Co-funded by the European Union

# D3.1 MODULE DE FORMARE PENTRU STUDENȚII DIN ÎNVĂȚĂMÂNTUL SUPERIOR

# CYBER AGENT 09.2025

**Call: ERASMUS-EDU-2022-PI-ALL-INNO**
**Type of Action: ERASMUS-LS**
**Project No. 101111732**

Pachet de lucru 3: Dezvoltarea resurselor de învățare CyberAgent

rezultatul 3.1: MODULE DE FORMARE PENTRU STUDENȚII DIN ÎNVĂȚĂMÂNTUL SUPERIOR

Coordonator al WP3 – TIMTAL. Coordonator al D3.1 – VU.

# CONŢINUT

# INTRODUCERE

Conform raportului D2.2, IMM-urile se confruntă cu o lipsă semnificativă de specialiști calificați în securitate cibernetică, iar angajații existenți adesea nu dispun de cunoștințele sistemice necesare pentru a răspunde în mod corespunzător amenințărilor cibernetice din ce în ce mai complexe. Prin urmare, în învățământul superior este deosebit de important să se pregătească specialiști care să își poată aplica cunoștințele în mediul IMM-urilor – atât în domenii tehnice, cât și manageriale. În acest context, în documentul D2.3 a fost creată o cale de învățare bazată pe competențe, împărțită în diferite domenii tematice și axată pe dezvoltarea abilităților practice.

Acest document prezintă unul dintre principalele rezultate ale proiectului – modulele de formare pentru studenții din învățământul superior (IIS) (D3.1). Obiectivul acestei activități este de a crea programe de formare pentru instituțiile de învățământ superior (IIS) care să acopere domeniile cheie ale cunoștințelor, abilităților și competențelor în domeniul securității cibernetice, relevante pentru întreprinderile mici și mijlocii (IMM-uri).

Aceste module sunt rezultatul unei munci consecvente bazate pe o analiză detaliată a nevoilor (D2.2), în cadrul căreia au fost chestionați reprezentanți ai IMM-urilor, instituțiilor de învățământ profesional și de formare (VET) și instituțiilor de învățământ superior, precum și pe o structură clar definită a traseului de învățare (D2.3).

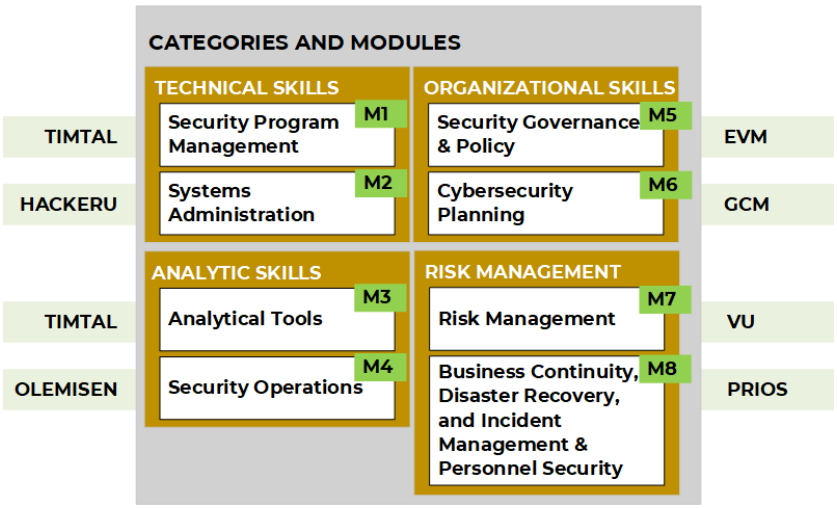
Programul de formare, corespunzător nivelurilor 5-6 ale Cadrului European al Calificărilor (CEC), este conceput pentru studenții din învățământul superior și angajații IMM-urilor cu experiență. Acesta constă din opt module de bază și un modul inspirațional, acoperind patru domenii esențiale de competență:

- **Competențe tehnice** (Managementul programelor de securitate, Administrarea sistemelor).
- **Competențe analitice** (Instrumente analitice, Operațiuni de securitate).
- **Competențe organizatorice** (Guvernanță și politici de securitate, Planificarea securității cibernetice).
- **Managementul riscurilor (**Managementul și atenuarea riscurilor, Continuitatea afacerii, Recuperare în caz de dezastru și Managementul incidentelor și Securitatea personalului).

Fiecare modul valorează 3 credite ECTS (corespunzător unei sarcini de lucru de 75 de ore pentru studenți), este aliniat cu principiile Spațiului Învățământului Superior și respectă recomandările metodologice specificate în D2.3: educația se bazează pe metode de învățare activă (de exemplu, studii de caz, învățare bazată pe proiecte) și învățare autodirijată, cu rezultate ale învățării clar diferențiate la nivelurile de cunoștințe, abilități și competențe.

Fiecare modul de 3 credite ECTS a fost dezvoltat de diferiți parteneri din consorțiu, valorificând experiența lor specifică în domeniu și profesională.

Modulele dezvoltate acoperă următoarele domenii cheie, identificate ca fiind de importanță critică în raportul D2.2:



# 1. M1: MANAGEMENTUL PROGRAMULUI DE SECURITATE

| Titlul modulului | Codul modulului |
|---|---|
| **MANAGEMENTUL PROGRAMULUI DE SECURITATE** | |

| Lector (i) | Instituția sau departamentul unde se predă modulul |
|---|---|
| | |

| Modalitatea de livrare | Limba |
|---|---|
| *Față în față, online, hibrid* | *Engleză, Finlandeză, Turcă, Norvegiană, Lituaniană, Română, Franceză, Poloneză, Spaniolă* |

| Cerințe preliminare |
|---|
| Nici una |

| Numărul de credite ECTS alocate | Volumul de muncă al studentului | Contact orele de lucru | Program de lucru individual |
|---|---|---|---|
| 3 | 75 ore | 50 ore | 25 ore |

**Scopul și rezultatele modulului**

După finalizarea acestui curs, studenții vor dobândi abilitățile necesare pentru a gestiona eficient programele de securitate ca răspuns la amenințările de securitate cibernetică. Aceștia vor dezvolta strategii de apărare împotriva amenințărilor actuale, cum ar fi phishing-ul, ransomware-ul și atacurile DDoS, în cadrul managementului de proiect și resurse. În plus, studenții vor învăța să aplice indicatori de securitate și metode de asigurare a calității, dobândind capacitatea de a optimiza programele de securitate, de a gestiona eficient resursele și de a spori securitatea organizațională prin utilizarea instrumentelor adecvate împotriva amenințărilor în evoluție. Acest curs le va dezvolta, de asemenea, competența în evaluarea, raportarea și comunicarea amenințărilor, permițându-le să implementeze eficient strategii de securitate cibernetică în cadrul organizațiilor lor.

| Rezultatele învățării ale modulului | Metode de predare si invatare | Metode de evaluare |
|---|---|---|
| **Cunoștințe:** Cursanții vor dobândi cunoștințe practice despre cele mai recente amenințări cibernetice, inclusiv phishing, ransomware și atacuri DDoS, și despre cum să le gestioneze printr-o gestionare eficientă a proiectelor și resurselor și implementarea măsurilor de asigurare a calității și control. | A se selecta de către lector, din Partea 1.3. [Metode de predare, de exemplu, prelegeri teoretice, invitați, chestionare, jocuri, sarcini practice/laboratoare, predare și învățare reciprocă, învățare autoghidată etc.] din D2.3 „Structura căii de învățare pentru agenții schimbării în domeniul securității cibernetice pentru IMM-uri” | Teste de autoevaluare<br>Test de evaluare a cunoștințelor |

| | | |
|---|---|---|
| **Competențe:** Cursanții vor fi abilități de utilizare a instrumentelor și software-ului pentru protecția împotriva amenințărilor cibernetice în continuă evoluție și vor aplica practici robuste de securitate în managementul proiectelor și resurselor pentru a îmbunătăți indicatorii generali de securitate și controlul calității în cadrul organizațiilor lor. | A se selecta de către lector, din Partea 1.3. [Metode de predare, de exemplu, sarcini practice/laboratoare, activități practice, medii simulate, chestionare, jocuri, studii de caz etc.] din D2.3 „Structura căii de învățare pentru agenții schimbării în domeniul securității cibernetice pentru IMM-uri” | Evaluări practice |
| **Competențe:** Cursanții vor fi competenți în evaluarea și atenuarea potențialelor amenințări la adresa securității, comunicarea eficientă a problemelor de securitate cibernetică și raportarea cu precizie a amenințărilor și încălcărilor prin canalele adecvate din cadrul organizației lor. | A se selecta de către lector, din Partea 1.3. [Metode de predare, de exemplu, medii simulate, concursuri de capturare a steagului, 5E-uri, CBL, CL, POGIL, PBL etc.] din D2.3 „Structura căii de învățare pentru agenții schimbării în domeniul securității cibernetice pentru IMM-uri” | Simulări<br>Competiții |

| **Conținutul modulului: defalcarea subiectelor** | **Ore de lucru direct** | | | | | **Ore de lucru și sarcini individuale** | |
|---|---|---|---|---|---|---|---|
| | Lector(i) | Consultatii | Practica | Teste | **Toate lucrările** | **Munca** | **Cerințe** |
| **Management de proiect**<br>• Planificarea proiectului<br>· Definirea obiectivelor proiectului<br>· Definirea domeniului de aplicare și a cerințelor proiectului<br>· Pregătirea calendarului proiectului<br>· Instrumente de management de proiect<br>· Amenințări cibernetice actuale (DDoS, ransomware, malware, phishing, zero-day, atacuri IoT etc.)<br>· Modelarea amenințărilor și analiza vulnerabilităților<br>· Planuri de răspuns la situații de urgență și incidente | 8 | 0,5 | 3 | 0,5 | **12** | **6** | · Planificați un proiect de conștientizare a securității cibernetice pentru angajații IMM-urilor.<br>· Definiți obiective clare pentru proiectul de conștientizare a securității cibernetice pentru a îmbunătăți înțelegerea de către angajații IMM-urilor a potențialelor amenințări la adresa securității.<br>· Descrieți domeniul de aplicare și cerințele proiectului de conștien- |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| • · Raportarea amenințărilor și incidentelor cibernetice | | | | | | | tizare a securității cibernetice pentru angajații IMM-urilor, inclusiv subiectele de instruire și resursele necesare.<br>· Pregătiți calendarul pentru proiectul de conștientizare a securității cibernetice pentru angajații IMM-urilor.<br>· Utilizați instrumente de management de proiect pentru a monitoriza progresul și utilizarea resurselor pentru proiectul de conștientizare a securității cibernetice destinat angajaților IMM-urilor.<br>· Cercetați amenințările actuale la adresa securității cibernetice și compilați constatările într-un raport.<br>· Creați un model simplificat de amenințări pentru a ajuta angajații IMM-urilor să identifice potențialele vulnerabilități de securitate în operațiunile lor zilnice.<br>· Găsiți și examinați exemple de planuri de răspuns la situații de urgență și incidente.<br>· Ce pași ar trebui luați în considerare la pregătirea unui raport privind raportarea amenințărilor și incidentelor de securitate cibernetică? Cercetați și rezumați. |
| **Managementul resurselor**<br>• Managementul resurselor umane (echipe de proiect)<br>· Conștientizare în materie de securitate și instruire a echipei<br>· Managementul inventarului de hardware și software<br>· Instrumente și software de securitate<br>· Utilizarea eficientă a resurselor tehnologice<br>• · Buget și alocare a resurselor | 8 | 0,5 | 3 | 0,5 | **12** | **6** | · Planificați o strategie de gestionare a resurselor pentru a asigura utilizarea eficientă a resurselor pentru o IMM fictivă.<br>· Creați un plan tematic exemplu pentru instruirea în domeniul conștientizării securității cibernetice.<br>· Pregătiți un inventar de hardware și software |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | pentru o IMM fictivă.Research commonly used security tools and software.<br>· Creați un exemplu de buget și plan de alocare a resurselor pentru un IMM ipotetic. |
| **Indicatori de securitate**<br>• Indicatori de securitate și tehnici de măsurare<br>· Colectare de date cu SIEM<br>· Analiza indicatorilor de securitate<br>· Monitorizarea proiectului și evaluarea performanței<br>· Revizuirea acțiunilor și adaptarea proiectului<br>• · Raportarea indicatorilor de securitate | 8 | 0,5 | 4 | 0,5 | **13** | **6** | · Cercetați indicatorii de securitate utilizați pentru a evalua poziția de securitate cibernetică în IMM-uri.<br>· Cercetați sursele din care software-ul SIEM colectează jurnalele.<br>· Configurați și examinați un software SIEM open-source.<br>· Analizați indicatorii de securitate prin colectarea de jurnalele folosind software SIEM.<br>· Raportați rezultatele analizei indicatorilor de securitate cu grafice și elemente vizuale. |
| **Asigurarea calității și controlul calității**<br>• Managementul calității<br>· Standarde de calitate în securitatea cibernetică<br>· Audituri de conformitate și calitate<br>· Tehnici de testare și validare<br>· Recomandări de evaluare și îmbunătățire | 8 | 0,5 | 4 | 0,5 | **13** | **7** | · Cum ar trebui planificate procesele de asigurare a calității și de control al calității pentru a spori eficacitatea aplicațiilor de securitate cibernetică în IMM-uri? Cercetați și rezumați.<br>· Cercetați elementele de control din anexa A la ISO/IEC 27001:2022.<br>· Cercetați și raportați ce sunt tehnicile de testare și validare.<br>· Ce beneficii oferă IMM-urilor revizuirea și îmbunătățirea continuă a proceselor de calitate? |
| **Total** | **32** | **2** | **14** | **2** | **50** | **25** | |

| **Strategia de evaluare** | **Procentul de greutate comparativ** | **Criterii de evaluare** |
|---|---|---|
| Test de autoevaluare I | 10% | 10 puncte - 95-100% răspunsuri corecte |

| | |
|---|---|
| Test de autoevaluare II | 10% |
| Test de autoevaluare III | 10% |
| Test de autoevaluare IV | 10% |
| Test de evaluare a cunoștințelor | 60% |

