CYBER MSME IO4:

LINEE GUIDA

PER L'IMPLEMENTAZIONE DEI RISULTATI DEL PROGETTO

Co-funded by the Erasmus+ Programme of the European Union

Con il sostegno di Erasmus+ Programma dell'Unione europea.

Questo documento e il suo contenuto riflettono solo le opinioni degli autori e la Commissione non può essere ritenuta responsabile per qualsiasi uso che possa essere fatto delle informazioni in esso contenute.

INDICE

Co-funded by the Erasmus+ Programme of the European Union

Con il sostegno di Erasmus+ Programma dell'Unione europea.

Questo documento e il suo contenuto riflettono solo le opinioni degli autori e la Commissione non può essere ritenuta responsabile per qualsiasi uso che possa essere fatto delle informazioni in esso contenute.

INTRODUZIONE GENERALE 3

RISULTATI DELL'APPRENDIMENTO.....5

IL PROFILO PROFESSIONALE DI MSME CYBER SECURITY EXPERT..... 6

PREPARAZIONE DEL PILOTING PROGRAMME..... 8

LA PIATTAFORMA CYBER OER COME ALLEATO DIGITALE..... 10

NOTE INSEGNANTI/MENTORI 12

ALCUNE RACCOMANDAZIONI..... 12

ALCUNE NOTE FINALI..... 13

Co-funded by the Erasmus+ Programme of the European Union

Con il sostegno di Erasmus+ Programma dell'Unione europea.

Questo documento e il suo contenuto riflettono solo le opinioni degli autori e la Commissione non può essere ritenuta responsabile per qualsiasi uso che possa essere fatto delle informazioni in esso contenute.

1. INTRODUZIONE GENERALE

Cyber MSME (Cybersecurity for Micro, Small & Medium Enterprises) è un progetto internazionale co-finanziato dal programma Erasmus+ dell'Unione Europea e realizzato da un consorzio di sei partner provenienti da cinque paesi diversi, che si sono riuniti per rispondere a una serie di sfide che le micro, piccole e medie imprese devono affrontare nel loro percorso professionale. Il progetto affronta le esigenze organizzative, come ad esempio cercare di colmare le lacune di competenze identificate a livello UE e nazionale per le micro e piccole imprese in materia di sicurezza informatica, contribuendo al contempo alla competitività delle micro e piccole imprese dell'UE fornendo loro programmi di formazione più pertinenti, aggiornati e di alta qualità.

Nel corso della durata del progetto, i sei partner hanno lavorato insieme per sviluppare il Toolkit Cyber-MSME, ovvero una serie di materiali di formazione che affrontano vari argomenti progettati per professionisti della sicurezza informatica entry-level, mid-level e avanzati che vogliono apprendere le competenze e le conoscenze di cui hanno bisogno per svolgere i loro compiti e per poter rispondere alle sfide nel campo della sicurezza informatica. I sei partner hanno sviluppato cinque toolkit e undici corsi, preparati per porre rimedio alle lacune che emergono dalla letteratura e si incentrano su argomenti come il miglioramento della sicurezza della rete attraverso alcune operazioni di base, il miglioramento del piano di gestione della sicurezza informatica, il riconoscimento di URL credibili, suggerimenti essenziali per la sicurezza del router e l'elenco dell'inventario. Ciascuno dei toolkit è arricchito da una serie di corsi che affrontano argomenti simili.

I toolkit includono linee guida, casi studio, liste di controllo e un ricco set di risorse, che forniscono strumenti di apprendimento gratuiti e pronti all'uso per tutte le organizzazioni e i professionisti interessati a comprendere, anticipare, gestire e contenere

Co-funded by the Erasmus+ Programme of the European Union

Con il sostegno di Erasmus+ Programma dell'Unione europea.
Questo documento e il suo contenuto riflettono solo le opinioni degli autori e la Commissione non può essere ritenuta responsabile per qualsiasi uso che possa essere fatto delle informazioni in esso contenute.

le minacce alla sicurezza informatica, migliorando al contempo la capacità operativa di implementare la sicurezza informatica nelle micro, piccole e medie imprese. Questo pubblico a cui sono destinate le risorse è formato dall'ecosistema di sostegno all'imprenditorialità e dagli ecosistemi digitali legati alle TIC. Alcune delle parti interessate sono agenzie di promozione dell'imprenditorialità, attori pubblici, associazioni imprenditoriali, istituti di istruzione, consulenti IT, università, centri di ricerca, ecc.

