CyberAgent

Co-funded by the European Union

RAPORTUL DE IDENTIFICARE A NEVOILOR DE FORMARE ALE AGENȚILOR DE SCHIMBARE A SECURITĂȚII CIBERNETICE PENTRU IMM-URI

CYBER AGENT 10.2023

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

Finanțat de Uniunea Europeană. Punctele de vedere și opiniile exprimate aparțin, însă, exclusiv autorului (autorilor) și nu reflectă neapărat punctele de vedere și opiniile Uniunii Europene sau ale Agenției Executive Europene pentru Educație și Cultură (EACEA). Nici Uniunea Europeană și nici EACEA nu pot fi considerate răspunzătoare pentru acestea.

Pachet de lucru 2: Abordarea și proiectarea structurii CyberAgent

Livrabil 2.2: Raportul de identificare a nevoilor de formare ale agenților de schimbare a securității cibernetice pentru IMM-uri

Responsabil WP2 – Olemisen Balanssia ry
Responsabil livrabil 2.2 – Olemisen Balanssia ry

CUPRINS

INTRODUCERE

Acest raport își propune să analizeze și să identifice nevoile de formare pentru a determina competențele adecvate necesare unui agent de schimbare a securității cibernetice pentru IMM-uri. Printr-o revizuire cuprinzătoare a ofertelor educaționale actuale și prin înțelegerea preferințelor IMM-urilor în ceea ce privește problemele de securitate cibernetică, acest raport încearcă să reducă decalajul dintre competențele actuale și să definească setul ideal de abilități necesare.

Pe măsură ce amenințările cibernetice cresc în complexitate, există o mare nevoie ca IMM-urile să se asigure că au personal pregătit adecvat pentru a combate aceste amenințări. Agenții de schimbare din domeniul securității cibernetice joacă un rol crucial în acest context. Acest raport analizează peisajul securității cibernetice prin diferite perspective: educație și formare, incluziunea de gen și starea actuală în IMM-uri și instituții școlare.

1. METODOLOGIE

Pentru acest proces de identificare am folosit o abordare mixtă care combină cercetarea literaturii de specialitate și cercetarea pe teren.

În cadrul cercetării literaturii de specialitate, a fost efectuată o analiză cuprinzătoare pentru:

- Revizuirea dispozițiilor educaționale existente și emergente la nivelurile VET și IIS în domeniul securității cibernetice în fiecare țară parteneră. Identificarea și îmbinarea de articole, documente, cercetări și rapoarte legate de conținutul și nevoile de formare în domeniul securității cibernetice.
- Analiza cursurilor VET și IIS, programelor acestora și relevanța lor pentru provocările de securitate cibernetică din lumea reală.
- Obiectivele au fost:
- Să identifice componentele curriculare actuale ale cursurilor de securitate cibernetică oferite la nivelurile VET și IIS în fiecare țară.
- Să evalueze modul în care aceste programe se aliniază cu provocările de securitate cibernetică.
- Să identifice dacă există strategii sau programe specifice pentru a implica mai multe femei în studiile de securitate cibernetică.

În faza de cercetare de teren, am efectuat 2 sondaje. Unul conceput pentru profesori și formatori din ambele categorii VET și IIS din fiecare țară pentru a înțelege nuanțele dispozițiilor actuale de formare. Celălalt, adaptat IMM-urilor, pentru a obține o viziune și o înțelegere a situației din companii în ceea ce privește securitatea cibernetică: modul în care angajații sunt implicați în acele subiecte, provocările și nevoile. Accentul prin această cercetare de teren a fost, de asemenea, de a determina caracteristicile, nevoile de formare și preferințele de învățare, evidențiind în special nevoile femeilor în securitatea cibernetică.

Am ajuns la un număr semnificativ de răspunsuri pentru ambele chestionare. 190 de profesori și formatori din domeniul VET și IIS și 176 angajați ai IMM-urilor.

Sondaj 1: identificarea nevoilor de formare pentru agenții de schimbare a securității cibernetice pentru IMM-uri - sondaj VET și IIS.

Tipul instituției	**Răspunsuri**	**Feminin**	**Masculin**	**Prefer să nu spun**
IIS (Instituții de Învățământ Superior)	104	28	73	3
VET (Educație și Formare Profesională)	86	36	48	2
Total	**190**	**64**	**121**	**5**

Sondajul 2: identificarea nevoilor de instruire pentru agenții de schimbare a securității cibernetice pentru IMM-uri - sondaj IMM-uri.

Număr de răspunsuri	**Număr**
IMM-uri	176
Total	**176**

Chestionarele si datele complete pot fi găsite în Anexele C și D.

2. CERCETARE (TOȚI PARTNERII)

2.1. DISPOZIȚII ACTUALE DE EDUCAȚIE ȘI FORMARE

Această secțiune prezintă cercetarea și oferă perspective derivate din analiza literaturii de specialitate și sondajele aplicate, evidențiind punctele forte și lacunele din infrastructura actuală de educație și formare din țările partenere.

2.1.1. VET & IIS PREZENTARE GENERALĂ A EDUCAȚIEI DE SECURITATE CIBERNETICĂ

Am realizat o analiză amplă a peisajului educației în domeniul securității cibernetice în toate țările partenere pentru a descrie starea sa actuală și a declanșa aspectele relevante ale educației și formării în domeniul securității cibernetice.

În Lituania, o căutare în baza de date AIKOS a evidențiat un total de șase programe formale de educație în domeniul securității cibernetice oferite de instituțiile lituaniene, cuprinzând atât nivelurile de licență, cât și de master:

Specializare	Program de studii	Instituție	ECTS	Nivel de studii
Inginerie informatică	Securitatea informatiei si tehnologiei informației[1]	Universitatea de Tehnologie din Kaunas	120	Master în Informatică
Management	Managementul securității cibernetice[2]	Universitatea Mykolas Romeris	90	Master în Managementul Afacerilor
Inginerie informatică	Securitatea informației și tehnologiei informației[3]	Universitatea Tehnică Vilnius Gediminas	120	Master în Informatică
Inginerie informatică	Sisteme informatice și securitate cibernetică[4]	Universitatea Vilnius	210	Licență în Informatică
Inginerie informatică	Tehnologii ale Sistemelor Informaționale și Securității Cibernetice[5]	Colegiul Marijampole	180	Licență profesională în informatică
Inginerie informatică	Sisteme cibernetice și securitate[6]	Colegiul Kaunas	180	Licență profesională în informatică

Programele de securitate cibernetică la nivel de master prezintă abordări distincte, dar complementare. Universitatea Kaunas pune accent pe metodologia de cercetare, metodele de

[1] https://www.aikos.smm.lt/studijuoti/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=LO&f=MokGal&key=8618_2023&pt=of&ctx_sr=8Gzz1EUgIeKfy0cWNVrrVdABKo0%3d
[2] https://www.aikos.smm.lt/Registrai/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=PROG&f=Prog&key=2845&pt=of&ctx_sr=za5dHDvp0IGJ2%2fD6Fkt7rIse6a8%3d
[3] https://www.aikos.smm.lt/studijuoti/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=LO&f=MokGal&key=1442_2023&pt=of&ctx_sr=8Gzz1EUgIeKfy0cWNVrrVdABKo0%3d
[4] https://www.aikos.smm.lt/Registrai/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=PROG&f=Prog&key=9664&pt=of&ctx_sr=za5dHDvp0IGJ2%2fD6Fkt7rIse6a8%3d
[5] https://www.aikos.smm.lt/Registrai/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=PROG&f=Prog&key=2775&pt=of&ctx_sr=za5dHDvp0IGJ2%2fD6Fkt7rIse6a8%3d
[6] https://www.aikos.smm.lt/Registrai/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=PROG&f=Prog&key=3797&pt=of&ctx_sr=za5dHDvp0IGJ2%2fD6Fkt7rIse6a8%3d

securitate a informațiilor și aspectele legale ale spațiului electronic, concentrându-se pe dezvoltarea abilităților de proiectare și implementare a sistemelor IT securizate. Universitatea Tehnică Vilnius Gediminas prioritizează formarea de specialiști cu o abordare sistematică a problemelor de securitate a informațiilor, combinând cunoștințele științifice cu metode și tehnologii pentru asigurarea securității informațiilor, alături de încurajarea gândirii critice și a leadershipului. Universitatea Mykolas Romeris, totuși, înclină în mod distinct spre managementul securității cibernetice, urmărind să producă specialiști abili în supravegherea mediilor IT moderne și a sarcinilor complexe de securitate cibernetică, cu un accent puternic pe managementul strategic în contexte tehnologice dinamice.

Programele de studii la nivel de licență în domeniul securității cibernetice au în comun un accent principal pe dezvoltarea profesioniștilor calificați în informatică și securitate cibernetică, dar fiecare cu accente distincte. Programul Universității din Vilnius este orientat spre furnizarea unei baze cuprinzătoare în inginerie informatică, concentrându-se pe analiza, proiectarea, dezvoltarea și întreținerea sistemelor informaționale securizate. Colegiul Marijampole, deși își propune să producă specialiști în informatică competenți, pune un accent mai puternic pe aspecte practice, cum ar fi crearea, întreținerea și administrarea rețelelor și sistemelor de calculatoare. Colegiul Kaunas se diferențiază prin scopul de a pregăti specialiști cu abilități nu numai în proiectarea și implementarea sistemelor cibernetice, ci și în conducerea echipelor, înțelegerea implicațiilor etice, legale și sociale și lucrul eficient în medii multiculturale. În timp ce toate cele trei instituții își propun să doteze studenții cu abilități tehnice în domeniul securității cibernetice, obiectivele lor variază de la competență tehnică (Universitatea din Vilnius), aplicare practică și dezvoltarea abilităților soft (Colegiul Marijampole), până la un amestec de considerații tehnice, de conducere și etice (Colegiul Kaunas).

Căutarea a evidențiat, de asemenea, patru programe de educație non-formală a adulților înregistrate în domeniul securității cibernetice, fiecare concentrându-se pe abilități esențiale pentru recunoașterea, investigarea și prevenirea atacurilor cibernetice, în special folosind criptografia. Deși toate programele împărtășesc acest obiectiv principal, abordările și domeniile lor diferă. Unele sunt concentrate pe securitate cibernetică și strategii preventive, în timp ce altele oferă un curriculum mai larg, inclusiv programare, acoperind domenii precum ingineria socială, managementul identității și managementul riscurilor. În special, mai multe programe încep cu programarea de bază și progresează către subiecte avansate de securitate cibernetică, potrivite pentru începători. Un program remarcabil, în colaborare cu Cybint, se adresează celor cu cunoștințe IT limitate, oferind abilități practice, din lumea reală, atât în format full-time, cât și part-time. Aceste programe urmăresc în mod colectiv să dezvolte diverse competențe de securitate cibernetică, de la programare de bază până la învățare aprofundată, axată pe aplicații.

Mai multe politici de consolidare a securității și apărării naționale a Finlandei au influențat programele de educație legate de securitatea cibernetică. A existat un număr tot mai mare de inițiative de cercetare și dezvoltare, programe educaționale și de formare și profesioniști certificați în domeniul securității cibernetice. Strategia finlandeză de securitate cibernetică (2019) (**https://turvallisuuskomitea.fi/en/finlands-cyber-security-strategy-2019/**) și Programul

de dezvoltare a securității cibernetice (2021) subliniază importanța dezvoltării competențelor naționale de securitate cibernetică prin educație și cercetare. Pentru sistemul de învățământ școlar, scopul este de a dota elevii cu abilități și cunoștințe pentru a naviga în lumea digitală în siguranță și conștientizarea amenințărilor cibernetice și a măsurilor de protecție Lehto-IWS-018.pdf (jyu.fi)

În educația și formarea profesională (VET) finlandeză, securitatea cibernetică nu este evidențiată în mod explicit ca un obiectiv separat sau specializat în majoritatea materialelor. Cu toate acestea, acest lucru nu înseamnă neapărat că securitatea cibernetică este complet absentă din programele VET. Având în vedere importanța tot mai mare a alfabetizării digitale și a securității cibernetice în toate sectoarele, aceste subiecte sunt integrate în programe mai largi de educație IT și tehnică. Este important de reținut că furnizorii de VET din Finlanda au autonomie de a-și organiza ofertele educaționale în conformitate cu cerințele regionale și specifice domeniului. Educația și formarea profesională finlandeză a suferit recent cea mai amplă reformă din aproape 20 de ani. Obiectivul reformei din 2018 a fost de a crea un sistem EFP mai eficient și mai flexibil, bazat pe competențe și orientat către clienți, să-și îmbunătățească eficiența și să alinieze mai bine calificările cu nevoile pieței muncii. Acest lucru se realizează în principal prin reducerea reglementărilor și introducerea autonomiei și responsabilității pentru furnizorii de VET. (Sursa: **https://www.cedefop.europa.eu/files/8133_en.pdf**). Aceasta înseamnă că unele instituții ar putea oferi module mai specializate în domenii precum securitatea cibernetică, în funcție de cerințele industriei locale și de parteneriate. Pe baza cercetărilor lui Lehto, securitatea cibernetică nu este un subiect separat, ci integrat în subiecte diferite, în special în contextul Tehnologiilor Informației și Comunicațiilor (TIC). Responsabilitatea predării depinde de profesori să încorporeze educația în domeniul securității cibernetice în cadrul disciplinelor lor. Această abordare duce la o variație a modului în care aceasta este implementată în diferite școli și clase și evidențiază necesitatea unor abordări mai structurate și mai consecvente pentru predarea securității cibernetice, inclusiv făcându-l un subiect separat sau o parte mai proeminentă a educației TIC.

La nivel de învățământ superior (IIS), universitățile finlandeze oferă programe cuprinzătoare în securitate cibernetică. Aceste programe sunt concepute pentru a dota studenții cu cunoștințe și abilități avansate în diferite domenii ale securității cibernetice. Mulți oferă o diplomă de master în securitatea informației și tehnologia informației, concentrându-se pe implicațiile și aplicațiile din lumea reală ale acestor concepte. Sunt accesibile cursuri la zi și la distanță.

Sectorul securității cibernetice din Belgia se confruntă cu o cerere crescută de profesioniști calificați, cu aproximativ 4.000 de posturi vacante de securitate cibernetică (în noiembrie 2022). Recunoscând urgența și necesitatea de a umple acest gol, au fost introduse diverse inițiative și programe educaționale pentru a dezvolta expertiza țării în domeniul securității cibernetice. Numeroase instituții din Belgia precum KU Leuven, Solvay Business School, Howest University of Applied Sciences și multe altele au dezvoltat programe specializate în engleză, franceză și olandeză, capabile să ajungă la un public larg. Totuși, cercetările efectuate de organizația belgiană Agoria au subliniat necesitatea formării continue și în rândul profesioniștilor care nu

mai frecventează universitatea, pentru a-i ține la curent cu domeniul securității cibernetice și amenințările sale. Strategia belgiană de securitate cibernetică pentru anii 2021-2025 recunoaște nivelul ridicat de integrare a securității cibernetice în mediul academic al țării și subliniază rolul esențial pe care universitățile și alte instituții de învățământ îl joacă în stimularea eforturilor de cercetare și dezvoltare în domeniu. Conform bazei de date a CBB (Centrul de Securitate Cibernetica Belgia), în Belgia, există 33 de cursuri (licență, master și certificări) oferite de instituțiile de învățământ superior, care se adaugă unei game de programe VET oferite atât în sectorul public, cât și în cel privat. CBB este organismul care supraveghează, coordonează și monitorizează punerea în aplicare a strategiei belgiene de securitate cibernetică și dezvoltă în prezent un curs gratuit de conștientizare a securității cibernetice a angajaților pentru angajații belgieni, pentru a răspândi și mai mult cunoștințele privind securitatea cibernetică în rândul populației. În general, strategia belgiană de securitate cibernetică subliniază importanța răspândirii cunoștințelor și abilităților în domeniul securității cibernetice prin educație și se angajează să extindă cursurile academice, să promoveze cercetarea în domeniu, să încurajeze educația STEM și să ofere oportunități de formare practică pentru a răspunde cererii tot mai mari de profesioniști în peisajul securității cibernetice belgian.

În Norvegia, securitatea cibernetică nu este o materie principală pe care o poți studia la nivel VET. Elemente ale programului sunt incluse într-un program VET numit „Computer and Electronics". Nu există un cadru al Ministerului Educației pentru securitatea cibernetică, doar se menționează în abilitățile generale de alfabetizare digitală de bază pentru toată educația că studenții ar trebui să fie capabili să utilizeze și să navigheze resursele digitale în interiorul și în afara rețelelor și să protejeze securitatea informațiilor și a datelor.

Strategia națională pentru competența de securitate cibernetică (**https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhetskompetanse/id2627189/**) subliniază, pe 14 noiembrie 2023, importanța ca elevii școlilor VET să învețe despre securitatea cibernetică. Pentru multe discipline profesionale, acest lucru este foarte relevant și important. Există o lipsă de materiale de învățare privind securitatea cibernetică în cursurile profesionale, iar profesorii nu au abilitățile de a preda, în special în domenii precum confidențialitatea, tehnologia casei inteligente și IoT. Programele existente pentru educația în domeniul securității cibernetice, cum ar fi GenCyber și CyberFirst, nu abordează în mod specific nevoile acestui program profesional. (sursa 1 – 2)

Printr-o colaborare între UiO, NTNU și profesorii din școlile VET selectate, planul este de a dezvolta material de învățare pentru securitate cibernetică, care ulterior va fi disponibil pe platforma națională de învățare NDLA (National Digital Learning Arena, **https://ndla.no/**).

În învățământul superior, găsim atât program de un an în cultura securității digitale, cât și programe de licență în securitate cibernetică. Subiectul este inclus și într-o serie de programe de master în Științe ale datelor și informaticii. Există o varietate de studii specifice de securitate cibernetică, cum ar fi tehnologia informatică și informatică aplicată, licență în securitate cibernetică, licență în criminalistică digitală, infrastructură digitală și securitate cibernetică,

cultură de securitate digitală și master bazat pe experiență în securitatea informațiilor. Există, de asemenea, studii în care securitatea cibernetică este inclusă ca și cultură HSE și de conducere, pregătire municipală pentru situații de urgență și studiu anual în managementul crizelor.

Pentru Polonia, în ultimii ani, studiile cibernetice au crescut. Din ce în ce mai multe cursuri cibernetice se deschid în universități și, în același timp, numărul de cursuri VET crește.

Cererea pentru profesii cibernetice a crescut în Polonia în ultimii ani, iar gradul de conștientizare a ciberneticului a crescut și în delegația poloneză care încurajează companiile să angajeze experți cibernetici și să protejeze informațiile.

În Polonia, la fel ca majoritatea țărilor europene, o diplomă academică este considerată obligatorie, prin urmare, cursurile cibernetice sunt adesea un studiu suplimentar după diploma pentru că majoritatea studiilor Akshmi sunt mai lungi, dar într-o manieră teoretică. Există cursuri cibernetice care sunt scurte, dar cele mai multe dintre ele se concentrează pe învățarea practică care te pregătește pentru munca reală.

Marea provocare pentru un student în domeniul cibernetic este că majoritatea instituțiilor VET nu au finanțare proprie, deci este necesară o soluție financiară și, prin urmare, această opțiune nu este întotdeauna potrivită pentru cei interesați.

Chiar dacă securitatea cibernetică ar trebui să fie o prioritate pentru toate domeniile de activitate, sistemul educațional VET din România nu este încă pregătit să se asigure că studenții sunt competenți în acest domeniu. Într-o analiză a Curriculum-ului pentru ciclul inferior al liceului - domeniul tehnologic - în orice domeniu al formării profesionale, programa școlară de cultură tehnică nu oferă unități de rezultate ale învățării privind securitatea cibernetică. Unele competențe specifice în domeniu se regăsesc în programa de cunoștințe generale, la disciplina Tehnologia Informației și Comunicațiilor, în programa de clasa a IX-a. Acestea sunt:

1. Descrierea și aplicarea măsurilor de securitate în utilizarea internetului:

- • Utilizarea inteligentă a Internetului
- • Importanța criptării transmisiei de date
- • Utilizarea semnăturii digitale
- • Modalități de apărare împotriva virușilor

2. Folosind serviciul de chat:

- • Prezentarea aplicațiilor colaborative pentru videoconferințe
- • Prezentarea regulilor rețelei IRC

Pentru ciclul superior al liceului, clasa a XI-a, doar domeniul de pregătire profesională Automatizări electronică pentru specializările Tehnician telecomunicații, Tehnician operator calculator, Tehnician operator telematică, oferă câteva conținuturi despre instalarea aplicațiilor

de securitate. În clasa a XII-a, doar la specializarea Tehnician Informatică, modulul de specialitate cuprinde conținuturi precum:

- • Principii de bază ale securității sistemelor informatice și a rețelelor de calculatoare
- • Dezvoltarea politicilor de securitate în rețea
- • Amenințări de securitate ale rețelelor
- • Protecție pentru navigarea pe Internet
- • Viruși și aplicații de Securitate

În ceea ce privește IIS, Universitatea Transilvania din Brașov demonstrează un angajament puternic față de educația în domeniul securității cibernetice, oferind un program cuprinzător de master în Securitate cibernetică desfășurat integral în limba engleză. Devotamentul universității de a promova expertiza în acest domeniu critic este evidentă în curriculum-ul extins oferit pentru program.

Acest program de master de la Universitatea Transilvania este o oportunitate excelentă pentru studenții care caută o educație completă în domeniul securității cibernetice într-un cadru academic internațional. Combinația dintre un curriculum robust și instruirea în limba engleză oferă absolvenților oportunitatea de a avea succes în domeniul dinamic și provocator al securității cibernetice.

Universitatea Babeș-Bolyai din Cluj-Napoca, prin Facultatea de Matematică și Informatică, a inițiat din anul universitar 2023-2024 un program de master în limba engleză în Securitate Cibernetică, care vizează pregătirea viitorilor specialiști în acest domeniu de o importanță vitală în context. a tranziţiei la societatea informaţională. Cursurile noului program încep în luna octombrie a acestui an, odată cu anul universitar 2023-2024, admiterea aducând o competiție peste așteptări. Peste 40 de studenți, inclusiv din străinătate, admiși în program vor deveni specialiști în domeniul Securității Cibernetice, candidații admiși putând chiar alege să studieze un an universitar la alte universități de renume din Europa.

La Facultatea de Matematică și Informatică, Programul de Master Tehnologii Internet (în limba engleză) oferă în al doilea semestru al anului I, un curs de Criptografie și Securitate a Sistemelor, care introduce studenții în domeniul securității cibernetice și a metodelor specifice de criptarea datelor.

În plus, programul de master Tehnologii moderne în ingineria sistemelor software oferă în primul semestru al celui de-al doilea an un curs opțional numit securitate sisteme IT, centrat în jurul principalelor provocări ale securității cibernetice.

Ambele cursuri permit masteranzilor de la Facultatea de Matematică și Informatică să obțină perspectivă și expertiză în acest subiect, care în contextul internațional actual este de o importanță vitală, și să conștientizeze provocările criptării și securității sistemelor moderne.