9 puncte – 85-94 % răspunsuri corecte.
8 puncte – 75-84 % răspunsuri corecte.
7 puncte - 65-74 % răspunsuri corecte.
6 puncte – 55-64 % răspunsuri corecte.
5 puncte – 45-54 % răspunsuri corecte.
4 puncte – 35-44 % răspunsuri corecte.
3 puncte – 25-34 % răspunsuri corecte.
2 puncte – 15-24 % răspunsuri corecte.
1 puncte – 0-14 % răspunsuri corecte.

| |
|---|
| **Material de studiu** (Nume, Inițiala prenumelui, (An, Lună, Zi). Titlul articolului. Titlul revistei/jurnalului/ziarului, Numărul volumului (Numărul ediției), Numerele de pagină ale întregului articol, Editura, URL) |
| **Lectură obligatorie** |
| |
| **Lectură recomandată** |
| https://sansorg.egnyte.com/dl/RFrVIbX2oc<br>https://edwps.com/wp-content/uploads/2018/04/Cyber-PMO-U.S.-Cyber-Magazine.pdf<br>https://healthybyte.net/cybersecurity/what-is-a-security-program-management |

## 2. M2: ADMINISTRAREA SISTEMELOR

| Titlul modulului | Codul modulului |
|---|---|
| **ADMINISTRAREA SISTEMELOR** | |

| Lector (i) | Instituția sau departamentul unde se predă modulul |
|---|---|
| | |

| Modalitatea de livrare | Limba |
|---|---|
| *Față în față, online, hibrid* | *Engleză, Finlandeză, Turcă, Norvegiană, Lituaniană, Română, Franceză, Poloneză, Spaniolă* |

| Cerințe preliminare | |
|---|---|
| Nici una | None |

| Numărul de credite ECTS alocate | Volumul de muncă al studentului | Orele de lucru direct | Program de lucru individual |
|---|---|---|---|
| 3 | 75 | 50 | 25 |

| Scopul și rezultatele modulului | | |
|---|---|---|
| După finalizarea acestui curs, studenții vor fi capabili să gestioneze (identifice, analizeze, evalueze, estimeze, atenueze) continuu riscurile legate de securitatea cibernetică ale infrastructurilor, sistemelor și serviciilor TIC prin planificarea, aplicarea, raportarea și comunicarea analizei, evaluării și tratării riscurilor. Studenții vor cunoaște fundamentele rețelelor pentru a gestiona corect dispozitivele de rețea, a opera atât pe servere Linux, cât și pe servere Windows, gestionând și securizând-o. De asemenea, cunoștințele despre Cloud și AI în contextul securității cibernetice le vor fi foarte utile pentru a accelera în mod corespunzător sarcinile și a efectua automatizări și scalare. Studenții vor învăța, de asemenea, cum să consolideze sistemele, să efectueze vânătoarea de amenințări și să pună la dispoziție serverele (acronim de la triada CIA). | | |
| **Rezultatele învățării ale modulului** | **Metode de predare si invatare** | **Metode de evaluare** |
| **Cunoștințe:** Cursanții vor dobândi cunoștințe în Administrarea Rețelelor, Sisteme de Operare, Fundamentele Rețelelor, Instrumente de Administrare a Rețelelor, Securitatea Dispozitivelor de Rețea, Administrarea Sistemelor Linux, Administrarea Sistemelor Windows, Virtualizare, Cloud Computing folosind IA pentru proceduri de creare de rețele și securitate cibernetică, Proceduri de Securitate Cibernetică, Detectarea Amenințărilor, Analiza Amenințărilor, Răspunsul la Amenințări, Remedierea Amenințărilor, Fundamentele Securității Cibernetice, Apărarea Organizațiilor împotriva atacurilor, Securitatea Infrastructurii și a Rețelelor, Monitorizarea și Analiza Rețelelor, Gestionarea Incidentelor. Aceștia vor putea stabili și descrie proceduri eficiente de administrare a sistemului, rutine operaționale adaptate nevoilor specifice ale locurilor de muncă din IMM-uri în conformitate cu standardele de conformitate. | La alegere de către lector, cursuri live, înregistrări video, prezentări, dispozitive virtuale (dacă este cazul), analiză bibliografică, invitați specializați, predare și învățare între colegi, mentorat. | Teste de autoevaluare și teste de evaluare a cunoștințelor |
| **Competențe:** Cursanții vor fi abilitați în utilizarea metodologiilor și instrumentelor pentru a proiecta și implementa arhitecturi de sisteme securizate - inclusiv sisteme de operare, baze de date, rețele și infrastructuri cloud pentru locurile de muncă ale IMM-urilor. | La alegere de către lector, cursuri live, înregistrări video, prezentări, dispozitive virtuale (dacă este cazul), analiză bibliografică, invitați specializați, predare și învățare între colegi, mentorat. | Teste de autoevaluare și teste de evaluare a cunoștințelor |

| | | |
|---|---|---|
| **Competențe:** Cursanții vor fi competenți să dezvolte și să implementeze cadre strategice de securitate cibernetică pentru administrarea sistemelor, să conducă proiecte și echipe pentru a îmbunătăți consolidarea și disponibilitatea sistemelor și să ia decizii etice în menținerea unor practici robuste de securitate cibernetică în diverse domenii administrative pentru locurile de muncă ale IMM-urilor. | La alegere de către lector, cursuri live, înregistrări video, prezentări, dispozitive virtuale (dacă este cazul), analiză bibliografică, invitați specializați, predare și învățare între colegi, mentorat. | Teste de autoevaluare și teste de evaluare a cunoștințelor |

