Alfabetizare digitală în domeniul VET prin cursuri de securitate cibernetică și tehnologii imersive

---

GHID DE BUNE PRACTICI

Co-funded by the European Union

Project implemented by:

Această lucrare este licențiată sub o licență:
Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

Acest proiect a fost finanțat cu sprijinul Comisiei Europene. Publicația reflectă exclusiv opinia autorului, iar Comisia sau Agenția Națională nu pot fi considerate responsabile pentru modul în care sunt utilizate informațiile conținute în aceasta.

Ghid de bune practici

CONȚINUT

Ghid de bune practici

1. Introducere

1.1 Proiectul și obiectivele acestuia

Proiectul CybARverse, lansat în cadrul programului Erasmus+, este conceput pentru a îmbunătăți standardele de alfabetizare digitală și competențele de securitate cibernetică, prin utilizarea tehnologiilor imersive în cadrul educației și formării profesionale (***VET***). Coordonat de Asociacija „Langas į ateitį" din Lituania și în parteneriat cu S.C.P. Serv Limited, Cyprus Computer Society din Cipru, Tech.mt din Malta, și Fundatia EOS - Educating for an Open Society din România, proiectul își propune să abordeze decalajele existente în materie de competențe digitale, prin includerea tehnologiilor de ultimă generație de realitate augmentată (***AR***) și realitate virtuală (***VR***) în programele VET. Această abordare nu numai că îmbogățește activitatea de învățare, ci și pune la dispoziția educatorilor și formatorilor instrumentele necesare pentru a transmite cunoștințe esențiale privind securitatea cibernetică, sporind, astfel, capacitatea de reziliență a mediilor educaționale împotriva amenințărilor cibernetice.

1.1.1 Obiectivele principale ale proiectului CybARverse

Proiectul CybARverse este structurat în jurul a patru obiective principale, fiecare având scopul de a favoriza un impact cuprinzător și durabil în domeniul educației pentru securitate cibernetică::

1. **Consolidarea competențelor profesionale, personale și digitale:**

- **Dezvoltare profesională**: Însușirea de către educatori și formatori a cunoștințelor și practicilor de ultimă oră din domeniul securității cibernetice, pentru a aborda și atenua cu eficiență amenințările cibernetice aflate în continuă evoluție.
- **Creștere personală**: Promovarea competențelor esențiale precum gândirea critică, rezolvarea problemelor și luarea deciziilor prin intermediul activităților de învățare interactive și bazate pe scenarii.
- **Fluență digitală**: Dezvoltarea competențelor digitale ale cadrelor didactice și profesioniștilor din domeniul VET, cu un accent deosebit pe utilizarea competentă a tehnologiilor AR și VR, pentru a simula și a răspunde provocărilor în materie de securitate cibernetică.

2. **Integrarea tehnologiilor moderne și imersive:**

- Implementarea AR și VR pentru a crea medii de formare dinamice și atractive, care să simuleze scenarii de securitate cibernetică din lumea reală, punând la dispoziție activități de învățare practice, interactive, care depășesc metodele educaționale tradiționale.

3. **Calificare profesională structurată:**

- Elaborarea unui program de formare cuprinzător, pe mai multe niveluri, care îmbunătățește în mod sistematic conștientizarea și experiența în domeniul securității cibernetice, de la cunoștințe de bază la competențe operaționale avansate.

4. **Sustenabilitatea impactului educațional:**

- Stabilirea unui model educațional sustenabil, care include dezvoltarea profesională continuă și actualizarea materialelor de formare, astfel încât programa să fie actualizată în funcție de evoluția rapidă a amenințărilor și tehnologiilor de securitate cibernetică. În plus, se va promova o comunitate de practică, care să sprijine învățarea continuă și schimbul de bune practici între educatorii din domeniul securității cibernetice.

1.2 Îndrumări pedagogice - Înțelegerea rolului „Îndrumărilor pedagogice” în cadrul proiectului CybARverse

Ca parte a abordării cuprinzătoare de îmbunătățire a educației privind securitatea cibernetică în cadrul educației și formării profesionale (VET), proiectul CybARverse a elaborat un document esențial intitulat „Îndrumări pedagogice”. Acest document joacă un rol cheie în orientarea educatorilor VET cu privire la modalitățile eficiente de integrare a tehnologiilor digitale avansate și imersive în practicile lor didactice.

1.3 Scopul și impactul Îndrumărilor pedagogice

Îndrumările pedagogice sunt concepute pentru a asigura educatorilor și formatorilor o înțelegere detaliată a modului de utilizare a tehnologiilor de realitate augmentată (***AR***) și realitate virtuală (***VR***) într-un mod pedagogic fundamentat. Aceste îndrumări sunt esențiale pentru atingerea obiectivelor principale ale proiectului CybARverse:

1. **Consolidarea competențelor digitale**: Prin detalierea aplicării tehnologiilor AR și VR în contexte educaționale, îndrumările pedagogice asigură educatorilor competențele necesare pentru a încorpora în mod eficient aceste tehnologii în programele lor de învățământ, îmbunătățind, astfel, competențele digitale ale cursanților.

2. **Trasee de învățare structurate**: Îndrumările pedagogice prezintă abordări structurate ale utilizării tehnologiilor imersive, asigurând că formarea oferită este sistematică și cuprinzătoare. Acest lucru contribuie la crearea unui cadru de educatori VET calificați care sunt experți în securitate cibernetică și alfabetizare digitală.

3. **Promovarea practicilor educaționale atractive**: Prin metodele de predare inovatoare sugerate în îndrumările pedagogice, educatorii pot crea activități de învățare mai antrenante și cu un nivel de interactivitate mai ridicat. Acest lucru nu numai că îmbunătățește calitatea educației, dar face și învățarea mai atractivă și mai eficientă pentru cursanți.

4. **Sustenabilitatea practicilor educaționale**: Îndrumările pedagogice recomandă actualizări și adaptări continue ale strategiilor de predare, pentru a ține pasul cu progresele tehnologice. Această abordare garantează păstrarea relevanței conținutului educațional și menținerea în timp a beneficiilor proiectului.

Îndrumările pedagogice reprezintă un produs independent în cadrul proiectului CybARverse, completând, în același timp, obiectivele mai ample subliniate în Ghidul de bune practici, prin furnizarea de aplicații practice ale cadrelor teoretice discutate. Educatorii care utilizează Ghidul de bune practici vor găsi în Îndrumările pedagogice o resursă neprețuită pentru implementarea eficientă a practicilor recomandate.

Îndrumările pedagogice nu sunt doar un set de instrucțiuni; ele sunt un instrument de transformare, care permite educatorilor să utilizeze potențialul tehnologiilor moderne pentru educația în domeniul securității cibernetice. Prin detalierea utilizării eficiente a tehnologiilor AR și VR, aceste Îndrumări pedagogice contribuie la reducerea decalajului dintre metodele tradiționale de predare și cerințele erei digitale.

Menționarea acestor Îndrumări în Ghidul de bune practici subliniază angajamentul proiectului CybARverse față de o strategie educațională holistică, care este, deopotrivă, orientată spre viitor și bazată pe aplicații practice. Această discuție evidențiază interconexiunea dintre cele două documente și impactul lor colectiv asupra îmbunătățirii practicilor educaționale.

Documentul privind Îndrumările pedagogice poate fi consultat aici.

1.4 Prezentarea generală a nivelurilor de formare

Proiectul CybARverse propune trei niveluri progresive de instruire, fiecare dintre acestea fiind concepute pentru a răspunde diferitelor niveluri de cunoștințe și competențe în domeniul tehnologiilor digitale și al securității cibernetice ale participanților:

1. **Începător:** Această etapă inițială prezintă concepte fundamentale de alfabetizare digitală și securitate cibernetică, vizând educatorii și formatorii care sunt începători în domeniul digital. Astfel, se pun bazele unei învățări mai complexe.

2. **Intermediar:** Acest nivel extinde cunoștințele de bază, explorând protocoale de securitate cibernetică și practici digitale mai complexe. Participanții se implică în scenarii interactive AR și VR care simulează amenințări cibernetice din lumea reală, ceea ce le îmbunătățește cunoștințele analitice și de rezolvare a problemelor.