Universitatea din București, Facultatea de Matematică și Informatică, oferă un Master, "Program Security and Applied Logic" (în limba engleză), care asigură o serie de cursuri dedicate criptografiei și securității sistemelor. Studenții pot dobândi cunoștințe în domeniile securității sistemelor de operare, criptografie, securitate rețelelor și securitate cibernetică, fiind astfel pregătiți să facă față provocărilor acestui domeniu.

În Spania, majoritatea studiilor în domeniul securității cibernetice sunt la nivel de învățământ superior, diplome sau master. Potrivit datelor recuperate de Institutul Național de Securitate Cibernetică din Spania, există:

- • Aproximativ 87 de diplome de master în securitate cibernetică oferite de universități publice și private și alte instituții de învățământ superior.
- • 4 specializări, majoritatea specializări în criminalistică informatică.
- • 3 diplome universitare, toate oferite de sectorul privat.

În ceea ce privește formarea la nivel VET, există aproximativ 60 de cursuri disponibile la institutele spaniole de formare profesională. Toate sunt reglementate de aceeași programă de studii, aprobată de Ministerul Educației în mai 2020 prin Decretul Regal 479/2020, din 7 aprilie, prin care se stabilește cursul de specializare în securitate cibernetică în mediile tehnologiei informației.

În ciuda programelor existente, se recunoaște necesitatea unor eforturi suplimentare. Spania a implementat diverse planuri, inclusiv Planul național de competențe digitale, Planul de digitalizare a IMM-urilor 2021-2025 și Planul Spania Digital 2025, cu accent cheie pe crearea de noi talente pentru a răspunde cererii tot mai mari de competențe digitale, în special în domeniul securității cibernetice.

În Turcia, nevoia de securitate cibernetică a crescut rapid și a devenit foarte importantă în țara lor, precum și în întreaga lume, mai ales în ultimii ani. Concomitent cu evoluțiile tehnologice, riscurile și amenințările cibernetice s-au schimbat și ele în același ritm și au devenit complexe. Riscurile și amenințările cibernetice au atins potențialul de a provoca consecințe mult mai cuprinzătoare și negative decât atacurile fizice. Cu sectoare precum finanțele, comunicațiile electronice, energia, transporturile și aviația care oferă servicii într-un mediu digital securizat, asigurarea securității cibernetice naționale a devenit una dintre prioritățile de top pentru țara noastră. În acest context, studiile continuă să difuzeze formarea în domeniul securității cibernetice în formarea profesională și în învățământul superior în concordanță cu nevoile sectorului și să dezvolte și să îmbogățească conținuturile de formare.

În cadrul acestor studii, în învățământul profesional: Curs de securitate cibernetică fundamentală în operarea rețelelor în domeniul tehnologiilor informaționale. În domeniul securității cibernetice, programare fundamentelă, securitatea sistemului, tehnologiile de rețea, dezvoltarea software securizată, testarea de penetrare și răspunsul la incidente cibernetice, criminalistica informatică etc. Realizările cursului sunt oferite studenților.

În învățământul superior, programul de diplomă asociat „Cyber Security Analyst and Operator" în școlile profesionale de securitate cibernetică, programul de licență de inginerie informatică criminalistică la universități și programele de master relevante sunt oferite în universități.

În plus, centrele de educație continuă ale universităților, centrele publice de educație ale municipalităților, instituțiile oficiale precum TÜBİTAK, TSE și instituțiile de învățământ private oferă, de asemenea, instruire în domeniul securității cibernetice.

2.1.2. PROVOCĂRILE ȘI NEVOILE INDUSTRIEI DE SECURITATE CIBERNETICĂ

Pe baza unei analize amănunțite a literaturii de specialitate, am enumerat provocările de securitate cibernetică cu care se confruntă IMM-urile din țările proiectului. În peisajul evolutiv al securității cibernetice, întreprinderile mici și mijlocii (IMM-uri) din Lituania se confruntă cu multiple provocări în materie de securitate cibernetică. Pe măsură ce aceste companii se bazează din ce în ce mai mult pe tehnologiile digitale pentru operațiunile lor, ele devin mai vulnerabile la un spectru de amenințări cibernetice, necesitând o înțelegere cuprinzătoare și o abordare strategică pentru a gestiona eficient aceste riscuri.

În studiul din 2022, Bukauskas și colaboratorii, au diferențiat tipuri distincte de organizații pe baza maturității lor de securitate cibernetică și a nevoilor de competență. Organizațiile mici, conform studiului, sunt comparabile cu persoanele individuale din societate, deoarece principalul parametru al securității spațiului de lucru digital este nivelul de igienă cibernetică, care este influențat de înțelegerea generală a amenințărilor la securitatea cibernetică. La acest nivel, securitatea cibernetică este coordonată intern în cadrul organizației, ceea ce duce la posibile breșe de securitate în procesele de afaceri. În cadrul companiilor mijlocii, managementul și reglementarea securității cibernetice sunt, de asemenea, slab coordonate. Răspunsurile la incidente sau alte activități de securitate cibernetică nu sunt, de asemenea, accentuate în cadrul organizației. Având în vedere că întreprinderile mici din Lituania reprezintă 97% din totalul companiilor, Bukauskas și colaboratorii (2022) au concluzionat că există o nevoie semnificativă de specialiști IT care furnizează servicii IT, consultă utilizatorii și ale căror funcții includ asigurarea principiilor fundamentale de securitate cibernetică. Ei au subliniat, de asemenea, că se observă o lipsă notabilă în informațiile despre amenințări și cercetarea științifică și o nevoie vizibilă de specialiști în securitate cibernetică în ingineria securității și ciclul de viață al sistemelor.

Cu câțiva ani mai devreme, programul „Creați pentru Lituania", în colaborare cu Ministerul Apărării Naționale, a organizat o consultare publică privind creșterea gradului de conștientizare a securității cibernetice în rândul întreprinderilor mici și mijlocii. De asemenea, inițiativa a ajuns la concluzia că este evident că nivelul de conștientizare a securității cibernetice în rândul IMM-urilor din Lituania nu este ridicat și că întreprinderile mici nu au atins un nivel adecvat de rezistență cibernetică din cauza lipsei de înțelegere a riscurilor digitale. Mai mult, s-a remarcat faptul că mai mult de jumătate (57%) dintre liderii companiilor au declarat că fie le lipsesc, fie nu sunt siguri dacă au suficiente cunoștințe pentru a alege soluții de securitate cibernetică, iar peste trei sferturi dintre angajați au fost de acord că le lipsesc informații ușor de înțeles.

Comparând constatările lui Bukauskas (2022) și inițiativa anterioară „Creați pentru Lituania" (2019), este evident că situația privind securitatea cibernetică în rândul IMM-urilor din Lituania a înregistrat progrese limitate. Ambele studii subliniază o lipsă persistentă de cunoștințe de bază în materie de securitate cibernetică și de pregătire în aceste întreprinderi. În ciuda dependenței crescute de tehnologiile digitale, IMM-urile continuă să prezinte vulnerabilități din cauza rezistenței cibernetice inadecvate și a unei neînțelegeri generale a riscurilor digitale. Această provocare continuă evidențiază nevoia urgentă de îmbunătățire a conștientizării securității cibernetice și a formării în rândul IMM-urilor, un sector critic care constituie cea mai mare parte a peisajului de afaceri al Lituaniei.

În Finlanda, un studiu realizat de ETLA (Elinkeinoelämän tutkimuslaitos), Institutul de Cercetare Economică din Finlanda a evidențiat că numărul de încălcări ale datelor în companii finlandeze, inclusiv IMM-uri, s-a dublat în doi ani. Companiile finlandeze au raportat încălcări ale datelor de trei ori mai multe decât media europeană în 2019, majoritatea incidentelor fiind legate de escrocherii, atacuri de phishing, încălcări ale datelor, malware și vulnerabilități. Acest studiu subliniază, de asemenea, lipsa de profesioniști calificați în domeniul securității cibernetice ca principală provocare pentru IMM-urile finlandeze. **https://www.etla.fi/en/publications/kyberuhat-yleistyvat-miten-suomen-yritykset-parjaavat/**

Centrul Național de Securitate Cibernetică Finlanda (NCSC-FI) (**https://www.kyberturvallisuuskeskus.fi/en**) este o inițiativă condusă de guvernul finlandez. Funcționează ca parte a Agenției finlandeze de transport și comunicații (Traficom), care este o agenție guvernamentală responsabilă de reglementarea sectoarelor de comunicații și transport din Finlanda. Acestea oferă informații despre starea actuală a securității cibernetice și oferă îndrumări și instrumente atât persoanelor, cât și organizațiilor, pentru a-și îmbunătăți practicile de securitate cibernetică. Centrul se implică, de asemenea, în inițiative naționale de securitate cibernetică, cum ar fi alerte de vulnerabilitate, și promovează conștientizarea și pregătirea împotriva amenințărilor cibernetice.

Evaluările lor săptămânale oferă o perspectivă bună asupra provocărilor cu care se confruntă IMM-urile. Aflăm că IMM-urile finlandeze, ca multe altele, s-au confruntat cu aceleași probleme de securitate descrise de institutul ETLA, fiind vizate de multe mesaje de phishing și înșelătorie. Acestea includ încercările de a uzurpa identitatea unor servicii legitime, cum ar fi Suomi.fi, pentru a obține acreditări sau alte informații sensibile. Resursele financiare ale IMM-urilor pot reprezenta o limitare pentru implementarea soluțiilor moderne de securitate cibernetică pentru a se apăra împotriva amenințărilor cibernetice. Totodată, IMM-urile deja echipate au probleme în a rămâne la curent cu amenințările emergente la adresa securității cibernetice.

În efortul nostru de a înțelege situația securității cibernetice cu care se confruntă IMM-urile din Belgia, am efectuat o cercetare amănunțită. Cu toate acestea, am fost o provocare să obținem date sau surse cuprinzătoare care abordează această problemă critică. Această lipsă de

informații face dificilă crearea de strategii și soluții eficiente care pot ajuta IMM-urile să își protejeze activele digitale împotriva amenințărilor cibernetice.

Am putut ajunge la profesioniști care sunt implicați activ în domeniul securității cibernetice în Belgia, datorită rețelei extinse a Fundației Women4Cyber. Acești experți ne-au oferit perspective vitale care ne-au ajutat să înțelegem diferitele provocări cu care se confruntă IMM-urile în domeniul securității cibernetice. Am primit informații de la Iva Tasheva, o membră remarcabilă a Women4Cyber Belgium, care ne-a împărtășit experiența și cunoștințele vaste cu privire la provocările cu care se confruntă IMM-urile atunci când încearcă să își protejeze infrastructura digitală de amenințările cibernetice.

IMM-urile se confruntă cu mai multe provocări în materie de securitate cibernetică, cum ar fi dificultăți în accesarea asistenței ad-hoc, lipsa de instruire în domeniul managementului identității și accesului pentru personalul lor și înțelegerea limitată a rolurilor și responsabilităților serviciilor cloud. În plus, IMM-urile au acces limitat la soluții accesibile de scanare a vulnerabilităților și instrumente de monitorizare, făcându-le mai expuse la amenințările cibernetice. Hiperconectivitatea omniprezentă în mediile de afaceri expune IMM-urile la furtul de identitate și la activități frauduloase, în timp ce phishingul și escrocheriile prezintă riscuri continue. Pentru a face față acestor provocări, IMM-urile trebuie să ia măsuri proactive, să implementeze protocoale de securitate robuste și să ofere angajaților o educație cuprinzătoare pentru a-și consolida competențele și a se proteja împotriva potențialelor încălcări și pierderi financiare.

Securitatea cibernetică a devenit una dintre prioritățile de top pentru întreprinderile din Spania, inclusiv pentru întreprinderile mici și mijlocii (IMM-uri). Creșterea lucrului la distanță și a cursurilor online a dus la utilizarea pe scară largă a funcțiilor desktop la distanță, cloud computing și instrumente de colaborare, printre altele, crescând riscurile și atacurile computerizate. Raportul Centrului Criptologic Național (CCN-CERT) leagă creșterea lucrului la distanță și utilizarea tehnologiei cu creșterea acestor riscuri. Cele mai frecvente atacuri pe care le-au suferit companiile sunt ransomware-ul și atacurile asupra sistemelor de acces la distanță. Creșterea amenințărilor cibernetice a determinat companiile să crească numărul de persoane repartizate în echipele de securitate cibernetică, fie intern, fie extern. Cu toate acestea, companiile încă externalizează aproximativ 50% din aceste funcții.

În plus, există încă 21% dintre companiile din Spania care nu au Centre de Operații de Securitate (SOC) pentru procesarea incidentelor. În ceea ce privește educația în domeniul securității cibernetice în mediul de afaceri, analiza Deloitte evidențiază că în 2022 orele de instruire online în domeniul securității cibernetice pentru angajații organizațiilor analizate au crescut cu aproape 30% față de datele pentru 2021. Totuși, aproape 50% dintre companiile din Spania nu dețin nicio certificare în domeniul securității cibernetice, ceea ce reprezintă o provocare clară pentru viitor.

Așadar, cea mai mare provocare cu care se confruntă companiile spaniole este încă lipsa de pregătire în domeniul securității cibernetice. Conform raportului „Analiză și diagnosticare a

pregătirii în domeniul securității cibernetice în Spania" elaborat de ObservaCiber, în 2021 Spania avea un decalaj de personal instruit estimat la 24.119. În 2024, se estimează că Spania va avea nevoie de peste 83.000 de experți, ridicând diferența de nivel de instruire la 57,5%.

Se pare că cea mai slabă verigă care determină IMM-urile să se confrunte cu provocări de securitate cibernetică este factorul „uman". Cea mai mare provocare pentru IMM-uri este că personalul responsabil cu securitatea cibernetică nu poate aloca suficient timp domeniului securității cibernetice deoarece are responsabilități în mai mult de un domeniu. Legat de aceasta, lipsa unei echipe separate de securitate cibernetică ocupă locul trei în lista dificultăților întâmpinate de IMM-uri în managementul securității cibernetice. IMM-urile au probleme în recrutarea și menținerea angajaților calificați în domeniul securității cibernetice.

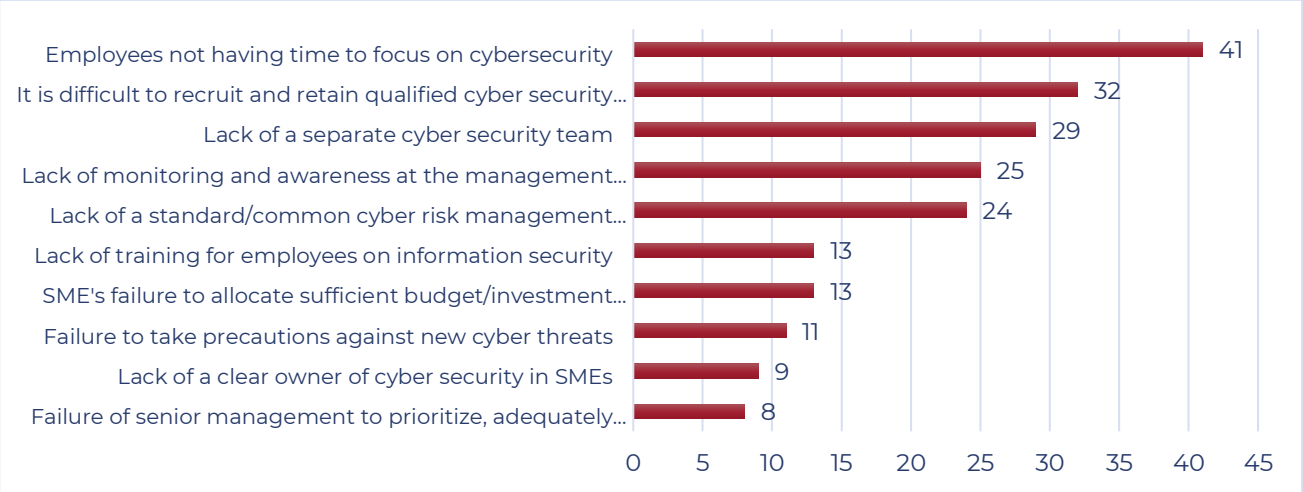


Figura 1 – provocări ale IMM-urilor – cercetare Turcia

În România, mediul online aduce oportunități de afaceri și conexiuni care pot ajuta IMM-urile să se dezvolte, dar conține și multe riscuri.

Securitatea cibernetică nu mai este o poveste, este o realitate și în România, chiar dacă, până acum, nu a avut loc un atac cibernetic major.

Sursa de informații utilizată este RAPORTUL VERIZON privind amenințările cibernetice în anul 2023 - principalele puncte cheie pentru IMM-uri (RAPORTUL DE INVESTIGAȚII ÎN DATE BREACH - DBIR), bazat pe 16.312 incidente de securitate dintre care 5.199 au fost confirmate ca încălcări ale securității datelor.

Puncte de interes pentru IMM-uri:

- • Suprafețele de atac pentru IMM-uri și corporații sunt similare, deoarece folosesc software bazat pe cloud. Pătrunderea neautorizată în sistem, tehnicile de inginerie socială și atacurile de bază ale aplicațiilor web reprezintă 92% din totalul tipurilor de atacuri pentru încălcări înregistrate de IMM-uri (85% pentru corporații).
- • ransomware 24% din cazuri (datele sunt furate înainte de a fi criptate)

- • pătrundere neautorizată în sistem - atacuri complexe bazate pe malware și/sau hacking pentru a-și atinge obiectivele.
- • Atacatorii externi reprezintă cea mai mare amenințare care provoacă 83% dintre brețele actuale de securitate, ajungând la 94% în cazul atacurilor IMM-urilor. 94% dintre actorii implicați în răspândirea amenințărilor sunt externi, față de 89% în cazul organizațiilor mari, iar 98% dintre încălcări sunt motivate financiar, față de 97% în cazul corporațiilor.
- • Motivația financiară este numărul unu în 95% din cazuri, procentul crescând la 98% în cazul atacurilor asupra IMM-urilor. Doar 1% sunt motivați de spionaj.
- • Angajații reprezintă veriga slabă a lanțului de securitate - 74% din toate cazurile (conștientizarea slabă a amenințărilor cibernetice). Principala metodă de intruziune se poate datora utilizării acreditărilor furate - 49% și phishing - 12% sau a altor metode, precum configurarea greșită sau trimiterea eronată a datelor sensibile.
- • E-mailuri de afaceri compromise - victima este păcălită să transfere sume mari de bani în conturile atacatorilor.

În Norvegia, întreprinderile mici și mijlocii (IMM-uri) se confruntă cu provocări semnificative în domeniul securității cibernetice. Mulți nu au o înțelegere profundă a riscurilor implicate, ceea ce duce la potențiale vulnerabilități. Există un decalaj vizibil în formarea eficientă a angajaților în domeniul securității cibernetice, făcând din eroarea umană un factor de risc comun. IMM-urile, în special cele care raportează că au resurse limitate, se luptă adesea să investească în măsuri avansate de securitate cibernetică și în personal calificat. De asemenea, trebuie să navigheze prin legi complexe de protecție a datelor, crescând complexitatea asigurării conformității, salvând în același timp informațiile sensibile. Creșterea atacurilor de phishing și a ingineriei sociale arată și mai mult vulnerabilitatea acestora, la fel ca securitatea insuficientă a rețelei și riscul amenințărilor interne. Gestionarea acestor riscuri este esențială, dar IMM-urile consideră adesea o provocare în evaluarea și managementul eficient al riscurilor. În plus, dependența de furnizori terți introduce un alt nivel de complexitate, expunând IMM-urile la amenințări suplimentare la securitatea cibernetică.

2.2. FEMEILE ÎN SECURITATE CIBERNETICĂ

Am analizat nevoile de formare și sprijin pentru femei, calificările și competențele existente ale femeilor în domeniul securității cibernetice și recomandări pentru implicarea mai multor femei angajate în provocările de securitate cibernetică.

Microsoft a realizat un sondaj, în 35 de țări europene, mai puțin de 1 din 5 absolvenți de informatică erau femei. Interesul pentru știință, tehnologie, inginerie și matematică (subiecte STEM) scade mult prea devreme. De fapt, Programul OCDE pentru Evaluarea Studenților Internaționali (PISA) dezvăluie că băieții sunt mult mai probabil decât fetele să se imagineze ca profesioniști, oameni de știință sau ingineri TIC. (Microsoft, 2017).

Când se analizează ponderea femeilor în rândul specialiștilor TIC în muncă, în UE27, în 2020, doar 18,5% din toți specialiștii TIC erau femei. Cele mai mari ponderi de femei au fost în Bulgaria – 28,2%, Grecia – 26,6% și România – 26,2% (vezi graficul 5 (Women go tech, 2021)). Țările din regiunea nord-baltică s-au aflat, de asemenea, în cea mai mare parte aproape de topul listei, cu excepția Norvegiei, care se află mai mult la mijlocul clasamentului țărilor. (Women go tech, 2021).

Potrivit Departamentului de Statistică al Republicii Lituania, numărul angajaților din categoria informații și comunicare în trimestrul IV, 2022 a fost de 29,4 mii bărbați și 21,5 mii femei. În primul trimestru al anului 2023, au fost 34,6 mii bărbați și 20,7 mii femei. Pentru trimestrul II, 2023, au fost 36,8 mii bărbați și 14,8 mii femei, iar în trimestrul III, 2023 cifrele au fost de 34,5 mii bărbați și 18,0 mii femei. Există o scădere vizibilă a numărului de angajate de la T1 la T2 2023, urmată de o creștere în T3 2023 (Rodiklių Duomenų Bazė - Oficialiosios Statistikos Por-talas, n.d.).

Cu până la 11% dintre femei care lucrează în securitatea cibernetică, a fost realizat un sondaj pentru a afla părerile publicului despre perspectivele femeilor în acest domeniu. În dispute, 44,4% dintre respondenți au susținut că numărul femeilor în domeniul securității cibernetice ar trebui să fie între 30 și 60%. Cea mai mare pondere a respondenților au spus că femeile ar trebui să reprezinte între 30 și 60% dintre femeile profesioniste (35,2%). Analizând răspunsurile pe sex și grupe de vârstă, se poate observa că femeile, în special cele mai tinere (sub 25 și 25-45), de cele mai multe ori cred că numărul femeilor ar trebui să fie în jur de jumătate. Tinerii (sub 25 de ani) cred că până la 30% dintre femei ar trebui să fie femei. Se poate observa că femeile însele tind să vadă un număr mult mai mare de femei în domeniul securității cibernetice decât este cazul în prezent pe piață. Aceasta este o veste bună, deoarece atragerea femeilor în domeniu nu numai că ar ajuta la abordarea deficitului de profesioniști, ci și la creșterea securității organizațiilor înșeși. (Bukaus-kas și colab., 2022).

În Finlanda, ca și în multe țări europene, există o înțelegere comună cu privire la dezechilibrul de gen în domeniul securității cibernetice și în domeniul IT, în general. Au crescut inițiativele și eforturile de sprijinire a femeilor în domeniul securității cibernetice și de promovare a implicării acestora în abordarea provocărilor legate de securitatea cibernetică. Cele mai multe dintre ele sunt susținute de organizații non-profit.