| **Conținutul modulului: defalcarea subiectelor** | **Ore de lucru direct** | | | | | **Ore de lucru și sarcini individuale** | |
|---|---|---|---|---|---|---|---|
| | Lector(i) | Consultatii | Practica | Teste | **Toate lucrările** | **Munca individuală** | **Cerințe** |
| **Administrarea sistemului de operare**<br>• Sisteme de operare<br>· Relația dintre hardware și software<br>· Binare, numărare hexazecimală<br>· Biți și octeți<br>· Linie de comandă în sistemul de operare<br>· Comenzi Windows și Linux<br>· Client și server Windows<br>· Aplicații, procese și servicii în Windows<br>· Extensii și tipuri de fișiere<br>· Chei și valori de registry<br>· Setări panou de control<br>· Utilizatori și grupuri<br>· Structura domeniului și manager de server<br>· AD și GPO<br>· Interfețe și kernel Linux<br>· Procese în Linux<br>· Convenții de denumire a fișierelor și directoarelor<br>· Shell-uri Linux și sintaxa comenzilor<br>· Manipularea fișierelor și folderelor<br>· Lucrul cu comenzi de monitorizare a conductelor și a sistemului<br>· Gestionarea proceselor și controlul joburilor<br>· Gestionarea serviciilor | 4 | 0,5 | 2 | 0,5 | **7** | **3,5** | Numărarea hexazecimală<br>Exersarea comenzilor Windows<br>Exersarea comenzilor Linux<br>Exersarea Managerului de activități<br>Crearea și gestionarea fișierelor<br>Modificarea și vizualizarea cheilor și valorilor de registry<br>Modificarea setărilor panoului de control<br>Gestionarea utilizatorilor și grupurilor<br>Gestionarea structurii domeniului<br>Crearea și ștergerea obiectelor Active Directory<br>Gestionarea proceselor în Linux<br>Manipularea fișierelor și folderelor<br>Lucrul cu Pipe<br>Comenzi de monitorizare a sistemului<br>Gestionarea serviciilor Linux |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Administrarea sistemului de baze de date**<br>· Depozite și liste de surse<br>· Gestionarea unui server web<br>· Jurnale de sistem și monitorizarea jurnalelor<br>· Programarea sarcinilor în Linux<br>· Depanarea serverului și a rețelei<br>· Copiere de rezervă și recuperare<br>· Securizarea GRUB<br>· Firewall-uri<br>· Gestionarea obiectelor Active Directory și a GPO-urilor<br>· DNS și DHCP<br>· Noțiuni fundamentale despre PowerShell<br>· Microsoft BitLocker, AppLocker și Firewall<br>· LDAP și Kerberos<br>· NTLM<br>· Politici de parolă și blocare<br>· Autentificare și control al accesului<br>· Protocolul de mesaje de control Internet (ICMP)<br>· TCP vs UDP<br>· NetBIOS și SMB<br>· SSL și TLS<br>· Certificate<br>· Protocoalele Telnet și Secure Shell (SSH)<br>· HTTP și HTTPS<br>· Protocoalele sistemelor de e-mail<br>· Protocolul sistemului de nume de domeniu (DNS)<br>· FTP și RDP<br>· Încapsulare vs. Decapsulare<br>· Sniffer-uri de rețea și Wireshark<br>· TCP/UDP<br>· DHCP, DNS | 4 | 0,5 | 2 | 0,5 | **7** | **3,5** | Gestionarea depozitelor și a listelor de surse<br>Gestionarea unui server web<br>Verificarea și gestionarea jurnalelor de sistem și a monitorizării jurnalelor<br>Planificarea sarcinilor în Linux<br>Depanarea serverului<br>Restaurarea copiilor de rezervă<br>Securizarea GRUB<br>Gestionarea serviciilor bazei de date<br>Configurarea politicilor de parolă<br>Configurarea politicilor de blocare a contului<br>Configurarea autentificării și a controlului accesului |
| **Administrarea rețelei**<br>• Tipuri de rețele și rețele wireless<br>· Rețele și topologii<br>· Dispozitive, identitate și acces<br>· Infrastructură și dispozitive de securitate<br>· Dispozitive specializate și arhitectură de rețea<br>· Rețele virtuale<br>· Adrese fizice și logice<br>· OSI și modele de rețea<br>· Încapsulare și decapsulare a datelor | 4 | 0,5 | 2 | 0,5 | **7** | **3,5** | Crearea topologiilor de rețea<br>Gestionarea dispozitivelor de rețea<br>Construirea rețelei<br>Securizarea dispozitivelor de rețea<br>Crearea rețelelor virtuale<br>Configurarea protocoalelor de rețea și a numerelor de port |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| · Protocoale de rețea și numere de port<br>· Medii și cabluri de rețea<br>· Tehnologii wireless<br>· Instrumente de administrare a rețelei<br>· Cisco Packet Tracer<br>· Clase de rețea și subrețele<br>· Protocol de rezoluție a adreselor (ARP)<br>· Adresare IP statică vs. dinamică<br>· Traducerea adreselor de rețea (NAT)<br>· Switch-uri și Cisco IOS<br>· Securitatea porturilor switch-urilor și interfețele routerului<br>· Configurarea VLAN-urilor și DTP<br>· Rutare inter-VLAN<br>· Introducere în ACL-uri<br>· Depanare rețea | | | | | | | Lucrul cu Cisco Packet TracerLucrul cu Address Resolution Protocol (ARP)<br>Planificarea unei rețele<br>Configurarea adresei IP statice și dinamice<br>Configurarea DHCP și NAT<br>Lucrul cu Cisco IOS<br>Configurarea VLAN-urilor<br>Depanarea rețelei |
| **Administrare cloud**<br>• Hypervisori și mașini virtuale<br>· Containere<br>· Securizarea mediilor virtuale<br>· Backup și recuperare<br>· Cloud Computing și CSP-uri<br>· Ce sunt modelele de servicii cloud<br>· Tipuri de implementare în cloud<br>· Rețele virtuale<br>· Servicii de calcul AWS<br>· Amazon Elastic Compute Cloud (EC2)<br>· Instrumente de monitorizare cloud<br>· Instrumente de automatizare și orchestrare<br>· Amenințări și vulnerabilități la adresa securității cloud<br>· Gestionarea identității și accesului (IAM)<br>· Controlul accesului bazat pe roluri (RBAC)<br>· Autentificare multi-factor (MFA)<br>· Criptarea datelor în cloud<br>· Cloud privat virtual (VPC)<br>· Docker și Kubernetes | 4 | 0,5 | 2 | 0,5 | **7** | **3,5** | Crearea de mașini virtuale<br>Configurarea containerelor<br>Securizarea mediilor virtuale<br>Lucrul cu copii de rezervă<br>Gestionarea rețelelor în cloud<br>Configurarea rețelelor virtuale<br>Lucrul cu instrumente de monitorizare în cloud<br>Implementarea automatizării și orchestrării<br>Detectarea amenințărilor și vulnerabilităților la adresa securității în cloud<br>Configurarea gestionării identității și accesului (IAM)<br>Implementarea criptării datelor în cloud<br>Lucrul cu Docker și Kubernetes |
| **Administrarea sistemelor cibernetice și fizice**<br>• Securitate și control al accesului<br>· Tipuri de autentificare<br>· TACACS+ și RADIUS<br>· Configurație AAA<br>· Obiective de gestionare a riscurilor<br>· Criptare și decriptare | 4 | 0,5 | 2 | 0,5 | **7** | **3,5** | Configurarea componentelor principale ale infrastructurii<br>Implementarea controalelor de securitate<br>Lucrul cu TACACS+ și RADIUS<br>Configurarea AAA |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| · Hashing și tabele Rainbow<br>· MAC Spoofing și ARP Poisoning<br>· VLAN Hopping și Rogue DHCP<br>· ICMP Flood<br>· TCP & UDP Flood<br>· Session Hijacking<br>· DNS Spoofing<br>· Defense in Depth (DID) și Zero Trust<br>· Zone Demilitarizate (DMZ)<br>· Honeypot-uri și Securizarea Rețelei<br>· Cele mai bune practici pentru o rețea securizată<br>· VPN-uri<br>· SSH și VNC<br>· Firewall-uri Stateful vs. Stateless<br>· Bazate pe gazdă vs. Bazate pe rețea<br>· Firewall-uri Hardware vs. Software<br>· Firewall pentru aplicații web (WAF)<br>· AI în firewall-uri<br>· IDS și IPS<br>· NIDS și HIDS<br>· Snort<br>· tcpdump | | | | | | | Experimentarea criptării și decriptării<br>Analiza atacurilor comune și a tehnicilor de apărare<br>Configurarea zonelor demilitarizate (DMZ)<br>Cercetarea honeypot-urilor<br>Consolidarea securității prin intermediul celor mai bune practici pentru o rețea securizată<br>Instalarea VPN<br>Lucrul cu Secure Shell (SSH)<br>Lucrul cu Virtual Network Computing (VNC)<br>Tehnici de lucru cu firewall-uri<br>Implementarea inteligenței artificiale în firewall-uri<br>Utilizarea Snort și tcpdump pentru protecție și detectare |
| **Consolidarea sistemului**<br>• **T**ehnici GenAI<br>· Generare de cod<br>· Gestionarea conturilor de utilizator și controlul accesului<br>· Detectarea anomaliilor și depanarea problemelor<br>· Rezolvarea erorilor serviciului Apache2<br>· Gestionarea și actualizările patch-urilor<br>· Copiere de rezervă și recuperare automată<br>· Gestionarea și inventarierea activelor IT<br>· Recuperarea fișierelor șterse cu GenAI<br>· Proceduri de securitate cibernetică<br>· Detectarea și analiza amenințărilor<br>· Răspunsul și remedierea amenințărilor<br>· Utilizarea inteligenței artificiale pentru detectarea amenințărilor în timp real<br>· Validarea și testarea modelelor GenAI<br>· Guvernanță și cadre de reglementare<br>· Configurarea și securitatea DNS<br>· Configurarea și securitatea DHCP<br>· Fundamentele PowerShell<br>· Securitatea porturilor de comutare<br>· Sistem de bază de intrare/ieșire a rețelei (NetBIOS)<br>· Protocolul Server Message Block (SMB) | 4 | 0,5 | 2 | 0,5 | **7** | **3,5** | Lucrul cu tehnici GenAI<br>Gestionarea conturilor de utilizator și controlul accesului<br>Detectarea și depanarea anomaliilor<br>Rezolvarea erorilor serviciului Apache2 cu GenAI<br>Configurarea gestionării patch-urilor și a actualizărilor<br>Configurarea backup-ului și recuperării automate<br>Gestionarea activelor IT<br>Recuperarea fișierelor șterse cu GenAI<br>Implementarea securității DNS și DHCP<br>Lucrul cu Microsoft BitLocker și Microsoft AppLocker<br>Configurarea paravanului de protecție Microsoft<br>Configurarea securității porturilor de comutare |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| · Secure Sockets Layer (SSL) și Transport Layer Security (TLS)<br>· Certificate de securitate<br>· Protocoale ale sistemelor de e-mail<br>· Domain Name System Protocol (DNS)<br>· File Transfer Protocol (FTP)<br>· Remote Desktop Protocol (RDP)<br>· Programarea sarcinilor în Linux<br>· Depanarea serverului<br>· Depanarea rețelei<br>· Copiere de rezervă și recuperare<br>· Securizarea GRUB<br>· Configurarea și securizarea firewall-urilor | | | | | | | Securizarea protocolului de transfer de fișiere (FTP)<br>Securizarea protocolului Protocolul Desktop la distanță (RDP)<br>Planificarea sarcinilor de securitate în Linux<br>Securizarea GRUB<br>Configurarea și securizarea firewall-urilor (iptables) |
| Disponibilitate<br>· IR vs. SOC<br>· Evenimente și incidente<br>· Detectarea alertelor și triajul alertelor<br>· Documentație și raportare<br>· Ce sunt atacurile web?<br>· DoS și DDoS<br>· Injecție SQL și XSS<br>· Injecție de comenzi și includere locală de fișiere (LFI)<br>· Falsificarea cererilor între site-uri (CSRF)<br>· Forță brută și umplerea credențialelor<br>· Transmiterea hash-ului și transmiterea tichetului<br>· Recunoaștere LDAP<br>· Controlul accesului defectat<br>· Ransomware<br>· Virus și viermi informatici<br>· Cal troian și adware<br>· Keylogger și Cryptojacking<br>· Malware fără fișiere<br>· Înțelegerea răspândirii malware-ului<br>· Analiza malware statică și dinamică<br>· Analiza malware sigură<br>· Analiză hibridă Investigarea malware-ului<br>· Efectuarea analizei malware statice și dinamice<br>· Gestionarea IOC-urilor și a politicilor de parolă<br>· Politici de utilizare acceptabilă (AUP)<br>· Politici de tip „Adu-ți propriul dispozitiv” (BYOD)<br>· Politici de acces la distanță | 4 | 0,5 | 3 | 0,5 | **8** | **4** | Detectarea evenimentelor și incidentelor<br>Efectuarea triajului alertelor<br>Întocmirea documentației și raportarea corespunzătoare<br>Implementarea activităților post-incident<br>Efectuarea și protejarea împotriva DoS și DDoS<br>Detectarea atacurilor web și a răspândirii programelor malware<br>Efectuarea analizei statice și dinamice sigure a programelor malware<br>Gestionarea IOC-urilor<br>Configurarea politicilor de parolă<br>Configurarea politicilor „Bring Your Own Device” (BYOD)<br>Configurarea politicilor de acces la distanță |
| **Total** | **28** | **3,5** | **15** | **3,5** | **50** | **25** | |

| Strategia de evaluare | Procentul de greutate comparativ | Criterii de evaluare |
|---|---|---|
| Test de autoevaluare (1) | 5% | 10 puncte - 95-100% răspunsuri corecte. |
| Test de autoevaluare (2) | 5% | 9 puncte – 85-94 % răspunsuri corecte. |
| Test de autoevaluare (3) | 5% | 8 puncte – 75-84 % răspunsuri corecte. |
| Test de autoevaluare (4) | 5% | 7 puncte - 65-74 % răspunsuri corecte. |
| Test de autoevaluare (5) | 5% | 6 puncte – 55-64 % răspunsuri corecte. |
| Test de autoevaluare (6) | 5% | 5 puncte – 45-54 % răspunsuri corecte. |
| Test de autoevaluare (7) | 5% | 4 puncte – 35-44 % răspunsuri corecte. |
| Test de evaluare a cunoștințelor | 65% | 3 puncte – 25-34 % răspunsuri corecte. |
| | | 2 puncte – 15-24 % răspunsuri corecte. |
| | | 1 puncte – 0-14 % răspunsuri corecte. |

## 3. M3: INSTRUMENTE ANALITICE

| Titlul modulului | Codul modulului |
|---|---|
| **INSTRUMENTE ANALITICE** | |

| Lector (i) | Instituția sau departamentul unde se predă modulul |
|---|---|
| | |

| Modalitatea de livrare | Limba |
|---|---|
| *Față în față, online, hibrid* | *Engleză, Finlandeză, Turcă, Norvegiană, Lituaniană, Română, Franceză, Poloneză, Spaniolă* |

| Cerințe preliminare |
|---|
| Nici una |

| Numărul de credite ECTS alocate | Volumul de muncă al studentului | Orele de lucru direct | Program de lucru individual |
|---|---|---|---|
| 3 | 75 | 50 | 25 |

| Scopul și rezultatele modulului | | |
|---|---|---|
| După finalizarea acestui curs, studenții vor dobândi abilitățile necesare pentru a proteja activele organizaționale utilizând indicatori de performanță, analiză de date și informații de securitate. Vor învăța să aplice eficient instrumente analitice pentru a identifica potențialele riscuri și vulnerabilități de securitate cibernetică, să utilizeze informații bazate pe date pentru a îmbunătăți măsurile de securitate și să utilizeze indicatori de performanță legați de parole, utilizarea browserului, e-mail și aplicații de procesare a datelor. Până la sfârșitul modulului, participanții vor putea evalua și atenua potențialele amenințări de securitate utilizând instrumente adecvate și vor raporta orice amenințări sau perturbări către canalele de reglementare corecte. | | |
| **Rezultatele învățării ale modulului** | **Metode de predare si invatare** | **Metode de evaluare** |
| **Cunoștințe:** Cursanții vor dobândi cunoștințe practice despre cum să aplice măsurătorile de performanță, analiza datelor și informațiile de securitate pentru a proteja activele organizației. | A se selecta de către lector, din Partea 1.3. [Metode de predare, de exemplu, prelegeri teoretice, invitați, chestionare, jocuri, sarcini practice/laboratoare, predare și învățare reciprocă, învățare autoghidată etc.] din D2.3 „Structura căii de învățare pentru agenții schimbării în domeniul securității cibernetice pentru IMM-uri” | Teste de autoevaluare<br>Test de evaluare a cunoștințelor |
| **Competențe:** Cursanții vor fi pricepuți să utilizeze instrumente analitice pentru a identifica potențialele riscuri și vulnerabilități de securitate cibernetică, să aplice informații bazate pe date pentru a consolida practicile de securitate cibernetică și să utilizeze indicatori de performanță pentru a evalua și îmbunătăți securitatea parolelor, a navigării, a e-mailului și a gestionării datelor. | A se selecta de către lector, din Partea 1.3. [Metode de predare, de exemplu, sarcini practice/laboratoare, activități practice, medii simulate, chestionare, jocuri, studii de caz etc.] din D2.3 „Structura căii de învățare pentru agenții schimbării în domeniul securității cibernetice pentru IMM-uri” | Evaluări practice |
| **Competențe:** Cursanții vor fi competenți în evaluarea și atenuarea potențialelor amenințări de securitate utilizând instrumente analitice, raportând cu precizie amenințările și încălcările de securitate către canalele corespunzătoare din cadrul organizației lor. | A se selecta de către lector, din Partea 1.3. [Metode de predare, de exemplu, medii simulate, concursuri de capturare a steagului, 5E-uri, CBL, CL, POGIL, PBL etc.] din D2.3 „Structura căii de învățare pentru agenții schimbării în domeniul securității cibernetice pentru IMM-uri” | Simulări<br>Competiții |

| Conținutul modulului: defalcarea subiectelor | Ore de lucru direct | | | | | Ore de lucru și sarcini individuale | |
|---|---|---|---|---|---|---|---|
| | Lector(i) (învățământ | Consultatii | Practica (învățământ | Teste | **Lucru direct** | **Munca individuală** | **Cerințe** |
| **Măsurători de performanță (metrici)**<br>• Indicatori de performanță<br>· Monitorizare sistem și rețea<br>· Monitorizare indicatori de performanță<br>· Mapare rețea<br>· Scanare vulnerabilități<br>· Analiza traficului de rețea | 10 | 0,5 | 5 | 0,5 | **16** | **8,5** | · Efectuați cercetări privind indicatorii și instrumentele de performanță. Comparați instrumentele de monitorizare a performanței și identificați diferențele dintre acestea.<br>· Finalizați instalarea Zabbix și efectuați configurația de bază.<br>· Creați o aplicație pentru a monitoriza indicatorii de performanță cu Zabbix.<br>· Identificați vulnerabilitățile din sistemul țintă folosind software de mapare a rețelei (cum ar fi nmap, rustscan etc.).<br>· Efectuați o scanare a vulnerabilităților pe sistemul țintă folosind software-ul Nessus. Pregătiți un raport de testare a vulnerabilităților.<br>· Efectuați analiza traficului de rețea folosind Wireshark. |
| **Analiza datelor**<br>• Colectarea datelor<br>· Curățarea și preprocesarea datelor<br>· Analiza datelor<br>· Vizualizarea datelor<br>· Instrumente analitice<br>· Aplicații ale analizei datelor în securitatea cibernetică | 10 | 0,5 | 5 | 0,5 | **16** | **8,5** | · Efectuați pași de curățare și preprocesare a datelor pe un set de date legate de probleme de securitate cibernetică pregătit pentru un SME ipotetic.<br>· Analizați setul de date curățat și preprocesat din SME ipotetic și vizualizați rezultatele.<br>· Care sunt exemple de aplicații de analiză a datelor în domeniul securității cibernetice? Vă rugăm să cercetați. |
| **Informații de Securitate** | 10 | 0,5 | 7 | 0,5 | **18** | **8** | · Investigați modul în care informațiile de securitate |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| • Înțelegerea informațiilor de securitate<br>• Surse de informații de securitate<br>• Metode de colectare a informațiilor despre amenințări<br>• Cadre de informații despre amenințări<br>• Platforme de informații de securitate bazate pe inteligență artificială<br>• Studii de caz privind aplicațiile de informații de securitate | | | | | | | contribuie la strategiile proactive de securitate ale IMM-urilor.<br>• Care sunt cele mai comune surse pentru obținerea de informații de securitate? Cum evaluați fiabilitatea acestor surse?<br>• Definiți avantajele și limitele fiecărei metode de colectare a informațiilor despre amenințări.<br>• Explicați caracteristicile principale ale cadrelor de colectare a informațiilor despre amenințări, cum ar fi MI-TRE ATT&CK și Cyber Kill Chain.<br>• Examinați un studiu de caz real în care au fost utilizate informațiile de securitate. Descrieți metodele de colectare a informațiilor utilizate în studiul de caz respectiv. |
| **Total** | **30** | **1,5** | **17** | **1,5** | **50** | **25** | |