Sono stati concentrati notevoli sforzi nello sviluppo del toolkit Cyber-MSME affinché possa fungere da strumento patrimoniale per tutte le entità economiche attuali e future che non vogliono sacrificare il vantaggio strategico della sicurezza digitale. Inoltre, per assicurarsi che le risorse di apprendimento soddisfino effettivamente le esigenze del pubblico destinatario, e siano sviluppate in linea con le loro esigenze di apprendimento, è stata condotta una convalida reale dei materiali di formazione, con tutti i partner che distribuiscono la formazione pilota ad almeno 150 studenti che rappresentano i gruppi target. Ciò ha fornito al consorzio un feedback significativo su vari aspetti della formazione, ad esempio sulla fruizione, sull'adeguatezza alle loro esigenze e preferenze, sui mezzi di implementazione, sul contenuto e sulle risposte che si sono rivelate significative ai fini della convalida dei materiali di formazione.

Le esperienze raccolte costituiscono i pilastri di questo documento, le linee guida promuovono la scalabilità del progetto, la sua trasferibilità e la replicabilità dei suoi risultati in altri domini di pratica simili alla sicurezza informatica. Questo rapporto prenderà in considerazione tutte le raccomandazioni chiave, i takeaway e le lezioni apprese estrapolate dall'implementazione del progetto su come sfruttare appieno i materiali di formazione e applicare efficacemente le conoscenze in seguito.

Questo rapporto mira a fornire ai potenziali utenti alcune informazioni pratiche basate sull'esperienza raccolte dal pilotaggio e dall'implementazione dei toolkit sviluppati. Copre una serie di raccomandazioni su come comunicare con i partecipanti, come mantenere la partecipazione attiva durante l'erogazione dei programmi di formazione, come fare affidamento sulla piattaforma cyber OER in chiave di risorsa preziosa durante

Co-funded by the Erasmus+ Programme of the European Union

Con il sostegno di Erasmus+ Programma dell'Unione europea.
Questo documento e il suo contenuto riflettono solo le opinioni degli autori e la Commissione non può essere ritenuta responsabile per qualsiasi uso che possa essere fatto delle informazioni in esso contenute.

l'implementazione dei programmi di apprendimento, nonché alcune intuizioni dei formatori in termini di approcci più adatti all'erogazione della formazione e alla collaborazione con gli studenti. Pur fornendo il punto di partenza, le nostre intuizioni e opinioni basate sull'esperienza sull'implementazione del toolkit Cyber-MSME, queste linee guida non fungono da regole precise per l'implementazione dei corsi di formazione Cyber-MSME. Al contrario, i potenziali utenti sono fortemente incoraggiati a sperimentare e ad utilizzare il proprio input nella fornitura dei corsi di formazione, crescendo ulteriormente e contribuendo allo sviluppo di preziose conoscenze e competenze nel campo della sicurezza informatica, arricchendo il nostro lavoro e gli sforzi in questo campo.

2. RISULTATI DI APPRENDIMENTO

I toolkit e i corsi di formazione Cyber sono basati sui risultati dell'apprendimento e allineati con EQF 3-5, come segue:

- Conoscenza di fatti, principi, processi e concetti generali nel campo della sicurezza informatica, con una serie di competenze cognitive e pratiche necessarie per svolgere compiti e risolvere problemi selezionando e applicando metodi, strumenti, materiali e informazioni di base;
- Conoscenze fattuali e teoriche in ampi contesti nel campo della sicurezza informatica, con una gamma di competenze cognitive e pratiche necessarie per generare soluzioni a problemi specifici nel campo della sicurezza informatica;
- Conoscenze complete, specializzate, fattuali e teoriche nel campo della sicurezza informatica e consapevolezza dei confini di tale conoscenza, con una gamma completa di abilità cognitive e pratiche necessarie per sviluppare soluzioni creative a problemi astratti.