Domeniul securității cibernetice a cunoscut mai multe inițiative de dezvoltare a unor parcursuri educaționale și de carieră, programe de formare și evenimente de networking. Strategia se bazează, de asemenea, pe promovarea modelelor de urmat prin evidențierea carierei femeilor de succes în domeniul securității cibernetice și împărtășirea poveștilor lor pentru a inspira mai multe femei să urmeze cariere în acest domeniu. Women4Cyber și inițiativele enumerate subliniază importanța diversității și a incluziunii nu numai pentru a aborda dezechilibrul inegalității de gen, ci și pentru a contribui la puterea și reziliența generală a sectorului securității cibernetice. Instituțiile publice și private susțin, de asemenea, această strategie prin includerea acestei dimensiuni a egalității de gen ca prioritate de vârf în toate inițiativele lor.

Women4Cyber Finland (W4CFI)

Înființată în august, 2021, W4CFI este o organizație non-profit care vizează creșterea numărului de femei angajate în industria finlandeză de securitate cibernetică. Face parte din inițiativa mai largă Women4Cyber la nivelul UE și se concentrează pe sprijinirea unei industrii mai diverse și mai incluzive în Finlanda. W4CFI este implicată în diverse activități, inclusiv furnizarea de îndrumare, schimbul de cunoștințe și creșterea gradului de conștientizare pentru a crește și a sprijini implicarea femeilor în securitatea cibernetică. **https://www.women4cyberfinland.com/**

Ministerul finlandez al Transporturilor și Comunicațiilor și proiectul Universității Aalto

Ministerul finlandez al Transporturilor și Comunicațiilor, în colaborare cu Universitatea Aalto, dezvoltă un pachet educațional pentru a face din securitatea cibernetică o abilitate civică în întreaga Uniune Europeană. Această inițiativă evidențiază importanța tot mai mare a securității cibernetice în viața de zi cu zi și nevoia de conștientizare și abilități în rândul tuturor cetățenilor, inclusiv al femeilor. Acesta subliniază rolul instituțiilor de învățământ în furnizarea de educație și formare accesibilă în domeniul securității cibernetice, care este esențială pentru împuternicirea femeilor în domeniu. Finlanda stimulează educația în domeniul competențelor de securitate cibernetică în UE. **https://digital-skills-jobs.europa.eu/en** (europa.eu)

Mișcarea „Mimmit koodaa" (Codul femeilor).

Această inițiativă oferă ateliere de lucru, instruire, oportunități de creare de rețele, seminarii web și sprijin în carieră. Se concentrează pe provocarea stereotipurilor și pe încurajarea mai multor femei să exploreze cariere în tehnologie, inclusiv în securitatea cibernetică. Această organizație își propune să creeze căi pentru ca femeile să intre și să exceleze în domeniul securității cibernetice. **https://mimmitkoodaa.fi/in-english/**

În peisajul securității cibernetice din Belgia, femeile reprezintă 19% din forța de muncă conform primului studiu socio-economic privind sectorul securității cibernetice din Belgia emis de Agoria în 2022. Cu coordonarea Ministerului Belgian pentru Economie (FPS Belgia), politicienii competenți din Belgia au elaborat un plan pe cinci ani pentru femeile din domeniul digital numit „Femeile în digital – Strategie națională și intersecțională 2021-2026". Planul cincinal include o strategie comună și intersectorială bazată pe cinci obiective strategice utile pentru a combate prejudecățile și pentru a aborda obstacolele structurale care împiedică femeile să participe la economia digitală. Cele cinci obiective sunt următoarele:

1. Asigurarea că mai multe femei absolvă în sectorul digital; 2. Stimularea tuturor femeilor să participe pe piața digitală a muncii și/sau sectorul digital; 3. Îmbunătățirea reținerii femeilor în sectorul digital; 4. Crearea de noi imagini care să promoveze rolul femeii în domeniu (pe și în afara ecranului); 5. Reducerea decalajului de gen între grupurile țintă specifice (chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.bedigitaltogether.be/wp-content/uploads/2022/03/52786_9_WiD-Strategy-EN-2021.pdf).

Fundația Women4Cyber cu sediul la Bruxelles, organizează și sprijină o gamă largă de activități care vizează femeile care lucrează sau își încep cariera în securitatea cibernetică în Belgia și în Europa. În Belgia, Fundația sprijină și cooperează cu Capitolul Național Belgian (**https://www.linkedin.com/company/women4cyber-belgium/**) în aceste activități. Capitolul național belgian numără aproximativ 20 de membri activi care lucrează la inițiative. Activitățile, evenimentele și programele organizate de Capitol sunt, de exemplu: întâlniri de rețea și evenimente (virtuale și în persoană), cum ar fi „cafea virtuală", unde Capitolul W4C Belgia invită experți din diverse domenii legate de cibernetică și securitatea informațiilor pentru a vorbi; webinarii și sesiuni de informații; programe de mentorat menite să ajute femeile să-și îmbunătățească abilitățile și să progreseze în cariera de securitate cibernetică la toate nivelurile; proiecte și evenimente în colaborare cu Coaliția Belgiană pentru Securitate Cibernetică (cum ar fi organizarea Zilei Internaționale a Femeii 2023 **https://blog.cybersecuritycoalition.be/webcasts/women4cyber-belgium-international-womens-day-2023/**) ; promovarea de burse pentru programe educaționale legate de cibernetica, precum cele organizate de Solvay Brussels School of Economics & Management.

În Norvegia, abordarea decalajului de gen în securitatea cibernetică este crucială pentru construirea unei forțe de muncă rezistente și diversificate. Proporția femeilor în IT este de doar 29%. Numărul scăzut este puternic legat de numărul de femei care aleg discipline matematice și tehnice la nivel secundar.

Nevoile de instruire și sprijin și recomandări pentru implicarea femeilor

Este nevoie de programe de securitate cibernetică personalizate, concepute special pentru a încuraja participarea femeilor. Aceste programe ar trebui să echilibreze aspectele tehnice cu problemele organizaționale și de securitate cibernetică centrate pe om. Există mai multe studii tehnice ulterioare în domeniu, în timp ce ofertele educaționale ulterioare în majoritatea ocupațiilor tipice pentru femei (ocupații pedagogice – sanitare) nu au astfel de oferte și dezvoltarea unor oferte de formare mai scurte în securitate cibernetică legate de acele ocupații ar putea ajunge la mai multe femei. Acest lucru este susținut și de sectorul însuși, care a declarat că diversitatea poate aduce perspective unice provocărilor de securitate cibernetică. Creșterea gradului de conștientizare în rândul femeilor cu privire la carierele interne de securitate cibernetică ar putea avea loc prin ateliere, seminarii și programe de informare în școli și universități, pote inspira mai multe femei să intre în acest domeniu.

O altă abordare sugerată de multe dintre primele 50 de femei norvegiene din domeniul tehnologiei nominalizate în 2022 este crearea de programe de mentorat și oportunități de

creare de rețele pentru femei în securitate cibernetică, pentru a oferi îndrumări și sprijin esențial, ajutându-le să navigheze și să avanseze în acest domeniu.

Sectorul securității cibernetice însuși sugerează că organizațiile ar trebui să implementeze practici și politici de angajare incluzive care încurajează în mod activ recrutarea și menținerea femeilor în roluri de securitate cibernetică. 32% dintre femeile cu roluri tehnice sunt adesea „singura femeie din încăpere" la locul de muncă, conform raportului McKinsey „Women in the Workplace 2022".

În cele din urmă, promovarea femeilor în poziții de conducere în securitatea cibernetică poate oferi modele de urmat și poate inspira alte femei să urmeze căi similare, cum ar fi, de exemplu, Mia Landsem **https://www.orangecyberdefense.com/no/innsikt/nyheter/mia-landsem-etisk-hacker-i-orange-cyberdefense-er-blant-norges-fremste-tech-kvinner**.

În România, securitatea cibernetică rămâne unul dintre cele mai dinamice și interesante sectoare tehnologice. Cu toate acestea, acest sector are nevoie de o schimbare sistemică în reprezentarea și compensarea femeilor. În ciuda interesului crescut în domeniul securității cibernetice, disparitatea de gen persistă. Femeile sunt încă sever subreprezentate, în timp ce majoritatea locurilor de muncă sunt predominant masculine. Viitorul securității cibernetice este influențat de capacitatea de a atrage, reține și promova mai mulți profesioniști cibernetici, inclusiv mai multe femei.

Au fost multe studii efectuate pentru a arăta cât de subevaluate sunt femeile pe tot globul, dar și pentru a face pe toată lumea să înțeleagă importanța femeilor în toate domeniile, și în special în securitatea cibernetică. Diferența extremă de gen în rândul angajaților din domeniul securității cibernetice indică faptul că alte forțe de la locul de muncă nu sunt deloc egale. Femeile reprezintă 39% din totalul forței de muncă. Aceștia reprezintă 38% dintre lucrătorii din locurile de muncă STEM, dar doar aproximativ 25% din forța de muncă din domeniul securității cibernetice, potrivit Cybersecurity Ventures.

Există diverse bariere care țin femeile departe de securitatea cibernetică. Potrivit unei cercetări de la (ISC)2, o organizație nonprofit care se concentrează pe formarea și certificarea în domeniul securității cibernetice, majoritatea femeilor care au lucrat în domeniu raportează discriminare bazată pe gen. Aproape toate femeile (87%) au declarat că au suferit o discriminare inconștientă, în timp ce 19% au declarat că au fost supuse discriminării deschise. Femeile au citat, de asemenea, întârzieri inexplicabile în avansarea în carieră (53%) și răspunsuri exagerate la erori (29%).

Discriminarea se manifestă și printr-un decalaj de compensare. Cercetările (ISC)2 arată că 32% dintre bărbații care lucrează în domeniul securității cibernetice câștigă în medie între 50.000 și 100.000 USD anual, în timp ce doar 18% dintre femeile din domeniul securității cibernetice ocupă aceeași categorie de venituri. Și 25% dintre bărbați față de 20% dintre femei câștigă între 100.000 și 500.000 de dolari anual.

Există argumente puternice pentru creșterea numărului de femei în securitatea cibernetică, cum ar fi beneficiile diversității, inovației, empatia emoțională și o perspectivă imparțială, care sunt toate abilități valoroase pentru locul de muncă în domeniul securității cibernetice.

Jay Koehler, membru al consiliului de administrație Women in Cybersecurity, a oferit o altă perspectivă: „Femeile abandonează pentru că este un club de „băieți" și există un sentiment scăzut de apartenență". Această problemă poate fi abordată prin angajamentul și responsabilitatea de a oferi siguranță psihologică și un loc de muncă prietenos cu genul și prin crearea de rețele de femei.

Există speranță că securitatea cibernetică nu va mai fi o „meserie dominată de bărbați", ci plină de oameni talentați de toate genurile și din toate mediile.

Literatura despre participarea femeilor la securitatea cibernetică în Spania este limitată. Cea mai mare parte a literaturii existente arată un dezechilibru pronunțat de gen în comunitatea științifică mai largă, inclusiv în disciplinele STEM, cu o scădere vizibilă a progresiei femeilor către etapele superioare ale carierei, considerate în mod obișnuit ca „fenomenul pipeline". În ceea ce privește învățământul superior, decalajul de gen este încă pronunțat, doar 18% dintre cei care finalizează studiile la aceste discipline fiind femei. Numărul de femei angajate de IMM-uri pe posturi legate de I+D este încă foarte scăzut, neatingând nici măcar 30% conform datelor Institutului Național de Statistică. În ceea ce privește femeile cercetătoare în domeniul securității cibernetice pentru instituțiile de învățământ superior din Spania, foarte puține dintre ele demonstrează un personal echilibrat în ceea ce privește genul. Din cele 31 de instituții de învățământ superior analizate de Fundación Alternativas, 11 dintre ele nu au nicio femeie care participă în echipele lor de cercetare și doar 5 dintre ele demonstrează o forță de muncă mai egalitară. Ca răspuns la aceste provocări, analiza nevoilor de formare și asistență identifică domenii cheie de îmbunătățire. Ar trebui dezvoltate inițiative pentru a încuraja mai multe femei să urmeze studii universitare de doctorat și pentru a asigura o reprezentare echilibrată pe întregul circuit educațional. Abordarea părtinirilor în procesele de avansare în carieră este crucială, iar programele de mentorat pot juca un rol esențial în ghidarea femeilor prin complexitățile domeniului securității cibernetice. În plus, se recomandă colaborarea cu organizațiile din industria privată pentru a investiga traiectorii de carieră și pentru a stimula implicarea femeilor în rolurile de securitate cibernetică din industriile private. Evaluarea calificărilor și competențelor subliniază importanța programelor de formare personalizate, subliniind abilitățile și competențele specifice de securitate cibernetică.

2.3. ANALIZA OCUPAȚIILOR ESCO

Interpretăm clasificarea existentă ESCO (Clasificarea multilingvă europeană a aptitudinilor, competențelor și ocupațiilor) în ceea ce privește rezultatele învățării identificate, inclusiv cunoștințele, abilitățile și competențele. Obiectivul este de a:

- • Analiza ocupațiile ESCO existente legate de securitatea cibernetică.
- • Creiona rezultatele învățării identificate la ocupațiile ESCO în termeni de cunoștințe, abilități, competențe etc.

Pentru fiecare ocupație, există un set de competențe, abilități și cunoștințe. Mai jos sunt enumerate definiții și exemple de competențe, abilități, cunoștințe și valoare.

Competența se referă la capacitatea unui individ de a îndeplini în mod eficient o anumită sarcină sau de a de descurca la un loc de muncă. Aceasta cuprinde o combinație de cunoștințe, abilități și comportamente aplicate pentru a îmbunătăți performanța. Exemplu: a fi competent în managementul proiectelor implică o combinație de abilități organizaționale, cunoaștere a proceselor de management de proiect și capacitatea de a comunica eficient cu membrii echipei.

Abilitățile sunt capacități sau abilități specifice dobândite prin practică, antrenament sau experiență care permit unui individ să îndeplinească sarcini. Exemplu: abilități de testare a penetrației, capacitatea de a utiliza instrumente și software de securitate cibernetică, abilități de programare și capacitatea de a analiza și de a răspunde la amenințări în timp real.

Cunoașterea se referă la faptele, informațiile și înțelegerea învățate prin educație sau experiență. Acesata cuprinde înțelegerea teoretică a faptelor și principiilor legate de un anumit domeniu. Exemplu: înțelegerea modului în care sunt efectuate diferite tipuri de atacuri cibernetice (de exemplu, phishing, ransomware, atacuri DDoS) sau cunoașterea diferitelor metode de criptare și familiarizarea cu cele mai recente tendințe și evoluții în domeniul securității cibernetice.

Această analiză este împărțită în 2 faze:

Faza 1: Revizuirea și selectarea ocupațiilor ESCO

Consultare pe portalul ESCO pentru filtrarea ocupațiilor legate de securitatea cibernetică și documentarea în secțiunea următoare a fiecărei ocupații, acordând o atenție deosebită abilităților, competențelor, cunoștințelor enumerate.

Denumirea ocupației ESCO	Cunoștințe	Abilități	Competențe
3512.3 - Tehnician în securitate TIC	• rețele TIC • vectori de atac hardware • contramăsuri pentru atacuri cibernetice	• abordarea problemelor în mod critic • analiza sistemului TIC	• integrarea componentelor sistemului • furnizarea documentației tehnice

	· achiziționarea sistemelor de operare TIC · echipamente de rețea · aplicație web · amenintari de securitate	· asigurarea unui management adecvat al documentelor · executarea de teste software identificarea punctele slabe ale sistemului TIC	· rezolvarea problemelor sistemului TIC · utilizarea software de control acces
2529.1 - Ofițer șef de securitate TIC - Include persoanele care îndeplinesc funcții de securitate corporativă.	· riscuri de securitate a rețelei TIC · legislația privind securitatea TIC · standarde de securitate TIC · vectori de atac · tehnici de audit · contramăsuri pentru atacuri cibernetice · securitate cibernetică · protejarea datelor · sisteme de sprijinire a deciziei · confidențialitatea informațiilor · strategia de securitate a informațiilor · politica internă de management al riscului · rezistența organizațională	· educarea cu privire la confidențialitatea datelor · asigurarea aderării la standardele TIC organizaționale · asigură conformitatea cu cerintele legale · asigurarea cooperării între departamente · asigurarea confidențialității informațiilor · identificarea riscurilor de securitate TIC · implementarea managementului riscului TIC · implementarea politicilor de siguranță TIC · implementarea guvernanței corporative	· conduce exerciții de recuperare în caz de dezastru · menținerea planului de continuitate a operațiunilor · gestionați conformitățile de securitate IT · gestionarea planurilor de recuperare în caz de dezastru · monitorizarea evoluțiilor în domeniul de expertiză · monitorizarea tendințelor tehnologice utilizarea sistemul de sprijinire a deciziilor
2529.2 - Expert criminalistică digitală - preia și analizează informații de pe computere și alte tipuri de dispozitive de stocare a datelor; examinează mediile digitale care ar fi putut fi ascunse, criptate sau deteriorate, în mod criminalistic, cu scopul de a identifica, păstra, recupera, analiza și prezenta fapte și opinii despre informațiile digitale.	· riscuri de securitate a rețelei TIC · standarde de securitate TIC · criminalistica informatică · contramăsuri pentru atacuri cibernetice · confidențialitatea informațiilor · instrument de testare la penetrare · limbaje de interogare · limbajul de interogare a cadrului de descriere a resurselor	· aplicarea ingineriei inverse · dezvoltarea strategiei de securitate a informațiilor · educarea cu privire la confidențialitatea datelor · culege date în scopuri criminalistice · identificarea riscurilor de securitate TIC · identificarea punctelor slabe ale sistemului TIC · implementarea instrumentelor de diagnosticare a rețelei TIC · oferirea de consultanță în	· gestionarea conformitățile de securitate IT · gestionarea datelor pentru chestiuni legale · efectuarea conservării criminalistice ale dispozitivelor digitale

		domeniul TIC · securizarea informațiilor sensibile ale clienților · utilizarea programării prin scripting · utilizarea software-ului pentru păstrarea datelor · efectuarea de teste de securitate TIC	
2529.3 - Inginer de securitate a sistemelor încorporate - inginerii de securitate a sistemelor încorporate se concentrează pe produsele conectate și rețelele de suport ale acestora, și mai puțin pe securitatea organizațională ca în cazul inginerului de securitate TIC.	· riscuri de securitate a rețelei TIC · standarde de securitate TIC · internetul Lucrurilor · programare pe calculator · contramăsuri pentru atacuri cibernetice · sisteme integrate · strategia de securitate a informațiilor · anomalii software	· analiza sistemului TIC · crearea diagramei de flux · definirea politicilor de securitate · dezvoltarea driverului de dispozitiv TIC · dezvoltarea prototipului de software · execută teste software · identificarea riscurilor de securitate TIC · identificarea punctelor slabe ale sistemului TIC · interpretarea textelor tehnice · oferirea de consultanță în domeniul TIC · efectuarea de teste de securitate TIC · furnizarea documentației tehnice	· ține pasul cu cele mai noi soluții de sisteme informatice · gestionarea conformitățile de securitate IT · monitorizarea performanței sistemului · efectuarea analizei de risc · raportarea rezultatelor testelor utilizează modele de proiectare software · utilizarea bibliotecii de software · utilizarea instrumentelor de inginerie software asistate de calculator · definirea cerințelor tehnice
2529.4 - Hacker etic - efectuează evaluări ale vulnerabilităților de securitate și teste de penetrare în conformitate cu metodele și protocoalele acceptate de industrie; analizează sistemele pentru potențiale vulnerabilități care pot rezulta din configurarea necorespunzătoare a sistemului, defecte hardware sau software sau slăbiciuni operaționale.	· vectori de atac · criminalistica informatică · contramăsuri pentru atacuri cibernetice · etică · cerințele legale ale produselor TIC · instrument de testare la penetrare · anomalii software · instrumente pentru automatizarea testelor TIC · amenințări la securitatea aplicațiilor web	· efectuarea de teste de securitate TIC · furnizarea documentației tehnice · dezvoltă exploit-uri de cod · execută audituri TIC · execută teste software · identificarea riscurilor de securitate TIC · identificarea punctelor slabe ale sistemului TIC	· abordarea problemelor în mod critic · analiza contextul unei organizații · monitorizarea performanței sistemului
2529.5 - Manager de reziliență TIC - cercetează, planifică și	· tehnici de recuperare TIC · securitate cibernetică	· elaborarea planurilor de urgență pentru	· analiza proceselor de afaceri

dezvoltă modele, politici, metode, tehnici și instrumente care îmbunătățesc securitatea cibernetică, reziliența și recuperarea în caz de dezastru a unei organizații	internă · politica de management al riscurilor · rezistența organizațională · cele mai bune practici de backup de sistem	situații de urgență · dezvoltarea strategiei de securitate a informațiilor · executa audituri TIC · identificarea riscurilor de securitate TIC · implementarea sistemului de recuperare TIC · implementarea managementului riscului TIC	· analiza contextul unei organizaţii · respectarea reglementărilor legale · conduce exerciții de recuperare în caz de dezastru · gestionarea conformităților de securitate IT · gestionarea planurilor de recuperare în caz de dezastru · gestionarea securității sistemului · efectuarea de teste de securitate TIC
2529.6 - Administrator de securitate ICT - planifică și efectuează măsuri de securitate pentru a proteja informațiile și datele împotriva accesului neautorizat, atacurilor deliberate, furtului și corupției.	· riscuri de securitate a rețelei TIC · internetul lucrurilor · contramăsuri pentru atacuri cibernetice · instrumente de dezvoltare a bazelor de date · guvernarea internetului · managementul dispozitivelor mobile · sisteme de operare · rezistența organizațională · metodologii de asigurare a calităţii · cele mai bune practici de backup de sistem	· identificarea punctelor slabe ale sistemului TIC · interpretarea textelor tehnice · menținerea managementului identității TIC · menţinerea securităţii bazei de date	· aplica politicile companiei · se ocupă de calitatea sistemelor TIC · asigură un management adecvat al documentelor · gestionarea arhitecturii de date TIC · gestionarea conformităților de securitate IT · efectuarea depanării TIC · rezolvarea problemelor sistemului TIC
2529.7 - Inginer de securitate ICT - consiliază și implementează soluții de control al accesului la date și programe și asigură protecția misiunii și proceselor de afaceri ale organizației.	· legislația privind securitatea TIC · standarde de securitate TIC · vectori de atac · analiza afacerii · contramăsuri pentru atacuri cibernetice · securitate cibernetică · tehnologii emergente · arhitectura informaţiei · strategia de securitate a informațiilor · sisteme de operare · rezistența organizațională · managementul riscurilor · date nestructurate	· dezvoltarea strategiei de securitate a informațiilor · educarea cu privire la confidențialitatea datelor · asigurarea securității informațiilor · execută audituri TIC · execută teste software · identificarea riscurilor de securitate TIC · identificarea punctelor slabe ale sistemului TIC · implementarea managementului riscului TIC · să ofere consultanță în	· definirea criteriilor de calitate a datelor · definirea cerințelor tehnice · păstrarea evidenței sarcinilor · ține pasul cu cele mai noi soluții de sisteme informatice · gestionarea conformităților de securitate IT · gestionarea planurilor de recuperare în caz de dezastru · monitorizarea performanței sistemului · efectuarea analizei datelor

		domeniul TIC · analiza sistemului TIC · definirea politicilor de securitate	· efectuarea analizei de risc · raportarea rezultatelor testelor de depanare · verificarea specificaţiilor formale TIC
2529.8 - Manager securitate ICT - propune și implementează actualizările de securitate necesare; sfătuiește, sprijină, informează și oferă instruire și conștientizare în materie de securitate și ia măsuri directe asupra întregii rețele sau a unei părți sau a unei rețele.	· tehnici de management al problemelor TIC · managementul proiectelor TIC · politica calității TIC · standarde de securitate TIC · Cerințele utilizatorilor sistemului TIC · internetul lucrurilor · vectori de atac · criminalistica informatică · strategia de securitate a informațiilor · politica internă de management al riscului · guvernarea internetului · cerințele legale ale produselor TIC	· definirea politicilor de securitate · dezvoltarea strategiei de securitate a informațiilor · stabilirea unui plan de prevenire a securității TIC · implementarea managementului riscului TIC	· conduce exerciții de recuperare în caz de dezastru · menținerea managementului identității TIC · gestionarea conformităților de securitate IT · gestionarea planurilor de recuperare în caz de dezastru · rezolvarea problemelor sistemului TIC
2529.9 - Inginer de cunoștințe - integrează cunoștințe structurate în sisteme informatice (baze de cunoștințe) pentru a rezolva probleme complexe care necesită în mod normal un nivel ridicat de expertiză umană sau metode de inteligență artificială.	· business intelligence · modelarea proceselor de afaceri · instrumente de dezvoltare a bazelor de date · extragerea informaţiilor · prelucrarea limbajului natural al structurii informaţiei · principiile inteligenței artificiale · limbajul de interogare a cadrului de descriere a resurselor · ciclul de viață al dezvoltării sistemelor · teoria sistemelor · algoritmizarea sarcinilor · programare web	· utilizează o interfață specifică aplicației · utilizează baze de date · utilizează limbaje de marcare	· analiza cerințelor de afaceri · aplicarea teoriei sistemelor TIC · evaluarea cunoștințelor TIC · crează arbori semantici · definirea cerințelor tehnice · gestionarea integrării semantice TIC · gestionarea cunoștințelor de afaceri · gestionarea bazei de date

Faza 2: Cartografierea ocupației ESCO și a rezultatelor învățării

Cu tabelul anterior, am analizat ocupațiile documentate și am identificat rezultatele învățării asociate fiecărui rol. Am folosit cadrul ESCO pentru a clasifica aceste rezultate în cunoștințe, abilități și competențe.