3. **Avansat:** Cel mai avansat nivel este personalizat pentru participanții care dețin cunoștințe solide despre instrumentele digitale și securitatea cibernetică. Se concentrează pe domenii specializate, precum analiza amenințărilor, tehnici avansate de codare și implementarea strategică a măsurilor de securitate cibernetică în contexte educaționale.

1.5 Scurtă descriere a conținutului și structurii cursului

Cadrul de formare al proiectului CybARverse este structurat cu atenție, pentru a asigura o activitate educațională completă, care să fie deopotrivă atractivă și informativă. Conținutul cursului este elaborat în mod strategic, pentru a dezvolta competențe atât în ceea ce privește alfabetizarea digitală, cât și aplicațiile practice privind securitatea cibernetică, completate de tehnologiile inovatoare AR și VR.

- **Conținutul cursului:** Programa include un ansamblu de cunoștințe teoretice și abilități practice de securitate cibernetică, precum și o aprofundare a tehnologiilor AR și VR și a aplicării acestora în mediul educațional. Fiecare modul este conceput pentru a se baza pe cel anterior, îmbunătățind nivelul de cunoștințe și de competențe pe măsură ce se înaintează în programă.

- **Structura cursului:** Cursul este modular, permițând o abordare concentrată a fiecărui aspect al securității cibernetice și al alfabetizării digitale. Acesta integrează elemente interactive, precum simulări AR și VR, ateliere și webinarii live conduse de experți în domeniu. Fiecare modul este urmat de evaluări detaliate, pentru a asigura înțelegerea și pregătirea participanților pentru nivelurile următoare.

- **Componente interactive:** Utilizând tehnologiile AR și VR, cursul creează scenarii realiste, în care participanții își pot aplica competențele de securitate cibernetică într-un mediu virtual, dar realist. Această metodă nu numai că le consolidează învățarea, dar îi și pregătește să facă față în mod eficient unor provocări similare în contexte din lumea reală.

Pe lângă curriculumul de bază, proiectul CybARverse include componente de dezvoltare profesională continuă, permițând educatorilor și formatorilor să țină pasul cu cele mai recente tendințe în materie de securitate cibernetică și cu progresele tehnologice. Acest proces de învățare continuă asigură faptul că metodologiile de predare rămân actuale și eficiente, consolidând și mai mult postura generală de securitate cibernetică a mediilor educaționale respective.

Prin integrarea acestor instrumente tehnologice avansate în conținutul educațional conceput de experți, Ghidul de bune practici CybARverse își propune să asigure educatorilor și formatorilor VET competențele necesare pentru a preda eficient securitatea cibernetică, contribuind, astfel, la crearea unui viitor digital mai sigur. Prin promovarea unui ecosistem de învățare și adaptare continuă, CybARverse se asigură că beneficiarii săi sunt pregătiți să conducă și să inoveze în peisajul digital în continuă evoluție, sporind în cele din urmă impactul și eficacitatea lor educațională.

2. Sistemul de gestionare a învățării (LMS)

Conținutul cursului este disponibil în Sistemul de gestionare a învățării al platformei LearnPress (LMP). Acesta este una dintre cele mai utilizate LMS-uri pentru cursurile online, oferind posibilitatea de a crea o programă ce include lecții și teste, și care conține o interfață ușor de utilizat pentru cursanți și utilizatori.

2.1 Conceptul și structura cursului

Cursul este structurat pe un model modular, permițând, astfel, o abordare concentrată a fiecărui aspect al securității cibernetice și al alfabetizării digitale. Acesta integrează elemente interactive, precum simulări VR și AR, ateliere și webinarii live conduse de experți în domeniu. Fiecare modul este urmat de evaluări detaliate, pentru a asigura înțelegerea și pregătirea participanților pentru nivelurile următoare.

Cursul cuprinde 17 module de învățare care sunt împărțite în trei niveluri diferite, astfel încât cursanții să le poată alege pe cele care sunt cele mai relevante pentru ei.

Nivelul începător acoperă șase subiecte esențiale de securitate cibernetică pentru începători, cu o durată de învățare de 6 ore:

- Introducere în malware,
- Ingineria socială,
- Racolarea online,
- riscurile de securitate cibernetică pe rețelele sociale,
- phishing,
- și atacurile din Internetul Obiectelor (IoT).

Nivelul intermediar al cursului aprofundează șase amenințări avansate de securitate cibernetică cu o durată de învățare de 8 ore:

- ransomware,
- rootkit-uri,
- pharming,
- cryptojacking,
- cross-site scripting,
- și injecția SQL.

Nivelul avansat se concentrează pe 5 amenințări complexe la adresa securității cibernetice, cu o durată de învățare de 10 ore:

- atacurile de tip man-in-the-middle – intermediar inserat,
- exploatarea avansată a vulnerabilităților existente în Internetul obiectelor (IoT)
- exploatarea vulnerabilităților de tip „zero-day”
- atacurile DoS ,
- și atacurile DDoS.

Fiecare modul conține aceeași structură:

1. Lecturi teoretice care acoperă descrierea amenințării în sine, caracteristicile care permit recunoașterea amenințării și mijloacele de atenuare și/sau prevenire a riscurilor. Noțiunile teoretice sunt predate într-un mod structurat, dar cuprinzător, astfel încât cursantul să înțeleagă amenințarea cu mai multă ușurință.
2. Mai multe studii de caz, pentru a înțelege mai bine relevanța amenințării descrise în lumea online de astăzi.
3. Componente interactive - videoclipuri, tehnologii AR/VR/WebVR, care permit crearea de scenarii realiste, în care participanții își pot aplica competențele de securitate cibernetică într-un mediu virtual, dar realist.

4. Fiecare modul include planuri de lecții pentru a simula și înțelege aceste amenințări și, de asemenea, pentru a preda cursanților cunoștințele aferente.

5. Fiecare nivel de curs se încheie cu un examen conceput pentru ca formatorii VET să își evalueze cunoștințele și experiența dobândite. Pentru a primi certificatul de curs este necesară promovarea examenului.

2.2. Strategii eficiente de învățare online

Cursul conceput prin intermediul proiectului poate fi utilizat pentru învățarea individuală în ritm propriu sau instituția VET poate organiza cursuri online sau mixte pentru întregul grup de cursanți.

Cursanții ar putea primi sprijin din partea instructorului atât cu privire la subiect, cât și la utilizarea LMS și a resurselor.

2.2.1 Pentru instructori și educatori

Următoarele puncte trebuie luate în considerare atunci când organizați cursuri de formare utilizând materialul din acest curs online:

a. Conceptul și structura cursului

- **Obiective clare**: definirea unor obiective și rezultate clare ale învățării pentru fiecare modul. Acest lucru îi ajută pe cursanți să înțeleagă ce se așteaptă de la ei să învețe și să dobândească.
- **Conținut modular**: conținutul cursului este împărțit în module sau unități ușor de gestionat. Fiecare modul ar trebui să acopere un subiect sau o competență specifică în securitatea cibernetică.
- **Elemente interactive**: fiecare modul încorporează elemente interactive precum teste, demonstrații, simulări, studii de caz și laboratoare practice VR/AR. Aceste activități contribuie la consolidarea învățării și mențin implicarea cursanților.
- **Resurse multimedia**: utilizarea de resurse multimedia, inclusiv cele disponibile în cadrul cursului sau videoclipuri online, pentru a răspunde diferitelor stiluri de învățare.

b. Implicare și interacțiune

- **Forumuri de discuții**: crearea de forumuri de discuții (de exemplu, pe rețele sociale), în care cursanții pot pune întrebări, împărtăși idei și colabora. Se încurajează participarea activă prin adresarea de întrebări care stimulează gândirea.
- **Sesiuni live**: programarea de sesiuni live regulate (webinarii sau săli de clasă virtuale) pentru a asigura interacțiune și feedback în timp real. Aceste sesiuni sunt folosite pentru întrebări și răspunsuri, discuții și prelegeri din partea experților din domeniu.
- **Mecanisme de feedback**: monitorizarea progresului cursanților și furnizarea de feedback oportun și constructiv.

c. Evaluare și analiză

- **Evaluări cu caracter formativ și sumativ**: fiecare curs include un test final ca evaluare sumativă, dar instructorul poate utiliza propriile sarcini (teme) scurte pentru a evalua nivelul de înțelegere a cunoștințelor de către cursanți pe parcursul cursului. Acest lucru permite intervenția în timp util, dacă este necesar.

d. Asistență tehnică și resurse

- **Îndrumare tehnică:** Furnizarea de instrucțiuni clare și sprijin pentru utilizarea platformei și a instrumentelor de învățare online. Punerea la dispoziție a unor tutoriale și a unor seturi de întrebări frecvente (FAQ-uri) pentru a ajuta cursanții să utilizeze tehnologia.
- **Accesibilitatea resurselor**: Se va asigura că toate materialele de curs sunt accesibile cursanților cu dizabilități. Se utilizează formate accesibile și se furnizează resurse alternative, atunci când este necesar.

e. Integrarea activităților online și offline

- **Tranziție continuă**: Asigurarea unei tranziții fără întreruperi între activitățile online și offline. Alinierea modulelor online cu sesiunile în persoană pentru a consolida învățarea.
- **Sarcini hibride**: Elaborarea sarcinilor (temelor) care necesită atât cercetare online, cât și aplicare offline. Acest lucru îi ajută pe cursanți să integreze cunoștințele din diverse surse.

