dirijată; - Studiu de caz; -Demonstrație practică; - Discuții libere; *Practică*: - Studiu de caz aplicativ; - Exerciții aplicate; - Simulare; - Dezbateri; - Discuții libere în grup	- Firewall-uri; - Sisteme de prevenire/detectare a intruziunilor; - Token de autentificare multifactor; - Sisteme de acces biometric; - Conexiune Internet; - Platforme/instrumente software de testare/simulare a vulnerabilităților/penetrare; - Platformă de management riscuri; - Soluții de criptare; - Dashboard-uri de raportare; - Platformă de videoconferință, comunicare și colaborare online; - Legislație, protocoale, standarde specifice; - Resurse digitale online; - Fișe de practică; - Suport de curs; - Videoproiector; - Ecran de proiecție/monitor;	– Capacitatea de a evidenția rolul analizei de risc în planificarea măsurilor de securitate. – Corelarea riscurilor informatice cu standardele și reglementările aplicabile. – Clasificarea coerentă a activelor în funcție de valoare, sensibilitate și impact. – Folosirea adecvată a metodelor pentru identificarea riscurilor asociate activelor. – Relevanța amenințărilor identificate în raport cu procesele critice. – Prioritizarea adecvată a amenințărilor în funcție de impactul estimat. – Corectitudinea aplicării metodelor de evaluare a riscurilor. – Capacitatea de a stabili scoruri de risc rezultate din analiza probabilității și impactului. – Propunerea corectă a modului de tratare a riscului în raport cu pragurile de acceptare. – Capacitatea de a stabili un mod de tratare a riscului (obiective, termene, responsabilități).		

Nr. crt.	DICIPLINĂ/ MODUL	CONȚINUT TEMATIC	METODE/ FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	4	5	6	7	8	9
		– Matrice risc/impact și scoruri de risc. *5. Măsuri de protecție și planuri de atenuare* – Controale de securitate: preventive, detective, corective. – Măsuri tehnice (firewall, criptare, autentificare multifactor) și organizaționale (politici, instruire). – Planul de atenuare: structură, responsabilități, termene. *6. Raportarea riscurilor și urmărirea măsurilor* – Structura unui raport managerial de tip analiză de risc. – Comunicarea rezultatelor către management și factorii relevanți. – Monitorizează implementarea măsurilor. – Trasabilitatea acțiunilor: revizuiri, actualizări, aprobări.		- Coli flipchart, coli A4, markere, etc.	– Redactarea unei analize de risc completă și corectă. – Calitatea documentării măsurilor implementate și a trasabilității acțiunilor.		
		Coordonarea securității informatice a infrastructurii critice, a echipamentelor mobile și a muncii la distanță: *1. Riscuri și politici privind mobilitatea și munca la distanță* – Identificarea riscurilor specifice asociate dispozitivelor mobile, conexiunilor externe și accesului în afara perimetrului fizic securizat.. – Politici BYOD (Bring Your Own Device) vs. politici restrictive. – Reguli și bune practici privind utilizarea echipamentelor mobile, a rețelelor Wi-Fi publice și accesul prin VPN.	*Teorie*: - Expunere; - Prezentare statică și interactivă; - Dezbaterea dirijată; - Studiu de caz; -Demonstrație practică; - Discuții libere; *Practică*:	- Servere, unități de stocare dedicate; - Echipamente de rețea (fizice sau virtuale); - Firewall-uri; - Sisteme de prevenire/detectare a intruziunilor; - Token de autentificare multifactor; - Sisteme de acces biometric; - Conexiune Internet;	– Capacitatea de a identifica riscurile specifice asociate mobilității și muncii la distanță. – Diferențierea corectă între politicile BYOD și politicile restrictive privind utilizarea echipamentelor mobile. – Aplicarea corectă a regulilor și bunelor practici privind accesul prin VPN și utilizarea rețelelor Wi-Fi publice.	**5**	**10**