| Strategia de evaluare | Procentul de greutate comparativ | Criterii de evaluare |
|---|---|---|
| Test de autoevaluare I | 15% | 10 puncte - 95-100% răspunsuri corecte.<br>9 puncte – 85-94 % răspunsuri corecte.<br>8 puncte – 75-84 % răspunsuri corecte.<br>7 puncte - 65-74 % răspunsuri corecte.<br>6 puncte – 55-64 % răspunsuri corecte.<br>5 puncte – 45-54 % răspunsuri corecte.<br>4 puncte – 35-44 % răspunsuri corecte.<br>3 puncte – 25-34 % răspunsuri corecte.<br>2 puncte – 15-24 % răspunsuri corecte.<br>1 puncte – 0-14 % răspunsuri corecte. |
| Test de autoevaluare II | 15% | |
| Test de autoevaluare III | 15% | |
| Test de evaluare a cunoștințelor | 55% | |

| **Material de studiu** (Nume, Inițiala prenumelui, (An, Lună, Zi). Titlul articolului. Titlul revistei/jurnalului/ziarului, Numărul volumului (Numărul ediției), Numerele de pagină ale întregului articol, Editura, URL) |
|---|
| **Lectură obligatorie** |
| ... |
| **Lectură recomandată** |
| **https://brainstation.io/career-guides/what-tools-do-cybersecurity-analysts-use**<br>**https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it**<br>**https://medium.com/@jcm3/wireshark-traffic-analysis-part-1-tryhackme-walkthrough-a9bec11d94d9**<br>**https://www.kali.org/tools/nmap/**<br>**https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/**<br>**https://www.varonis.com/blog/cyber-kill-chain**<br>**https://www.youtube.com/watch?v=kVnvIBNiC58** |

# 4. M4: OPERAȚIUNI DE SECURITATE

| Titlul modulului | Codul modulului |
|---|---|
| **OPERAȚIUNI DE SECURITATE** | |

| Lector (i) | Instituția sau departamentul unde se predă modulul |
|---|---|
| | |

| Modalitatea de livrare | Limba |
|---|---|
| *Față în față, online, hibrid* | *Engleză, Finlandeză, Turcă, Norvegiană, Lituaniană, Română, Franceză, Poloneză, Spaniolă* |

| Cerințe preliminare |
|---|
| Nici una |

| Numărul de credite ECTS alocate | Volumul de muncă al studentului | Orele de lucru direct | Program de lucru individual |
|---|---|---|---|
| 3 | 75 | 50 | 25 |

| Scopul și rezultatele modulului | | |
|---|---|---|
| După finalizarea acestui curs, studenții vor putea gestiona eficient operațiunile de securitate în cadrul infrastructurilor, sistemelor și serviciilor TIC. Vor dobândi abilitățile de a monitoriza, detecta, răspunde și recupera după incidentele de securitate cibernetică, aplicând cele mai bune practici, instrumente și cadre relevante pentru operațiunile de securitate. | | |
| **Rezultatele învățării ale modulului** | **Metode de predare si invatare** | **Metode de evaluare** |
| **Cunoștințe:** Cursanții vor dobândi cunoștințe avansate despre operațiunile de securitate, inclusiv monitorizarea, detectarea, răspunsul la incidente și recuperarea. Vor putea stabili și descrie rutine operaționale eficiente de securitate cibernetică, adaptate nevoilor specifice ale locurilor de muncă ale IMM-urilor, în conformitate cu standardele de securitate cibernetică. | A se selecta de către lector, din Partea 1.3. [Metode de predare, de exemplu, prelegeri teoretice, analiză a literaturii de specialitate, invitați, predare și învățare reciprocă, mentorat etc.] din D2.3 „Structura căii de învățare pentru agenții schimbării în domeniul securității cibernetice pentru IMM-uri” | Teste de autoevaluare<br>Test de evaluare a cunoștințelor |

| | | |
|---|---|---|
| **Competențe:** Cursanții vor dobândi competențe în aplicarea metodologiilor și instrumentelor avansate pentru a îndeplini sarcini operaționale de securitate, a proiecta și implementa strategii eficiente de monitorizare, a desfășura activități de răspuns la incidente și a dezvolta rutine operaționale robuste, special adaptate pentru locurile de muncă ale IMM-urilor. | A se selecta de către lector, din Partea 1.3. [Metode de predare, de exemplu, prelegeri teoretice, analiză a literaturii de specialitate, invitați, predare și învățare reciprocă, mentorat etc.] din D2.3 „Structura căii de învățare pentru agenții schimbării în domeniul securității cibernetice pentru IMM-uri” | Teste de autoevaluare<br>Test de evaluare a cunoștințelor |
| **Competențe:** Cursanții vor fi competenți în dezvoltarea și implementarea politicilor și procedurilor strategice de operațiuni de securitate pentru locurile de muncă ale IMM-urilor. | A se selecta de către lector, din Partea 1.3. [Metode de predare, de exemplu, prelegeri teoretice, analiză a literaturii de specialitate, invitați, predare și învățare reciprocă, mentorat etc.] din D2.3 „Structura căii de învățare pentru agenții schimbării în domeniul securității cibernetice pentru IMM-uri” | Teste de autoevaluare<br>Test de evaluare a cunoștințelor |

| **Conținutul modulului: defalcarea subiectelor** | **Ore de lucru direct** | | | | | **Ore de lucru și sarcini individuale** | |
|---|---|---|---|---|---|---|---|
| | Lector(i) (învățământ | Consultatii | Practica (învățământ | Teste | **Lucru direct** | **Munca individuală** | **Cerințe** |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Noțiuni fundamentale despre operațiunile de securitate**<br>- Înțelegerea operațiunilor de securitate și a SOC (Centrul de operațiuni de securitate)<br>- Roluri și responsabilități în operațiunile de securitate<br>- Prezentare generală a instrumentelor și tehnologiilor pentru operațiunile de securitate | 6 | 0,5 | 2 | 0,5 | **9** | 6 | Identificarea și înțelegerea structurii și funcției unui SOC, analizarea diverselor roluri în cadrul operațiunilor de securitate, cercetarea instrumentelor utilizate în operațiunile de securitate și analizarea unui studiu de caz. |
| **Convergența securității**<br>- Înțelegerea convergenței securității<br>- Fundamentele securității fizice (principii de securitate fizică, protejarea activelor fizice, politici)<br>- Studiu de caz care evidențiază principiile convergenței securității | 8 | 0,5 | 4 | 0,5 | **13** | 6 | Revizuirea definiției și principiilor convergenței securității, recunoașterea importanței integrării operațiunilor de securitate fizică și digitală, identificarea și evaluarea riscurilor în domeniile cibernetice și fizice. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Managementul informațiilor și evenimentelor de securitate**<br>- Revizuirea principiilor de monitorizare a securității<br>- Implementarea soluțiilor SIEM | 8 | 0,5 | 4 | 0,5 | **13** | 6 | Introducere în monitorizarea securității și implementarea SIEM. Principii de bază, cum ar fi tipurile de jurnale, metodele de detectare și ciclul de viață al monitorizării. Aspecte practice ale implementării unui SIEM, inclusiv arhitectura, colectarea datelor, crearea de reguli și gestionarea alertelor. |
| **Practici de operațiuni de securitate**<br>**-** Identificarea surselor de date și optimizarea colectării jurnalelor<br>- Centralizarea alertelor cu SIEM<br>- Testarea SIEM-ului | 4 | 0,5 | 10 | 0,5 | **15** | 7 | Program de instruire cuprinzător și orientat spre practică, cu cunoștințe esențiale și abilități practice în gestionarea jurnalelor, configurarea SIEM și detectarea amenințărilor în diverse medii IT. |
| **Total** | **26** | **2** | **20** | **2** | **50** | **25** | |

| **Strategia de evaluare** | **Procentul de greutate comparativ** | **Criterii de evaluare** |
|---|---|---|
| Test de autoevaluare (1) | 10% | 10 puncte - 95-100% răspunsuri corecte.<br>9 puncte – 85-94 % răspunsuri corecte.<br>8 puncte – 75-84 % răspunsuri corecte.<br>7 puncte - 65-74 % răspunsuri corecte.<br>6 puncte – 55-64 % răspunsuri corecte.<br>5 puncte – 45-54 % răspunsuri corecte.<br>4 puncte – 35-44 % răspunsuri corecte.<br>3 puncte – 25-34 % răspunsuri corecte.<br>2 puncte – 15-24 % răspunsuri corecte.<br>1 puncte – 0-14 % răspunsuri corecte. |
| Test de autoevaluare (2) | 10% | |
| Test de autoevaluare (3) | 10% | |
| Test de autoevaluare (4) | 10% | |
| Test de evaluare a cunoștințelor | 60% | |

| |
|---|
| **Material de studiu** (Nume, Inițiala prenumelui, (An, Lună, Zi). Titlul articolului. Titlul revistei/jurnalului/ziarului, Numărul volumului (Numărul ediției), Numerele de pagină ale întregului articol, Editura, URL) |
| **Lectură obligatorie** |
| Cybellium (2024). *Ghid de studiu pentru Centrele de Operațiuni de Securitate (SOC): Un ghid cuprinzător pentru a învăța despre Centrele de Operațiuni de Securitate (SOC)*<br>Muniz, J. (2021). *Centrul de Operațiuni de Securitate Modernă*. Pearson Education.<br>ENISA (2017). *Strategii pentru răspunsul la incidente și cooperarea în caz de crize cibernetice.* ***Strategii pentru răspunsul la incidente și cooperarea în caz de crize cibernetice — ENISA (europa.eu)*** |
| **Lectură recomandată** |
| Basta, A., Basta, N., Anwar, W., Essar, M. I. (2024). Centrul de operațiuni de securitate (SOC) open-source: un ghid complet pentru stabilirea, gestionarea și întreținerea unui SOC modern.<br>Cybellium (2023). Gestionarea unui centru de operațiuni de securitate (SOC). |

# 5. M5: GUVERNANȚĂ ȘI POLITICĂ DE SECURITATE

| Titlul modulului | Codul modulului |
|---|---|
| **GUVERNANȚĂ ȘI POLITICĂ DE SECURITATE** | |

| Lector (i) | Instituția sau departamentul unde se predă modulul |
|---|---|
| | |

| Modalitatea de livrare | Limba |
|---|---|
| *Față în față, online, hibrid* | *Engleză, Finlandeză, Turcă, Norvegiană, Lituaniană, Română, Franceză, Poloneză, Spaniolă* |

| Cerințe preliminare |
|---|
| Nici una |

| Numărul de credite ECTS alocate | Volumul de muncă al studentului | Orele de lucru direct | Program de lucru individual |
|---|---|---|---|
| 3 | 75 | 50 | 25 |

**Scopul și rezultatele modulului**

Tema „Guvernanță și Politică de Securitate" își propune să pregătească studenții pentru a face față provocărilor legate de securitatea cibernetică în IMM-uri, integrând guvernanța securității în strategia de afaceri și asigurând conformitatea cu reglementările legale, cum ar fi GDPR. Modulul acoperă aspecte precum identificarea amenințărilor și vulnerabilităților, proiectarea unor politici de securitate robuste și adaptive și gestionarea eficientă a incidentelor. În plus, se concentrează pe dezvoltarea unor structuri de guvernanță care atribuie roluri clare în cadrul organizației, aliniind securitatea cibernetică cu obiectivele strategice. Studenții vor dobândi competențe tehnice în evaluarea și atenuarea riscurilor cibernetice și vor dezvolta abilități de analiză pentru a propune îmbunătățiri în maturitatea securității. De asemenea, vor deveni abili în comunicarea eficientă a nevoilor de securitate cibernetică către directori, sprijinind luarea deciziilor informate și asigurând conformitatea cu reglementările și etica în domeniul securității cibernetice. Modulul „Guvernanță și Politică de Securitate" include, de asemenea, o examinare concentrată a prevenirii phishing-ului, a atacurilor cibernetice bazate pe inteligență artificială și a gestionării ransomware-ului, analizând modul în care aceste amenințări specifice necesită o abordare integrată a guvernanței și conformității. Eficacitatea politicilor de securitate nu va fi măsurată doar prin capacitatea lor de a preveni incidentele, ci și prin adaptabilitatea lor la amenințările emergente și conformitatea cu reglementările legale actuale.