Co-funded by the Erasmus+ Programme of the European Union

Con il sostegno di Erasmus+ Programma dell'Unione europea.
Questo documento e il suo contenuto riflettono solo le opinioni degli autori e la Commissione non può essere ritenuta responsabile per qualsiasi uso che possa essere fatto delle informazioni in esso contenute.

Tuttavia, i toolkit e la formazione Cyber-MSME sono incentrati su una serie di risultati di apprendimento specifici per ciascuno dei moduli, e ne menzioneremo solo alcuni in questa linea guida per avere una chiara panoramica degli obiettivi di questi materiali di formazione. Al termine dei moduli, i discenti saranno in grado di:

- Identificare le crisi informatiche e i potenziali rischi nella tua organizzazione;
- Evitare errori informatici comuni, migliorando al contempo il piano di gestione delle crisi informatiche;
- Definire e riconoscere il design centrato sull'uomo;
- Definire e creare un programma di bug bounty;
- Riconoscere e distinguere le tecniche di ingegneria sociale più comunemente utilizzate;
- Comprendere la scansione delle vulnerabilità, l'hacking del sistema e i programmi dannosi;
- Acquisire familiarità con il framework EntreComp e su come può essere rilevante per la sicurezza informatica e la competenza IT;
- Familiarizzare con il DigComp Framework - il quadro ufficiale dell'UE per l'istruzione e la formazione delle competenze digitali;
- Sapere cosa fare prima, durante e dopo un attacco informatico;
- Utilizzare gli strumenti più pertinenti per identificare e reagire agli attacchi informatici.

Tutti questi risultati di apprendimento sono discussi all'interno dei materiali di formazione, ognuno dei quali analizza un argomento specifico, come il panorama europeo per la sicurezza informatica, l'EntreComp per la preparazione al rischio informatico, l'ingegneria sociale, gli strumenti ICT per prevenire e riconoscere il rischio informatico in un mondo digitale, la gestione delle crisi, ecc. Come accennato in precedenza, tutti questi moduli, con i loro risultati di apprendimento specifici, sono accessibili in qualsiasi momento e gratuitamente sulla piattaforma OER.

Co-funded by the Erasmus+ Programme of the European Union

Con il sostegno di Erasmus+ Programma dell'Unione europea.
Questo documento e il suo contenuto riflettono solo le opinioni degli autori e la Commissione non può essere ritenuta responsabile per qualsiasi uso che possa essere fatto delle informazioni in esso contenute.

3. IL PROFILO PROFESSIONALE DI MSME CYBER SECURITY EXPERT

Prima di dare una panoramica della preparazione del programma pilota, definiremo il profilo professionale dell'esperto di Cyber Security MSME e il percorso di carriera allineato, che è essenziale per sapere come condurre ulteriormente l'implementazione della formazione in un'organizzazione per ottenere tale status.

L'esperto di sicurezza informatica dovrebbe padroneggiare una serie di aree di conoscenza, come ad esempio:

- Come soddisfare i requisiti delle norme di sicurezza nell'Unione europea;
- Minacce informatiche e punti deboli nel piano di gestione della sicurezza;
- Strumenti utili per organizzare un ambiente di lavoro sicuro;
- Terminologia specialistica necessaria per comprendere un ambiente di sicurezza informatica;
- Come reagire e recuperare dopo gli attacchi;
- Come raggiungere il prossimo livello di conoscenza della sicurezza informatica.

Inoltre, oltre a padroneggiare determinate conoscenze, un responsabile della sicurezza informatica dovrebbe essere in grado di fare quanto segue:

- Creare e implementare procedure di sicurezza;
- Lavorare in un ambiente Internet sicuro;
- Utilizzare strumenti e sistemi per evitare minacce informatiche;
- Creare condizioni di lavoro sicure a basso costo;
- Implementare il piano di gestione delle crisi e di disaster recovery;
- Sviluppare un'azienda e le competenze dei suoi dipendenti condividendo le sue conoscenze.

Co-funded by the Erasmus+ Programme of the European Union

Con il sostegno di Erasmus+ Programma dell'Unione europea.
Questo documento e il suo contenuto riflettono solo le opinioni degli autori e la Commissione non può essere ritenuta responsabile per qualsiasi uso che possa essere fatto delle informazioni in esso contenute.