Un rezultat al învățării este o declarație clară și specifică care descrie ceea ce se așteaptă ca elevii să învețe și să poată face la finalizarea unei perioade de instruire. Declarația include cunoștințe, abilități și atitudini.

În secțiunea de clasificare a ocupațiilor ESCO, profesioniștii în tehnologia informației și comunicațiilor se află în două subsecțiuni: Dezvoltatori și analiză de software și aplicații și Profesioniști în baze de date și rețele. Ultimul este format din patru grupuri: profesioniști în baze de date și rețele, administratori de sisteme, profesioniști în rețele de calculatoare și profesioniști în baze de date și rețele neclasificați în altă parte. Toate ocupațiile de securitate cibernetică prezentate în tabel au fost găsite în acest grup de unități. De exemplu, grupul include specialiști în securitatea tehnologiei informației și comunicațiilor.

În astfel de cazuri, sarcinile ar include:

(a) elaborarea de planuri pentru a proteja fișierele computerizate împotriva modificărilor, distrugerii sau dezvăluirii accidentale sau neautorizate și pentru a satisface nevoile de prelucrare a datelor de urgență.

(b) formarea utilizatorilor și promovarea conștientizării securității pentru a asigura securitatea sistemului și pentru a îmbunătăți eficiența serverului și a rețelei.

(c) comunicarea cu utilizatorii pentru a discuta probleme precum nevoile de acces la date computerizate, încălcările securității și modificările de programare.

(d) monitorizarea rapoartelor curente privind virușii informatici pentru a determina când să actualizeze sistemele de protecție împotriva virușilor.

(e) modificarea fișierelor de securitate a computerului pentru a încorpora software-ul nou, corectarea erorilor sau modificarea statutului de acces individual.

(f) monitorizarea utilizării fișierelor de date și reglementarea accesului la informațiile de siguranță din fișierele computerizate.

(g) efectuarea de evaluări de risc și efectuarea de teste ale sistemului de prelucrare a datelor pentru a asigura funcționarea activităților de prelucrare a datelor și a măsurilor de securitate.

(h) criptarea transmisiilor de date și construirea de firewall-uri pentru a ascunde informațiile confidențiale pe măsură ce acestea sunt transmise și pentru a evita transferurile digitale afectate.

Descrierea rezultatelor învățării pentru fiecare ocupație:

Ocupație	Rezultatele învățării
Tehnician în securitate TIC (3512.3)	· Demonstrează o înțelegere cuprinzătoare a rețelelor TIC, a vectorilor de atac hardware, a contramăsurilor împotriva atacurilor cibernetice și a sistemelor de operare. · Analizează critic și diagnostichează vulnerabilitățile din sistemele TIC pentru a îmbunătăți securitatea sistemului. · Implementează și gestionează strategii solide de gestionare a documentelor care să adere la protocolele de securitate TIC. · Dezvoltă și execută planuri detaliate de testare a software-ului pentru a identifica și rectifica vulnerabilitățile software. · Integrează componentele sistemului și utilizează software-ul de control al accesului pentru a construi sisteme TIC sigure și eficiente.
Ofițer șef de securitate TIC (2529.1)	· Înțelege și analizează riscurile de securitate a rețelei TIC, legislația și standardele pentru a proteja informațiile organizaționale. · Dezvoltă și implementează strategii de securitate a informațiilor și politici interne de gestionare a riscurilor. · Conduce exerciții de recuperare în caz de dezastru și menține planurile de continuitate operațională. · Educă personalul cu privire la confidențialitatea datelor și asigură cooperarea între departamente pentru practici de securitate îmbunătățite.
Expert în criminalistică digitală (2529.2)	· Analizează și testează securitatea sistemelor încorporate, în special în mediul Internet of Things (IoT). · Dezvoltă și execută prototipuri și teste software și utilizează instrumente de inginerie software asistate de calculator. · Gestionează conformitățile de securitate IT și efectuează analize de risc și monitorizare a performanței sistemului. · Definește și implementează politicile de securitate

	și cerințele tehnice pentru sistemele încorporate.
Inginer Securitate Sisteme Încorporate (2529.3)	· Analizează și testează securitatea sistemelor încorporate, în special în mediul Internet of Things (IoT). · Dezvoltă și execută prototipuri și teste software și utilizează instrumente de inginerie software asistate de calculator. · Gestionează conformitățile de securitate IT și efectuează analize de risc și monitorizare a performanței sistemului. · Definește și implementează politicile de securitate și cerințele tehnice pentru sistemele încorporate.
Hacker Etic (2529.4)	· Efectuează evaluări ale vulnerabilităților de securitate și teste de penetrare folosind metode acceptate de industrie. · Identifică și exploatează potențialele vulnerabilități în sisteme pentru a îmbunătăți măsurile de securitate. · Dezvoltă exploatările de cod și execută audituri TIC pentru a asigura integritatea sistemului. · Analizează contextul unei organizații pentru a adapta eficient strategiile de securitate
Manager Reziliență TIC (2529.5)	· Dezvoltă și implementează planuri de urgență și strategii de securitate a informațiilor pentru scenarii de urgență. · Implementează și gestionează sistemele de recuperare TIC și procesele de management al riscului. · Conduce exerciții de recuperare în caz de dezastru și gestionează securitatea sistemului în timpul crizelor. · Analizează procesele de afaceri pentru a îmbunătăți rezistența organizațională și conformitatea cu reglementările legale.
Administrator de securitate TIC (2529.6)	· Planifică și implementează măsuri de securitate pentru protejarea datelor și gestionarea sistemelor de identitate TIC. · Menține securitatea bazei de date și asigură integ-

	ritatea și rezistența sistemului. · Rezolvă problemele sistemului TIC și realizează metodologiilor de depanare și de asigurare a calității. · Gestionează arhitectura datelor și respectă politicile organizaționale pentru protecția datelor.
Inginer de securitate TIC (2529.7)	· Consiliază și implementează soluții pentru a controla accesul la date și pentru a proteja procesele de afaceri. · Analizează sistemele TIC și definește politicile de securitate și criteriile de calitate a datelor. · Efectuează analize de date și analize de risc și gestionează conformitățile de securitate IT și planurile de recuperare în caz de dezastru. · Este la curent cu tehnologiile emergente și soluțiile sistemelor informaționale
Manager de securitate TIC (2529.8)	· Propune și implementează actualizări de securitate și gestionează securitatea TIC în diferite proiecte. · Conduce exerciții de recuperare în caz de dezastru și stabilește planuri de prevenire a securității TIC. · Menține și gestionează sistemele de management ale identității TIC și rezolvă problemele complexe ale sistemului. · Dezvoltă și implementează strategii de securitate a informațiilor și gestionează planuril de recuperare în caz de dezastru.
Inginer de cunoștințe (2529.9)	· Integrează cunoștințele structurate în sistemele informatice folosind instrumente avansate precum limbajul de interogare RDF și programarea web. · Gestionează integrarea semantică și sistemele de baze de date pentru a îmbunătăți gestionarea cunoștințelor de afaceri. · Analizează cerințele de afaceri și aplică teoria sistemelor TIC pentru a dezvolta baze de cunoștințe eficiente. · Crează arbori semantici și evaluează cunoștințele TIC pentru a rezolva probleme complexe folosind metode AI.

3. ANALIZĂ SI CONSTATĂRI

3.1. ANALIZA CERCETĂRII PE TEREN

Analiza cercetărilor pe teren VET și IIS

Datele sondajului din "Raportul de identificare a nevoilor de formare ale agenților de schimbare a securității cibernetice pentru IMM-uri" conțin o serie de întrebări care se concentrează pe formarea în domeniul securității cibernetice în contextul educației și formării profesionale (VET) și al instituțiilor de Învățământ Superior (IIS). Am colectat date despre subiecte incluse în formarea în domeniul securității cibernetice, metodele de predare, incluziunea de gen și demografia respondenților.

Scopul acestui studiu este de a analiza răspunsurile pentru a înțelege starea actuală a formării în domeniul securității cibernetice, metodologiile utilizate și percepțiile despre incluziune și eficacitate în acest domeniu.

Analiza răspunsurilor se va baza pe următoarea structură cheie:

- • Demografie
- • Curriculum, nevoile de formare și preferințele de învățare
- • Cerințe de competență și abilități viitoare
- • Perspective specifice genului

Date demografice:

Repartiția de gen în rândul respondenților la sondaj între instituțiile de învățământ și formare profesională (VET) și Instituțiile de Învățământ Superior (IIS) este următoarea:

Total de respondenți pe tip de instituție

Tipul institutiei	Răspunsuri	Feminin	Masculin	Prefer să nu spun
IIS (Instituții de Învățământ Superior)	104	28	73	3
VET (Educație și formare profesională)	86	36	48	2
Total	**190**	**64**	**121**	**5**

Deși există un dezechilibru de gen atât în IIS, cât și în instituțiile VET, decalajul este mai mic în instituțiile VET. Pentru a oferi o imagine mai clară a reprezentării de gen în raport cu numărul total de răspunsuri din fiecare instituție și pentru a ajusta rezultatele în ceea ce privește numărul de părtinire a răspunsurilor, am calculat procentul fiecărui gen în ambele tipuri de instituții.

Distribuția respondenților pe tip de instituție

Tipul instututiei	Feminin %	Masculin %	Prefer sa nu spun %	Total
IIS (Instituții de Învățământ Superior)	27	70	3	**100%**
VET (Educație și formare profesională)	42	56	2	**100%**

Analiza ajustată pentru părtinirea răspunsului confirmă că, deși ambele tipuri de instituții au o proporție mai mare de respondenți de sex masculin, diferența dintre reprezentarea bărbaților și femeilor rămâne mai mică în instituțiile VET. Motivul ar putea fi divers (de exemplu, factori culturali, structurali sau politici care influențează diversitatea de gen în educația în domeniul securității cibernetice în aceste tipuri de instituții). Procentul mai mare de respondenți de sex feminin în VET sugerează domenii potențiale de investigare ulterioară a practicilor care susțin un mediu mai cuprinzător de gen în formarea profesională, comparativ cu învățământul superior.

Curriculum, nevoi de formare și preferințe de învățare

Subiecte incluse în cursurile existente în domeniul securității cibernetice pentru IIS și VET

Subiect	Răspunsuri	IIS	VET
Fundamentele securității cibernetice	151	90	61
Securitatea rețelei	123	72	51
Analiza și managementul amenințărilor	99	65	34
Criptografie	92	57	35
Răspuns la incident	82	49	33
Managementul riscului	77	43	34
Legile și politicile de securitate cibernetică	73	42	31
Tehnici avansate de atenuare a amenințărilor	54	33	21

Se pare că, cunoștințele și abilitățile de bază și securitatea rețelei sunt o prioritate. Analiza și managementul amenințărilor, Criptografia și Răspunsul la incident sugerează o acoperire cuprinzătoare a amenințărilor de securitate cibernetică în cadrul cursurilor. Legile și politicile privind managementul riscurilor și securitatea cibernetică, în ciuda faptului că indică conștientizarea necesității unei abordări holistice care să includă înțelegerea contextului legal și gestionarea eficientă a riscurilor, nu este întotdeauna selectată. Este interesant de observat că tehnicile avansate de atenuare a amenințărilor sunt mai puțin incluse în cursuri.

Pentru a furniza rezultatele fără părtinirea introdusă de numărul de respondenți din fiecare tip de instituție (IIS și VET), datele au fost normalizate prin numărul total de răspunsuri pentru

fiecare tip de instituție. Această abordare ne permite să vedem proporția instituțiilor care includ fiecare subiect în programele lor de formare în domeniul securității cibernetice.

Subiecte	Proporție IIS	Proporție VET
Fundamentele securității cibernetice	15.76%	15.48%
Securitatea rețelei	12.61%	12.94%
Analiza și managementul amenințărilor	11.38%	8.63%
Criptografie	9.98%	8.88%
Răspuns la incident	8.58%	8.38%
Managementul riscului	7.53%	8.63%
Legile și politicile de securitate cibernetică	7.36%	7.87%
Tehnici avansate de atenuare a amenințărilor	5.78%	5.33%

Interesant este că există priorități similare, cu mici variații. Atât instituțiile de învățământ superior, cât și instituțiile VET pun un accent semnificativ pe „Fundamentele securității cibernetice" și „Securitatea rețelei". Acest lucru indică faptul că aceste subiecte sunt recunoscute ca și componente critice ale educației în domeniul securității cibernetice. Proporțiile sunt strâns corelate, „Fundamentele securității cibernetice" puțin mai accentuate în instituțiile de învățământ superior în comparație cu VET și „Securitatea rețelei" prezentând un model similar, dar cu un decalaj mai mic.

Există o variație notabilă în accentul pus pe subiecte mai specializate, cum ar fi „Analiza și managementul amenințărilor", „Criptografie" și „Tehnici avansate de atenuare a amenințărilor". Instituțiile de învățământ superior tind să aloce o proporție puțin mai mare din programele lor de formare acestor subiecte în comparație cu VET. Poate fi explicat prin faptul că instituțiile de învățământ superior se concentrează pe furnizarea unei înțelegeri mai cuprinzătoare, bazate pe teorie, a securității cibernetice, care include adesea o gamă mai largă de subiecte specializate. Pe de altă parte, instituțiile VET, deși acoperă în continuare un spectru larg de subiecte, pot acorda prioritate aplicațiilor practice și pregătirii imediate pentru angajare.

Metode de predare

Metode de predare	Proporție IIS	Proporție VET
Studii de caz	60.91%	39.09%
Proiecte de grup	58.95%	41.05%
Laboratoare practice	59.02%	40.98%
Prelegeri	56.97%	43.03%
Flipped classroom	34.78%	65.22%
Simulări online	51.35%	48.65%

Metodele studii de caz, proiecte de grup, laboratoare practice, prelegeri sunt utilizate pe scară largă în ambele tipuri de instituții, cu o preferință în IIS decât în VET. În ceea ce privește metoda flipped classroom, aceasta este mai răspândită în VET (65,22%) decât în IIS (34,78%), indicând o înclinație spre modelul de învățare interactivă în învățământul profesional. Flipped classroom

prioritizează învățarea activă și implicarea studenților, care se aliniază bine cu abordarea practică și bazată pe competențe caracteristică VET.

Eficacitatea metodelor de predare

Metode de predare	Număr
Sesiuni practice de antrenament	141
Ateliere personale	134
Simulări interactive	104
Cursuri online	100
Tutoriale video	73
Webinarii	68

Această prezentare generală evidențiază o diversitate în metodele de predare preferate, dar cu un accent clar pe experiențe de învățare practice, interactive și flexibile. Sesiunile practice și atelierele în persoană sunt foarte apreciate, deoarece oferă o experiență de învățare interactivă și practică. Simulările interactive și cursurile online au primit, de asemenea, mențiuni semnificative care arată importanța modalităților de învățare accesibile.

Provocări cu care se confruntă instituțiile școlare.

Întrebați despre principalele provocări cu care se confruntă instituțiile școlare, iată un rezumat al celor mai recurente subiecte:

- **Diversitatea abilităților și experienței participanților**: formatorii se confruntă cu dificultăți din cauza mediilor și nivelurilor de expertiză variate ale participanților. Personalizarea instruirii pentru a se potrivi întregului grup și asigurarea faptului că atât persoanele tehnice, cât și cele non-tehnice pot beneficia de sesiuni este o provocare.
- **Menținerea actuală a materialelor de curs**: evoluția rapidă a amenințărilor la adresa securității cibernetice necesită actualizări continue ale materialelor de instruire și metodelor de predare pentru a asigura relevanța.
- **Constrângeri practice de formare**: există o provocare semnificativă în furnizarea de experiență practică. Limitările includ facilități insuficiente de laborator, lipsa capacităților de simulare în lumea reală și dificultatea de a crea scenarii realiste de atac cibernetic pentru practică.
- **Limitări de resurse**: formatorii trebuie adesea să se confrunte cu resurse financiare limitate, lipsa de personal calificat, materiale de studiu învechite și instrumente hardware și software insuficiente necesare pentru o formare eficientă.
- **Implicarea și motivarea elevilor**: menținerea atenției elevilor și motivarea acestora să participe activ la învățarea lor este dificilă, mai ales cu nevoia de a acoperi conținut tehnic complex și uneori sec.

- **Curriculum și structură educațională**: este nevoie de programe cuprinzătoare, multidisciplinare, care să acopere toate aspectele securității cibernetice. În plus, încorporarea securității cibernetice în curriculum, în special la nivel de liceu, rămâne o provocare semnificativă.
- **Accesul la instrumente și tehnologii actualizate**: Oferirea studenților acces la cele mai recente instrumente și tehnologii de securitate cibernetică pentru învățarea practică este adesea o provocare, ceea ce este crucial pentru înțelegerea practică.
- **Probleme legate de limbă și localizare**: este posibil ca resursele de securitate cibernetică să nu fie întotdeauna disponibile în limbile materne ale studenților, adăugând un nivel de complexitate pregătirii în regiunile care nu vorbesc engleza.
- **Alinierea industriei și educaționale**: echilibrarea nevoii de a preda bazele teoretice cu abilitățile practice care se potrivesc nevoilor industriei este o provocare. Există, de asemenea, necesitatea pregătirii studenților pentru piața muncii cu competențe relevante.
- **Capacitatea și dezvoltarea profesorilor**: asigurarea faptului că educatorii au cunoștințe actualizate și sunt capabili să transmită în mod eficient concepte complexe este crucială, dar o provocare.

Alinierea la nevoile specifice ale IMM-urilor

Opțiunea de răspuns	Număr
Neutru	82
Potrivit	67
Ușor potrivit	19
Foarte potrivit	17
Nepotrivit	5

Majoritatea răspunsurilor indică o potrivire neutră, ceea ce sugerează că există loc de îmbunătățire în ceea ce privește acel punct. Un număr semnificativ de respondenți și-au evaluat programele ca fiind potrivite, în timp ce foarte puțini educatori cred că programele lor sunt foarte potrivite sau nu sunt potrivite cu nevoile industriei. Răspunsurile de la capătul inferior al scalei (nepotrivite și ușor potrivite) reflectă preocupările sau provocările în alinierea completă a conținutului educațional cu natura în evoluție a securității cibernetice din industrie. Această distribuție a răspunsurilor arată că provocarea de a asigura o educație în domeniul securității cibernetice, adaptată la tendințele și cerințele industriei este încă relevantă. Subliniază relevanța proiectului CyberAgent, care își propune să ofere actualizări continue ale curriculumului, parteneriate din industrie și oportunități de formare practică pentru a îmbunătăți alinierea programelor de formare în domeniul securității cibernetice la nevoile industriei de securitate cibernetică.

Teme specifice pentru IMM-uri

Subiect/Abilitate	Număr
Securitate cibernetică de bază pentru IMM-uri	91
Protecția datelor și confidențialitatea pentru IMM-uri	75
Nu sunt incluse în program niciun subiect sau abilități specifice IMM-urilor	**64**
Răspunsul la incident pentru IMM-uri	58
Evaluarea și managementul riscurilor în contextul IMM-urilor	53
Dezvoltarea politicii de securitate cibernetică pentru IMM-uri	46

Se pune un accent puternic pe principiile fundamentale de securitate cibernetică și protecția datelor. Subiectele cele mai frecvent menționate, Securitatea cibernetică de bază pentru IMM-uri și Protecția datelor și confidențialitatea pentru IMM-uri, indică faptul că educatorii acordă prioritate dotării IMM-urilor cu cunoștințele necesare pentru a-și proteja datele și pentru a înțelege conceptele de bază de securitate cibernetică. Numărul „Niciun subiect sau abilități specifice IMM-urilor nu sunt incluse în program" indică un decalaj în unele programe de formare în domeniul securității cibernetice în ceea ce privește conținutul personalizat pentru Întreprinderile Mici și Mijlocii (IMM-uri). Acesta evidențiază un domeniu critic pentru îmbunătățirea formării în domeniul securității cibernetice, mai ales având în vedere provocările și amenințările cu care se confruntă IMM-urile.