Nr. crt.	DICIPLINĂ/ MODUL	CONȚINUT TEMATIC	METODE/ FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	4	5	6	7	8	9
		– Responsabilitățile angajaților și procedurile în caz de pierdere sau furt de echipamente și date. *2. Managementul și securizarea dispozitivelor mobile (MDM/EMM)* – Funcții și beneficii ale soluțiilor de management centralizat al dispozitivelor mobile. – Înregistrarea, inventarierea, blocarea de la distanță și ștergerea securizată. – Integrarea politicilor de management al dispozitivelor mobile în strategia de securitate organizațională. *3. Acces securizat la distanță în context organizațional* – Tehnologii de acces securizat: VPN, tuneluri securizate, autentificare multifactor, SSO. – Stabilirea de politici contextuale de acces (geo-locație, oră, dispozitiv autorizat). – Monitorizarea activităților la distanță și detectarea anomaliilor. *4. Criptarea și controlul accesului pe terminale* – Tipuri de criptare: la nivel de fișier, de disc, de comunicație. – Protejarea datelor în repaus și în tranzit. – Mecanisme de control al accesului adaptate pentru mobilitate (parole complexe, autentificare biometrică, tokenuri hardware/software).	- Studiu de caz aplicativ; - Exerciții aplicate; - Simulare; - Dezbateri; - Discuții libere în grup	- Platforme/instrumente software de testare/simulare a vulnerabilităților/penetrare; - Platformă de management riscuri; - Soluții de criptare; - Dashboard-uri de raportare; - Platformă de videoconferință, comunicare și colaborare online; - Legislație, protocoale, standarde specifice; - Resurse digitale online; - Fișe de practică; - Suport de curs; - Videoproiector; - Ecran de proiecție/monitor; - Coli flipchart, coli A4, markere, etc.	– Cunoașterea procedurilor aplicabile în caz de pierdere sau furt de echipamente sau date. – Capacitatea de a descrie funcțiile și beneficiile soluțiilor MDM/EMM pentru gestionarea dispozitivelor mobile. – Aplicarea corectă a procedurilor de înregistrare, inventariere, blocare și ștergere securizată de la distanță. – Capacitatea de a integra politicile de management al dispozitivelor mobile în strategia de securitate organizațională. – Descrierea corectă a politicilor contextuale de acces, în funcție de factori precum locație, oră și dispozitiv autorizat. – Capacitatea de a monitoriza activitățile desfășurate la distanță și de a detecta anomaliile. – Selectarea corectă a tipurilor relevante de criptare pentru protejarea datelor. – Enumerarea corectă a modului de asigurare a protecției eficiente a datelor în repaus și în tranzit. – Utilizarea adecvată a mecanismelor de autentificare		

Nr. crt.	DICIPLINĂ/ MODUL	CONȚINUT TEMATIC	METODE/ FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	4	5	6	7	8	9
		5. Integrarea măsurilor de securitate fizică pentru infrastructura digitală critică – Legătura dintre securitatea fizică și cea informatică în cazul infrastructurii critice. – Amenințări fizice cu impact cibernetic (furt, sabotaj, dezastre naturale). – Identificarea și clasificarea zonelor critice (camere server, UPS, noduri de comunicații). *6. Politici și proceduri de securitate fizică* – Politici de acces fizic și responsabilități ale personalului. – Proceduri pentru vizitatori, subcontractori, furnizori sau personal de întreținere. – Gestiunea cheilor și cardurilor de acces. – Reguli speciale pentru accesul în afara orelor de program și trasabilitatea intrărilor și ieșirilor. *7. Prevenirea și gestionarea incidentelor fizice care afectează infrastructura digitală* – Tipuri de incidente: acces neautorizat, incendiu, întreruperi de curent, vandalism. – Măsuri imediate de răspuns și notificare. – Simulări și exerciții pentru scenarii critice. – Integrarea incidentelor fizice în planul de continuitate și recuperare IT. *8. Auditul periodic al măsurilor și procedurilor de securitate fizică, în colaborare cu echipele IT și non-IT* – Cooperarea dintre echipa de securitate IT și departamentele de infrastructură, pază, mentenanță.			pentru mobilitate (parole, biometrie, tokenuri). – Capacitatea de a recunoaște interdependențele dintre securitatea fizică și cea informatică în infrastructura critică. – Identificarea corectă a amenințărilor fizice cu impact asupra securității cibernetice. – Clasificarea corectă a zonelor fizice critice relevante pentru protecția infrastructurii IT. – Aplicarea politicilor și procedurilor de acces fizic și asumarea responsabilităților de către personal. – Demonstrarea capacității de a implementa și de a monitoriza procedurile privind accesul vizitatorilor, subcontractorilor și furnizorilor. – Aplicarea corectă a procedurii de trasabilitate a accesului fizic. – Cunoașterea modului de a reacționa la incidente fizice precum incendii, pene de curent sau acces neautorizat. – Listarea corectă a măsurilor imediate de răspuns și de		