| Rezultatele învățării ale modulului | Metode de predare si invatare | Metode de evaluare |
|---|---|---|
| **Cunoștințe:** Cursanții vor dobândi cunoștințe avansate despre cum să implementeze | **Prelegeri (lecturi dirijate):** Prelegerile vor oferi o bază conceptuală solidă în domeniul securității cibernetice, guvernanței, confidențialității și | **Teste de autoevaluare:** Autotestele permit studenților să își evalueze înțelegerea fiecărei |

| | | |
|---|---|---|
| noi rutine și fluxuri de lucru în domeniul securității cibernetice în cadrul IMM-urilor, încorporând principiile actuale în domeniul securității cibernetice, tendințele și conformitatea cu legislația națională și internațională relevantă pentru industria lor.<br><br>Dobândește cunoștințe avansate despre cum să integreze prevenirea phishing-ului, să gestioneze amenințările generate de inteligența artificială și să răspundă la ransomware în mediile IMM-urilor. | conformității, încurajând participarea activă a studenților.<br><br>Include prelegeri interactive care încorporează sesiuni regulate de întrebări și răspunsuri, sondaje și exerciții live de rezolvare a problemelor. Folosind instrumente precum Mentimeter și Poll Everywhere.<br><br>**Participarea la discuții și forumuri:** Participarea la discuții și forumuri va permite studenților să dezbată și să analizeze critic problemele de securitate cibernetică, dezvoltându-le abilitățile argumentative. Aceasta va fi aplicată problemelor legate de etică, politici și luarea deciziilor în domeniul securității cibernetice.<br><br>**Studii de caz:** Studiile de caz vor permite studenților să analizeze situații de securitate cibernetică în IMM-uri, aplicând cunoștințe teoretice pentru a rezolva probleme reale. Acestea se vor concentra pe subiecte precum gestionarea încălcărilor de date, ransomware, phishing, atacuri bazate pe inteligență artificială, implementarea politicilor de securitate și guvernanță. | subteme printr-o varietate de întrebări, oferind feedback continuu pentru a identifica domeniile de îmbunătățire. Acestea nu afectează nota finală, dar sunt esențiale pentru învățarea autonomă.<br><br>**Examen final (opțional):** Examenul final este opțional și permite studenților să obțină un certificat de absolvire prin evaluarea înțelegerii generale a cursului prin întrebări de dezvoltare, analiză de caz și răspunsuri multiple. Promovarea acestuia este necesară pentru obținerea certificatului de absolvire, iar cei care nu îl susțin vor primi un certificat de participare. |
| **Competențe:** Cursanții vor dobândi competențe în utilizarea metodologiilor avansate pentru a efectua evaluări ale riscurilor, a proiecta și implementa noi rutine de securitate cibernetică și a pregăti strategii de răspuns, asigurând o guvernanță eficientă și conformitate în cadrul locurilor de muncă ale IMM-urilor. | **Ateliere practice:** Atelierele practice vor permite studenților să aplice concepte de securitate cibernetică prin exerciții precum dezvoltarea de politici și simulări de incidente, cu feedback în timp real din partea instructorului. Acestea sunt concepute pentru a consolida abilitățile practice și a pregăti studenții să aplice ceea ce au învățat în situații reale.<br><br>**Lucrări practice și proiecte individuale:** Lucrările practice și proiectele individuale vor permite | **Evaluări practice:** Evaluările practice pe parcursul cursului vor permite studenților să aplice cunoștințele teoretice în situații simulate, cum ar fi dezvoltarea politicilor de securitate cibernetică și simulările de incidente, cu obiectivul de a evalua capacitatea lor de a rezolva probleme reale în contextul |

| | | |
|---|---|---|
| Va dezvolta abilități în proiectarea și implementarea unor rutine complete de securitate cibernetică care să abordeze amenințările **avansate și să asigure conformitatea organizațională.** | studenților să aplice concepte de securitate cibernetică prin sarcini precum redactarea de politici și analiza riscurilor, dezvoltarea abilităților de lucru autonom și aplicarea practică a cunoștințelor teoretice.<br><br>**Proiecte de colaborare:** Proiectele de colaborare vor permite studenților să lucreze în echipe pentru a dezvolta soluții de securitate cibernetică pentru IMM-uri, inclusiv politici de securitate și modele de guvernanță. Acestea vor încuraja munca în echipă, managementul de proiect și aplicarea practică a cunoștințelor dobândite, cu feedback din partea profesorilor și a colegilor. | IMM-urilor.<br><br>**Proiecte de grup:** Proiectele de grup vor permite studenților să dezvolte un proiect cuprinzător de securitate cibernetică, de la identificarea riscurilor până la propunerea de modele de guvernanță și planuri de răspuns la incidente, evaluând atât calitatea conținutului, cât și capacitatea de colaborare. Acest proiect este esențial pentru evaluarea finală și integrează toate cunoștințele din curs. |
| **Competențe:** Cursanții vor fi competenți în dezvoltarea și implementarea politicilor strategice de securitate cibernetică, conducerea inițiativelor de stabilire a unor noi rutine și fluxuri de lucru la locul de muncă al IMM-urilor și luarea unor decizii etice care să se alinieze cu obiectivele organizației și cerințele de conformitate.<br><br>Deveniți competenți în formularea și executarea politicilor de securitate cibernetică care previn amenințările cibernetice sofisticate și asigură conformitatea cu reglementările internaționale de securitate cibernetică. | **Simulări de scenarii:** Simulările de scenarii vor permite studenților să gestioneze incidentele de securitate cibernetică în medii virtuale care reproduc atacuri reale, luând decizii strategice sub presiune. Această metodă îmbunătățește abilitățile de gestionare a crizelor și de răspuns la incidente și este esențială pentru predarea evaluării politicilor de securitate și a luării deciziilor în situații critice.<br><br>Studenții vor trebui să demonstreze cum ar aplica politicile de guvernanță pentru a preveni sau a răspunde la incidente specifice, cum ar fi atacurile de phishing, ransomware și atacurile bazate pe inteligență artificială; evaluându-le înțelegerea cadrului de reglementare relevant. | **Simulări și Managementul Incidentelor:** Studenții vor fi evaluați în funcție de capacitatea lor de a gestiona incidente de securitate cibernetică în simulări care reproduc crize reale într-o IMM. Obiectivul este de a măsura capacitatea lor de a gestiona presiunea, de a lua decizii strategice și de a executa planuri de răspuns în timp real, evaluând aplicarea lor practică în situații dinamice. |

| Conținutul modulului: defalcarea subiectelor | Ore de lucru direct | | | | | Ore de lucru și sarcini individuale | |
|---|---|---|---|---|---|---|---|
| | Lector(i) (învățământ | Consultatii | Practica (învățământ | Teste | **Lucru direct** | **Munca individuală** | **Cerințe** |
| **Context organizațional**<br>- Evoluția securității cibernetice în IMM-uri<br>- Principalele amenințări și vulnerabilități actuale<br>- Impactul securității cibernetice asupra strategiei de afaceri<br>- Provocările specifice securității cibernetice în IMM-uri față de întreprinderile mari<br>- Înțelegerea implicațiilor de reglementare ale practicilor de securitate cibernetică și a modului în care acestea se aliniază cu structurile de guvernanță.<br>- Provocările comune în domeniul securității cibernetice specifice IMM-urilor, cum ar fi bugetele limitate, lipsa personalului de securitate dedicat și metodele practice de prioritizare a investițiilor în securitate cibernetică. | 5 | 0,5 | 3 | 0,5 | **9** | **4** | Citire, cercetare, pregătire studii de caz |
| **Confidențialitate**<br>- Principii de confidențialitate în securitatea cibernetică<br>- Protecția datelor cu caracter personal și GDPR<br>- Impactul confidențialității asupra operațiunilor IMM-urilor<br>- Instrumente și tehnici pentru protejarea confidențialității | 4 | 0,5 | 3 | 0,5 | **8** | **4** | Analiză de politici, sarcină individuală |
| **Legi, etică și conformitate**<br>- Organizații, politici și standarde de securitate cibernetică<br>- Legislație națională și internațională relevantă<br>- Conformitatea cu reglementările în IMM-uri<br>- Etica în securitatea cibernetică<br>- Consecințele juridice ale neconformității în domeniul securității cibernetice<br>- Analiza modului în care instrumentele bazate pe inteligență artificială pot fi utilizate pentru a consolida guvernanța securității cibernetice și a asigura conformitatea prin monitorizare continuă și răspuns automat la amenințări. | 5 | 0,5 | 3 | 0,5 | **9** | **5** | Studiu de caz, analiză legislativă |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Guvernanța securității**<br>- Structura guvernanței securității cibernetice<br>- Roluri și responsabilități în managementul securității<br>- Modele de maturitate în domeniul securității cibernetice<br>- Integrarea securității cibernetice în guvernanța corporativă<br>- Îmbunătățirea abilităților de efectuare a evaluărilor de risc și de formulare a planurilor strategice de răspuns în condiții de criză simulate (ransomware, atac de phishing, ...) | 4 | 0,5 | 3 | 0,5 | **8** | **4** | Analiza scenariilor de management al riscului |
| **Comunicare la nivel executiv și la nivel de consiliu de administrație**<br>- Strategii de comunicare în domeniul securității cibernetice<br>- Raportare privind securitatea către managementul superior<br>- Luarea deciziilor pe baza datelor de securitate<br>- Managementul crizelor și comunicarea în domeniul securității cibernetice<br>- Stăpânirea abilităților de gestionare a crizelor și de luare a deciziilor în scenarii cu stres ridicat care implică atacuri bazate pe inteligență artificială și ransomware. | 4 | 0,5 | 3 | 0,5 | **8** | **4** | Pregătirea prezentării, comunicarea cu părțile interesate |
| **Politică managerială**<br>- Dezvoltarea politicilor de securitate<br>- Implementarea și monitorizarea politicilor<br>- Evaluarea și îmbunătățirea continuă a politicilor<br>- Adaptarea politicilor de securitate la schimbările tehnologice și de reglementare<br>- Explorarea modului în care politicile eficiente de instruire și conștientizare pot fi o componentă crucială a conformității cu reglementările și a atenuării riscurilor. | 4 | 0,5 | 3 | 0,5 | **8** | **4** | Redactarea și revizuirea unui document de politici |
| **Total** | **26** | **3** | **18** | **3** | **50** | **25** | |

| **Strategia de evaluare** | **Procentul de greutate comparativ** | **Criterii de evaluare** |
|---|---|---|
| Autotestare I | 10% | Evaluarea conceptelor fundamentale privind contextul organizațional. |
| Autotestare II | 10% | Evaluarea conceptelor fundamentale privind confidențialitatea. |
| Autotestare III | 10% | Evaluarea legilor, eticii și politicilor de conformitate. |
| Autotestare IV | 10% | Evaluarea politicilor de securitate cibernetică. |

| | | |
|---|---|---|
| Autotestare V | 10% | Evaluarea comunicării la nivel executiv. |
| Autotestare VI | 10% | Evaluarea politicilor manageriale și crearea de politici în domeniul securității. |
| Test de evaluare a cunoștințelor | 40% | Examen final care acoperă întrebări integrative pe toate temele cursului. |

10 points - 95-100% răspunsuri corecte.
9 points – 85-94 % răspunsuri corecte.
8 points – 75-84 % răspunsuri corecte.
7 points - 65-74 % răspunsuri corecte.
6 points – 55-64 % răspunsuri corecte.
5 points – 45-54 % răspunsuri corecte.
4 points – 35-44 % răspunsuri corecte.
3 points – 25-34 % răspunsuri corecte.
2 points – 15-24 % răspunsuri corecte.
1 points – 0-14 % răspunsuri corecte.

**Material de studiu** (Nume, Inițiala prenumelui, (An, Lună, Zi). Titlul articolului. Titlul revistei/jurnalului/ziarului, Numărul volumului (Numărul ediției), Numerele de pagină ale întregului articol, Editura, URL)

**Lectură obligatorie**

...

**" „Legislația UE în domeniul securității cibernetice: Guvernarea rezilienței și coerenței în era digitală”,** de Luisa Marin

- Această carte oferă o analiză aprofundată a legilor și politicilor UE în domeniul securității cibernetice, crucială pentru înțelegerea modului în care guvernanța securității cibernetice este structurată și implementată în contextul UE.

**„Securitatea cibernetică în Uniunea Europeană: Reziliență și adaptabilitate în politica de guvernanță”,** de George Christou

- Această carte explorează cadrele de guvernanță și procesele de elaborare a politicilor pentru securitatea cibernetică în cadrul UE, ajutând studenții să înțeleagă interacțiunea dinamică dintre diferitele niveluri de guvernanță.