2.2.2 Pentru participanți

1. **Gestionarea timpului**

   - **Stabilirea unui calendar**: Crearea unui calendar de studiu, care să includă timp dedicat participării la sesiunile live, finalizării temelor și revizuirii materialelor de curs. Respectarea acestui calendar pentru a fi în grafic.
   - **Prioritizarea sarcinilor**: Prioritizarea sarcinilor în funcție de termene limită și importanță. Folosirea de instrumente, precum liste de sarcini și calendare pentru gestionarea eficientă a volumului de muncă.

2. **Participare activă**

   - **Implicarea în discuții**: Participarea activă la forumuri de discuții și sesiuni live. Partajarea opiniilor proprii, adresarea de întrebări și colaborarea cu colegii.
   - **Solicitarea de feedback**: Nu ezitați să solicitați feedback de la instructori și colegi. Utilizarea acestui feedback pentru a vă îmbunătăți înțelegerea și performanța.

3. **Auto-motivare și disciplină**

   - **Stabilirea obiectivelor**: Stabilirea unor obiective specifice, realizabile, pentru fiecare sesiune de învățare. Acest lucru ajută la menținerea concentrării și a motivării.
   - **Menținerea disciplinei**: Menținerea disciplinei prin reducerea la minimum a distragerilor în timpul orelor de învățare. Crearea unui mediu de învățare favorabil, lipsit de întreruperi.

4. **Utilizarea resurselor**

   - **Utilizarea resurselor multimedia furnizate în cadrul cursului**: Urmărirea de videoclipuri și resurse vizuale pentru consolidarea cunoștințelor dobândite.
   - **Exersarea abilităților practice**: Participarea la simulări VR/AR pentru a aplica cunoștințele teoretice la scenarii practice. Acest lucru este deosebit de important în formarea în domeniul securității cibernetice.

2.3. Considerații privind accesibilitatea și incluziunea pentru cursanți diverși

Crearea de materiale de învățare și site-uri web accesibile și incluzive este esențială pentru a se asigura că toți cursanții, indiferent de abilitățile sau formarea anterioară, pot participa pe deplin și beneficia de procesul educațional. Deși proiectul oferă materiale de învățare gata pregătite, acestea vor trebui actualizate, pot fi localizate în alte țări și vor fi utilizate de diferiți educatori pentru a putea pune la dispoziție, de exemplu, cursuri de învățare mixtă.

2.3.1 Accesibilitate - considerente cheie

În continuare sunt prezentate câteva considerente cheie pentru elaborarea și aplicarea cursurilor:

1. Design universal pentru învățare (UDL)

Designul universal pentru învățare (UDL) este un cadru educațional care urmărește să creeze un mediu de învățare care să se adapteze tuturor cursanților. Principiile UDL includ:

- **Mijloace multiple de reprezentare:** furnizează informații în diverse formate, cum ar fi text, videoclipuri, înregistrări audio și elemente interactive, pentru a răspunde diferitelor preferințe de învățare.
- **Mijloace multiple de exprimare:** permit cursanților să își demonstreze cunoștințele în diverse moduri, cum ar fi lucrări scrise, prezentări sau proiecte.
- **Mijloace multiple de implicare:** încurajează motivarea și implicarea, prin propunerea de activități și sarcini diverse, care sunt adaptate intereselor și nevoilor cursanților.

2. Accesibilitate

Asigurarea accesibilității înseamnă punerea materialelor de învățare la dispoziția tuturor, inclusiv la dispoziția persoanelor cu dizabilități. Aspectele cheie includ:

- **Text alternativ pentru conținutul vizual și audio**: se vor furniza descrieri text pentru imagini și subtitrări pentru videoclipuri pentru a asigura accesibilitatea întregului conținut.
- **Contrast cromatic adecvat**: se vor folosi combinații de culori care sunt ușor de citit și de înțeles, în special pentru persoanele cu deficiențe de vedere.

- **Compatibilitatea cu cititoarele de ecran**: se va asigura compatibilitatea site-urilor web și a documentelor cu cititoarele de ecran pentru a veni în sprijinul persoanelor cu deficiențe de vedere.
- **Navigarea cu ajutorul tastaturii**: se va asigura navigarea cu ușurință pe site folosind doar o tastatură, ceea ce este esențial pentru persoanele cu deficiențe motorii.

În practică, proiectarea site-ului web și a materialului educațional se bazează pe principalele orientări WCAG 2.0, dintre care următoarele sunt importante și pot fi puse în aplicare cu ușurință:

- Se va asigura că textul este ușor de citit, prin utilizarea unui contrast suficient între text și fundal. Dacă nu este necesar, se va evita folosirea unui fundal.
- Se vor folosi fonturi mai mari și și se va permite utilizatorilor să schimbe dimensiunea fontului, după cum este necesar. Se vor utiliza fonturi clare și simple, cum ar fi Arial sau Verdana. Se vor evita caracterele italice și sublinierile, care pot îngreuna citirea.
- Stilurile pentru titluri definesc structura textului și, prin urmare, ar trebui utilizate în mod consecvent, de la nivelul superior la cel inferior. De subliniat că acestea nu reprezintă elemente decorative pentru a evidenția textul.
- Nu se utilizează niciodată texte (cum ar fi titluri, meniuri, adaosuri) ca imagini. Astfel de informații nu pot fi citite de cititoarele de ecran și, în numeroase cazuri, nu pot fi redimensionate.
- Documente atașate: A se verifica dacă documentele atașate sunt compatibile cu cititoarele de ecran. Documentele PDF pot fi modificate cu ajutorul instrumentului online https://pave-pdf.org/index.html?lang=en.
- Material vizual: se adaugă text alternativ la toate imaginile (cu excepția elementelor decorative), pentru a permite cititoarelor de ecran să descrie imaginea. Se vor utiliza ilustrații și diagrame clare și ușor de înțeles.
- Materiale video și audio: se adaugă subtitrări la toate materialele video. Se furnizează transcrieri pentru înregistrările audio.
- Navigare și structură: se asigură că este ușor de navigat pe site cu ajutorul tastaturii. Se utilizează o structură clară și logică a site-ului, cu meniuri și link-uri uniforme.
- Accesibilitatea online a materialelor deschise poate fi verificată cu ajutorul instrumentului online https://www.accessibilitychecker.org/.

3. Limbaj și imagini

Utilizarea unui limbaj și a unor imagini incluzive îi ajută pe toți cursanții să se simtă apreciați și incluși:

- **Ușor de înțeles**: se folosesc propoziții și paragrafe scurte. Cele mai importante informații vor fi prezentate la început. Pentru a face informațiile mai ușor de înțeles, se utilizează liste obișnuite și liste cu marcatori.
- **Limbaj incluziv:** se vor evita prejudecățile și stereotipurile de gen. Se va folosi un limbaj neutru și incluziv, care să respecte toate persoanele.
- **Diverse materiale imagistice:** se utilizează imagini care reflectă diferite culturi, abilități și medii de formare, pentru a reprezenta diversitatea comunității de învățare.