Indubbiamente, tutte queste abilità e conoscenze non vengono raggiunte istantaneamente, ma richiedono determinati livelli di competenza, a cui i toolkit Cyber-MSME forniscono materiali di apprendimento pertinenti. Il primo livello, ovvero l'esperto di cybersecurity entry level, è rappresentato dagli analisti del crimine informatico, dai revisori IT e dagli incident responder, professionisti del settore che dovrebbero seguire corsi come "il quadro europeo delle competenze digitali: DigComp 2.1" e "il panorama europeo per la sicurezza informatica: politiche, strategie e risorse di supporto". Entrambi questi corsi forniscono una panoramica sul contesto istituzionale di rilevanza e sulla rete di supporto, oltre a stabilire un modello di riferimento comune per ciò che la Commissione europea prevede come le competenze e le abilità chiave nel campo dell'alfabetizzazione informatica e della competenza digitale, conoscenze essenziali per qualsiasi specialista di sicurezza informatica entry level che desideri raggiungere le basi nel campo della sicurezza informatica.

Il livello intermedio dell'esperto di sicurezza informatica è rappresentato da analisti di sicurezza informatica, consulenti di sicurezza informatica e tester di penetrazione, che già padroneggiano i fondamenti della sicurezza informatica e vogliono comprendere meglio la sicurezza per tenere lontane le minacce informatiche dall'organizzazione per cui lavorano, oltre a essere in grado di utilizzare gli strumenti ICT per prevenire i rischi informatici nel mondo digitale. Per questi obiettivi, il progetto Cyber-MSME ha sviluppato due toolkit e tre corsi raccomandati che possono essere utilizzati in ciascuna organizzazione.

L'esperto avanzato di sicurezza informatica è rappresentato dai responsabili della sicurezza informatica e dagli architetti della sicurezza informatica, con una vasta esperienza e conoscenza della sicurezza e dei sistemi informatici, nonché della sicurezza della rete e della crittografia, che possono migliorare le loro conoscenze con i toolkit e i corsi offerti dal progetto Cyber-MSME, come "Human-centered design vs. Priorità aziendali - linee guida" e "Gestione delle crisi - mi hanno hackerato, e poi?".

Co-funded by the Erasmus+ Programme of the European Union

Con il sostegno di Erasmus+ Programma dell'Unione europea.
Questo documento e il suo contenuto riflettono solo le opinioni degli autori e la Commissione non può essere ritenuta responsabile per qualsiasi uso che possa essere fatto delle informazioni in esso contenute.

Tutte queste risorse di apprendimento possono essere utilizzate sia in un'organizzazione che per individui che cercano di sviluppare nuove competenze e conoscenze in un campo che è sempre più presente nella società di oggi, come la sicurezza informatica. Ad esempio, qualsiasi persona attiva nella ricerca di un lavoro dovrebbe interessarsi a tali risorse di apprendimento, in quanto forniscono informazioni e abilità pratiche che possono rivelarsi una risorsa nel loro percorso professionale.

Inoltre, tutti questi corsi di formazione dovrebbero essere adattati al pubblico di destinazione, con particolare attenzione alle esigenze dei tirocinanti e al loro campo di competenza. Vi presenteremo ulteriormente il nostro programma pilota e il modo in cui abbiamo implementato questi corsi di formazione con il pubblico destinatario.

4. PREPARAZIONE DEL PROGRAMMA PILOTA

La preparazione del programma pilota può essere suddivisa in due livelli, la preparazione a livello di progetto e a livello di organizzazione. A livello di progetto, CTS Customized Training Solutions, uno dei sei partner, ha preparato un documento che specifica il programma, i compiti e i mezzi per implementare la versione pilota della formazione, che includeva anche suggerimenti su come organizzare le attività di apprendimento e quali strumenti utilizzare per raccogliere feedback dagli utenti. Questo si è rivelato un passo prezioso nella preparazione del programma pilota, poiché tutti i partner hanno avuto accesso a una struttura chiara e a una guida operativa nell'ulteriore preparazione del programma pilota a livello di organizzazione.