IMM-urile operează adesea cu resurse limitate și este posibil să nu aibă acces la expertiză specializată în securitate cibernetică, ceea ce le face deosebit de vulnerabile la amenințările cibernetice. Absența conținutului specific IMM-urilor în programele de formare în domeniul securității cibernetice sugerează că aceste programe s-ar putea să nu răspundă pe deplin nevoilor distincte ale IMM-urilor, lăsând potențial un gol în pregătirea și rezistența acestora împotriva atacurilor cibernetice. Remedierea acestui decalaj necesită integrarea unor subiecte și competențe special concepute pentru a satisface nevoile de securitate cibernetică ale IMM-urilor, cum ar fi evaluarea riscurilor adaptată operațiunilor comerciale mai mici, practici de securitate cibernetică rentabile și strategii pentru dezvoltarea unei politici eficiente de securitate cibernetică cu resurse limitate.

Deficitul de competențe al angajaților IMM-urilor

Abilitate/ Subiect	Număr
Detectarea amenințărilor și răspunsul	103
Expertiza securității cloud	87
Răspuns la incident și recuperare	69
Confidențialitatea și protecția datelor	67
Managementul și analiza riscurilor	63
Tehnologii emergente	58
Securitatea rețelei	41
Cunoștințe privind conformitatea și reglementările	36

Analiza relevă faptul că angajaților le lipsesc abilitățile în domenii cheie, detectarea și răspunsul amenințărilor fiind cele mai frecvent menționate. Acest lucru evidențiază importanța pregătirii studenților pentru a identifica și a răspunde la amenințările de securitate cibernetică ca o capacitate esențială în domeniu. Expertiza în domeniul securității în cloud ocupă locul al doilea, arătând încrederea în tehnologiile cloud și nevoia de cunoștințe specializate pentru a securiza mediile cloud de la angajați. Răspunsul la incident și recuperarea, confidențialitatea și protecția datelor și gestionarea și analiza riscurilor sunt de asemenea apreciate. Se consideră că în ceea ce privește tehnologiile emergente, necesitatea de a rămâne la curent cu ultimele progrese în domeniu nu este o zonă deficitară. La fel și pentru securitatea rețelei, care este un domeniu fundamental care face parte din majoritatea programelor de formare în domeniul securității cibernetice. Arată eficacitatea antrenamentelor în acest punct.

Amenințări

Amenințări	Număr
Atacurile cibernetice determinate de AI	117
Atacurile ransomware	96
Phishing și inginerie socială	87
Încălcări de securitate în cloud	82
Vulnerabilități IoT	75
Amenințări deepfake	51
Amenințări din interior	25

Analiza dezvăluie o concentrare semnificativă asupra atacurilor cibernetice determinate de inteligență artificială ca fiind cea mai frecvent menționată amenințare emergentă pentru securitatea cibernetică, indicând o preocupare față de sofisticarea și complexitatea amenințărilor cibernetice alimentate de inteligența artificială. Atacurile ransomware și phishingul și ingineria socială s-au clasat, de asemenea, la un loc înalt, arătând prezența acestor vectori de atac în IMM-uri. Încălcările securității în cloud și vulnerabilitățile IoT evidențiază preocupările legate de securitatea serviciilor cloud și de extinderea Internetului obiectelor, reflectând provocările în protejarea ecosistemelor tehnologice diverse și distribuite pentru IMM-uri. Amenințările deepfake și amenințările interne nu sunt considerate vectori mari de amenințări. Un program de instruire care acoperă primele 5 subiecte poate echipa mai bine studenții și angajații IMM-urilor pentru a aborda amenințările cu care se confruntă.

Tendințe emergente

Zonă	Număr
Inteligența artificială și învățarea automată în securitatea cibernetică	160
Identitate digitală și confidențialitate	96
Hacking etic și abilități defensive	82
Amenințări de calcul cuantic	67
Sisteme de securitate descentralizate (de exemplu, Blockchain)	52
Concentrare pe abilități soft și formare interdisciplinară	47

Se pune un accent puternic pe inteligența artificială și învățarea automată în domeniul securității cibernetice, ca domeniu cel mai frecvent menționat, reflectând importanța acestor tehnologii în îmbunătățirea măsurilor de securitate cibernetică și nevoia de profesioniști calificați în aceste domenii. Identitatea digitală și confidențialitatea reprezintă un alt obiectiv important care evidențiază importanța protejării identităților digitale și a asigurării confidențialității. Scorul Ethical Hacking și Defensive Skills indică o cerere pentru abilități practice, care permit profesioniștilor să identifice vulnerabilitățile și să se apere împotriva atacurilor în mod eficient. Amenințările de calcul cuantic, sistemele de securitate descentralizate, cum ar fi tehnologia Blockchain, soft skills și pregătirea interdisciplinară nu au fost considerate tendințe emergente. Distribuția răspunsurilor evidențiază diversitatea domeniului securității cibernetice și importanța pregătirii profesioniștilor cu un set divers de abilități și cunoștințe pentru a aborda provocările actuale și viitoare. Dar subiectul AI rămâne în partea de sus a listei.

Egalitatea sexelor

Procentul de femei	Număr de răspunsuri
Sub 10%	57
10% - 25%	79
26% - 50%	43
51% - 75%	8
Peste 75%	3

Procentul de femei în programele de formare în domeniul securității cibernetice relevă o disparitate în diversitatea de gen, majoritatea răspunsurilor indicând o participare scăzută a femeilor. În detalii, 79 de răspunsuri au plasat participarea femeilor între 10% și 25%, iar 57 de răspunsuri au indicat că a fost mai mică de 10%. Un nivel moderat de diversitate de gen este sugerat în unele programe, 43 de respondenți estimând rata de participare a femeilor între 26% și 50%. Cu toate acestea, programele cu un procent ridicat de participante feminine sunt deosebit de rare, evidențiate de doar 8 răspunsuri care indică un interval de 51% până la 75% și un număr minim de 3 răspunsuri care estimează mai mult de 75%. Aceste date subliniază provocarea în atingerea diversității de gen în cadrul programelor de formare în domeniul securității cibernetice, evidențiind un decalaj substanțial în participarea femeilor în majoritatea programelor raportate.

Inițiative de gen

Raăpuns	Număr de răspunsuri
Da	30
Nu	160

Datele indică faptul că o majoritate semnificativă a respondenților, 160 în total, nu folosesc inițiative sau strategii specifice pentru a încuraja participarea femeilor la formarea în domeniul securității cibernetice. Doar 30 de respondenți au confirmat implementarea unor astfel de

măsuri. Acest lucru sugerează că, deși există o anumită conștientizare și efort pentru creșterea participării femeilor la formarea în domeniul securității cibernetice prin inițiative specifice, este posibil ca majoritatea programelor să nu prioritizeze sau să implementeze încă strategii specifice pentru a aborda diversitatea de gen. Această lipsă de inițiative direcționate ar putea contribui la procentele scăzute de participare a femeilor, așa cum sa menționat în răspunsurile la întrebarea anterioară.

Formare care să includă genul

Răspuns	Număr de răspunsuri
Da	47
Nu	44
Nesigur	72
Fără relevanță pentru mine	27

Rezultatele sugerează o opinie împărțită în rândul respondenților cu privire la disponibilitatea modulelor de formare care să includă genul în domeniul securității cibernetice. Cel mai mare grup, format din 72 de respondenți, și-a exprimat incertitudinea („Nesigur”), indicând o lipsă de consens clar sau de cunoștințe despre prezența materialelor care includ genul. Există o divizare aproape egală între cei care cred că există suficiente module care includ genul (47 de răspunsuri) și cei care nu o fac (44 de răspunsuri). În plus, 27 de respondenți au considerat că întrebarea nu este relevantă pentru experiența sau contextul lor.

Această diviziune reflectă dezbaterea în curs și percepțiile variate despre incluziunea conținutului de formare în domeniul securității cibernetice. Numărul mare de răspunsuri nesigure evidențiază un potențial decalaj în conștientizarea sau accesibilitatea resurselor de formare care să includă genul în cadrul ecosistemului de educație și formare în domeniul securității cibernetice.

Bariere împotriva incluziunii de gen

Barieră	Număr
Stereotipuri sau norme culturale	107
Lipsa de conștientizare a oportunităților în securitatea cibernetică	86
Lipsa de mentorat sau modele de urmat	74
Provocări privind echilibrul dintre viața profesională și viața privată	60
Prejudecățile de gen percepute în industrie	58

Cele mai semnificative bariere în calea participării femeilor la securitatea cibernetică, așa cum sunt percepute de respondenții la sondaj, sunt stereotipurile sau normele culturale (107 mențiuni) și lipsa de conștientizare a oportunităților în securitatea cibernetică (86 mențiuni). Aceste două bariere sugerează că percepțiile societale și informațiile insuficiente despre traseele de carieră împiedică în mod semnificativ intrarea femeilor în domeniul securității cibernetice. Lipsa de mentorat sau modele de urmat și provocările echilibrului dintre viața profesională și viața privată sunt, de asemenea, bariere substanțiale, subliniind importanța

rețelelor de sprijin și a mediilor de lucru flexibile în încurajarea participării femeilor. În plus, părtinirea de gen percepută în industrie indică necesitatea unor schimbări culturale și sistemice în domeniu pentru a-l face mai primitor și mai echitabil pentru femei.

Program specific de promovare a diversității și incluziunii

Răspuns	Număr de răspunsuri
Da	44
Nu	85
Nesigur	61

Datele arată că o parte semnificativă a instituțiilor chestionate, cu 85 de răspunsuri, nu au politici sau programe specifice pentru promovarea diversității și incluziunii pentru femei în formarea în domeniul securității cibernetice. Totuși, 44 de respondenți au indicat că instituțiile lor implementează astfel de inițiative, evidențiind o abordare pentru încurajarea diversității de gen în domeniu. Cu toate acestea, un număr notabil de respondenți, 61, nu sunt siguri dacă instituțiile lor au astfel de politici sau programe, indicând o potențială lipsă de comunicare sau conștientizare cu privire la eforturile existente de diversitate și incluziune. De asemenea, acest răspuns mixt sugerează că, în timp ce unele instituții fac pași către incluziune în formarea în domeniul securității cibernetice, rămâne un decalaj substanțial, atât în implementarea programelor de diversitate, cât și în conștientizarea unor astfel de inițiative în rândul profesorilor, personalului și studenților.

Sugestie de îmbunătățiri

Sugestie	Număr
Vizibilitate sporită a profesioniștilor de succes în domeniul securității cibernetice	95
Mai multe femei instructoare de securitate cibernetică sau personal de formare	89
Oferiți burse sau stimulente	81
Oportunități de mentorat	49
Conținut de instruire care evită părtinirile de gen	33
Actualizați în mod regulat politicile pentru a sprijini incluziunea	31
Studii de caz și scenarii care includ genul	24
Programe de instruire personalizate	21
Mai multe sesiuni de antrenament numai pentru femei	18

Analiza răspunsurilor, cu privire la sugestiile pentru a face formarea în domeniul securității cibernetice mai incluzivă de gen, relevă un consens puternic asupra importanței mai multor strategii cheie. Cea mai susținută sugestie, cu 95 de mențiuni, este vizibilitatea sporită a femeilor profesioniste de succes în securitate cibernetică. Acest lucru subliniază rolul critic al modelelor de urmat și al figurilor aspiraționale în inspirarea femeilor să urmeze o carieră în securitatea cibernetică. Următoarea, cu 89 de mențiuni, este apelul pentru mai multe femei

instructoare de securitate cibernetică sau personal de formare, evidențiind nevoia de reprezentare în cadrul forței de muncă din învățământ. Oferirea de burse sau stimulente, cu 81 de mențiuni, este identificată ca fiind crucială pentru a face domeniul mai accesibil financiar și mai atrăgător pentru femei. Oportunitățile de mentorat, remarcate de 49 de respondenți, subliniază importanța îndrumării și sprijinului din partea profesioniștilor cu experiență în domeniu. Nevoia de conținut de formare care să evite părtinirile de gen și politici actualizate în mod regulat pentru a sprijini incluziunea, indică necesitatea unor ajustări ale curriculumului și ale politicilor care reflectă și promovează diversitatea.

Analiza sondajului pe teren pentru IMM-uri

Demografie:

Sondajul a primit răspunsuri din partea țărilor partenere. România are cel mai mare număr de respondenți (28), urmată de Norvegia (23), apoi Lituania, Spania și Belgia, fiecare cu 21 de respondenți. Finlanda și Turcia au, de asemenea, un număr semnificativ de răspunsuri, 20 fiecare, iar Polonia 19 respondenți.

Sectorul companiei

Sectorul companiei	Număr
IT	18
Educație	6
Construcții	4
Consultanță	4
Securitate cibernetică	4

Datele indică o reprezentare puternică a sectorului IT, 18 respondenți identificându-și compania ca activând în acest sector. Sectoarele educație, construcții, consultanță și securitate cibernetică au, de asemenea, reprezentări notabile, fiecare cu numere variind de la 4 la 6. Dincolo de primele cinci, există o listă lungă de sectoare cu mai puține răspunsuri, ilustrând abordarea largă a sondajului în diverse industrii.

Profilul respondenților

Poziția în companie	Număr
Manager	48
Executiv/Proprietar	35
Tehnic (inginer/dezvoltator/analist)	27
Altele	25
Coordonator/Administrator	8
Vânzări & Marketing	8
Specialist/Expert	8
Angajat	8
Consultant	3

Poziția în companie	Număr
Educație/Predare	2
Contabilitate financiară	1
Management de proiect	1
HR	1
Total	**175**

Există o mare varietate de titluri de post, cu un public profesional divers și un panou mare de posturi, cum ar fi „Angajat” și „Director”, care indică un spectru larg de respondenți, care acoperă diferite niveluri în cadrul ierarhiilor organizaționale. Securitatea cibernetică este o problemă transversală care implică indivizi în diferite roluri și responsabilități în cadrul companiilor.

Gen

Distribuția de gen în rândul respondenților la sondaj relevă o reprezentare mai mare a bărbaților (102) comparativ cu femeile (69), o mică parte a respondenților (4) preferând să nu dezvăluie genul lor. Această distribuție sugerează o diferență de gen în domeniul reprezentat de sondaj, care reflectă tendințele mai ample din sectoarele securității cibernetice și tehnologiei, unde este adesea raportată dominația masculină. Cu toate acestea, numărul semnificativ de respondenți de sex feminin indică o participare semnificativă a femeilor în domeniu, indicând schimbări continue în diversitatea de gen a sectorului. În timp ce decalajul de gen este evident, diversitatea răspunsurilor indică, de asemenea, un peisaj în schimbare treptată în securitatea cibernetică.

Distribuția de gen pe țară

Țară	Feminin	Masculin	Prefer să nu spun
Belgia	10	10	1
Finlanda	9	11	0
Lituania	9	12	0
Norvegia	8	15	0
Polonia	8	9	2
Romania	12	16	0
Spania	6	14	1
Turcia	7	13	0

Tabelul arată distribuția de gen în diferite țări. Respondenții de sex masculin sunt mai mulți decât respondenții de sex feminin în fiecare țară, în concordanță cu distribuția generală pe sexe discutată mai devreme. Cu toate acestea, decalajul variază în funcție de țară, unele țări precum Belgia prezentând un număr egal de respondenți de sex masculin și feminin (10 fiecare) și Polonia având o distribuție mai apropiată între bărbați (9) și femei (8), un număr mic de respondenți preferând să nu precizeze sexul lor (2). Țări precum România și Norvegia au un număr mai mare de respondenți în general și mențin un raport mai mare între bărbați și femei.

Această defalcare de gen în funcție de țară oferă o înțelegere nuanțată a componenței demografice a respondenților la sondaj, evidențiind atât disparitățile de gen, cât și diversitatea geografică în domeniul securității cibernetice.

Dimensiunea companiei

Dimensiunea companiei	Număr
Până la 10 angajati	64
11-50	60
51-250	51

Răspunsurile la sondaj indică un număr semnificativ de întreprinderi mici și mijlocii printre participanți. Cel mai mare grup sunt companiile cu până la 10 angajați (64 de respondenți), urmate îndeaproape de cele cu 11 până la 50 de angajați (60 de respondenți), iar apoi de companiile cu 51 până la 250 de angajați (51 de respondenți).

Predominanța companiilor mai mici în rândul respondenților evidențiază importanța soluțiilor de securitate cibernetică personalizate, care abordează nevoile și constrângerile specifice ale IMM-urilor.

Nivelul de cunoștințe

Nivelul de cunoștințe in Securitate cibernetica	Număr
Mediu	85
Începător	64
Avansat	26

Răspunsurile la sondaj indică faptul că majoritatea respondenților evaluează nivelul actual de cunoștințe de securitate cibernetică al angajaților lor drept „Intermediar” (85), urmați de cei care îl consideră la un nivel „Începător” (64), iar o parte mai mică își consideră angajații ca având cunoștințe „avansate” în domeniul securității cibernetice (26).

Această distribuție sugerează un potențial semnificativ de creștere și dezvoltare a competențelor de securitate cibernetică în cadrul organizațiilor reprezentate. Majoritatea nivelurilor „Intermediar” și „Începător” indică necesitatea inițiativelor de formare și educație continuă pentru a ridica baza de cunoștințe privind securitatea cibernetică a acestor angajați. Evidențiază o oportunitate pentru programe de formare în domeniul securității cibernetice specifice, care se adresează diferitelor niveluri de cunoștințe, asigurându-se că principiile fundamentale ale securității cibernetice sunt bine înțelese de către începători.

Prezența angajaților cu cunoștințe avansate, deși mai puține, este încurajatoare, deoarece indică un nivel fundamental de expertiză în domeniul securității cibernetice în cadrul unor organizații.

Nivelul de cunoștințe în funcție de dimensiunea companiei.

Dimensiunea companiei	Avansat	Începător	Mediu
Până la 10 angajați	6	25	33
11-50	10	20	30
51-250	10	19	22

Tabelul indică modul în care nivelurile de cunoștințe în domeniul securității cibernetice (avansat, începător, intermediar) sunt distribuite pe diferite dimensiuni ale companiei. Companiile mici (Până la 10 angajați) arată o înclinație spre nivelul „Intermediar" de cunoștințe de securitate cibernetică, urmat de „Începător". Acest lucru sugerează că, în timp ce companiile mici pot avea o anumită înțelegere a securității cibernetice, există încă o parte semnificativă la nivelul începătorilor, ceea ce indică loc de îmbunătățire și necesitatea unei pregătiri de bază. Companiile Mijlocii (11-50 de angajați) au o distribuție echilibrată pe nivelurile de cunoștințe, cu o ușoară preferință pentru cunoștințele „Intermediare". Acest lucru ar putea reflecta o abordare mai structurată a formării în domeniul securității cibernetice în organizații puțin mai mari, dar indică în mod similar prezența atât a nevoilor de înțelegere avansată, cât și a nevoilor de învățare fundamentală. IMM-urile mai mari (51-250 de angajați) urmează un model similar cu companiile mijlocii, cu un număr egal de niveluri avansate și începători și un număr ușor mai mic de cunoștințe intermediare.

La toate dimensiunile companiilor, nivelul „Intermediar" de cunoștințe privind securitatea cibernetică este cel mai frecvent.

Angajații care se ocupă de sarcini de securitate cibernetică

Număr de angajați	Număr
1-5	88
0	22
6-10	17
21+	12
11-20	5

Media de angajați în securitate cibernetică	Număr
0-4	113
5-9	17
10-14	13
20-24	4
25-50	6
+100	9

Tabelele arată distribuția numărului de angajați care desfășoară activități legate de securitatea cibernetică în diferite organizații. Oferă o imagine mai clară asupra modului în care

responsabilitățile de securitate cibernetică sunt distribuite în diferite game de număr de angajați. Marea majoritate a răspunsurilor se încadrează în intervalul 0-4, indicând un număr mare de organizații cu echipe de securitate cibernetică foarte mici sau chiar niciuna dedicată în mod special securității cibernetice. Există o scădere semnificativă a frecvenței pe măsură ce trecem la intervale mai înalte, cu o oarecare renaștere în organizațiile care au peste 100 de angajați dedicați securității cibernetice. Se explică prin faptul că acele companii lucrează în domeniul securității cibernetice ca ocupație principală.

În detalii, datele sugerează o gamă largă în ceea ce privește dimensiunea echipelor de securitate cibernetică, cea mai comună dimensiune fiind un singur angajat, urmată de niciun angajat dedicat securității cibernetice, indicând faptul că multe organizații se bazează minim sau deloc pe personalul dedicat securității cibernetice. Există o scădere vizibilă a frecvenței pe măsură ce dimensiunea echipei crește.

Distribuția evidențiază un decalaj potențial în alocarea forței de muncă în domeniul securității cibernetice, în cazul în care un număr semnificativ de întreprinderi mici și mijlocii (IMM-uri) ar putea să nu aibă resurse adecvate dedicate securității cibernetice, expunându-le la riscuri mai mari. Prezența unor echipe mai mari în unele organizații sugerează o recunoaștere a importanței securității cibernetice în anumite sectoare sau companii mai mari.

Femeile în securitatea cibernetică

Media femeilor în securitatea cibernetică	Număr
0	78
1-5	57
6-10	8
11-15	4
16-20	1

Rezultatele întrebării „Câți dintre acești angajați sunt femei?” evidențiază o diferență semnificativă de gen în forța de muncă în domeniul securității cibernetice din cadrul IMM-urilor. Cea mai frapantă observație este că majoritatea companiilor, 78 în total, au raportat că nu au femei în rolurile lor de securitate cibernetică. Acest lucru indică o problemă predominantă a subreprezentării femeilor în acest domeniu critic în IMM-urile chestionate. Se remarcă o scădere treptată a numărului pe măsură ce numărul femeilor în roluri de securitate cibernetică crește, 31 de companii având o femeie într-o astfel de poziție. Prezența câtorva companii cu 10 sau mai multe femei în roluri de securitate cibernetică, deși pozitivă, rămâne mai degrabă o excepție decât o normă. Aceste instanțe ar putea reprezenta organizații cu echipe de securitate cibernetică mai mari sau cele care au pus un accent specific pe diversitatea de gen în forța lor de muncă în domeniul securității cibernetice. Subliniază necesitatea unor inițiative menite să încurajeze și să sprijine femeile în urmarirea unei cariere în securitatea cibernetică. Numărul semnificativ de companii fără femei în roluri de securitate cibernetică evidențiază un domeniu critic de intervenție pentru promovarea diversității de gen și a incluziunii în sector. Reducerea

acestei decalaje de gen ar putea contribui la perspective mai diverse în abordarea provocărilor de securitate cibernetică.

Utilizarea serviciilor externe

Răspuns	Număr
Nu	115
Da	60

Răspunsurile relevă un aspect semnificativ al modului în care IMM-urile abordează securitatea cibernetică. Majoritatea companiilor chestionate, 115 din 175, indică faptul că nu angajează servicii externe pentru munca de securitate cibernetică. Acest lucru sugerează o preferință sau necesitate pentru gestionarea eforturilor de securitate cibernetică la nivel intern în cadrul unui segment mare al populației IMM-urilor. Diferiți factori ar putea determina această tendință, cum ar fi constrângerile bugetare, controlul perceput asupra practicilor de securitate cibernetică sau convingerea că resursele lor interne existente sunt suficiente pentru a satisface nevoile lor de securitate cibernetică. Această situație face ca proiectul CyberAgent să fie extrem de relevant pentru a dota angajatul cu abilități și cunoștințe fundamentale.