4. Accesibilitatea tehnologiei

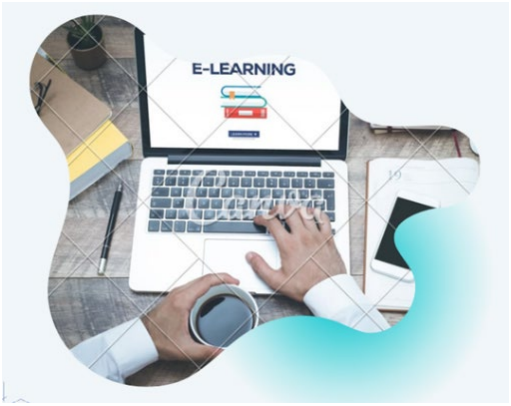
Se va asigura că toți cursanții au acces la tehnologia necesară:

- **Accesul la tehnologie:** se va asigura accesul cursanților la instrumentele necesare și la conexiuni fiabile la internet. Deoarece cursanții au rareori acces personal la echipamentele VR și AR, este necesar să li se ofere posibilitatea de a utiliza aceste echipamente într-un interval orar stabilit de instituția de învățământ VET, unde pot primi și suportul tehnic necesar.
- **Restricții internaționale:** se va lua în considerare specificul internațional privind utilizarea tehnologiei și se va asigura că materialele sunt accesibile tuturor cursanților, indiferent de locul în care se află.

5. Accesibilitatea în funcție de timp

Se vor avea în vedere constrângerile de timp ale cursanților:

- **Calendar flexibil**: pentru a se adapta diferitelor calendare/grafice, se oferă termene limită flexibile și oportunități de a revizui materialele în orice moment.



2.3.2 Recomandări

Realitatea augmentată și realitatea virtuală (AR și VR) pot fi deosebit de utile în procesul de formare, însă este important să se asigure că aceste tehnologii sunt sigure pentru persoanele cu dizabilități. Iată câteva recomandări:

1. **Siguranța fizică:**

   - Se asigură că utilizatorii au suficient spațiu pentru a se deplasa și sunt protejați împotriva obstacolelor.
   - Se vor prezenta instrucțiuni cu privire la modul de utilizare a echipamentului în condiții de siguranță și se vor supraveghea utilizatorii, pentru a evita eventuale vătămări.

2. **Siguranța emoțională**:

   - Se recomandă utilizarea unor medii VR simple și mai puțin stimulative, pentru a evita supraîncărcarea senzorială excesivă, care poate provoca stres sau anxietate.
   - Se vor evita luminile puternice și imaginile care se mișcă rapid.
   - Se va monitoriza continuu bunăstarea fizică și emoțională a cursanților care utilizează tehnologia VR. Utilizarea pe termen lung a tehnologiei VR poate duce la deficiențe cognitive pe termen scurt, cum ar fi tulburări de atenție, probleme de memorie și dificultăți de orientare în medii din lumea reală.
   - Se va permite cursanților să se retragă dintr-o sesiune în orice moment, dacă se simt inconfortabil sau experimentează un disconfort.

Respectând aceste recomandări, se poate dezvolta un mediu de învățare accesibil și incluziv, în care toți cursanții pot obține progrese și își pot atinge potențialul maxim

3 Module de învățare

3.1 Integrarea studiilor de caz

Pentru formatorii VET, integrarea studiilor de caz în modulele de învățare CybARverse constituie un instrument eficient pentru îmbunătățirea predării noțiunilor de securitate cibernetică. Studiile de caz servesc drept exemple practice, din lumea reală, care permit formatorilor să treacă dincolo de instruirea teoretică și să își implice cursanții în rezolvarea unor probleme reale de securitate cibernetică. Aceste scenarii atent elaborate permit o abordare directă pentru a înțelege modul în care se manifestă amenințările cibernetice și pașii necesari pentru a le atenua, ceea ce le transformă într-o parte esențială a curriculumului pentru formatorii care doresc să le asigure cursanților competențe concrete.

Sistemul online de gestionare a învățării (LMS) CybARverse Learning Management System (LMS) include o gamă largă de planuri de lecții detaliate, fiecare structurat în jurul unor studii de caz specifice, care acoperă diverse tipuri de incidente de securitate cibernetică. Aceste planuri de lecții cu o durată de 45 de minute sunt concepute pentru a fi flexibile și pot fi adaptate la diferite stiluri de predare și niveluri de cunoștințe. Formatorii pot accesa aceste resurse prin intermediul LMS, ceea ce le permite să integreze cu ușurință studiile de caz în programele lor existente. Fiecare plan de lecție prezintă obiectivele, rezultatele învățării și îndrumări pas cu pas pentru prezentarea studiului de caz, asigurându-se că formatorii pot conduce în mod eficient discuțiile, pot facilita activitățile de rezolvare a problemelor și pot evalua cunoștințele cursanților.

Studiile de caz sunt organizate astfel încât să abordeze o varietate de subiecte de securitate cibernetică, cum ar fi programele malware, atacurile de phishing, incidentele ransomware și tacticile de inginerie socială. Pentru fiecare scenariu, planurile de lecție includ informații generale și exemple-cheie de securitate cibernetică, pentru a ghida cursanții în analiza cazului. Această structură îi ajută pe formatori să pună accentul pe gândirea critică și pe luarea deciziilor, pe măsură ce cursanții explorează cum și de ce apar breșele de securitate și ce se poate face pentru a le preveni. În plus, planurile de lecție includ sesiuni de discuții de grup și de rezolvare în grup a problemelor, în cadrul cărora formatorii își pot ajuta cursanții să își dezvolte atât cunoștințele tehnice, cât și competențele transversale necesare pentru a avea succes în rolurile din domeniul securității cibernetice.

LMS oferă, de asemenea, formatorilor posibilitatea de a urmări progresul cursanților prin intermediul evaluărilor legate de fiecare studiu de caz. Aceste evaluări, care variază de la teste la exerciții practice, îi ajută pe formatori să analizeze gradul de înțelegere a materialului de către cursanți și să identifice domeniile de dezvoltare ulterioară. Instrumentele de analiză ale platformei oferă informații despre performanțele cursanților, permițând formatorilor să își adapteze predarea pentru a răspunde mai bine nevoilor cursanților lor.

Pentru formatorii VET includerea studiilor de caz nu înseamnă doar predarea conceptelor de securitate cibernetică, ci și oferirea posibilității ca participanții la curs să aplice aceste concepte în scenarii reale. Prin exploatarea planurilor de lecții și a resurselor disponibile prin CybARverse LMS, formatorii pot propune o activitate de învățare captivantă și cu impact, care îi pregătește pe cursanți pentru provocările peisajului modern al securității cibernetice.

Flexibilitatea și accesibilitatea resurselor studiilor de caz asigură faptul că formatorii le pot integra cu ușurință în predarea lor, în timp ce platforma LMS pune la dispoziție toate instrumentele necesare pentru a monitoriza progresul cursanților, a facilita discuțiile și a asigura o învățare eficientă. Trebuie subliniat faptul că platforma LMS este disponibilă în 5 limbi (engleză, greacă, lituaniană, malteză și română).

3.2 Scenarii din lumea reală pentru învățarea aplicată

Pentru formatorii VET includerea scenariilor din lumea reală în formarea în domeniul securității cibernetice este esențială pentru a pune la dispoziția cursanților activități practice. Modulele de învățare CybARverse sunt concepute pentru a prezenta incidente cibernetice din lumea reală, permițând cursanților să aplice cunoștințele teoretice în medii reale, controlate. Această metodă de învățare aplicată reduce decalajul dintre învățarea în clasă și provocările dinamice cu care se confruntă profesioniștii din domeniul securității cibernetice, ceea ce o face o componentă esențială a procesului de formare.

Sistemul online de gestionare a învățării (LMS) al proiectului CybARverse pune la dispoziție exemple de scenarii din lumea reală, pe care formatorii le pot integra cu ușurință în lecțiile lor. Fiecare scenariu este elaborat cu atenție, pentru a reflecta amenințările actuale la adresa securității cibernetice, cum ar fi ingineria socială, pharming-ul, incidentele de injectare SQL și atacurile de tip „zero-day”. Aceste scenarii sunt însoțite de planuri de lecție detaliate care descriu obiectivele, instrucțiunile pas cu pas și rezultatele așteptate, permițând formatorilor să le includă fără probleme în predarea lor.