**„Phishing și contramăsuri: Înțelegerea problemei tot mai mari a furtului de identitate electronică”** de Markus Jakobsson și Steven Myers

- Deși nu este specifică UE, explorarea detaliată a tehnicilor de phishing și a contramăsurilor din această carte poate fi contextualizată în cadrul UE, concentrându-se pe conformitatea cu GDPR și principiile de protecție a datelor.

**„Legislația și reglementarea europeană în domeniul securității cibernetice”,** editată de Nadya Purtova și Bert-Jaap Koops

- Acest volum editat acoperă măsurile legale și de reglementare specifice securității cibernetice în Uniunea Europeană, inclusiv provocările legate de conformitate și cadre precum Directiva NIS și GDPR.

**„Ransomware: Înțelegerea extorcării digitale și a amenințării acesteia la adresa organizației dumneavoastră”,** de Allan Liska și Timothy Gallo

- Acest text, completat cu studii de caz și exemple specifice UE, va ajuta studenții să înțeleagă implicațiile atacurilor ransomware în temeiul reglementărilor UE.

| **Lectură recomandată** |
|---|
| **„Regulamentul general privind protecția datelor (RGPD) al UE: un comentariu”** de Lukas Feiler și Nikolaus Forgó<br>• Acest comentariu oferă informații detaliate despre GDPR, esențiale pentru înțelegerea peisajului de reglementare din UE și a impactului acestuia asupra practicilor de securitate cibernetică.<br>**„Protecția datelor și securitatea cibernetică în Europa: Cadre juridice și considerații practice”** de Paul Lambert<br>• Această carte oferă perspective practice asupra alinierii strategiilor de protecție a datelor și de securitate cibernetică în UE, inclusiv respectarea reglementărilor și a celor mai bune practici privind măsurile de securitate.<br>**„Securitatea rețelelor și a informațiilor: perspective europene și internaționale”,** editată de Jeanne Pia Mifsud Bonnici și Joe Cannataci<br>• Această colecție examinează peisajul securității rețelelor și informațiilor atât din perspectivă europeană, cât și internațională, oferind un context mai larg pentru eforturile UE în domeniul securității cibernetice.<br>**„Inteligența artificială în cibersecuritatea: practici, provocări și etică”** de Elena Fersman și Martin Fredriksson<br>• O prezentare generală cuprinzătoare a integrării tehnologiilor de inteligență artificială în securitatea cibernetică, abordând provocările etice, operaționale și de reglementare, pertinente în special în contextul UE.<br>**„Securitatea cibernetică în era digitală: instrumente, tehnici și aplicații”** de Gregory B. White, Eric A. Fisher și James L. Antonakos<br>• Deși nu se concentrează exclusiv pe UE, această carte acoperă și o gamă largă de aspecte moderne ale securității cibernetice |

| **Material de studiu** (materiale originale HackerU și Cybint) |
|---|
| **Lectură obligatorie** |
| • Administrarea rețelei TCP/IP: Ajutor pentru administratorii de sistem Unix, ediția a 3-a, de Craig Hunt (O'Reilly)<br>• Referință esențială de buzunar pentru administrarea sistemului: Comenzi și formate de fișiere (Pocket Administrator) de Eleen Frisch (O'Reilly)<br>• Rețele de calculatoare: Ghidul începătorului pentru stăpânirea rețelelor de calculatoare, a internetului și a modelului OSI de Ramon Nastase |
| **Lectură recomandată** |
| • Certificare CompTIA A+ All-in-One For Dummies (Calculatoare/Tehnologie) Ediția a 5-a de Glen E. Clarke, Edward Tetz, Timothy L. Warner<br>• Coding All-in-One For Dummies Ediția 1 de Nikhil Abraham<br>• Informații esențiale Volumul 1: Introducere în sistemele informatice de Eric Frick<br>• Arhitectură IT For Dummies Ediția 1 de Kalani Kirk Hausman, Susan L. Cook<br>• Securitate cibernetică For Dummies (Calculatoare/Tehnologie) Ediția 1 de Steinberg<br>• Linux For Dummies, Ediția a 10-a Ediția a 10-a de Richard Blum<br>• Windows 10 For Dummies, Ediția a 3-a (Calculatoare/Tehnologie) Ediția a 3-a de Rathbone<br>• Networking For Dummies Ediția a 12-a de Doug Lowe |

# 6. M6: PLANIFICAREA SECURITĂȚII CIBERETICE

| Titlul modulului | Codul modulului |
|---|---|
| **PLANIFICAREA SECURITĂȚII CIBERETICE** | |

| Lector (i) | Instituția sau departamentul unde se predă modulul |
|---|---|
| | |

| Modalitatea de livrare | Limba |
|---|---|
| *Față în față, online, hibrid* | *Engleză, Finlandeză, Turcă, Norvegiană, Lituaniană, Română, Franceză, Poloneză, Spaniolă* |

| Cerințe preliminare |
|---|
| - |

| Numărul de credite ECTS alocate | Volumul de muncă al studentului | Orele de lucru direct | Program de lucru individual |
|---|---|---|---|
| 3 | 75 | 50 | 25 |

**Scopul și rezultatele modulului**

După absolvirea acestui curs, studenții vor putea înțelege și aplica principiile de bază ale planificării și managementului securității cibernetice. Vor dobândi capacitatea de a implementa standarde și cadre internaționale, de a dezvolta strategii de securitate pe termen lung, de a gestiona măsuri operaționale și tactice de securitate cibernetică și de a planifica arhitecturi de rețea securizate, cum ar fi cloud și zero trust. În plus, studenții vor fi echipați pentru a proiecta planuri eficiente de răspuns la incidente și a implementa strategii de continuitate a afacerii, asigurând reziliența organizațională și măsuri eficiente de securitate cibernetică în fața amenințărilor în continuă evoluție.

| Rezultatele învățării ale modulului | Metode de predare si invatare | Metode de evaluare |
|---|---|---|
| **Cunoștințe:** Cursanții vor dobândi cunoștințe avansate despre cum să integreze principiile avansate de securitate cibernetică și tendințele actuale în planificarea strategică și managementul operațional | Prelegeri, studii de caz, discuții de grup, învățare autodirijată | Teste de autoevaluare, Teste de evaluare a cunoștințelor |
| **Competențe:** Cursanții vor dobândi competențe în planificare strategică și management operațional, ceea ce le va permite să proiecteze și să implementeze eficient strategii de securitate cibernetică care abordează riscurile emergente și asigură răspunsuri tactice robuste. | Exerciții practice, Ateliere, Studii de caz | Evaluări bazate pe proiecte, Evaluări practice |

| | | |
|---|---|---|
| **Competențe:** Cursanții vor fi competenți în dezvoltarea și implementarea unor cadre strategice de securitate cibernetică, conducerea și gestionarea inițiativelor de securitate cibernetică. | Ateliere, Seminarii, Exerciții de Joc de Rol | Evaluare continuă, testare bazată pe scenarii |

| **Conținutul modulului: defalcarea subiectelor** | **Ore de lucru direct** | | | | | **Ore de lucru și sarcini individuale** | |
|---|---|---|---|---|---|---|---|
| | Lector(i) (învățământ | Consultatii | Practica | Teste | **Lucru direct** | **Munca individuală** | **Cerințe** |
| **1. Introducere în planificarea securității cibernetice:** Securitatea datelor, a oamenilor și a societății<br>- securitatea datelor - Securitatea stocării informațiilor, Procesul de investigare<br>- securitatea datelor - Tehnici de atac prin parolă<br>- securitatea umană - Conștientizare și înțelegere<br>- Securitatea societală – ce este criminalitatea cibernetică, etica cibernetică<br>- Securitatea societală - Dreptul cibernetic - Dovezi digitale, Contracte digitale, Convenții (acorduri) multinaționale | 8 | 0,5 | 6 | 0,5 | **15** | **8** | Definiți aspectele juridice ale datelor, securității umane și societale, legilor și politicilor care guvernează datele în IMM-uri.<br>Clasificați tipurile de atacuri cibernetice relevante pentru IMM-uri.<br>Identificați instrumente utile pentru prevenirea atacurilor cibernetice. |
| **2. Planificare strategică**<br>- Definirea obiectivelor și scopurilor de securitate cibernetică<br>- Analiza SWOT (Puncte forte, Puncte slabe, Oportunități, Amenințări)<br>- Dezvoltarea strategiilor de securitate pe termen lung<br>- Stabilirea indicatorilor cheie de performanță (KPI)<br>- Revizuirea și actualizarea strategiei de securitate | 8 | 2 | 6 | 2 | **18** | **8** | Definiți obiectivele de securitate cibernetică relevante pentru IMM-uri folosind o analiză SWOT, dezvoltați strategii pe termen lung pentru a aborda riscurile, alocați resursele și bugetul în consecință, stabiliți indicatori cheie de performanță (KPI) pentru a măsura progresul și actualizați periodic strategia pe baza noilor amenințări. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **3. Management operațional și tactic**<br>- Implementarea controalelor de acces<br>- Gestionarea patch-urilor și actualizări de software<br>- Monitorizarea continuă a sistemului<br>- Instruire privind conștientizarea securității angajaților | 8 | 1 | 6 | 2 | **17** | **9** | Implementați măsuri de control al accesului pentru a restricționa accesul neautorizat, întrețineți sistemele prin gestionarea patch-urilor, configurați monitorizarea activităților neobișnuite și oferiți angajaților instruire privind conștientizarea securității cibernetice. |
| **Total** | **24** | **3,5** | **18** | **4,5** | **50** | **25** | |

| **Strategia de evaluare** | **Procentul de greutate comparativ** | **Criterii de evaluare** |
|---|---|---|
| Test de autoevaluare (1) | 10% | 10 puncte - 96-100% răspunsuri corecte.<br>9 puncte – 91-95 % răspunsuri corecte.<br>8 puncte – 86-90 % răspunsuri corecte.<br>7 puncte - 80-85 % răspunsuri corecte.<br>6 puncte – 70-79 % răspunsuri corecte.<br>5 puncte – 60-69 % răspunsuri corecte.<br>4 puncte – 50-59 % răspunsuri corecte.<br>3 puncte – 40-49 % răspunsuri corecte.<br>2 puncte – 30-39 % răspunsuri corecte.<br>1 punct – 0-29 % răspunsuri corecte. |
| Test de autoevaluare (2) | 10% | |
| Test de autoevaluare (3) | 10% | |
| Test de evaluare a cunoștințelor | 70% | |
| | | |

**Material de studiu** *(Nume, Inițiala prenumelui, (An, Lună, Zi). Titlul articolului. Titlul revistei/jurnalului/ziarului, Numărul volumului (Numărul ediției), Numerele de pagină ale întregului articol, Editura, URL)*

**Lectură obligatorie**

1. Nair, A. și Greeshma, M. R. (2023). Stăpânirea managementului conformității cu securitatea informațiilor: Un manual cuprinzător privind conformitatea cu ISO/IEC 27001:2022. Packt Publishing Limited.

2. Falco, G. J. și Rosenbach, E. (2021). Confruntarea cu riscul cibernetic: O strategie de anduranță integrată pentru securitatea cibernetică. Oxford University Press.