60 de companii au raportat că au angajat servicii externe pentru sarcini de securitate cibernetică. Acest grup recunoaște probabil beneficiile externalizării, cum ar fi accesarea competențelor specializate, rămânerea la curent cu cele mai recente amenințări și contramăsuri de securitate cibernetică sau completarea capacităților lor interne. Decizia de a angaja servicii externe ar putea reflecta, de asemenea, o înțelegere a complexității amenințărilor la adresa securității cibernetice, care poate fi o provocare de gestionat în întregime intern, în special pentru IMM-urile cu resurse limitate.

Această împărțire evidențiază o divergență în strategia de securitate cibernetică în rândul IMM-urilor, echilibrând între managementul intern și externalizarea externă a funcțiilor de securitate cibernetică. Acesta subliniază importanța unei abordări personalizate a securității cibernetice, recunoscând că diferite organizații pot avea nevoi, capacități și resurse variate care le influențează deciziile cu privire la cererea de sprijin extern pentru eforturile de securitate cibernetică.

Eficacitatea programelor de instruire

Răspuns	Număr
1 (Ineficient)	8
2	38
3	79
4	39
5 (Foarte eficient)	11

Răspunsurile oferă o perspectivă asupra percepțiilor cu privire la eficacitatea programelor de formare actuale în pregătirea studenților pentru provocările de securitate cibernetică din lumea

reală în IMM-uri. Majoritatea respondenților, cu 79 de numărări, au evaluat eficacitatea programelor de formare curente la „3”, indicând o percepție neutră sau moderată a eficacității acestora. Acest lucru sugerează că, deși există un anumit nivel de încredere în aceste programe, există, de asemenea, loc semnificativ de îmbunătățire. Răspunsurile arată, de asemenea, o tendință spre capătul inferior al scalei, „2” primind 38 de contorizări, indicând spre scepticism cu privire la eficacitatea acestor programe de formare. La extreme, „1” (ineficient) a primit cel mai mic număr de voturi (8 numărări), iar „5” (foarte eficient) a primit puțin mai multe (11 numărări). Acest lucru indică faptul că foarte puțini respondenți consideră că actualele programe de formare sunt fie complet ineficiente, fie foarte eficiente în pregătirea studenților pentru provocările de securitate cibernetică în IMM-uri. Numărul echilibrat de răspunsuri pentru „4” (39 de numărări) sugerează că un segment notabil de participanți consideră programele de formare ca fiind relativ eficiente, deși nu fără limitări semnificative. În timp ce programele actuale de formare oferă o anumită pregătire pentru provocările de securitate cibernetică din lumea reală în IMM-uri, există un decalaj între formarea oferită și nevoile industriei. Acest decalaj s-ar putea datora mai multor factori, cum ar fi ritmul de evoluție a amenințărilor la adresa securității cibernetice, aplicarea practică a competențelor sau specificul provocărilor cu care se confruntă IMM-urile.

Top 3 domenii de formare în securitate cibernetica

Categorie	Număr
Detectarea amenințărilor și răspunsul	102
Managementul și analiza riscurilor	81
Răspuns la incident și recuperare	72
Confidențialitatea și protecția datelor	68
Expertiza securitatii cloud	51
Securitatea retelei	46
Cunoștințe privind conformitatea și reglementările	31
Tehnologii emergente	24

Analiza răspunsurilor dezvăluie că „Detectarea și răspunsul la amenințări” este considerat cel mai important domeniu în formarea în domeniul securității cibernetice, cu 102 de numărări, ceea ce indică o credință puternică în importanța sa pentru abordarea provocărilor de securitate cibernetică din lumea reală în IMM-uri. Această zonă este urmată îndeaproape de „Managementul și analiza riscurilor” și „Răspunsul la incident și recuperarea”, cu 81 și, respectiv, 72 de puncte, subliniind valoarea acordată înțelegerii riscurilor și capabilității de a răspunde la incidente în mod eficient. „Confidențialitatea și protecția datelor” primește, de asemenea, un vot semnificativ, reflectând importanța tot mai mare a legilor privind protecția datelor și nevoia de a proteja informațiile personale și sensibile în era digitală. „Expertiză în domeniul securității în cloud” este identificat ca un domeniu cheie de către 51 de respondenți, probabil din cauza adoptării tot mai mari a serviciilor cloud și a provocărilor unice de securitate pe care le prezintă. Securitatea rețelei, cu 46 de puncte, rămâne o preocupare fundamentală, subliniind nevoia de

apărare puternică împotriva amenințărilor bazate pe rețea. „Conformitatea și cunoștințele de reglementare” și „Tehnologiile emergente” sunt considerate mai puțin importante.

Competențe și cunoștințe

Zona de competențe și cunoștințe	Esențial (%)	Nevoie mare (%)	Nevoie medie (%)	Nevoie scăzută (%)	Nu este necesar (%)
Confidențialitatea și protecția datelor	38.29	38.29	13.14	10.29	0.00*
Evaluarea și managementul riscurilor	34.86	36.00	24.00	4.57	0.57
Răspuns la incident și recuperare	33.14	38.86	19.43	8.00	0.57
Abilități de comunicare	32.57	35.43	22.29	8.00	1.71
Cunoștințe tehnice	30.29	32.00	26.29	8.57	2.86
Inteligența și monitorizarea amenințărilor	29.71	37.14	24.00	8.57	0.57
Dezvoltarea și implementarea politicilor	24.00	37.14	24.00	12.57	2.29

*Procentul „Nu este necesar” pentru „Confidențialitatea și protecția datelor” nu este disponibil (NaN), ceea ce s-ar putea datora faptului că toți respondenții consideră că acest domeniu este cel puțin o oarecare nevoie, prin urmare poate fi considerat ca fiind 0%.

Tabelul prezintă scorurile medii pentru fiecare domeniu de competență și cunoștințe, derivate din răspunsurile la sondaj care evaluează importanța acestora pe o scară de la 1 (nu este necesar) la 5 (esențial). Aceste scoruri oferă o perspectivă cantitativă asupra modului în care respondenții acordă prioritate diferitelor zone din domeniu.

Acest tabel oferă o defalcare clară a modului în care fiecare competență și domeniu de cunoștințe este evaluat de respondenți. Domenii precum „Confidențialitatea și protecția datelor” și „Evaluarea și managementul riscurilor” au cel mai mare procent de evaluări „Esențiale”, reflectând importanța lor critică în domeniu. În schimb, „Elaborarea și implementarea politicilor” arată o distribuție mai largă a răspunsurilor, indicând o percepție mai variată a importanței acesteia. Rezultatele evidențiază un accent puternic pe cunoștințele tehnice, conștientizarea amenințărilor și capacitatea de a răspunde la incidente, împreună cu nevoia crucială de comunicare eficientă și practici de protecție a datelor.

Amenințări emergente la adresa securității cibernetice

Amenințări emergente la adresa securității cibernetice	Frecvență
Phishing și inginerie socială	105
Atacurile cibernetice determinate de AI	95
Atacurile ransomware	90
Încălcări de securitate în cloud	60
Amenințări deepfake	57
Vulnerabilități IoT	44
Amenințări din interior	31

Phishing-ul și ingineria socială sunt considerate cele mai presante amenințări, atacurile cibernetice determinate de AI și atacurile ransomware primind, de asemenea, o atenție semnificativă. Acest lucru sugerează o conștientizare puternică în rândul IMM-urilor cu privire la necesitatea de a se proteja atât de amenințările cibernetice tradiționale, cât și de cele emergente. Încălcările securității în cloud și amenințările deepfake sunt, de asemenea, evidențiate, reflectând preocupările cu privire la securitatea serviciilor cloud și potențiala utilizare greșită a inteligenței artificiale. Sunt identificate și vulnerabilitățile IoT și amenințările interne, deși sunt văzute ca fiind mai puțin iminente decât celelalte categorii. În special, există răspunsuri care indică faptul că unii respondenți nu sunt siguri cu privire la anumite amenințări sau nu au idei la nivelul lor de afaceri, sugerând un potențial decalaj în conștientizarea sau îngrijorarea cu privire la anumite amenințări emergente în rândul unor IMM-uri.

Decalaj în cunoștințe sau abilități în domeniul securității cibernetice

Decalaj în cunoștințe sau abilități în domeniul securității cibernetice	Frecvență
Nivel scăzut de conștientizare a amenințărilor	105
Nivel scăzut de instruire regulată în domeniul securității cibernetice	88
Nivel scăzut de evaluare a vulnerabilităților	80
Nivel scăzut de abilități tehnice	71
Nivel scăzut de înțelegere a politicilor și reglementărilor	50
Nivel scăzut de abilități soft	37

Cele mai semnificative lacune în cunoștințele sau abilitățile în domeniul securității cibernetice în rândul angajaților sunt în conștientizarea amenințărilor, cursuri regulate de securitate cibernetică, evaluarea vulnerabilității, abilitățile tehnice și înțelegerea politicilor și reglementărilor. Frecvența acestor răspunsuri evidențiază o nevoie crucială de educație și formare cuprinzătoare în domeniul securității cibernetice care să abordeze aceste domenii specifice. Conștientizarea amenințărilor este cel mai semnificativ decalaj, indicând faptul că angajații ar putea să nu fie pe deplin conștienți de amenințările de securitate cibernetică care le-ar putea afecta organizația. Acest decalaj subliniază importanța îmbunătățirii programelor de conștientizare și instruire pentru a ajuta angajații să recunoască potențialele amenințări mai eficient. Antrenamentele regulate în domeniul securității cibernetice sunt, de asemenea, văzute

ca un decalaj, indicând nevoia de educație continuă și actualizări cu privire la cele mai recente practici și amenințări de securitate cibernetică, mai degrabă decât sesiuni de formare unice.

Tendințe emergente

Tendințe emergente în formarea în domeniul securității cibernetice	Frecvență
Inteligența artificială și învățarea automată în securitatea cibernetică	134
Identitate digitală și confidențialitate	108
Hacking etic și abilități defensive	86
Concentrați-vă pe abilități soft și formare interdisciplinară	54
Amenințări de calcul cuantic	39
Sisteme de securitate descentralizate (de exemplu, Blockchain)	28

Analiza relevă un accent clar pe inteligența artificială și învățarea automată în securitatea cibernetică ca tendința cea mai așteptată pentru următorii cinci ani. Acest lucru indică o recunoaștere tot mai mare a rolului tehnologiilor avansate în îmbunătățirea apărării securității cibernetice și dezvoltarea de noi soluții de securitate. Frecvența ridicată a răspunsurilor din această categorie sugerează că programele de formare vor trebui să încorporeze din ce în ce mai mult AI și componente de învățare automată pentru a pregăti profesioniștii în securitate cibernetică pentru viitor. Identitatea digitală și confidențialitatea apar ca a doua tendință, evidențiind preocupările legate de protecția datelor cu caracter personal și gestionarea identităților digitale într-o lume din ce în ce mai online. Această tendință sugerează o cerere de instruire care să acopere complexitatea legilor privind confidențialitatea, tehnicile de protecție a datelor și soluțiile de gestionare a identității. Hackingul etic și abilitățile defensive sunt identificate ca a treia tendință cheie, reflectând importanța strategiilor proactive de apărare în securitatea cibernetică. Accentul pus pe hacking-ul etic arată o schimbare către formarea care le permite profesioniștilor în securitate cibernetică să gândească ca atacatorii pentru a-și apăra mai bine organizațiile.

Adecvarea programelor de formare

Raăpuns	Frecvență
Da	81
Nesigur	65
Nu	29

Analiza întrebării care a explorat punctele de vedere ale respondenților cu privire la adecvarea programelor actuale de formare în domeniul securității cibernetice, relevă o perspectivă mixtă în rândul participanților. O parte semnificativă, reprezentând majoritatea respondenților, consideră că actualele programe de formare în domeniul securității cibernetice sunt adecvate, așa cum indică răspunsurile „Da”. Acest lucru sugerează că un număr de persoane consideră că formarea disponibilă astăzi răspunde nevoilor organizațiilor lor sau se aliniază cu așteptările lor cu privire la ceea ce ar trebui să implice formarea în domeniul securității cibernetice. Cu toate acestea, un număr substanțial de respondenți „Nu sunt siguri” cu privire la adecvarea

programelor de formare actuale, evidențiind un grad de incertitudine sau lipsă de informații despre opțiunile de formare disponibile sau eficacitatea acestora în abordarea provocărilor actuale de securitate cibernetică. Această incertitudine ar putea fi atribuită naturii în evoluție a amenințărilor cibernetice și dificultății de a menține programele de formare la zi cu cele mai recente evoluții în domeniu. Răspunsurile „Nu", deși reprezintă cel mai mic grup, indică o îngrijorare clară că programele de formare existente nu sunt suficiente pentru a satisface nevoile actuale de securitate cibernetică. Acest grup ar putea avea lacune în ceea ce privește amenințările, tehnologiile sau metodologiile emergente.

Inclusivitatea programelor de formare

Răspuns	Frecvență
Da	81
Nesigur	65
Nu	29

Analiza răspunsurilor indică o perspectivă diversă asupra incluziunii programelor actuale de formare în domeniul securității cibernetice privind genul. O pluralitate de respondenți consideră că formarea actuală este incluzivă și abordează în mod eficient nevoile tuturor genurilor, așa cum indică răspunsurile „Da". Acest lucru sugerează că o parte semnificativă a comunității de securitate cibernetică consideră că eforturile actuale de formare fac pași în direcția incluziunii și egalității de gen. Cu toate acestea, un număr mare de respondenți „Nu sunt siguri" cu privire la incluziunea acestor programe, indicând o cantitate considerabilă de incertitudine sau lipsă de conștientizare cu privire la incluziunea de gen a formării în domeniul securității cibernetice. Acest răspuns ar putea evidenția un decalaj de comunicare între furnizorii de formare și participanți sau ar putea sugera că eforturile de incluziune ar putea să nu fie la fel de vizibile sau de impact precum s-ar fi dorit. Răspunsurile „Nu", reprezentând cel mai mic grup dintre respondenți, evidențiază totuși o preocupare critică că formarea actuală în domeniul securității cibernetice nu abordează suficient nevoile tuturor genurilor. Acest feedback indică un decalaj în eforturile de incluziune în cadrul programelor de formare în domeniul securității cibernetice, sugerând că este nevoie de mai multă muncă pentru a se asigura că aceste programe sunt primitoare și adaptate nevoilor persoanelor cu toate identitățile de gen.

3.2. PREFERINȚE ȘI NEVOI DE FORMARE

Pe baza rezultatelor cercetării pe teren, iată o descriere a caracteristicilor și nevoilor de formare identificate, preferințele de învățare, formarea și sprijinul femeilor implicate în securitatea cibernetică.

Identificarea nevoilor de formare:

Domeniul 1 - Cunoștințe și abilități fundamentale

O prioritate în educația în domeniul securității cibernetice. În special subiecte precum fundamentele securității cibernetice și securitatea rețelei. Există lacune semnificative în domenii precum detectarea și răspunsul la amenințări, expertiza în securitatea în cloud, răspunsul la incident și recuperarea, confidențialitatea și protecția datelor și gestionarea și analiza riscurilor. Programele de formare trebuie să abordeze aceste deficite de competențe. De asemenea, există o nevoie puternică de securitate cibernetică pentru conținutul orientat spre IMM-uri.

Domeniul 2 - Subiecte de specialitate

Aceasta este o nevoie de formare care să acopere un spectru larg de amenințări și contramăsuri la adresa securității cibernetice. Au fost evidențiate unele subiecte specializate precum analiza și gestionarea amenințărilor, criptografia și tehnicile avansate de atenuare a amenințărilor. Instruirea ar trebui să includă conținut despre cele mai frecvent menționate amenințări emergente, inclusiv atacuri cibernetice determinate de AI, atacuri ransomware, phishing și inginerie socială, încălcări ale securității în cloud și vulnerabilități IoT.

Domeniul 3 - Aplicație practică

Preferința pentru metodele de predare, cum ar fi laboratoarele practice, studiile de caz și proiectele de grup evidențiază importanța aplicării practice, interactive și în lumea reală în formarea în domeniul securității cibernetice**.**

Practici curente:

În ceea ce privește metoda de predare, putem remarca utilizarea diferitelor practici, cum ar fi studii de caz, proiecte de grup, laboratoare practice și prelegeri. Există un amestec de abordări teoretice și practice în programele de formare actuale.

Programele actuale de formare acoperă o gamă largă de subiecte de securitate cibernetică, subiectele fundamentale fiind prioritare. Cu toate acestea, există o absență remarcată a conținutului specific IMM-urilor în unele programe.

În ceea ce privește incluziunea și echilibrul de gen, unele programe au implementat inițiative pentru a crește participarea femeilor și a crea medii de formare care să includă genul, deși aceste eforturi par să fie minoritare.

Provocări:

Principalele provocări cu care se confruntă educația în domeniul securității cibernetice sunt:

- - Adaptarea instruirii pentru a se potrivi cu diverse medii și niveluri de expertiză este o provocare, deoarece există o diversitate de abilități și experiență
- - Menținerea actuală a materialelor de curs pentru a face față evoluției rapide a amenințărilor la adresa securității cibernetice. Necesită actualizări continue ale materialelor de instruire.
- - Constrângeri de formare practică din cauza limitărilor din facilitățile de laborator, capabilităților de simulare în lumea reală și creării de scenarii realiste de atac cibernetic pentru practică
- - Menținerea studenților implicați și motivați, în special cu conținut tehnic complex, este dificilă.
- - Alinierea industriei și educaționale cu echilibrarea bazelor teoretice cu abilități practice care se potrivesc nevoilor industriei reprezintă o provocare.

Sugestii pentru imbunătățirea formării:

- - Adaptarea formării la nevoile IMM-urilor: integrarea subiectelor și competențelor concepute special pentru a răspunde nevoilor de securitate cibernetică ale IMM-urilor.
- - Îmbunătățirea aplicației practice prin extinderea utilizării metodelor de predare interactive și practice pentru a îmbunătăți abilitățile practice și pregătirea pentru lumea reală.
- - Încorporarea unor tendințe emergente, cum ar fi AI și învățarea automată, identitatea digitală și confidențialitatea și hacking-ul etic. Ele sunt acum considerate domenii cheie pentru atenția viitoare în programele de formare.
- - Abordarea deficitelor de competențe trebuie sa se concentreze pe domeniile în care angajații au lipsuri, cum ar fi detectarea și răspunsul amenințărilor, securitatea în cloud și răspunsul la incident, pentru a-i pregăti mai bine pentru a face față provocărilor și a deveni agent de schimbare eficient și rezistent.
- - Dezvoltarea de inițiative privind diversitatea de gen pentru a crește participarea femeilor prin inițiative specifice, mentorat și modele de urmat.

4. PROFIL DE CALIFICARE AL UNUI AGENT DE SCHIMBARE A SECURITATII CIBERNETICE PENTRU IMM-URI

Pe baza constatărilor cercetării literaturii de specialitate și pe teren, iată un exemplu de set de cunoștințe, abilități și competențe pentru un agent de schimbare. Aceste rezultate reprezintă realizările așteptate de la participanții la programele de formare în domeniul securității cibernetice, asigurând o îmbunătățire a cunoștințelor și abilităților de bază la nivelul 4/5 EQF, dar și a abilităților mai avansate și orientate spre leadership la nivelul 6 EQF.

Profil de calificare CyberAgent	Cunoștințe	Abilități	Competențe
La nivelul 4/5 EQF	**Fundamentele securității cibernetice** - Concepte de bază ale securității cibernetice - Tipuri de amenințări cibernetice (phishing, ransomware, atacuri DDOS), vectori de atac - Importanța securității cibernetice în protecția activelor organizaționale. **Cadrul juridic și de date pentru securitate cibernetică** - Legislația, standardele și cerințele de conformitate în materie de securitate cibernetică - Strategii și politici pentru securitatea informațiilor - Protejarea datelor - Politici de management al riscului	**Securitate** - Identificarea potențialele riscuri de securitate cibernetică și vulnerabilități - Folosirea instrumentelor și software de securitate cibernetică pentru a se proteja împotriva amenințărilor cibernetice - Promovarea aplicării practice a practicilor de bază de securitate cibernetică, crearea de parole sigure, navigarea securizată, securitatea e-mailului și gestionarea în siguranță a datelor sensibile	**Managementul și diminuarea riscurilor** - Evaluați și reduceți potențialele amenințări la securitate **Comunicare eficientă cu privire la problemele de securitate cibernetică** - Capacitatea de a comunica eficient cu privire la problemele de securitate cibernetică - Raportarea amenințărilor și încălcărilor către canalele corespunzătoare din cadrul organizației.

La nivelul 6 EQF	**Concepte avansate de securitate cibernetică** - Înțelegerea principiilor avansate de securitate cibernetică, inclusiv amenințărilor cibernetice sofisticate și vectorilor de atac - Conștientizarea celor mai recente tendințe în ceea ce privește amenințările de securitate cibernetică și mecanismele de apărare **Legislația și conformitatea securității cibernetice** - Cunoașterea legislației naționale și internaționale în domeniul securității ciber-netice, a standardelor și a cerințelor de conformitate și a altora relevante pentru industria lor specifică.	**Evaluare și management avansat al riscului** - Capacitatea de a efectua evaluări cuprinzătoare ale riscurilor - Utilizarea metodologiilor și instrumentelor avansate - Proiectarea și implementarea strategiilor eficiente de gestionare a riscurilor pentru a atenua riscurile identificate. **Expertiza in arhitectura de securitate si apararea retelei** - Proiectarea, implementarea și evaluarea arhitecturii de rețea securizate, inclusiv utilizarea de firewall-uri, sisteme de detectare a intruziunilor (ID) și sisteme de prevenire a intruziunilor (ips). **Răspuns la incident și recuperare** - Capacitate de a se pregăti pentru, de a răspunde și de a se recupera după incidente de securitate cibernetică - Dezvoltarea planurilor de redresare si continuitate a afacerii.	**Planificarea și dezvoltarea politicilor** - Capacitatea de a dezvolta și implementa politici și cadre strategice de securitate cibernetică aliniate cu obiectivele și obligațiile de conformitate ale organizației. **Leadership în inițiativele de securitate cibernetică** -Conducerea și gestionarea proiectelor și echipelor de securitate cibernetică, inclusiv abilitatea de a inspira și ghida angajații în implementarea strategiilor de securitate cibernetică. **Luarea deciziilor** - Luarea deciziilor etice cu privire la practicile de securitate cibernet-ică

La nivelul 4/5 EQF, posibilele rezultate ale învățării ar putea fi:

- - Cursanții vor învăța conceptele fundamentale ale securității cibernetice, inclusiv terminologia de bază, tipurile de amenințări cibernetice, cum ar fi phishing, ransomware și atacuri DDoS, și vectorii de atac respectivi.
- - Cursanții vor fi capabili să identifice potențiale riscuri și vulnerabilități de securitate cibernetică, să folosească instrumente și software relevante pentru a atenua aceste riscuri și să implementeze practici de bază de securitate cibernetică, cum ar fi crearea de parole sigure și navigarea securizată.
- - Cursanții vor dobândi cunoștințe despre legislația, standardele și cerințele de conformitate în domeniul securității cibernetice, împreună cu strategiile și politicile pentru securitatea informațiilor și gestionarea riscurilor în cadrul unei organizații.
- - Cursanții își vor dezvolta competența de a evalua și a atenua potențialele amenințări la securitate și de a comunica în mod clar și eficient problemele de securitate cibernetică în cadrul organizației, inclusiv raportarea amenințărilor și încălcărilor către canalele adecvate.