Fiecare scenariu real este conceput pentru a putea fi adaptat diferitelor niveluri de competență, ceea ce îl face potrivit pentru formatorii VET care lucrează cu cursanți aflați în diferite etape ale pregătirii lor în domeniul securității cibernetice. Pentru începători, scenariile pot implica sarcini simple, cum ar fi identificarea tentativelor comune de phishing sau detectarea de bază a programelor malware. Pentru cursanții mai avansați, scenariile pot deveni din ce în ce mai complexe, solicitându-le să gestioneze vectori de atac sofisticați, cum ar fi amenințările persistente avansate (APT) sau atacurile multi-vector, în care luarea rapidă a deciziilor și aplicarea protocoalelor avansate de securitate cibernetică sunt esențiale.

Formatorii pot utiliza aceste scenarii din lumea reală pentru a stimula participarea activă și implicarea. Cursanții sunt încurajați să colaboreze cu colegii pentru a rezolva incidentele cibernetice simulate, imitând munca în echipă necesară în mediile profesionale ce se ocupă de securitatea cibernetică. Aceste exerciții de colaborare îmbunătățesc abilitățile de comunicare și promovează o înțelegere mai profundă a modului

în care profesioniștii din domeniul securității cibernetice trebuie să colaboreze, pentru a atenua și preveni amenințările cibernetice în timp real.

Integrarea scenariilor din lumea reală în modulele de învățare CybARverse asigură formatorilor VET o modalitate eficientă de a pune la dispoziție activități de învățare aplicate. Abordarea structurată, bazată pe scenarii, disponibilă prin LMS, asigură faptul că participanții la curs nu sunt expuși doar la concepte teoretice de securitate cibernetică, ci și la realitățile practice ale apărării împotriva amenințărilor cibernetice. Prin utilizarea acestor instrumente, formatorii pot asigura o activitate de învățare temeinică și mai interactivă, care le formează cursanților competențele necesare pentru a naviga în peisajul în continuă evoluție al securității cibernetice.

3.3 Folosirea materialelor video pentru activități de învățare captivante

Utilizarea conținutului video constituie o metodă cu impact pentru a crea activități de învățare captivante și imersive în cadrul programei proiectului CybARverse. Videoclipurile reprezintă un mijloc eficient de ilustrare a conceptelor complexe de securitate cibernetică, de demonstrare a aplicațiilor din lumea reală și de menținere a implicării active a cursanților pe parcursul procesului de formare. Prin includerea videoclipurilor scurte în lecțiile lor, formatorii pot spori gradul de aprofundare și calitatea predării, punând la dispoziția cursanților exemple vizuale și auditive care sunt mai ușor de înțeles și reținut.

Sistemul de gestionare a învățării (LMS) CybARverse propune nouă videoclipuri scurte pentru anumite scenarii, pe care formatorii le pot integra fără probleme în cursurile lor. Aceste videoclipuri disponibile pe canalul CybARverse YouTube Channel acoperă următoarele subiecte: inginerie socială, malware, phishing, riscurile de securitate cibernetică pe rețelele sociale și racolarea online în cadrul nivelului Începător și ransomware, pharming și cross-site scripting (XSS) în cadrul nivelului Intermediar, asigurându-se că formatorii VET au acces la materiale de înaltă calitate, adaptate diferitelor niveluri de calificare ale cursanților. Videoclipurile sunt concepute pentru a completa lecțiile teoretice și activitățile de învățare aplicate, constituind un instrument flexibil pentru îmbunătățirea înțelegerii și a implicării.

Această abordare vizuală a învățării contribuie la demistificarea conceptelor complexe, făcându-le mai accesibile pentru cursanți, în special pentru cei care ar putea avea dificultăți cu materialele bazate exclusiv pe text. Formatorii pot utiliza aceste videoclipuri ca puncte de pornire pentru dezbateri, încurajând cursanții să analizeze deciziile luate și să propună soluții alternative.

Videoclipurile reprezintă, de asemenea, un instrument valoros pentru diversificarea procesului de învățare, răspunzând diferitelor stiluri de învățare. Cei care învață prin mijloace vizuale beneficiază văzând conceptele demonstrate în acțiune, în timp ce cei care învață prin mijloace auditive pot asimila informațiile prin intermediul vocilor și explicațiilor experților. Formatorii pot utiliza această flexibilitate pentru a crea un mediu de învățare mai incluziv, asigurându-se că predarea rezonează cu o gamă mai largă de cursanți. LMS dispune, de asemenea, de caracteristici de accesibilitate, cum ar fi subtitrările și transcrierile, făcând

conținutul video accesibil cursanților cu deficiențe de auz sau celor care preferă să citească în timp ce privesc.

3.4 Integrarea tehnologiilor imersive (VR/AR)

Integrarea tehnologiilor imersive, în special realitatea virtuală (VR) și realitatea augmentată (AR), în modulele de învățare CybARverse reprezintă o abordare transformatoare a educației în domeniul securității cibernetice pentru formatorii VET și cursanții acestora. Aceste tehnologii creează medii de învățare extrem de interactive și atractive, care permit cursanților să experimenteze direct scenarii complexe de securitate cibernetică. Prin utilizarea VR și AR, formatorii pot îmbunătăți aplicarea practică a conceptelor de securitate cibernetică, făcând ca activitatea de formare să aibă un impact mai puternic și să fie mai interesantă.

Unul dintre principalele beneficii ale tehnologiilor VR și AR este capacitatea acestora de a implica cursanții în scenarii realiste. De exemplu, un modul VR poate simula un mediu corporativ, în care cursanții trebuie să identifice și să răspundă la un atac de phishing sau la un incident ransomware. Prin participarea activă la aceste simulări, cursanții își pot aplica cunoștințele teoretice în situații practice, sporindu-și cunoștințele de rezolvare a problemelor și abilitățile decizionale. Această experiență imersivă permite cursanților să înțeleagă urgența și complexitatea provocărilor de securitate cibernetică, stimulând un sentiment de pregătire și încredere în competențele lor.

Aplicația VR este disponibilă pe site-ul web al proiectului și include următoarele opt module de formare: malware, exploatarea avansată a vulnerabilităților existente în Internetul Lucrurilor (IoT), rootkit și ransomware în cadrul nivelului Începător, injecții SQL și cross-site scripting (XSS) în cadrul nivelului Intermediar și atacuri Dos/DDos în cadrul nivelului Avansat.

Integrarea tehnologiilor imersive precum VR și AR în modulele de învățare CybARverse pune la dispoziția formatorilor VET o modalitate dinamică de a îmbunătăți educația în domeniul securității cibernetice. Punând la dispoziția cursanților activități practice și interactive care simulează provocări din lumea reală, formatorii pot stimula o înțelegere mai profundă, gândirea critică și încrederea în competențele lor în domeniul securității cibernetice. Resursele disponibile prin LMS permit formatorilor să integreze cu ușurință aceste tehnologii în lecțiile lor, asigurându-se că participanții sunt bine pregătiți să navigheze în cadrul complex al domeniului securității cibernetice. Mai multe informații sunt disponibile în capitolul următor.

4 Configurarea și implementarea tehnologiei VR/AR

4.1 Căști acceptate

Meta Quest 2 și Meta Quest 3 sunt căștile VR acceptate.

4.2 Crearea unui cont Meta

Pentru a utiliza o cască Meta Quest, este necesară crearea unui cont Meta (anterior Facebook). În funcție de cerințe, se poate crea un cont Facebook personal sau un cont generic (utilizat doar în scopuri profesionale/organizaționale).

4.3 Pași pentru crearea unui cont Facebook personal:

- **Accesați Facebook**: accesați site-ul Facebook sau descărcați aplicația Facebook.
- **Înregistrare**: faceți clic pe „Creați un cont nou”.
- **Introduceți datele personale**: furnizați numele, numărul de telefon mobil sau adresa de e-mail, parola, data nașterii și sexul.
- **Verificare**: Facebook va trimite un cod de verificare la adresa dvs. de e-mail sau pe telefon. Introduceți codul pentru a confirma.
- **Configurați profilul**: Adăugați o imagine de profil și o fotografie de copertă și completați-vă profilul cu informații suplimentare.
- **Începeți să vă conectați**: adăugați prieteni, alăturați-vă grupurilor și urmăriți pagini.

4.4 Configurarea aplicației Meta Quest pe telefon

Aplicația Meta Quest este esențială pentru gestionarea experienței VR. Iată cum să o configurați

- **Descărcați** și deschideți aplicația Meta Quest pe telefon.
- Conectați-vă folosind contul Meta (personal sau profesional).
- Asociați casca Meta Quest urmând indicațiile de pe ecran.
- Utilizați aplicația pentru a configura setările, a descărca conținut și a vă gestiona dispozitivul.