A livello organizzativo, tutti i partner hanno definito il proprio programma: il formato e durata delle sessioni in cui avrebbero pilotato la formazione, seguita da una sessione di raccolta di feedback dai partecipanti per valutare le loro impressioni, commenti e suggerimenti su come migliorare la formazione. Al termine della fase di convalida, tutti i

Co-funded by the Erasmus+ Programme of the European Union

Con il sostegno di Erasmus+ Programma dell'Unione europea.
Questo documento e il suo contenuto riflettono solo le opinioni degli autori e la Commissione non può essere ritenuta responsabile per qualsiasi uso che possa essere fatto delle informazioni in esso contenute.

partner hanno fornito a CTS Customized Training Solutions questi moduli di feedback per consentire lo sviluppo di linee guida sulla continua accettazione della formazione.

A livello organizzativo, la preparazione del programma pilota ha incluso alcuni passaggi, come il reclutamento dei partecipanti, la creazione di una comunicazione con loro, la scelta di strumenti e strategie appropriati, la fornitura della formazione e la raccolta di feedback. In una rapida panoramica su come i partner hanno scelto i partecipanti e li hanno invitati all'evento, possiamo vedere che sono stati scelti tra i clienti aziendali di ciascun partner, in particolare dalle micro, piccole e medie imprese, nonché dal targeting dei social media. I partner hanno implementato azioni promozionali sui social media, rivolte a piccoli imprenditori, dipendenti e disoccupati, insegnanti e altri fornitori di IFP che hanno aderito agli eventi. I canali per raccogliere i partecipanti sono stati le e-mail e le pubblicità sui social media.

Dal punto di vista dell'organizzazione formativa, gli eventi si sono svolti in presenza, e hanno seguito alcuni passaggi: i formatori/insegnanti si sono presentati e hanno brevemente spiegato gli obiettivi del progetto, poi i tirocinanti si sono presentati ed hanno espresso le loro aspettative sul corso. Successivamente, gli insegnanti hanno presentato il contenuto dei materiali didattici sviluppati dai partner, nonché la piattaforma OER e i tirocinanti sono stati incoraggiati a porre domande frequenti per chiarire eventuali dubbi o per portare alla discussione le loro esperienze personali nel settore della cybersicurezza. Inoltre, i partecipanti sono stati incoraggiati ad accedere ai contenuti di apprendimento ogni volta che ne avevano bisogno come risorsa preziosa nell'affrontare le loro sfide legate alla sicurezza informatica. Come passo finale, ai partecipanti è stato chiesto di fornire il loro feedback onesto sull'evento e sui materiali didattici.

Co-funded by the Erasmus+ Programme of the European Union

Con il sostegno di Erasmus+ Programma dell'Unione europea.
Questo documento e il suo contenuto riflettono solo le opinioni degli autori e la Commissione non può essere ritenuta responsabile per qualsiasi uso che possa essere fatto delle informazioni in esso contenute.

5. LA PIATTAFORMA CYBER OER COME ALLEATO DIGITALE

Uno degli obiettivi principali di questo progetto è stato quello di costruire una piattaforma Internet come vettore per le risorse educative aperte (OER) per fungere da ambiente di apprendimento in cui vengono condivise varie conoscenze sui principali aspetti da considerare nel campo della sicurezza informatica. Poiché il progetto si rivolge alle micro, piccole e medie imprese che non dispongono degli strumenti e delle risorse necessari per gestire il rischio di sicurezza digitale, la piattaforma OER ha lo scopo di fornire ai potenziali studenti tutte le conoscenze necessarie, disponibili in un unico luogo, se tutti i contenuti saranno completamente aperti e disponibili gratuitamente.

Dal punto di vista tecnico, la piattaforma dispone di un front-end pubblico Cyber-MSME e di una sezione di back-office privata/nascosta attraverso la quale i contenuti dei siti web vengono gestiti attraverso lo sviluppo di PHP e di tecnologie ingegneristiche avanzate (Ajax, DHTML, Javascript) finalizzate alla realizzazione di un ambiente caratterizzato dall'usabilità, che permetta di scaricare e visualizzare contemporaneamente contenuti e strumenti in cinque lingue diverse: inglese, rumeno, italiano, polacco e spagnolo.