3. Cadrul de securitate cibernetică NIST (CSF) 2.0, Institutul Național de Standarde și Tehnologie, 26 februarie 2024

**Lectură recomandată**

1. Mehta, S. (2023). Ghid de examen ISACA Certified in Risk and Information Systems Control (CRISC®). Packt Publishing Limited.
2. Gregory, P. H. (2021). Ghid de examen all-in-one CISM Certified Information Security Manager. McGraw-Hill.
3. ISACA. (2021). Manual de revizuire CRISC, ediția a 7-a. ISACA.
4. Parlamentul European și Consiliul. (14 decembrie 2022). Regulamentul (UE) 2022/2554 privind reziliența operațională digitală pentru sectorul financiar.
5. Ghid privind Regulamentul general privind protecția datelor (GDPR), Biroul Comisarului pentru informații

# 7. M7: GESTIONAREA ȘI ATENUAREA RISCURILOR

| Titlul modulului | Codul modulului |
|---|---|
| **GESTIONAREA ȘI ATENUAREA RISCURILOR** | |

| Lector (i) | Instituția sau departamentul unde se predă modulul |
|---|---|
| | |

| Modalitatea de livrare | Limba |
|---|---|
| *Față în față, online, hibrid* | *Engleză, Finlandeză, Turcă, Norvegiană, Lituaniană, Română, Franceză, Poloneză, Spaniolă* |

| Cerințe preliminare | | | |
|---|---|---|---|
| Nici una | | | |
| **Numărul de credite ECTS alocate** | **Volumul de muncă al studentului** | **Orele de lucru direct** | **Program de lucru individual** |
| 3 | 75 | 50 | 25 |

| Scopul și rezultatele modulului | | |
|---|---|---|
| După finalizarea acestui curs, studenții vor fi capabili să gestioneze continuu (identificarea, analizarea, evaluarea, estimarea, atenuarea) riscurilor legate de securitatea cibernetică ale infrastructurilor, sistemelor și serviciilor TIC prin planificarea, aplicarea, raportarea și comunicarea analizei, evaluării și tratării riscurilor. | | |
| **Rezultatele învățării ale modulului** | **Metode de predare si invatare** | **Metode de evaluare** |
| **Cunoștințe:** Cursanții vor dobândi cunoștințe avansate despre procesele de gestionare a riscurilor, inclusiv identificarea, evaluarea și controlul riscurilor, permițându-le să stabilească și să descrie rutine eficiente de securitate cibernetică adaptate nevoilor specifice ale locurilor de muncă ale IMM-urilor, în conformitate cu standardele naționale și internaționale. | A se selecta de către lector, din Partea 1.3. *[Metode de predare, de exemplu, prelegeri teoretice, analiză a literaturii de specialitate, invitați, predare și învățare reciprocă, mentorat etc.] din D2.3 „Structura căii de învățare pentru agenții schimbării în domeniul securității cibernetice pentru IMM-uri”* | Teste de autoevaluare<br>Test de evaluare a cunoștințelor |

| | | |
|---|---|---|
| **Competențe:** Cursanții vor fi abilitați în aplicarea metodologiilor și instrumentelor avansate pentru a efectua evaluări complete ale riscurilor, a proiecta și implementa strategii eficiente de gestionare a riscurilor și a dezvolta rutine robuste de securitate cibernetică, special adaptate pentru locurile de muncă ale IMM-urilor. | A se selecta de către lector, din Partea 1.3. *[Metode de predare, de exemplu, sarcini practice/laboratoare, chestionare, jocuri, analiză video tehnică, studii de caz, activități practice etc.] din D2.3 „Structura căii de învățare pentru agenții schimbării în domeniul securității cibernetice pentru IMM-uri”* | Teste de autoevaluare<br>Test de evaluare a cunoștințelor |
| **Competențe:** Cursanții vor fi competenți în dezvoltarea și implementarea politicilor strategice de securitate cibernetică pentru locurile de muncă ale IMM-urilor | A se selecta de către lector, din Partea 1.3. *[Metode de predare, de exemplu, concursuri, CTF, medii simulate, 5E-uri, CBL, CL, PBL etc.] din D2.3 „Structura căii de învățare pentru agenții schimbării în domeniul securității cibernetice pentru IMM-uri”* | Teste de autoevaluare<br>Teste de evaluare a cunoștințelort |

| Conținutul modulului: defalcarea subiectelor | Ore de lucru direct | | | | | Ore de lucru și sarcini individuale | |
|---|---|---|---|---|---|---|---|
| | Lector(i) (învățământ superior) | Consultatii | Practica (învățământ superior) | Teste | **Lucru direct** | **Munca individuală** | **Cerințe** |
| **Evaluarea riscurilor**<br><br>Procesul general de gestionare a riscurilor<br><br>Cadrul general de gestionare a riscurilor<br><br>Principiile de gestionare a riscurilor<br><br>Standardele de gestionare a riscurilor<br>Exemple practice | 2 | 0 | 2 | 0 | **4** | **5** | Descrieți pe scurt etapele cheie din procesul de gestionare a riscurilor, inclusiv identificarea, evaluarea și controlul riscurilor.<br><br>Definiți contextele interne și externe ale gestionării riscurilor pentru un IMM. Specificați domeniul de aplicare al evaluării riscurilor și identificați factorii cheie de risc.<br><br>Dezvoltați criterii de risc specifice IMM-ului ales. |
| **Identificarea riscurilor**<br><br>Leadership și angajament în managementul riscurilor<br><br>Definirea domeniului de aplicare al activităților de management al riscurilor<br><br>Contextul extern și intern al contextului de management al riscurilor<br><br>Surse tangibile și intangibile de risc<br><br>Cauze și evenimente Amenințări și oportunități<br><br>Vulnerabilități și capacități<br><br>Schimbări în contextul extern și | 4 | 0 | 4 | 0 | **8** | **5** | Identificați sursele de risc atât tangibile, cât și intangibile pentru IMM. Clasificați riscurile pe baza cauzelor, evenimentelor, amenințărilor și oportunităților.<br><br>Analizați vulnerabilitățile și capacitățile interne ale IMM-ului și evaluați modul în care schimbările atât în contextul extern, cât și în cel intern ar putea afecta afacerea.<br><br>- |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| intern<br><br>Indicatori ai riscurilor emergente<br><br>Natura și valoarea activelor și resurselor<br><br>Consecințe și impactul acestora asupra obiectivelor<br><br>Limitările cunoștințelor și fiabilității informațiilor<br><br>Prejudecăți, presupuneri și convingeri ale celor implicați<br>Exemple practice și studii de caz | | | | | | | Identificați potențialele riscuri emergente pentru IMM și propuneți indicatori pentru monitorizarea acestora. Luați în considerare modul în care natura și valoarea activelor și resurselor influențează această analiză. |
| **Amenințări interne**<br>Definiția și tipurile de amenințări interne<br>Costurile amenințărilor interne<br>Elaborarea unui program de atenuare a amenințărilor interne<br>Detectarea și identificarea amenințărilor interne<br>Evaluarea amenințărilor interne<br>Gestionarea amenințărilor interne<br>Exemple practice și studii de caz | 6 | 0 | 6 | 0 | **12** | **5** | Definiți și clasificați diferite tipuri de amenințări interne relevante pentru IMM-uri. Discutați costurile potențiale pe care aceste amenințări le-ar putea impune afacerii.<br><br>Dezvoltați un program de bază de atenuare a amenințărilor interne pentru un IMM. Evidențiați componentele cheie, cum ar fi detectarea, identificarea și strategiile de gestionare.<br><br>Propuneți o metodă de evaluare a amenințărilor interne și subliniați pașii pentru a gestiona eficient aceste amenințări într-un context IMM. |
| **Modele și metodologii de măsurare și evaluare a riscurilor**<br>Modele și metodologii de evaluare cantitativă și calitativă a riscurilor | 6 | 0 | 6 | 0 | **12** | **5** | Comparați și contrastați un model cantitativ și unul calitativ de evaluare a riscurilor. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Probabilitatea evenimentelor și a consecințelor<br>Natura și magnitudinea consecințelor<br>Complexitate și conectivitate;<br>Factori legați de timp și volatilitate<br>Evaluarea eficacității controalelor existente<br>Sensibilitate și niveluri de încredere<br>Exemple practice și studii de caz | | | | | | | Evaluați probabilitatea unui eveniment de risc și natura și magnitudinea consecințelor acestuia pentru un IMM. Luați în considerare modul în care complexitatea, factorii legați de timp și volatilitatea influențează această evaluare.<br><br>Evaluați eficacitatea controalelor actuale în gestionarea riscurilor identificate. Includeți o analiză a nivelurilor de sensibilitate și încredere în măsurile de control. |
| **Controlul riscurilor**<br>Formularea și selectarea opțiunilor de tratament al riscurilor<br>Planificarea și implementarea tratamentului riscurilor<br>Evaluarea eficacității tratamentului respectiv<br>Decizia dacă riscul rămas este acceptabil<br>Monitorizare și revizuire<br>Înregistrare și raportare<br>Exemple practice și studii de caz | 6 | 0 | 6 | 0 | **12** | **5** | Identificați și selectați opțiunile adecvate de tratare a riscurilor pentru IMM-uri. Justificați selecția pe baza naturii riscurilor implicate.<br><br>Elaborați un scurt plan de tratare a riscurilor, subliniind modul în care opțiunile de tratare selectate vor fi implementate într-un mediu IMM.<br><br>Propuneți o metodă pentru evaluarea eficacității tratării riscurilor și determinarea dacă riscul rămas este acceptabil. |
| **Total** | **24** | **2** | **24** | **0** | **50** | **25** | |

| Strategia de evaluare | Procentul de greutate comparativ | Criterii de evaluare |
|---|---|---|
| Test de autoevaluare (1) | 5% | 10 puncte - 95-100% correct answers.<br>9 puncte – 85-94 % răspunsuri corecte.<br>8 puncte – 75-84 % răspunsuri corecte.<br>7 puncte - 65-74 % răspunsuri corecte.<br>6 puncte – 55-64 % răspunsuri corecte..<br>5 puncte – 45-54 % răspunsuri corecte.<br>4 puncte – 35-44 % răspunsuri corecte.<br>3 puncte – 25-34 % răspunsuri corecte.<br>2 puncte – 15-24 % răspunsuri corecte.<br>1 punct – 0-14 % răspunsuri corecte. |
| Test de autoevaluare (2) | 5% | |
| Test de autoevaluaret (3) | 5% | |
| Test de autoevaluare (4) | 5% | |
| Test de autoevaluare (5) | 5% | |
| Test de evaluare a cunoștințelor | 75% | |

**Material de studiu** *(Nume, Inițiala prenumelui, (An, Lună, Zi). Titlul articolului. Titlul revistei/jurnalului/ziarului, Numărul volumului (Numărul ediției), Numerele de pagină ale întregului articol, Editura, URL)*

**Lectură obligatorie**

1. Adarsh Nair și Greeshma M. R. (2023) Stăpânirea managementului conformității securității informațiilor: Un manual cuprinzător privind conformitatea cu ISO/IEC 27001:2022. Packt Publishing, Limited https://ebookcentral.proquest.com/lib/viluniv-ebooks/detail.action?docID=30652023&query=risk%20management
2. Gregory J. Falco, Eric Rosenbach (2021) Confruntarea cu riscul cibernetic: O strategie de anduranță integrată pentru securitatea cibernetică. Oxford University Press, eBook
3. Kristina Narvaez, Betty Simkins, John Fraser (2014) Implementarea managementului riscului la nivel de întreprindere: Studii de caz și cele mai bune practici. John Wiley & Sons
- ENISA (2022) Standarde de gestionare a riscurilor
4. Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în întreaga Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2)
5. ISO 31000 Gestionarea riscurilor — Orientări

**Lectură recomandată**

Shobhit Mehta (2023) Ghid de examen Certificat ISACA în Controlul Riscului și al Sistemelor Informatice (CRISC®). Packt Publishing, Limited https://ebookcentral.proquest.com/lib/viluniv-ebooks/detail.action?docID=30806680&query=risk%20management

Peter H. Gregory (2021) Ghid de examen Manager de Securitate a Informațiilor Certificat CISM all-in-one. McGraw-Hill ISACA (2021) Manual de revizuire CRISC, ediția a 7-a. ISACA

Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală pentru sectorul financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011

# 8. M8: CONTINUITATEA ACTIVITĂȚII, RECUPERARE ÎN CAZ DE DEZASTRE, GESTIONAREA INCIDENTELOR ȘI SECURITATEA PERSONALULUI

| Titlul modulului | Codul modulului |
|---|---|
| **CONTINUITATEA ACTIVITĂȚII, RECUPERARE ÎN CAZ DE DEZASTRE, GESTIONAREA INCIDENTELOR ȘI SECURITATEA PERSONALULUI** | |

| Lector (i) | Instituția sau departamentul unde se predă modulul |
|---|---|
| | |

| Modalitatea de livrare | Limba |
|---|---|
| *Față în față, online, hibrid* | *Engleză, Finlandeză, Turcă, Norvegiană, Lituaniană, Română, Franceză, Poloneză, Spaniolă* |

| Cerințe preliminare |
|---|
| Nici una |

| Numărul de credite ECTS alocate | Volumul de muncă al studentului | Orele de lucru direct | Program de lucru individual |
|---|---|---|---|
| 3 | 75 | 50 | 25 |

| Scopul și rezultatele modulului | | |
|---|---|---|
| La finalizarea acestui curs, studenții vor putea formula și administra planuri cuprinzătoare de continuitate a afacerii și recuperare în caz de dezastru (BC/DR), vor dezvolta un program funcțional de gestionare a incidentelor și vor stabili o politică de securitate a personalului puternică și eficientă. Studenții vor învăța cum să protejeze activele, să asigure evitarea pierderilor excesive, să prevină perioadele de nefuncționare, să evite sau să limiteze situațiile de criză și mediile de gestionare a crizelor.<br><br>La finalizarea acestui curs, studenții vor putea scrie și monitoriza implementarea susținută a unui manual complet de securitate cibernetică pentru IMM-uri, utilizând principii și tehnologii avansate de securitate cibernetică integrate în conformitate cu toate statutele naționale și internaționale. De asemenea, studenții vor urmări aplicarea legii. | | |
| **Rezultatele învățării ale modulului** | **Metode de predare si invatare** | **Metode de evaluare** |