4.5 Cerințe

- **Dispozitiv mobil**: asigurați-vă că aveți un smartphone utilizabil pentru aplicația Meta Quest pe telefon și pentru procesul de configurare.
- **Computer**: un computer care poate fi utilizat pentru a interacționa cu casca și pentru a încărca APK-ul.
- **Căști Oculus Quest**: dispozitivul Oculus pe care doriți să instalați aplicația.
- **Cablu de date USB (USB-A la USB-C)**: acesta va conecta căștile Oculus la computer pentru a transfera APK-ul.

4.5.1 Software:

- **Aplicația Meta Quest**: pentru a gestiona casca Oculus, este necesar să instalați aplicația Meta Quest pe dispozitivul mobil. Această aplicație vă va ajuta la configurarea inițială și la gestionarea permisiunilor dezvoltatorului.
- **Descărcarea și configurarea aplicației Meta Quest**: **https://www.meta.com/quest/setup/**
- **SideQuest**: descărcați și instalați SideQuest pe computer. SideQuest vă permite să încărcați lateral fișiere APK (aplicații Android) pe dispozitivul Oculus Quest.
- **Ghid de configurare SideQuest**: **https://sidequestvr.com/setup-howto**
- **Fișier APK**: asigurați-vă că fișierul APK al aplicației pe care doriți să o încărcați este descărcat și dezarhivat pe computerul dvs.

4.5.2 Permisiuni:

- **Crearea unei organizații de dezvoltatori Meta**: Pentru a activa modul de dezvoltator pe cască, este necesar să vă înregistrați și să creați o organizație de dezvoltatori accesând Panoul de Dezvoltatori Meta. Asigurați-vă că organizația dvs. este verificată și confirmată.
- **Tabloul de Bord pentru Dezvoltatori Meta**: **https://developer.oculus.com/manage/organizations/**
- **Drepturi de administrare pentru casca Oculus**: pentru a gestiona permisiunile căștii Oculus, este necesar să dețineți calitatea de administrator al acesteia. Aflați mai multe despre acest lucru în ghidul Meta's Developer Mode.
- **Configurarea modului Meta Quest Developer**: **https://developer.oculus.com/documentation/quest/latest/concepts/mobile-device-setup/**

- **Administrator membru al organizației Meta Developer**: administratorul căștii Oculus trebuie să fie membru al organizației Meta Developer creată anterior. Asigurați-vă că adăugați administratorul ca membru în tabloul de bord al dezvoltatorului utilizând link-ul furnizat mai sus.
- **Codul PIN al căștii Oculus**: configurați codul PIN pentru casca Oculus urmând instrucțiunile de pe pagina de asistență Meta.
- **Configurarea codului PIN pentru casca Oculus**: https://support.meta.com/279555412449097/?locale=en_US
- **Codul de acces pentru dispozitivul mobil**: asigurați-vă că dispozitivul mobil are un cod de acces activ sau o configurare biometrică.

4.6. Configurarea căștii Meta Quest

Pentru a configura casca Meta Quest:

- **Încărcați** casca înainte de prima utilizare.
- **Reglați** cureaua pentru cap într-o poziție confortabilă.
- **Porniți** dispozitivul cu butonul de pornire.
- **Urmați instrucțiunile de configurare**: Puneți casca și urmați instrucțiunile de pe ecran.
- **Conectați-vă la rețeaua Wi-Fi**: Selectați rețeaua și introduceți parola când vi se solicită.
- **Configurați limita de protecție**: Definiți o zonă de joacă sigură pentru a preveni accidentele în timpul utilizării căștii.

4.7. Utilizarea urmăririi mâinilor și a gesturilor în Meta Quest

Meta Quest permite urmărirea mâinilor, permițându-vă să interacționați cu mediul VR fără controlere. Pentru a utiliza această caracteristică:

- **Activați Hand Tracking în setările căștii**.
- **Învățați și exersați gesturile**: începeți cu gesturi de bază, cum ar fi ciupitul, apucatul și indicarea pentru a interacționa cu aplicațiile VR.
- **Testați în aplicații**: utilizați aplicații concepute pentru urmărirea mâinii pentru a deveni confortabil cu interacțiunea fără controler.
- Ghid pentru gesturile mâinii.

5. Testarea pilot

Cursul CybARverse a fost supus unei testări pilot în patru țări - Lituania, Cipru, Malta și România - la care au participat educatori IT și non-IT, inclusiv profesori, tutori și lectori. Acești educatori au oferit un feedback valoros prin intermediul unui proces extins de evaluare care a analizat eficacitatea cursului.

Au fost realizate trei sondaje separate: unul pentru participanții la curs, altul pentru experții care au analizat lecțiile individuale și un al treilea pentru experții care au evaluat diverse elemente ale cursului, cum ar fi navigarea, claritatea, designul, implicarea și utilizarea tehnologiei imersive. Fiecare sondaj a inclus o casetă de comentarii și sugestii pentru a colecta informații de tip calitativ, îmbunătățind și mai mult feedback-ul.

La evaluare au contribuit în total 70 de participanți, care au oferit opinii diverse cu privire la punctele forte și domeniile de îmbunătățire ale cursului. Experții au furnizat evaluări detaliate pentru fiecare dintre cele 17 lecții privind scenariul atacurilor cibernetice, rezultând 71 de răspunsuri. Acest feedback este esențial pentru perfecționarea cursului, pentru a răspunde mai bine nevoilor viitorilor cursanți.

În plus, 14 experți din țările participante și-au oferit punctele de vedere prin intermediul unui alt sondaj care s-a axat pe diverse aspecte ale cursului. Feedback-ul lor detaliat, inclusiv informațiile de tip calitativ din secțiunile de comentarii, vor contribui la dezvoltarea continuă a cursului CybARverse, asigurându-se că acesta devine mai eficient și mai receptiv la nevoile viitorilor participanți.

5.1 Constatări rezultate din testarea pilot inițială

a. **Structura și inteligibilitatea cursului**

Structura cursului online de securitate cibernetică a primit un feedback pozitiv, 79% dintre experți evaluând inteligibilitatea acestuia ca fiind excelentă. Acest lucru indică faptul că materialul cursului este prezentat într-un mod clar și accesibil, simplificând în mod eficient conceptele complexe de securitate cibernetică pentru cursanți. Punctajul ridicat reflectă caracterul solid al conceptului de formare, care asigură faptul că explicațiile sunt concise și susținute de materiale de înaltă calitate, contribuind la o activitate de învățare generală excelentă.

a. **Gramatică și sintaxă**

Gramatica și sintaxa cursului au fost foarte apreciate, 80% dintre participanți calificându-le drept excelente. Acest feedback pozitiv subliniază importanța unui limbaj clar și profesional în menținerea integrității și eficienței conținutului educațional. Gramatica și sintaxa adecvate nu numai că previn distragerea atenției, ci și sporesc concentrarea cursanților asupra materialului, ajutând astfel la o mai bună înțelegere.

b. **Relevanța conținutului**

Relevanța conținutului cursului pentru provocările actuale în materie de securitate cibernetică a constituit un alt punct forte, 70% dintre respondenți apreciind-o ca fiind excelentă, iar 27% au apreciat-o ca fiind foarte bună. Acest lucru indică faptul că materialul de curs este bine adaptat la cerințele lumii reale din domeniul securității cibernetice, punând la dispoziția cursanților cunoștințe pertinente și aplicabile.

c. Adaptabilitatea la stilurile de învățare și la nivelurile de cunoștințe

Reacțiile privind adaptabilitatea elementelor cursului la diverse stiluri de învățare și niveluri de cunoștințe au fost mixte. În timp ce o parte semnificativă a experților a apreciat abordarea incluzivă și variată a cursului, unii au considerat că acesta nu a răspuns în mod adecvat nevoilor lor specifice. Acest lucru indică o nevoie de perfecționare suplimentară pentru a răspunde mai bine întregului spectru de cursanți.

e. Eficiența chestionarelor online (quiz-uri)

Chestionarele online au beneficiat de reacții mixte, majoritatea experților recunoscând eficiența acestora, evidențiind, însă, și domenii care pot fi îmbunătățite. Deși majoritatea participanților au fost mulțumiți de durata alocată quiz-urilor, unii au considerat că timpul alocat a fost prea lung, iar conținutul quiz-urilor ar putea fi mai cuprinzător și mai variat pentru a evalua mai bine diferitele niveluri de cunoștințe ale participanților.

f. Nivelul general de dificultate

Nivelul general de dificultate al cursului a fost evaluat ca fiind excelent de 9% dintre experți, ceea ce sugerează că, deși cursul a fost potrivit pentru unii, este posibil să nu fi fost suficient de dificil pentru alții. Această percepție mixtă indică necesitatea de a echilibra mai eficient nivelul de dificultate.

g. Îmbunătățirea activității de interacțiune cu tehnologia VR/AR

Feedback-ul a evidențiat nevoia de mai multă interacțiune și implicare în cadrul elementelor VR/AR ale cursului. Participanții au subliniat, de asemenea, dificultățile întâmpinate în timpul instalării aplicației pe dispozitivele Oculus, subliniind importanța unor instrucțiuni clare, pas cu pas.