La nivelul 6 EQF, posibilele rezultate ale învățării ar putea fi:

- - Cursanții vor dezvolta o înțelegere avansată a principiilor de securitate cibernetică, inclusiv capacitatea de a identifica amenințările cibernetice sofisticate și vectorii de atac și de a rămâne informați cu privire la cele mai recente tendințe în domeniul apărării securității cibernetice.
- - Cursanții vor dobândi cunoștințe cuprinzătoare despre legislația națională și internațională de securitate cibernetică, standardele și cerințele de conformitate, adaptând această înțelegere la nevoile specifice ale industriei lor.
- - Cursanții vor putea să efectueze evaluări detaliate ale riscurilor folosind metodologii și instrumente avansate și să elaboreze strategii eficiente de gestionare a riscurilor pentru a atenua aceste riscuri.
- - Cursanții vor proiecta, implementa și evalua arhitecturi de rețea sigure, inclusiv stăpânirea utilizării tehnologiilor critice de securitate precum firewall-uri, IDS și IPS.
- - Cursanții vor fi competenți în planificarea și executarea strategiilor de răspuns la incident și de recuperare, asigurând rezistența organizațională prin planuri eficiente de recuperare și continuitate a afacerii.
- - Cursanții vor demonstra leadership în domeniul securității cibernetice prin dezvoltarea de politici strategice, gestionarea proiectelor și echipelor de securitate cibernetică și luând decizii informate și etice sub presiune.

5. ANEXE

5.1. ANEXA A: LISTA LITERATURII REVIZUITE

Prezentare generală a educației în domeniul securității cibernetice VET și IIS

1. https://ccb.belgium.be/en/ict-security-education-belgium
2. https://acdn.be/enewsv7/upload/whitepaper/CybersecurityReport.pdf
3. https://ccb.belgium.be/sites/default/files/CCB_Strategie%202.0_UK_WEB.pdf
4. https://www.enisa.europa.eu/topics/education/cyberhead#/programmes?country[]=fin
5. http://www.anc.edu.ro/standarde-pregatire-profesionala/
6. http://217.73.164.21/index.php/articles/curriculum/c556+592/
7. http://217.73.164.21/index.php/articles/c560/
8. https://www.agerpres.ro/english/2023/09/19/first-master-s-program-in-romania-in-cyber-security-accredited-by-eit-digital-at-ubb-cluj-napoca--1171675
9. https://dnsc.ro/invatamant/vezi/5
10. https://www.linkedin.com/posts/eit-digital_ubb-cluj-joins-eit-digital-adding-cybersecurity-activity-7031990099756081152-Sr77/?originalSubdomain=si
11. https://www.unitbv.ro/documente/curriculum-syllabus/Master/Plan%20inv/MI_master_TIN_2017_2018_PI.pdf
12. https://mateinfo.unitbv.ro/images/2023/planuri_inv/Plan_inv_2023_2025_Tehnologii_moderne_in_ingineria_sistemelor_soft.pdf
13. https://drive.google.com/drive/folders/1h9aC1xwobVtGN4qNukWMvDPXICf62FgF
14. Analysis and Diagnosis of Cybersecurity Talent in Spain, March 2022, Observaciber, https://www.observaciber.es/
15. Ciberseguridad. Informe de Situación 2022, Plataforma tecnológica española de tecnologías disruptivas, Ministerio de Ciencia e Innovación https://ptedisruptive.es/wp-content/uploads/2022/12/Informe-situacio%CC%81n-ciberseguridad-2022.pdf
16. Panorama actual de la Ciberseguridad en España, Google https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf
17. Catálogos de formación en ciberseguridad, INCIBE, 2023 https://www.incibe.es/incibe/formacion/catalogos-formacion-ciberseguridad
18. Plan Nacional de competencias digitales https://portal.mineco.gob.es/es-es/digitalizacionIA/Paginas/plan-nacional-competencias-digitales.aspx
19. Plan España Digital 2025 https://avancedigital.mineco.gob.es/programas-avance-digital/paginas/espana-digital-2025.aspx
20. Plan de Digitalización de PYMES 2021-2025 https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/210127_plan_digitalizacion_pymes.pdf
21. Real Decreto 479/2020, de 7 de abril, por el que se establece el Curso de especialización en ciberseguridad en entornos de las tecnologías de la información y se fijan los aspectos básicos del currículo https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-4963

Provocările de securitate cibernetică și nevoile industriei

1. El estado de la ciberseguridad en España, Deloitte, 2022 **https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html**
2. Ferreirós Orihuel, Inés (coord.). IV Informe sobre la Ciencia y Tecnología en España: Situar a España e el mapa geopolítico de la I+D+i. Fundación Alternativas: 187-206 (2023) **https://digital.csic.es/handle/10261/310469**
3. El reto de la ciberseguridad en España: un país vulnerable, Telefónica **https://www.telefonica.com/es/sala-comunicacion/blog/un-pais-vulnerable-el-reto-de-la-ciberseguridad-en-espana/**
4. Los retos de la ciberseguridad para las empresas españolas, Byte ti, 11 de enero de 2024 **https://revistabyte.es/tema-de-portada-byte-ti/retos-de-la-ciberseguridad/**
5. La falta de profesionales acentúa la amenaza de los ciberataques, el Periódico de España, 7 de Marzo de 2023 **https://www.epe.es/es/tecnologia/20230307/falta-profesionales-acentua-amenaza-ciberataques-84230209**
6. Analysis and Diagnosis of Cybersecurity Talent in Spain, March 2022, Observaciber, **https://www.observaciber.es/**
7. Ciberseguridad. Informe de Situación 2022, Plataforma tecnológica española de tecnologías disruptivas, Ministerio de Ciencia e Innovación **https://ptedisruptive.es/wp-content/uploads/2022/12/Informe-situacio%CC%81n-ciberseguridad-2022.pdf**
8. Panorama actual de la Ciberseguridad en España **https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf**
9. Plan España Digital 2025 **https://avancedigital.mineco.gob.es/programas-avance-digital/paginas/espana-digital-2025.aspx**
10. **Plan de Digitalización de PYMES 2021-2025 https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/210127_plan_digitalizacion_pymes.pdf**

11. https://esco.ec.europa.eu/sites/default/files/ethical%20hacker.pdf
12. http://data.europa.eu/esco/occupation/276ba420-ef09-4a0e-b215-2c2e2f80ad28
13. https://nsm.no/fagomrader/digital-sikkerhet/
14. https://www.bdo.no/nb-no/nyheter/2023/na-jakter-hackerne-de-sma-selskapene
15. https://www.evelon.no/artikler/trussellandskapet-i-europa
16. https://norsis.no/sikkerhetskultur2023/sammendrag/
17. https://serit.no/hva-er-god-datasikkerhet-i-bedriften/
18. https://www.duo.uio.no/bitstream/handle/10852/96151/5/Master_thesis_mariwilh.pdf

Femeile în securitate cibernetică

1. Microsoft. (2017, March). Why Europe's girls aren't studying STEM. Microsoft News. Retrieved January 20, 2024, from https://news.microsoft.com/uploads/2017/03/ms_stem_whitepaper.pdf
2. Women go tech. (2021, September). ICT workforce in Europe and its gender challenge after Covid-19. Women Go Tech. Retrieved January 20, 2024, from https://womengotech.com/app/uploads/2021/09/ICT-workforce-in-Europe-and-its-gender-challenge.pdf
3. Rodiklių duomenų bazė - Oficialiosios statistikos portalas. (n.d.) 1. https://osp.stat.gov.lt/statistiniu-rodikliu-analize#/
4. Bukauskas, Brilingaite, Ikamas, Juozapavicius, & Lepaite. (2022, August 5). Ataskaita Lietuvos kibernetinio saugumo kompetenciju¸ žemelapis. Vilnius University. Retrieved January 20, 2024, from https://cs.vu.lt/projects/P-REP-21-2/ataskaita.pdf
5. https://www.digi.no/artikler/debatt-flere-tech-jenter-ma-til-for-a-finne-morgendagens-losninger/535073
6. https://odanettverk.no/2022/03/08/dette-er-norges-50-fremste-tech-kvinner-2022/
7. https://e24.no/naeringsliv/i/k6Goma/etterlyser-flere-kvinner-til-cybersikkerhet
8. https://www.ssb.no/befolkning/artikler-og-publikasjoner/kvinner-velger-fortsatt-kvinneyrker
9. https://live.worldbank.org/en/event/2023/women-business-law-2023
10. https://wbl.worldbank.org/en/data/exploreeconomies/romania/2023
11. https://eige.europa.eu/gender-equality-index/2022/country/RO
12. https://cybernews.com/editorial/cyber-women-grim-statistics-big-opportunities/
13. https://www.weforum.org/agenda/2022/09/cybersecurity-women-stem/
14. https://www.bcg.com/publications/2022/empowering-women-to-work-in-cybersecurity-is-a-win-winFerreirós Orihuel, Inés (coord.). IV Informe sobre la Ciencia y Tecnología en España: Situar a España e el mapa geopolítico de la I+D+i. Fundación Alternativas: 187-206 (2023) https://fundacionalternativas.org/publicaciones/iv-informe-sobre-la-ciencia-y-la-tecnologia-en-espana/
15. Mujeres empleadas en ciencia y tecnología (reparto por sectores). España, UE-27 y UE-28. Serie 2019-2021. https://www.ine.es/jaxi/Tabla.htm?path=/t00/mujeres_hombres/tablas_1/l0/&file=c02002.px&L=0
16. La mujer en la ciencia española, en datos y gráficos, EpData, 7 de marzo de 2023 https://www.epdata.es/datos/mujer-ciencia-espanola-datos-estadisticas/298
17. Analysis and Diagnosis of Cybersecurity Talent in Spain, March 2022, Observaciber, https://www.incibe.es/ed2026/talento-hacker/publicaciones/diagnostico-talento-ciberseguridad
18. Ciberseguridad. Informe de Situación 2022, Plataforma tecnológica española de tecnologías disruptivas, Ministerio de Ciencia e Innovación https://ptedisruptive.es/wp-content/uploads/2022/12/Informe-situacio%CC%81n-ciberseguridad-2022.pdf
19. Panorama actual de la Ciberseguridad en España, Google https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf

5.2. ANEXA B: CHESTIONAR DE SONDAJ

Chestionar VET & IIS

Acest sondaj este conceput pentru a aduna informații despre starea actuală și nevoile viitoare ale formării în domeniul securității cibernetice și să contribuie la formarea unui program eficient de formare în domeniul securității cibernetice, adaptat provocărilor de securitate cibernetică pentru întreprinderile mici și mijlocii (IMM-uri).

Sondajul este împărțit în 4 secțiuni:

- Demografie
- Curriculum, nevoile de formare și preferințele de învățare
- Cerințe de competență și abilități viitoare
- Perspective specifice genului

Sondajul va dura aproximativ 8 minute pentru a fi completat.

DEMOGRAFIE

Care este țara ta?

▫ Lituania
▫ Belgia
▫ Norvegia
▫ Turcia
▫ Finlanda
▫ Romania
▫ Spania
▫ Polonia

În ce instituție școlară predați în prezent?

▫ VET (Învățământ și formare profesională)
▫ IIS (Instituție de Învățământ Superior)

Care este sexul tău?

▫ Bărbat
▫ Femeie
▫ Prefer să nu spun

Câți ani ați fost implicat în formarea în domeniul securității cibernetice?

▫ Mai puțin de 1 an
▫ 1-5 ani
▫ 6-10 ani
▫ Mai mult de 10 ani

CURRICULUM, NEVOI DE FORMARE ŞI PREFERINŢE DE ÎNVĂŢARE

Care dintre următoarele subiecte sunt incluse în programul dvs. de formare în domeniul securității cibernetice? (Selectați toate care se aplică)

▫ Fundamentele securității cibernetice
▫ Analiza și managementul amenințărilor
▫ Tehnici avansate de atenuare a amenințărilor

▫ Criptografia
▫ Securitatea rețelei
▫ Legile și politicile de securitate cibernetică
▫ Managementul riscurilor
▫ Răspuns la incident
▫ Altele: _____

Ce metode de predare folosiți în principal în formarea dumneavoastră în domeniul securității cibernetice? (Selectați toate care se aplică)

▫ Prelegeri
▫ Laboratoare practice
▫ Studii de caz
▫ Proiecte de grup
▫ Simulari online
▫ Flipped Classroom
Alte: _____

Ce formate de învățare ar fi cele mai eficiente pentru formarea în domeniul securității cibernetice? (Selectați toate care se aplică)

▫ Ateliere în persoană
▫ Cursuri online
▫ Webinarii
▫ Simulări interactive
▫ Tutoriale video
▫ Sesiuni practice de practică
▫ Altele: _____

Care sunt cele mai mari provocări cu care vă confruntați în furnizarea de formare eficientă în domeniul securității cibernetice?

Intrebare deschisa

Pe o scară de la 1 la 5, cât de eficient credeți că programele actuale de formare pregătesc studenții pentru provocările reale de securitate cibernetică a IMM-urilor?

▫ Foarte ineficient
▫ Oarecum ineficient
▫ Neutru
▫ Oarecum eficient
▫ Foarte eficient

Cât de bine credeți că formarea actuală în domeniul securității cibernetice se aliniază cu nevoile specifice ale IMM-urilor?

1 (Nepotrivit)
2 (Puțin potrivit)
3 (Potrivit)
4 (Bine potrivit)
5 (Foarte potrivit)

Există subiecte sau abilități specifice pe care le includeți în formarea dumneavoastră pentru a aborda nevoile unice de securitate cibernetică ale IMM-urilor? (Selectați toate care se aplică)

▫ Securitate cibernetică de bază pentru IMM-uri
▫ Evaluarea și managementul riscurilor în contextul IMM-urilor
▫ Răspuns la incident pentru IMM-uri
▫ Protecția datelor și confidențialitatea pentru IMM-uri
▫ Dezvoltarea politicii de securitate cibernetică pentru IMM-uri
▫ Altele: _____

Cât de des vă personalizați sau adaptați formarea în domeniul securității cibernetice pentru a răspunde mai bine IMM-urilor?

▫ Întotdeauna
▫ Adesea
▫ Uneori
▫ Rareori
▫ Niciodată

Primiți feedback sau sunteți în contact cu reprezentanți sau profesioniști ai IMM-urilor pentru a asigura relevanța conținutului dvs. de formare pentru nevoile acestora?

▫ Da, în mod regulat
▫ Ocazional
▫ Rareori
▫ Niciodată

Pe baza experienței dvs., cât de eficient credeți că este formarea actuală în domeniul securității cibernetice în echiparea profesioniștilor IMM-urilor pentru a face față provocărilor din domeniul securității cibernetice?

▫ Foarte ineficient
▫ Oarecum ineficient
▫ Neutru
▫ Oarecum eficient
▫ Foarte efficient

Ce sugestii aveți pentru îmbunătățirea relevanței și eficacității formării în domeniul securității cibernetice pentru IMM-uri?

Întrebare deschisă

<u>CERINȚE DE COMPETENȚĂ ȘI ABILITĂȚI VIITOARE</u>

În opinia dumneavoastră, care sunt principalele deficite de competențe în forța de muncă actuală în domeniul securității cibernetice pentru IMM-uri? (Alegeți până la trei)

▫ Detectarea și răspunsul amenințărilor
▫ Expertiza în securitate în cloud
▫ Conformitate și cunoștințe de reglementare
▫ Răspunsul la incident și recuperarea
▫ Managementul și analiza riscurilor
▫ Confidențialitatea și protecția datelor

▫ Tehnologiile emergente
▫ Securitatea rețelei

Vă rugăm să evaluați, de la o scară de la 1 (nu este necesar) la 5 (foarte necesar) competențele și nevoile de cunoștințe:

	Rating				
Evaluarea și managementul riscurilor Înțelegerea tipurilor de riscuri și impact.					
Cunoștințe tehnice Aspecte tehnice ale securității cibernetice și cunoștințe despre sistemele de operare, rețele și gestionarea bazelor de date.					
Răspuns la incident și recuperare Identificarea, răspunsul și recuperarea din încălcări și incidente de securitate.					
Dezvoltarea și implementarea politicilor Dezvoltarea și implementarea politicilor și practicilor de securitate eficiente.					
Inteligența și monitorizarea amenințărilor Fiți la curent cu cele mai recente tendințe de securitate cibernetică, amenințări și metodologii de atac.					
Abilități de comunicare Comunicare eficientă cu personalul, managementul și, eventual, clienții cu privire la problemele de securitate cibernetică.					
Confidențialitatea și protecția datelor Principiile confidențialității datelor și modul de protecție a informațiilor sensibile.					

Vedeți vreun set relevant de competențe și cunoștințe care nu sunt enumerate în întrebarea anterioară, care ar putea fi foarte necesar pentru IMM-uri?

Întrebare deschisă

Pentru ce amenințări emergente la securitatea cibernetică credeți că IMM-urile trebuie să fie pregătite în următorii 5 ani? (Alegeți până la trei)

▫ Atacurile ransomware
▫ Vulnerabilități IoT
▫ Încălcări de securitate în cloud
▫ Atacurile cibernetice determinate de AI
▫ Amenințări interne
▫ Altele: _____

Care credeți ca fiind primele 3 tendințe emergente în formarea în domeniul securității cibernetice pentru următorii 5 ani? (Alegeți până la 3 opțiuni)

▫ AI și învățarea automată în securitate cibernetică
▫ Concentrați-vă pe abilități soft și formare interdisciplinară
▫ Amenințări de calcul cuantic
▫ Hacking etic și abilități defensive
▫ Identitate digitală și confidențialitate

▫ Sisteme de securitate descentralizate (de exemplu, Blockchain)
▫ Altele: _____

Există anumite metode de instruire, instrumente sau platforme despre care considerați că sunt excepțional de eficiente pentru educația în domeniul securității cibernetice?

Întrebare deschisă

Orice comentarii sau sugestii suplimentare pentru îmbunătățirea formării în domeniul securității cibernetice pentru IMM-uri?

Întrebare deschis

PERSPECTIVE SPECIFICE DE GEN

Care este procentul estimat de femei printre participanții la programele dumneavoastră de formare în domeniul securității cibernetice?

▫ Mai puțin de 10%
▫ 10% - 25%
▫ 26% - 50%
▫ 51% - 75%
▫ Mai mult de 75%

Există inițiative sau strategii specifice pe care le utilizați pentru a încuraja participarea femeilor la formarea în domeniul securității cibernetice?

▫ Da
▫ Nu

Dacă da, vă rugăm să specificați: _____

Credeți că există suficiente module de formare care să includă genul disponibile în domeniul securității cibernetice?

▫ Da
▫ Nu
▫ Nesigur
▫ Nu este relevant pentru mine

Din experiența dumneavoastră, care sunt principalele bariere care împiedică femeile să participe sau să avanseze în formarea și cariera în domeniul securității cibernetice? (Selectați toate care se aplică)

▫ Lipsa de conștientizare a oportunităților în securitatea cibernetică
▫ Stereotipuri sau norme culturale
▫ Lipsa de mentorat sau modele de urmat
▫ Provocări privind echilibrul dintre viața profesională și viața privată
▫ Prejudecățile de gen percepute în industrie
▫ Altele: _____

Are instituția dumneavoastră politici sau programe specifice pentru a promova diversitatea și incluziunea, în special pentru femei, în formarea în domeniul securității cibernetice?

▫ Da

▫ Nu

▫ Nu sunt sigur

Ce ar putea face formarea în domeniul securității cibernetice să includă mai mult genul? (Alegeți până la trei)

▫ Mai multe femei instructoare de securitate cibernetică sau personal de formare

▫ Oferiți burse sau stimulente

▫ Conținut de instruire care evită prejudecățile de gen

▫ Vizibilitate sporită a profesioniștilor de succes în domeniul securității cibernetice

▫ Mai multe sesiuni de antrenament destinate exclusiv femeilor

▫ Studii de caz și scenarii care includ genul

▫ Programe de instruire personalizate

▫ Oportunități de mentorat

▫ Altele: _____

CHESTIONAR IMM-uri

Acest sondaj își propune să identifice nevoile de instruire pentru agenții de schimbare a securității cibernetice pentru IMM-uri. Răspunsurile dvs. vor ajuta la înțelegerea peisajului actual al cunoștințelor și abilităților în domeniul securității cibernetice în diferite IMM-uri, la identificarea lacunelor în formarea în domeniul securității cibernetice și la îmbunătățirea eficienței programelor de formare viitoare.
Sondajul este împărțit în 3 secțiuni:

- Demografie
- Nevoi de formare
- Inclusivitatea și nevoia femeilor în securitatea cibernetică.

Sondajul va dura aproximativ 5 minute pentru a fi completat.

DEMOGRAFIE

Care este țara ta?

▫ Lituania
▫ Belgia
▫ Norvegia
▫ Turcia
▫ Finlanda
▫ Romania
▫ Spania
▫ Polonia

Care este poziția și departamentul dvs. actual în companie?

Poziția: _____
Departament: _____

Care este sexul tău?
▫ Bărbat
▫ Femeie
▫ Prefer să nu spun

Câți angajați lucrează în companie?
▫ până la 10 angajați
▫ 11-50
▫ 51-250

Cum ați evalua nivelul actual de cunoștințe și abilități în materie de securitate cibernetică al angajaților?
▫ Începător
▫ Mediu
▫ Avansat

Câți angajați efectuează activități legate de securitatea cibernetică?
Introduceți numărul: _____

Angajați servicii externe pentru lucrări de securitate cibernetică?
▫ Da
▫ Nu

NEVOI DE FORMARE

Pe o scară de la 1 (ineficientă) la 5 (foarte eficient), cât de eficient credeți că programele actuale de formare pregătesc studenții pentru provocările reale de securitate cibernetică a IMM-urilor?
1- Ineficient
5- Foarte eficient

În opinia dumneavoastră, care sunt principalele deficite de competențe în forța de muncă actuală în domeniul securității cibernetice pentru IMM-uri? (Alegeți până la trei)
▫ Detectarea și răspunsul amenințărilor
▫ Expertiza în securitate în cloud
▫ Conformitate și cunoștințe de reglementare
▫ Răspunsul la incident și recuperarea
▫ Managementul și analiza riscurilor
▫ Confidențialitatea și protecția datelor
▫ Tehnologiile emergente
▫ Securitatea rețelei
▫ Altele: _____

Vă rugăm să evaluați, de la o scară de la 1 (nu este necesar) la 5 (esențial), competențele și nevoile de cunoștințe:

	Rating				
Evaluarea și managementul riscurilor Înțelegerea tipurilor de riscuri și impact.					
Cunoștințe tehnice Aspecte tehnice ale securității cibernetice și cunoștințe despre sistemele de operare, rețele și gestionarea bazelor de date.					
Răspuns la incident și recuperare Identificarea, răspunsul și recuperarea din încălcări și incidente de securitate.					
Dezvoltarea și implementarea politicilor Dezvoltarea și implementarea politicilor și practicilor de securitate eficiente.					