| | | |
|---|---|---|
| **Cunoștințe:** Cursanții vor dobândi cunoștințe avansate despre cum să creeze și să implementeze un manual cuprinzător de securitate cibernetică la locul de muncă pentru IMM-uri, care să încorporeze principii avansate de securitate cibernetică, cele mai recente mecanisme de apărare și respectarea legislației și standardelor naționale și internaționale în gestionarea incidentelor, continuitatea afacerii și securitatea personalului. | A se selecta de către lector, din Partea 1.3. [Metode de predare] a D2.3 „Structura căii de învățare pentru agenții schimbării în domeniul securității cibernetice pentru IMM-uri” | Teste de autoevaluare, Test de evaluare a cunoștințelor |
| **Competențe:** Cursanții vor fi abilitați de a crea și menține un manual de securitate cibernetică la locul de muncă pentru IMM-uri, utilizând metodologii avansate pentru a evalua riscurile, a concepe strategii eficiente de gestionare a riscurilor și de răspuns la incidente și a dezvolta planuri cuprinzătoare de continuitate a activității, adaptate nevoilor organizației lor. | A se selecta de către lector, din Partea 1.3. [Metode de predare] a D2.3 „Structura căii de învățare pentru agenții schimbării în domeniul securității cibernetice pentru IMM-uri” | Teste de autoevaluare, Test de evaluare a cunoștințelor |
| **Competențe:** Cursanții vor fi competenți în dezvoltarea și implementarea unui manual de securitate cibernetică pentru IMM-uri, conducerea eficientă a proiectelor și echipelor de securitate, asigurând alinierea cu obiectivele organizației și obligațiile de conformitate. | A se selecta de către lector, din Partea 1.3. [Metode de predare] a D2.3 „Structura căii de învățare pentru agenții schimbării în domeniul securității cibernetice pentru IMM-uri” | Teste de autoevaluare, Test de evaluare a cunoștințelor |

| **Conținutul modulului: defalcarea subiectelor** | **Ore de lucru direct** | | | | | **Ore de lucru și sarcini individuale** | |
|---|---|---|---|---|---|---|---|
| | Lector(i) [illegible] | Consultatii | Practica (Învățământ | Teste | **Lucru direct** | **Munca [illegible]** | **Cerințe** |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Răspuns la incidente**<br>**-** Definiția și importanța răspunsului la incidente în securitatea cibernetică<br>- Componentele cheie ale unei recuperări eficiente în urma unui răspuns la incidente<br>- Prezentare generală a amenințărilor comune de securitate cibernetică (phishing, amenințări interne)<br>- Elaborarea Planului de răspuns la incidente (IRP)<br>- Roluri și responsabilități în cadrul Echipei de răspuns la incidente<br>- Simularea incidentului: realizarea unui plan simulat. | 5 | 0,5 | 3 | 0,5 | **9** | **5** | Elaborați un Plan detaliat de Răspuns la Incidente pentru IMM-ul dumneavoastră, inclusiv rolurile, responsabilitățile și pașii de urmat în timpul unui incident de securitate cibernetică. Simulați un incident și efectuați un exercițiu simulat pentru a testa eficacitatea planului dumneavoastră. |
| **Recuperare în caz de dezastru**<br>- Înțelegerea recuperării în caz de dezastru<br>- Elaborarea unui plan de recuperare în caz de dezastru<br>- Roluri și responsabilități în recuperarea în caz de dezastru<br>- Pași de recuperare după dezastru | 5 | 0,5 | 3 | 0,5 | **9** | **5** | Creați un Plan de Recuperare în Caz de Dezastru care să prezinte procedurile pentru restaurarea infrastructurii IT și a datelor după un eveniment catastrofal. Includeți un calendar pentru recuperare și atribuiți responsabilități membrilor echipei pentru fiecare fază a procesului. |
| **Continuitatea afacerii**<br>- Înțelegerea continuității afacerii<br>- Dezvoltarea Planului de continuitate a afacerii (PCA)<br>- Roluri și responsabilități în continuitatea afacerii<br>- Analiza impactului asupra afacerii<br>- Testarea și îmbunătățirea PCA | 5 | 0,5 | 3 | 0,5 | **9** | **5** | Proiectați un Plan de Continuitate a Afacerii care să asigure că funcțiile critice ale afacerii rămân operaționale în timpul și după o întrerupere. Identificați serviciile și resursele esențiale și schițați strategii de contingență pentru a le menține în diverse scenarii. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Conștientizare, instruire și educație în domeniul securității**<br>- Înțelegerea conștientizării în domeniul securității<br>- Dezvoltarea unui program de instruire în domeniul securității<br>- Responsabilitățile angajaților în domeniul securității cibernetice<br>- Măsurarea eficacității conștientizării în domeniul securității | 1 | 0,5 | 2 | 0,5 | **4** | **1** | Dezvoltați un program de instruire în domeniul conștientizării securității pentru IMM-ul dumneavoastră, concentrându-vă pe politicile cheie de securitate cibernetică și pe cele mai bune practici. Organizați o sesiune de instruire pentru angajați și evaluați-le înțelegerea prin chestionare sau activități interactive. |
| **Practici de angajare în domeniul securității**<br>- Definirea cerințelor pentru rolurile de securitate<br>- Efectuarea de verificări ale antecedentelor<br>- Interviuri pentru componentele de securitate<br>- Evaluare și dezvoltare continuă | 1 | 0,5 | 2 | 0,5 | **4** | **1** | Stabiliți practici de angajare axate pe securitate, inclusiv verificări ale antecedentelor și întrebări de interviu concepute pentru a evalua gradul de conștientizare a candidaților în materie de securitate cibernetică. Creați o listă de verificare a calificărilor și trăsăturilor esențiale de securitate pentru potențialii angajați. |
| **Practici de încetare a accesului în contextul securității**<br>- Revocarea imediată a accesului<br>- Recuperarea datelor și a dispozitivelor<br>- Interviu de ieșire pentru informații despre securitate<br>- Notificarea echipelor relevante<br>- Considerații legale și de conformitate | 1 | 0,5 | 2 | 0,5 | **4** | **2** | Elaborați o procedură de reziliere securizată care include pași pentru revocarea accesului, recuperarea activelor companiei și efectuarea interviurilor de ieșire. Implementați un scenariu simulat de reziliere pentru a evalua eficacitatea procedurii dumneavoastră. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Securitatea terților**<br>- Evaluarea riscului față de terți<br>- Due diligence în selecția furnizorilor<br>- Implementarea contrastelor și a cerințelor de securitate<br>- Monitorizare și audit continuu<br>- Răspuns la incidente și comunicare | 2 | 0,5 | 2 | 0,5 | **5** | **2** | Identificați riscurile potențiale asociate cu furnizorii terți și creați o listă de verificare a evaluării securității pentru a evalua conformitatea acestora cu standardele de securitate cibernetică ale IMM-ului dumneavoastră. Elaborați un model de contract care să includă cerințe de securitate și penalități pentru nerespectare. |
| **Securitatea în procesele de revizuire**<br>- Incorporarea securității în revizuiri<br>- Efectuarea de audituri de securitate regulate<br>- Evaluarea vulnerabilităților și testarea penetrării<br>- Revizuiri post-incident | 1 | 0,5 | 1,5 | 0,5 | **3,5** | **2** | Dezvoltați un proces pentru revizuirea și actualizarea periodică a politicilor și procedurilor de securitate cibernetică ale IMM-ului dumneavoastră. Programați și efectuați un audit simulat pentru a vă asigura că toate măsurile de securitate sunt actualizate și conforme cu standardele relevante. |
| **Problemă specială privind confidențialitatea informațiilor personale ale angajaților**<br>- Limitări ale colectării datelor<br>- Stocarea și controlul accesului<br>- Respectarea reglementărilor privind confidențialitatea<br>- Partajarea datelor și terții<br>- Consimțământul și drepturile angajaților | 2 | 0,5 | 2 | 0,5 | **5** | **2** | Elaborați o politică de confidențialitate pentru gestionarea informațiilor personale ale angajaților, asigurând respectarea legilor privind protecția datelor și a celor mai bune practici. Efectuați o evaluare a riscurilor pentru a identifica potențialele vulnerabilități în modul în care datele angajaților sunt stocate și prelucrate. |
| **Total** | **23** | **2** | **20,5** | **4,5** | **50** | **25** | |

| **Strategia de evaluare** | **Procentul de greutate comparativ** | **Criterii de evaluare** |
|---|---|---|

| | | |
|---|---|---|
| Test de autoevaluare (1) | 5% | 10 puncte - 95-100% correct answers.<br>9 puncte – 85-94 % răspunsuri corecte.<br>8 puncte – 75-84 % răspunsuri corecte.<br>7 puncte - 65-74 % răspunsuri corecte.<br>6 puncte – 55-64 % răspunsuri corecte..<br>5 puncte – 45-54 % răspunsuri corecte.<br>4 puncte – 35-44 % răspunsuri corecte.<br>3 puncte – 25-34 % răspunsuri corecte.<br>2 puncte – 15-24 % răspunsuri corecte.<br>1 punct – 0-14 % răspunsuri corecte. |
| Test de autoevaluare (2) | 5% | |
| Test de autoevaluaret (3) | 5% | |
| Test de autoevaluare (4) | 5% | |
| Test de autoevaluare (5) | 5% | |
| Test de evaluare a cunoștințelor | 75% | |

**Material de studiu** *(Nume, Inițiala prenumelui, (An, Lună, Zi). Titlul articolului. Titlul revistei/jurnalului/ziarului, Numărul volumului (Numărul ediției), Numerele de pagină ale întregului articol, Editura, URL)*

**Lectură obligatorie**

- Gregory J. Falco, Eric Rosenbach (2021). Confruntarea cu riscul cibernetic: o strategie de anduranță integrată pentru securitatea cibernetică. Oxford University Press, eBook.

- Michael Wallace, Lawrence Webber (2017). Manualul de recuperare în caz de dezastru: un plan pas cu pas pentru a asigura continuitatea afacerii și a proteja operațiunile, instalațiile și activele vitale. AMACOM.

- Institutul Național de Standarde și Tehnologie (NIST). Ghid de planificare a situațiilor de urgență pentru sistemele de tehnologia informației. NIST SP 800-34 Rev. 1.

- Cochran, K.A. (2024). Răspuns la incidente, continuitatea afacerii și recuperarea în caz de dezastru. În: Cyber-security Essentials. Apress, Berkeley, CA. https://doi.org/10.1007/979-8-8688-0432-8_14

**Lectură recomandată**

- ISACA (2023). Manual de revizuire CISM, ediția a 15-a. ISACA.
- Peter H. Gregory (2021). Ghid de examen multifuncțional CISM Certified Information Security Manager. McGraw-Hill.
- Guvernanță IT (2022). ISO 22301:2019 – Sisteme de management al continuității afacerii. Cerințe.
- M. Souppaya, L. Feldman, G. Witte [2024], Ghid pentru recuperarea în urma incidentelor de securitate cibernetică, Divizia de Securitate a Calculatoarelor, Laboratorul de Tehnologie a Informației, Institutul Național de Standarde și Tehnologie, Departamentul de Comerț al SUA.
- Ihab Hanna Sawalha [2021]. Opinii despre continuitatea afacerii și recuperarea în caz de dezastru. Revista Internațională de Servicii de Urgență.

## ANEXE

## ȘABLOANE PENTRU PROGRAMĂ

**DESCRIEREA MODULULUI**

| Titlul modulului | Codul modulului |
|---|---|
| ... | |

| Lector (i) | Instituția sau departamentul unde se predă modulul |
|---|---|
| ... | ... |

| Modalitatea de livrare | Limba |
|---|---|
| *Față în față, online, hibrid, consultatii* | *Engleză, ...* |

| Cerințe preliminare |
|---|
| ... |

| Numărul de credite ECTS alocate | Volumul de muncă al studentului | Orele de lucru direct | Program de lucru individual |
|---|---|---|---|
| 3 | ... | ... | ... |

| Scopul și rezultatele modulului | | |
|---|---|---|
| ... | | |
| **Rezultatele învățării ale modulului** | **Metode de predare si invatare** | **Metode de evaluare** |
| | | |
| | | |
| | | |
| | | |

| Facilitarea resurselor (echipamente, software, tehnologie) |
|---|
| ... |

| Conținutul modulului: defalcarea subiectelor | Ore de lucru direct | | | | | Ore de lucru și sarcini individuale | |
|---|---|---|---|---|---|---|---|
| | Lector(i) (învățământ superior) | Consultatii | Practica (învățământ | Teste | **Lucru direct** | **Munca individuală** | **Cerințe** |
| 1 | | | | | | | |
| ... | | | | | | | |
| n | | | | | | | |
| **Total** | | | | | | | |

| Strategia de evaluare | Procentul de greutate comparativ | Criterii de evaluare |
|---|---|---|
| Autotestare I | | ... |
| ... | | ... |
| Autotestare n | | ... |
| Test de evaluare a cunoștințelor | | ... |
| | | |

| **Material de studiu** *(Nume, Inițiala prenumelui, (An, Lună, Zi). Titlul articolului. Titlul revistei/jurnalului/ziarului, Numărul volumului (Numărul ediției), Numerele de pagină ale întregului articol, Editura, URL)* |
|---|
| **Lectură obligatorie** |
| ... |
| **Lectură recomandată** |
| ... |

CyberAgent

Co-funded by the European Union

# Get social with the project!

www.cyberagents.eu

contact@cyberagents.eu

@Cyber-Agent-EU

@CyberAgent.EU

@CyberAgentEU

@Cyber.Agent.EU

@CyberAgentEU

## Project Partners

Vilniaus Universitetas 1579 Universitas Vilnensis

Kaunas Faculty

Prios

EVM

TEKNOPARK ISTANBUL Mesleki ve Teknik ANADOLU LİSESİ

HackerU by ThriveDX

Olemisen Balanssia ry

WOMEN 4CYBER European Cyber Security Organisation

Liceul Tehnologic Grigore C. Moisil Buzau