Rezultatele testării pilot evidențiază punctele forte ale cursului, în special structura, relevanța conținutului și claritatea acestuia. Cu toate acestea, abordarea feedback-ului legat de adaptabilitate, eficiența chestionarelor și interacțiunile VR/AR vor fi esențiale în perfecționarea ulterioară a cursului. Prin punerea în aplicare a acestor bune practici, cursul va fi mai bine poziționat pentru a răspunde nevoilor diverse ale cursanților, îmbunătățind procesul de învățare și succesul în domeniul securității cibernetice.

5.2 Îmbunătățiri/perfecționări puse în aplicare după testarea pilot

5.2.1 Îmbunătățiri ale sistemului de gestionare a învățării (LMS)

Pentru a optimiza activitatea utilizatorului și desfășurarea cursurilor, au fost aduse câteva îmbunătățiri cheie LMS-ului:

- **Conținut accesibil și ușor de utilizat:** conținutul cursului de pe site-ul web este acum extrem de accesibil și ușor de utilizat, oferind instrumente de accesibilitate complete, cum ar fi suport pentru dislexie, mărirea textului, contrast întunecat, fonturi lizibile, titluri și link-uri evidențiate și multe altele, permițând utilizatorilor să personalizeze interfața în funcție de nevoile proprii. În plus, o aplicație bazată pe inteligență artificială optimizează în permanență accesibilitatea, ajustând HTML-ul site-ului pentru cititoarele de ecran și funcțiile tastaturii pentru a sprijini utilizatorii cu deficiențe vizuale și motorii.
- **Afișare mai bună a meniului mobil:** meniul mobil a fost reproiectat pentru a asigura o navigare fără întreruperi pe toate dispozitivele, îmbunătățind accesibilitatea pentru utilizatorii care preferă să învețe pe platforme mobile.
- **Studii de caz asociate cu fișiere PDF (prin intermediul link-urilor)**: pentru a asigura un acces rapid la resurse, studiile de caz sunt acum asociate cu fișiere PDF descărcabile, mai degrabă decât cu site-uri web externe, asigurând un mediu de învățare mai coerent și reducând riscul de link-uri nefuncționale.
- **Verificarea înregistrării**: au fost implementate procese de verificare îmbunătățite pentru a simplifica înregistrarea utilizatorilor și pentru a garanta că doar participanții autorizați au acces la curs.

- **Descrieri personalizate ale nivelurilor**: fiecare nivel de curs are acum descrieri distincte, asigurând cursanților o înțelegere mai clară a conținutului și obiectivelor în fiecare etapă a parcurgerii lor.
- **Modificări ale profilului utilizatorului**: profilurile utilizatorilor au fost rafinate prin eliminarea funcțiilor inutile, cum ar fi listele de dorințe și comenzile, pentru a simplifica interfața și a se concentra pe informațiile esențiale legate de curs.

5.2.2 Optimizarea chestionarelor (quiz-urilor) și a conținutului

Pentru a evalua mai bine înțelegerea și implicarea cursanților, au fost efectuate mai multe modificări ale chestionarelor/evaluărilor:

- **Modificarea duratei de timp alocate**: durata de timp alocată chestionarelor a fost standardizată la 20 de minute, ceea ce a oferit timp suficient cursanților pentru a se implica în mod atent în rezolvarea întrebărilor, menținând în același timp caracterul de urgență.
- **Tipuri variate de întrebări**: întrebările chestionarului au fost diversificate pentru a include o gamă largă de formate, cum ar fi răspunsurile cu alegere multiplă și răspunsurile de tip „adevărat/fals”, pentru a evalua cu mai multă exactitate diferite aspecte ale cunoștințelor și înțelegerii cursanților.
- **Punctajul de promovare menținut la 60%**: pragul de reușită pentru chestionare a fost menținut la 60%, echilibrând nevoia de rigoare cu obiectivul de a asigura succesul și încrederea cursanților.

5.2.3 Îmbunătățiri ale aplicației VR/AR

Pentru a crea un mediu de învățare mai imersiv și mai interactiv, au fost efectuate mai multe actualizări ale aplicației VR/AR:

- **Simbol interactiv (figura feminină) cu caracteristici îmbunătățit**e: în simbolul interactiv reprezentat de figura feminină au fost integrate animații suplimentare, făcând activitatea de învățare mai dinamică și mai atractivă.
- **Adăugarea textului voiceover**: A fost introdusă o narațiune voiceover pentru a completa elementele vizuale, pentru a fi de folos cursanților care învață folosind auzul și pentru a îmbunătăți înțelegerea generală.
- **Indicatori de finalizare a modulului**: au fost adăugați indicatori vizuali pentru a urmări finalizarea modulelor, asigurând, astfel, cursanților un sentiment clar de progres și reușită.

- **Actualizări ale fundalului scenariilor**: fundalurile din scenariile selectate au fost actualizate pentru a furniza un mediu mai captivant și mai precis din punct de vedere contextual pentru cursanți.
- **Personalizarea muzicii**: au fost adăugate numeroase opțiuni pentru muzică de fundal, împreună cu posibilitatea de dezactivare a sunetului, permițând, astfel, cursanților să își personalizeze mediul de învățare.
- **Videoclip introductiv**: în aplicația VR a fost adăugat un tutorial menit să îndrume utilizatorii cu privire la caracteristicile aplicației și să pregătească terenul pentru procesul de învățare.
- **Logo-uri și clauze de exonerare de răspundere**: în secțiunea „Despre noi" au fost adăugate logo-uri și clauze de exonerare de răspundere, sporind transparența și oferind informații esențiale despre curs și creatorii acestuia.
- **Comenzile aplicației au fost revizuite și modificate**: comenzile pentru utilizator au fost revizuite în detaliu și modificate pentru a asigura o interacțiune intuitivă cu mediul VR/AR, îmbunătățind gradul general de utilizare.
- **Scenarii WebRV**: scenariile VR bazate pe web au fost reprezentate de exploatarea vulnerabilităților de tip „zero-day", atacuri de tip „man-in-the-middle (intermediar inserat)" și cryptojacking, făcând ca procesul imersiv să fie accesibil pe mai multe platforme.

Aceste îmbunătățiri au fost puse în aplicare în mod strategic, pentru a se asigura că acest curs online de securitate cibernetică nu este doar atractiv și interactiv, ci și eficient în procesul de învățare a cunoștințelor practice necesare pentru a excela în domeniu. Prin folosirea tehnologiilor imersive și perfecționarea atât a LMS, cât și a livrării de conținut, cursul urmărește să creeze o activitate de învățare cuprinzătoare și cu impact. În plus, aceste ajustări nu numai că vor îmbunătăți satisfacția utilizatorilor, dar vor asigura, de asemenea, că acest curs răspunde în mod eficient nevoilor de formare ale tuturor participanților.

5.3 Constatări

După finalizarea instruirii pilot a cursului de securitate cibernetică CybARverse, care utilizează tehnologia imersivă, au fost obținute mai multe informații-cheie care evidențiază eficiența și implicarea participanților în această abordare inovatoare. Mai jos sunt prezentate principalele constatări:

1. Angajament și retenție îmbunătățite

- **Niveluri ridicate de implicare**: participanții au fost mult mai implicați în comparație cu metodele tradiționale de formare. Tehnologia imersivă, cum ar fi realitatea virtuală (VR) sau realitatea augmentată (AR), împreună cu videoclipurile, au oferit o activitate practică care a făcut conceptele complexe de securitate cibernetică mai accesibile și mai ușor de înțeles.