Inteligența și monitorizarea amenințărilor Fiți la curent cu cele mai recente tendințe de securitate cibernetică, amenințări și metodologii de atac.					
Abilități de comunicare Comunicare eficientă cu personalul, managementul și, eventual, clienții cu privire la problemele de securitate cibernetică.					
Confidențialitatea și protecția datelor Principiile confidențialității datelor și modul de protecție a informațiilor sensibile.					

Vedeți vreun set relevant de competențe și cunoștințe care nu sunt enumerate în întrebarea anterioară, care ar putea fi foarte necesar pentru IMM-uri?

Întrebare deschisă

Pentru ce amenințări emergente la securitatea cibernetică credeți că IMM-urile trebuie să fie pregătite în următorii 5 ani? (Alegeți până la trei)

▫ Atacurile ransomware
▫ Vulnerabilități IoT
▫ Încălcări de securitate în cloud
▫ Atacurile cibernetice determinate de AI
▫ Amenințări interne
▫ Altele: _____

Ce lacune specifice, dacă există, credeți că există în cunoștințele sau competențele actuale ale angajaților în materie de securitate cibernetică?

▫ Nivel scăzut de abilități tehnice
▫ Nivel scăzut de abilități soft
▫ Nivel scăzut de evaluare a vulnerabilității
▫ Nivel scăzut de înțelegere a politicilor și reglementărilor
▫ Nivel scăzut de conștientizare a amenințărilor
▫ Nivel scăzut de instruire regulată în domeniul securității cibernetice
▫ Altele: _____

Care credeți ca fiind primele 3 tendințe emergente în formarea în domeniul securității cibernetice pentru următorii 5 ani? (Alegeți până la 3 opțiuni)

▫ AI și învățarea automată în securitate cibernetică
▫ Concentrați-vă pe abilități soft și formare interdisciplinară
▫ Amenințări de calcul cuantic
▫ Hacking etic și abilități defensive
▫ Identitate digitală și confidențialitate
▫ Sisteme de securitate descentralizate (de exemplu, Blockchain)
▫ Altele: _____

INCLUZIVITATE ȘI NEVOILE FEMEILOR ÎN SECURITATE CIBERNI

Considerați că formarea actuală în domeniul securității cibernetice este incluzivă și abordează în mod eficient nevoile tuturor genurilor?

▫ Da

▫ Nu

▫ Nu sunt sigur

Dacă vă identificați ca femeie, v-ați confruntat cu bariere sau provocări în accesarea sau participarea la cursuri/studii în domeniul securității cibernetice?

▫ Da

▫ Nu

▫ Prefer să nu spun

▫ Dacă da, vă rugăm să specificați: _____

Cunoașteți inițiative sau programe din cadrul organizației dumneavoastră care susțin sau promovează în mod specific participarea femeilor la securitatea cibernetică?

▫ Da

▫ Nu

▫ Nu sunt sigur

Ce tipuri de sprijin sau resurse ar încuraja mai multe femei din organizația dumneavoastră să participe la formarea în domeniul securității cibernetice? (deschis)

Întrebare deschisă

Ce îmbunătățiri sau inovații ați sugera pentru îmbunătățirea eficienței formării în domeniul securității cibernetice?

Întrebare deschisă

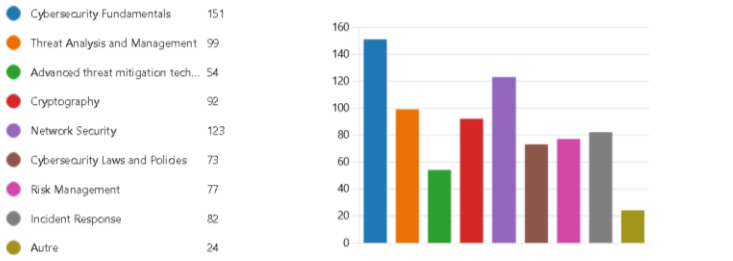
5.3. ANEXA C: REZULTATELE CHESTIONARELOR

VET & IIS

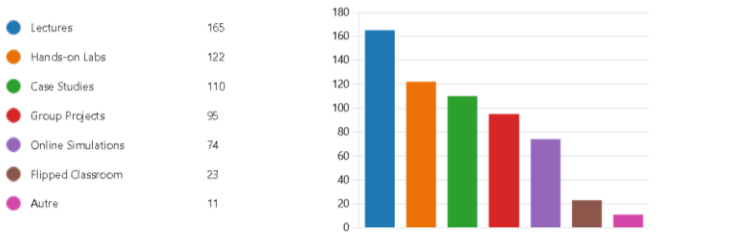
Mapping the training needs for SME Cyber Security Change Agents - VET and HEI survey

190 Responses

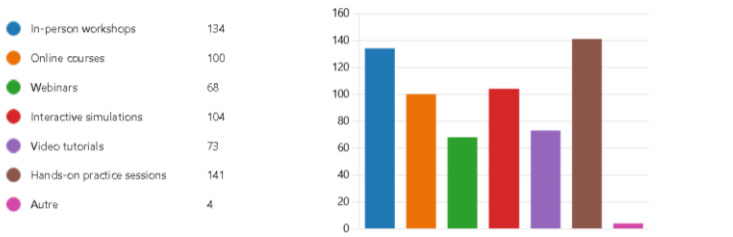
1. **Which of the following topics are included in your cybersecurity training program? (Select all that apply)**



2. **What teaching methods do you primarily use in your cybersecurity training? (Select all that apply)**



3. **What teaching method would be the most effective for cybersecurity training? (Select all that apply)**



4. **What are the biggest challenges you face in delivering effective cybersecurity training?**

190
Réponses

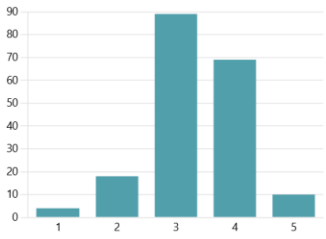
Dernières réponses
"-"
"-"
"keeping up with Technology Changes, Basic knowledge of the students, Soft...

Mettre à jour

34 répondants (**19**%) répondu **students** pour cette question.

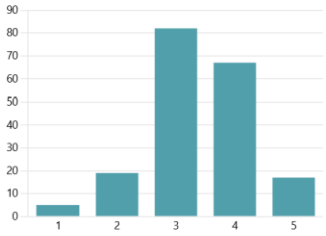
5. **On a scale of 1 (Very Ineffective) to 5 (Very Effective), how effectively do you think the current training programs prepare students for real-world SMEs cybersecurity challenges?**

3.33
Évaluation moyenne



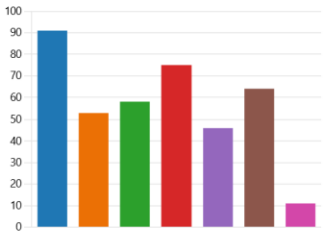
6. **On a scale of 1 (Not aligned) to 5 (Highly aligned), how well do you believe the current cybersecurity training aligns with the specific needs of SMEs?**

3.38
Évaluation moyenne



7. **Are there specific topics or skills that you include in your training to address the unique cybersecurity needs of SMEs? (Select all that apply)**

Basic Cybersecurity for SMEs	91
Risk Assessment and Managem...	53
Incident Response for SMEs	58
Data Protection and Privacy for ...	75
Cybersecurity Policy Developme...	46
No SME's specific topic or skills ...	64
Autre	11



8. **How often do you customize or adapt your cybersecurity training to better cater to SMEs?**

Always	14
Often	60
Sometimes	55
Rarely	47
Never	14

9. **Do you receive feedback or are you in contact with SME representatives or professionals to ensure the relevancy of your training content to their needs?**

Yes, regularly	43
Occasionally	64
Rarely	54
Never	29

10. **Based on your experience, how effective do you believe the current cybersecurity training is in equipping SME professionals to handle cybersecurity challenges?**

Very Ineffective	7
Somewhat Ineffective	21
Neutral	65
Somewhat Effective	88
Very Effective	9

11. **What suggestions do you have for improving the relevance and effectiveness of cybersecurity training for SMEs?**

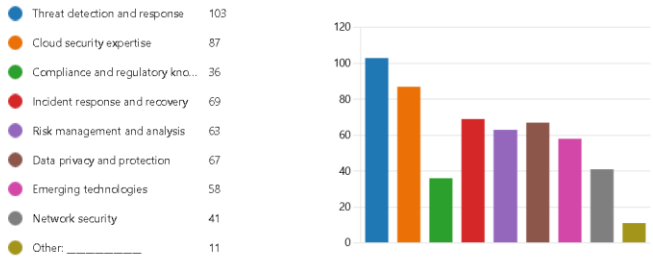
117
Réponses

Dernières réponses
"leverage external expertise, practical hands-on exercises, interactive training...

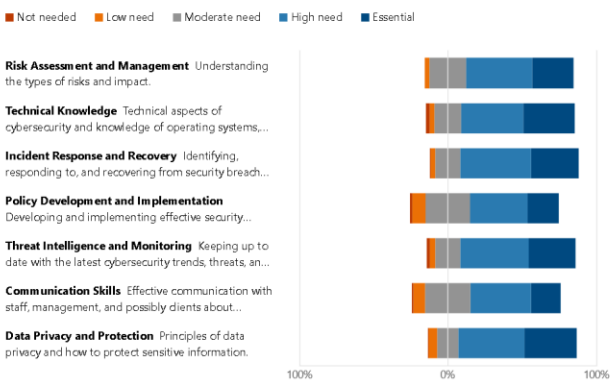
Mettre à jour

36 répondants (**31**%) répondu **trainings** pour cette question.

12. **In your opinion, what are the top skills deficits in the current SME cybersecurity workforce? (Choose up to three)**



13. **Please rate, from a scale from 1 (not needed) to 5 (essential) the competencies and knowledge needs:**



14. **Do you see any relevant set of skills and knowledge not listed in the previous question that might be highly needed for SMEs?**

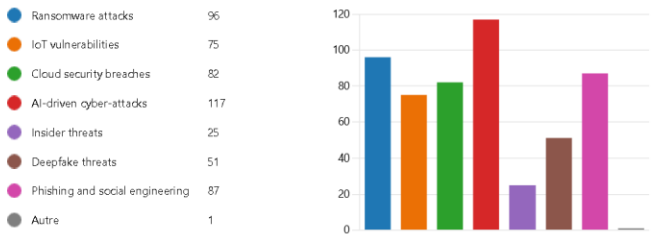
190
Réponses

Dernières réponses
"-"
"-"
"Cloud Security, AI"

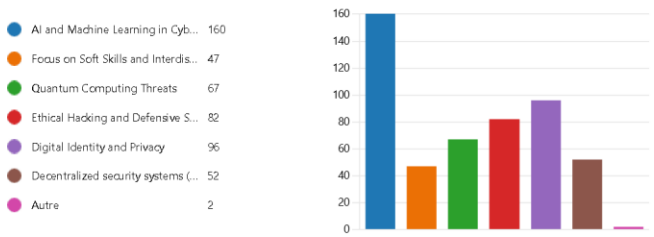
Mettre à jour

10 répondants (**5**%) répondu **skills** pour cette question.

15. **Which emerging cybersecurity threats do you believe SMEs need to be prepared for in the next 5 years? (Choose up to three)**



16. **What do you foresee as the top 3 emerging trends in cybersecurity training for the next 5 years? (Choose up to 3 options)**



17. **Are there any particular training methods, tools, or platforms that you believe are exceptionally effective for cybersecurity education?**

115
Réponses

Dernières réponses
"TryHackMe, HackTheBox"

Mettre à jour

12 répondants (**11**%) répondu **platform** pour cette question.

18. **Any additional comments or suggestions for improving cybersecurity training for SMEs?**

80
Réponses

Dernières réponses
"Uniform Course material"

Mettre à jour

9 répondants (**11**%) répondu **SMEs** pour cette question.

19. **What is the estimated percentage of women among the participants in your cybersecurity training programs?**

Less than 10%	57
10% - 25%	79
26% - 50%	43
51% - 75%	8
More than 75%	3

20. **Are there any specific initiatives or strategies you employ to encourage women's participation in cybersecurity training?**

Yes	30
No	160

21. **If you replied "Yes" to the previous question, please specify**

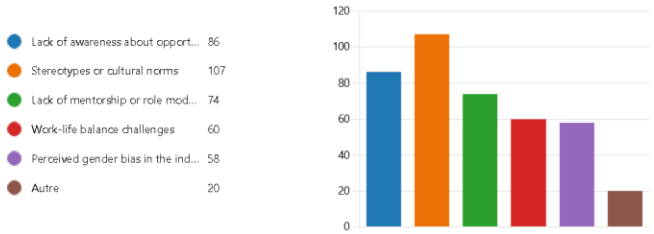
35
Réponses

Dernières réponses

13 répondants (**37**%) répondu **women** pour cette question.

22. **Do you believe there are enough gender-inclusive training modules available in cybersecurity?**

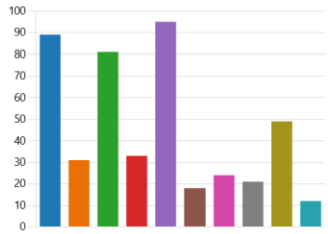
23. **In your experience, what are the primary barriers that prevent women from participating or advancing in cybersecurity training and careers? (Select all that apply)**



24. **Does your institution have specific policies or programs to promote diversity and inclusion, particularly for women, in cybersecurity training?**

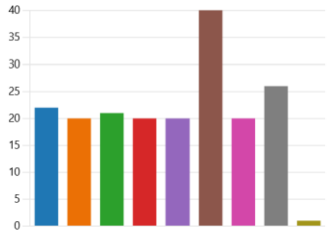
25. **What could make cybersecurity training more gender-inclusive? (Choose up to three)**

More female cybersecurity instr...	89
Regularly update policies to sup...	31
Offer scholarships or incentives	81
Training content that avoids gen...	33
Increased visibility of successful ...	95
More women-only training sessi...	18
Gender-inclusive case studies a...	24
Tailored training programs	21
Mentorship opportunities	49
Autre	12



26. **What is your country?**

Lithuania	22
Belgium	20
Norway	21
Türkiye	20
Finland	20
Romania	40
Spain	20
Poland	26
Azerbaijan	1



27. **In which school institution are you currently teaching?**

VET (Vocational Education and T...	86
HEI (Higher Education (HE) Instit...	104

28. **What is your gender?**

Male	121
Female	64
Prefer not to say	5

29. **How many years have you been involved in cybersecurity training? (Either general, specific, short and long trainings)**

Less than 1 year	21
1-5 years	85
6-10 years	53
More than 10 years	31

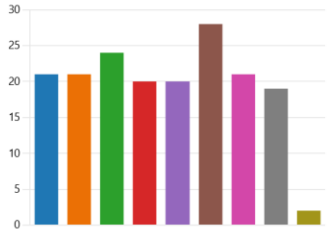
SMEs

Mapping the training needs for SME Cyber Security Change Agents - SMEs survey

176 Responses

1. **What is your country?**

Lithuania	21
Belgium	21
Norway	24
Türkiye	20
Finland	20
Romania	28
Spain	21
Poland	19
Azerbaijan	2



2. **What is your company sector?**

176
Réponses

Dernières réponses
"Consultancy"
"Cyber Security - Management Consultancy"
"Education, VET"

Mettre à jour

13 répondants (**7**%) répondu **education** pour cette question.

3. **What is your current position in the company?**

176
Réponses

Dernières réponses
"Team lead"
"Owner & Director"
"Teacher"

Mettre à jour

43 répondants (**25**%) répondu **Manager** pour cette question.

4. **What is your gender?**

5. **How many employees are working in the company?**

6. **How would you rate employees' current level of cybersecurity knowledge and skills?**

7. **How many employees perform work related to cybersecurity?**

176
Réponses

Dernières réponses
"3"
"2"
"3"

Mettre à jour

36 répondants (**21**%) répondu **1** pour cette question.

8. **How many of these employees are women?**

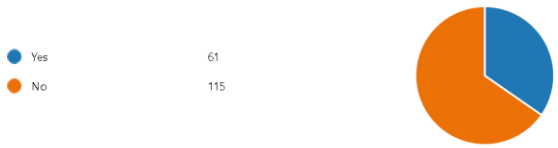
176
Réponses

Dernières réponses
"1"
"1"
"0"

Mettre à jour

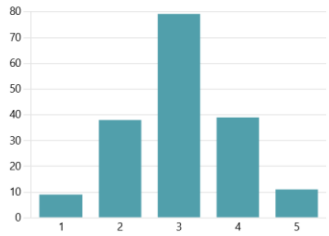
31 répondants (**18**%) répondu **1** pour cette question.

9. **Do you hire external services for cybersecurity work?**

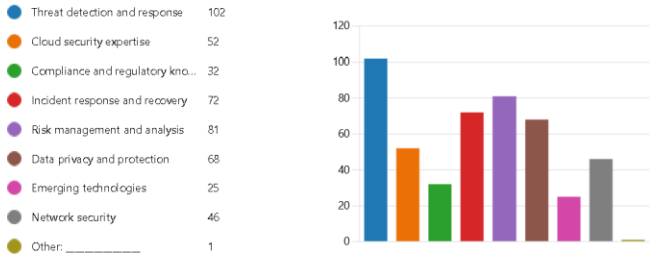


10. **On a scale of 1 (ineffective) to 5 (very effective), how effectively do you think the current training programs prepare students for real-world SMEs cybersecurity challenges?**

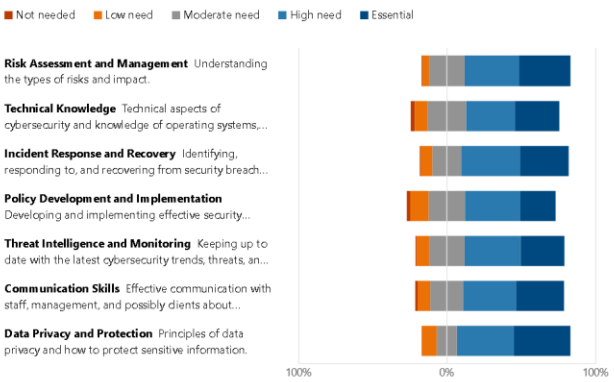
3.03
Évaluation moyenne



11. **In your opinion, what are the top skills deficits in the current SME cybersecurity workforce? (Choose up to three)**



12. **Please rate, from a scale from 1 (not needed) to 5 (essential) the competencies and knowledge needs:**



13. **Do you see any relevant set of skills and knowledge not listed in the previous question that might be highly needed for SMEs?**

175
Réponses

Dernières réponses

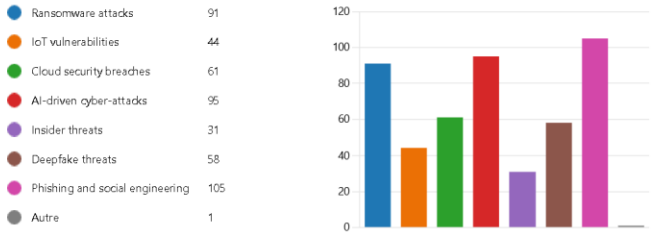
"My assumption is that Subject matter experts (SME's) in a big company are ...

"Cyber Security on all these topics arround Generative AI - which is complete...

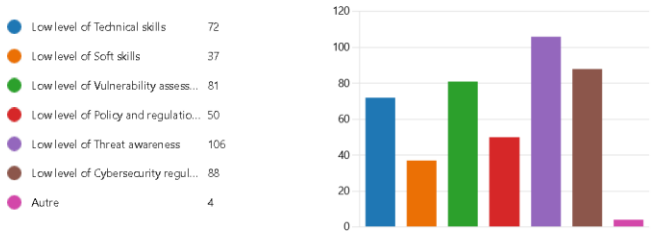
"Not sure"

4 répondants (**2**%) répondu **skills** pour cette question.

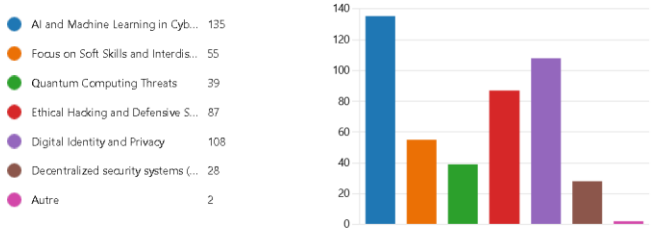
14. **Which emerging cybersecurity threats do you believe SMEs need to be prepared for in the next 5 years? (Choose up to three)**



15. **What specific gaps, if any, do you feel exist in employee's current cybersecurity knowledge or skills status? (Choose up to three)**

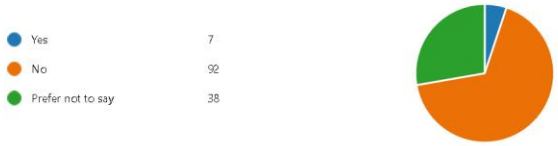


16. **What do you foresee as the top 3 emerging trends in cybersecurity training for the next 5 years? (Choose up to 3 options)**



17. **Do you feel that current cybersecurity training is inclusive and addresses the needs of all genders effectively?**

18. **If you identify as female, have you faced any barriers or challenges in accessing or participating in cybersecurity training/studies?**



19. **If you replied "Yes" to the previous question, please specify**

11
Réponses

Dernières réponses
"I feel that previous question is missing one more answer such as "I'm a male...
"I have to actively look for help and support for us females who work in the C...

Mettre à jour

3 répondants (**30**%) répondu **male** pour cette question.

20. **Are you aware of any initiatives or programs within your organization that specifically support or promote the participation of women in cybersecurity?**

21. **If you replied "Yes" to the previous question, please specify**

17
Réponses

Dernières réponses
"I am a strong female advocate for Cyber Security, Women Supporting Wom..."

8 répondants (**47**%) répondu **Women** pour cette question.

5.4. ANEXA D: LISTA OCUPATIILOR ESCO REVIZUITE

Referinte:

2529.1 https://esco.ec.europa.eu/sites/default/files/chief%20ICT%20security%20officer.pdf

2529.2 https://esco.ec.europa.eu/sites/default/files/digital%20forensics%20expert.pdf

2529.3 https://esco.ec.europa.eu/en/classification/occupation?uri=http%3A%2F%2Fdata.europa.eu%2Fesco%2Foccupation%2F1c5a896a-e010-4217-a29a-c44db26e25da

2529.4 https://esco.ec.europa.eu/sites/default/files/ethical%20hacker.pdf

2529.5 https://esco.ec.europa.eu/sites/default/files/ICT%20resilience%20manager.pdf

2529.6 https://esco.ec.europa.eu/sites/default/files/ICT%20security%20administrator.pdf

2529.7 https://esco.ec.europa.eu/sites/default/files/ICT%20security%20consultant.pdf

2529.8 https://esco.ec.europa.eu/sites/default/files/ICT%20security%20manager.pdf

2529.9 https://esco.ec.europa.eu/sites/default/files/knowledge%20engineer.pdf

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