Nr. crt.	DICIPLINĂ/ MODUL	CONȚINUT TEMATIC	METODE/ FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	4	5	6	7	8	9
		– Corelarea jurnalelor de acces fizic cu cele de securitate IT (SIEM). – Auditul periodic al măsurilor și procedurilor de securitate fizică.			notificare în cazul unor incidente fizice. – Capacitatea de a corela jurnalele de acces fizic cu datele din sistemele de securitate IT (ex. SIEM).		
		Elaborarea și testarea planurilor de continuitate și de recuperare în caz de dezastru și colaborarea cu autoritățile: *1. Noțiuni fundamentale: continuitate, dezastru, recuperare* – Definirea termenilor: continuitate, dezastru, recuperare. – Tipuri de incidente majore: cibernetice, fizice, operaționale, naturale. – Diferența între continuarea activității și recuperarea în caz de dezastru. – Rolul planurilor de continuitate sau de recuperare în asigurarea rezilienței organizaționale. *2. Evaluarea impactului și a riscurilor* – Analiza de impact asupra afacerii. – Identificarea proceselor critice și a resurselor dependente. – Evaluarea riscurilor potențiale care pot genera întreruperi semnificative. *3. Elaborarea planului de continuitate și de recuperare* – Structura unui plan de continuare afacere / plan de recuperare după dezastru: scop, domeniu, scenarii, roluri, măsuri, proceduri.	*Teorie*: - Expunere; - Prezentare statică și interactivă; - Dezbaterea dirijată; - Studiu de caz; -Demonstrație practică; - Discuții libere; *Practică*: - Studiu de caz aplicativ; - Exerciții aplicate; - Simulare; - Dezbateri; - Discuții libere în grup	- Servere, unități de stocare dedicate; - Echipamente de rețea (fizice sau virtuale); - Firewall-uri; - Sisteme de prevenire/detectare a intruziunilor; - Token de autentificare multifactor; - Sisteme de acces biometric; - Conexiune Internet; - Platforme/instrumente software de testare/simulare a vulnerabilităților/penetrare; - Platformă de management riscuri; - Soluții de criptare; - Dashboard-uri de raportare; - Platformă de videoconferință,	– Capacitatea de a evalua impactul întreruperii activității asupra funcționării organizației. – Capacitatea de a identifica rapid procesele critice și resursele esențiale afectate de un incident. – Abilitatea de a redacta un plan coerent și adaptat de continuitate/recuperare. – Abilitatea de a interpreta rezultatele testărilor periodice. – Capacitatea de a actualiza corect planurile de continuitate și de recuperare în funcție de riscuri și schimbări. – Cunoașterea avansată a cadrului legal național și european privind colaborarea instituțională în securitate IT. – Listarea corectă a canalelor oficiale de raportare a incidentelor. – Aplicarea corectă a procedurilor de raportare a	**5**	**10**

Nr. crt.	DICIPLINĂ/ MODUL	CONȚINUT TEMATIC	METODE/ FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	4	5	6	7	8	9
		– Relația cu alte planuri: securitate IT, incidente, evacuare, comunicare de criză. – Exemple de soluții: backup off-site, redundanță, contracte de failover, echipamente mobile de intervenție. *4. Testarea și actualizarea planurilor* – Tipuri de testări: simulări, testări parțiale, testări complete – Implicarea echipelor multidisciplinare în testare (IT, operațional, management, securitate). – Documentarea lecțiilor învățate și a disfuncționalităților identificate. – Revizuirea periodică în funcție de audituri, incidente sau modificări organizaționale. *5. Cadrul instituțional relevant în domeniul securității informației* – Principalele autorități naționale și europene din domeniul securității informatice. – Rolurile și responsabilitățile autorităților în contextul securității cibernetice. – Tipuri de relații dintre organizații și instituții (obligatorii, de bună practică, parteneriate). *6. Colaborarea profesională cu autoritățile* – Reguli de comunicare: transparență, completitudine, formalism, termene. – Exemple de bune practici în interacțiunile cu autoritățile. *7. Raportarea incidentelor de securitate*		comunicare și colaborare online; - Legislație, protocoale, standarde specifice; - Resurse digitale online; - Fișe de practică; - Suport de curs; - Videoproiector; - Ecran de proiecție/monitor; - Coli flipchart, coli A4, markere, etc.	incidentelor și documentarea completă a conținutului acestora. – Cunoștințe despre cerințele și etapele implicate într-un control sau audit extern. – Abilitatea de a răspunde argumentat la întrebări privind documentele și procedurile în cadrul unui audit IT.		

Nr. crt.	DICIPLINĂ/ MODUL	CONȚINUT TEMATIC	METODE/ FORME DE DESFĂȘURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂȚARE	CRITERII DE EVALUARE	NR. ORE	
						TEORIE	PRACTICĂ
1	2	4	5	6	7	8	9
		– Obligații de raportare conform legislației europene și naționale privind securitatea cibernetică și protecția datelor. – Canalele oficiale de raportare (portale, e-mail securizat, interfețe automatizate). – Structura unui raport de incident: informații tehnice, impact, măsuri luate, lecții învățate. *8. Participarea la audituri, controale și evaluări externe* – Tipuri de audituri externe (tehnice, de conformitate, tematice). – Rolul managerului de securitate informatică în procesul de audit/control. – Modul de pregătire: documente necesare, evidențe, planuri de remediere. – Exemple de neconformități identificate frecvent și măsuri corective. 9. *Inițiative colective de securitate IT* – Rețele naționale și europene de colaborare în domeniul securității. – Beneficii și riscuri, modalități de implicare.					
						60	**120**