- **Retenție îmbunătățită**: natura interactivă a cursului a condus la o mai bună reținere a informațiilor. Participanții au putut aplica în mod activ ceea ce au învățat în simulări în timp real, ceea ce le-a consolidat înțelegerea și memorarea principiilor cheie în materie de securitate cibernetică.

2. **Feedback pozitiv privind interacțiunea**

- **Interacțiunea a fost lăudată:** elementele interactive ale cursului au fost deosebit de bine primite. Participanții au apreciat posibilitatea de a interacționa cu medii virtuale care imitau îndeaproape scenariile din lumea reală. Această activitate interactivă nu numai că a făcut cursul mai atractiv, dar a permis și o activitate practică, experimentală, pe care participanții au considerat-o extrem de valoroasă.

- **Aplicații din lumea reală:** participanții au raportat că videoclipurile și studiile de caz au contribuit la reducerea decalajului dintre cunoștințele teoretice și aplicațiile practice. Ei s-au simțit mai pregătiți să gestioneze amenințările reale la adresa securității cibernetice după ce s-au implicat în simulări interactive.

3. **Creșterea încrederii în propriile abilități**

- **Creșterea încrederii:** tehnologia imersivă a ajutat participanții să dobândească încredere în competențele lor de securitate cibernetică. Posibilitatea de a exersa într-un mediu controlat și lipsit de riscuri le-a permis să facă greșeli, să învețe din ele și să își îmbunătățească competențele fără teama de consecințele din lumea reală.

4. **Experiența utilizatorului și accesibilitate**

- **Ușurința în utilizare:** deși majoritatea participanților au considerat tehnologia imersivă intuitivă și ușor de utilizat, au existat unele curbe de învățare inițiale pentru cei mai puțin familiarizați cu tehnologiile VR sau AR. Cu toate acestea, după o scurtă perioadă de aclimatizare, majoritatea participanților au raportat o activitate de învățare ușoară și plăcută.

- **Acces și echipamente:** unii participanți au menționat că accesul la echipamentul necesar (de exemplu, căștile VR) a reprezentat o posibilă barieră. Cu toate acestea, atunci când a fost furnizat, echipamentul a îmbunătățit semnificativ procesul de învățare.

- **Caracteristici privind accesibilitatea**: bariera de accesibilitate a fost eliminată cu ajutorul unor caracteristici îmbunătățite care susțin contrastul întunecat, citirea cu ajutorul unui ghid, fonturi lizibile

și spațiere între rânduri, precum și titluri și link-uri evidențiate, asigurând o activitate incluzivă pentru toți utilizatorii, inclusiv pentru persoanele cu dislexie.

5. Lucruri care pot fi îmbunătățite

- **Probleme tehnice:** câțiva participanți au întâmpinat probleme tehnice minore, cum ar fi defecțiuni sau dificultăți în navigarea în mediul virtual. Aceste probleme, deși nu sunt generalizate, evidențiază necesitatea unei asistențe tehnice susținute și a unor teste aprofundate înainte de o implementare pe scară mai largă.

- **Curbe de învățare variate:** deși majoritatea dintre participanți s-au adaptat bine la tehnologia imersivă, unii au avut nevoie de sprijin suplimentar. Adaptarea formării pentru a se potrivi diferitelor niveluri de competență tehnologică ar putea spori eficiența generală.

6. Satisfacție generală

- **Niveluri ridicate de satisfacție:** în general, participanții au fost foarte mulțumiți de formarea imersivă în domeniul securității cibernetice, precum și de videoclipuri. Aceștia au apreciat abordarea inovatoare și mediul captivant și interactiv.

- **Recomandare pentru o utilizare pe scară mai largă:** numeroși participanți și-au exprimat dorința de a le fi prezentate mai multe programe de formare care să adopte tehnologia imersivă, menționând calitatea sporită a procesului de învățare și potențialul acestor metode de a revoluționa formarea în domeniul securității cibernetice și nu numai.

6. Concluzie

6.1 Rezumatul celor mai bune practici pentru predarea cursurilor de securitate cibernetică

Desfășurarea eficientă a cursului de securitate cibernetică în cadrul platformei CybARverse, care se bazează pe tehnologia imersivă, depinde de câteva bune practici-cheie:

1. **Medii de învățare interactive**: utilizarea simulărilor imersive VR/AR pentru a crea scenarii realiste, practice, în care cursanții își pot exersa competențele de securitate cibernetică într-un mediu controlat și captivant.

2. **Furnizarea unor informații adaptabile**: conținutul cursului poate fi adaptat pentru a se potrivi diferitelor niveluri de cunoștințe ale cursanților. Furnizarea de materiale de bază pentru începători, a unor provocări de nivel intermediar și avansat pentru participanții cu experiență, asigurându-se că toți utilizatorii beneficiază de acest curs de formare.

3. **Evaluare**: evaluările/chestionarele de la sfârșitul fiecărui nivel incluse în curs urmăresc progresul și consolidează rezultatele învățării.

4. **Tehnologie accesibilă**: se va asigura că tehnologia imersivă necesară este ușor accesibilă și ușor de utilizat. La începutul cursului, se oferă sprijin cursanților care pot fi mai puțin familiarizați cu instrumentele VR/AR, pentru a reduce la minim obstacolele în calea participării.

5. **Considerații privind securitatea și confidențialitatea:** se va asigura că platforma tehnologică imersivă respectă cele mai înalte standarde de securitate, pentru a proteja datele utilizatorilor și a menține integritatea mediului de instruire.

6.2 Scopul și impactul ghidului

Scopul acestui ghid este de a oferi educatorilor, formatorilor și celor care elaborează materiale didactice un cadru cuprinzător pentru predarea de cursuri de securitate cibernetică eficiente și atractive utilizând platforma CybARverse. Prin respectarea celor mai bune practici prezentate în acest ghid, instructorii pot crea activități de învățare imersive, care nu numai că sporesc înțelegerea conceptelor complexe de securitate cibernetică, ci și îmbunătățesc semnificativ competențele practice ale cursanților.

Impactul acestui ghid se extinde dincolo de sesiunile individuale de formare. Prin adoptarea acestor practici, organizațiile se pot asigura că echipele lor de securitate cibernetică sunt mai bine pregătite pentru a face față amenințărilor din lumea reală, ceea ce conduce la un mediu digital mai sigur. În plus, ghidul

contribuie la standardizarea predării de cursuri de formare imersivă bazată pe tehnologie, promovând consecvența și calitatea în diferite medii de învățare.

6.3 Considerații finale și pașii de urmat în vederea perfecționării continue

Pe măsură ce evoluăm într-un peisaj tehnologic în continuă schimbare, este esențial să considerăm acest ghid un document dinamic. Domeniul securității cibernetice este într-o continuă evoluție, cu noi amenințări și tehnologii care apar regulat. Prin urmare, îmbunătățirea continuă și adaptarea sunt esențiale.

Pașii următori:

1. **Actualizări periodice**: Revizuirea și actualizarea periodică a ghidului pentru a reflecta cele mai recente evoluții în domeniul securității cibernetice și al tehnologiilor de învățare imersivă. Includerea feedback-ului de la instructori și cursanți pentru a perfecționa cele mai bune practici.

2. **Colaborarea cu comunitatea**: Promovarea colaborării între educatori, profesioniști din domeniul securității cibernetice și tehnicieni pentru a împărtăși idei, experiențe și inovații. Crearea unei comunități în jurul formării imersive în domeniul securității cibernetice poate duce la dezvoltarea de noi metode și instrumente.

3. **Scalabilitate și personalizare**: Explorarea modalităților de extindere a abordării de formare imersivă în diferite organizații și de personalizare a acesteia în funcție de nevoile specifice ale sectorului de activitate. Astfel, platforma CybARverse va deveni mai flexibilă și va putea fi aplicată pe scară largă.

În concluzie, adoptând aceste bune practici și angajându-ne în direcția îmbunătățirii continue, ne putem asigura că formarea în domeniul securității cibernetice din cadrul CybARverse nu numai că rămâne eficientă, dar este și lider în materie de experiențe de învățare inovatoare și imersive. Această abordare va oferi profesioniștilor din domeniul securității cibernetice cunoștințele și competențele de care au nevoie pentru a proteja lumea noastră digitală într-un peisaj al amenințărilor din ce în ce mai complex.