Al fine di garantire che la piattaforma soddisfi pienamente i suoi obiettivi e le esigenze dei potenziali studenti, i partner hanno assicurato la sua piena operatività e apertura, il che significa che non è richiesto alcun login o registrazione e tutti i contenuti sono disponibili gratuitamente e accessibili in qualsiasi momento. Inoltre, la costruzione della piattaforma soddisfa i requisiti della piattaforma ICT Open (ICT), che ha lo scopo di ampliare il gruppo target del progetto, in quanto serve gli studenti dell'istruzione e formazione professionale (IFP) e amplia e approfondisce le competenze digitali (TIC).

Passando all'aspetto dell'organizzazione e della visualizzazione dei contenuti sulla piattaforma OER, essa funge da piattaforma eLearning dove i contenuti formativi, con tutti i toolkit e i corsi, sono facilmente visualizzabili per area/argomento grazie alle funzionalità di navigazione intelligente. Queste Linee Guida sono anche incluse nella

Co-funded by the Erasmus+ Programme of the European Union

Con il sostegno di Erasmus+ Programma dell'Unione europea.
Questo documento e il suo contenuto riflettono solo le opinioni degli autori e la Commissione non può essere ritenuta responsabile per qualsiasi uso che possa essere fatto delle informazioni in esso contenute.

piattaforma, volte ad aumentare la possibilità di accettare e utilizzare i risultati dei progetti implementati all'interno dei gruppi target.

Una delle funzionalità implementate all'interno della piattaforma è il backoffice, che include quanto segue:

- La sezione utenti di back office, che ci consente di aggiungere utenti alla piattaforma;
- La sezione news, che ci permette di aggiungere notizie ed eventi divulgativi sulla parte pubblica, in ogni lingua;
- La sezione FAQ;
- La sezione partner;
- La sezione documenti, dove possiamo caricare risorse di apprendimento con la possibilità di inviare un avviso a tutti per informare che è stato caricato un nuovo documento;
- Una sezione di scadenza;
- Una sezione di glossario contenente termini che potrebbero essere utili;
- Una sezione associati;
- Una sezione di categorie, raggruppate in aree tematiche, come le simulazioni di crisi informatica e la lista di controllo della preparazione al cyberspazio;
- Una sezione di formazione, con materiali didattici elencati nella sezione formazione, che può essere ordinata per riferimento, titolo della formazione, data e lingua;
- Una sezione di contenuti formativi, con risorse di apprendimento facili da usare, ma concise e su misura per i gruppi di formazione, in base alle loro esigenze specifiche.

Come accennato in precedenza, la piattaforma OER ha lo scopo di fungere da alleato digitale per tutti i potenziali studenti che lavorano nel campo dell'istruzione

Co-funded by the Erasmus+ Programme of the European Union

Con il sostegno di Erasmus+ Programma dell'Unione europea.
Questo documento e il suo contenuto riflettono solo le opinioni degli autori e la Commissione non può essere ritenuta responsabile per qualsiasi uso che possa essere fatto delle informazioni in esso contenute.

professionale IFP, nonché per le persone che imparano in modo indipendente sul proprio ambito, che sono incoraggiati a fare affidamento su di essa per il pilotaggio sia in contesti di apprendimento digitali che faccia a faccia.

Dal nostro punto di vista sull'erogazione di questi corsi di formazione, la piattaforma OER si è dimostrata un alleato affidabile, in quanto i formatori hanno presentato la piattaforma come fonte di conoscenza, disponibile dopo la formazione in qualsiasi momento, e hanno mostrato agli studenti come utilizzarla per lo studio autonomo, per ampliare le loro conoscenze sull'area della sicurezza informatica e anche come accedere alle sezioni di feedback e test, che gli studenti hanno trovato intuitivo e coinvolgente.

6. NOTE PER INSEGNANTI/MENTORI

Tra gli altri obiettivi, queste Linee Guida mirano a offrire una panoramica basata sull'esperienza dell'erogazione di questi corsi di formazione, nonché alcuni approfondimenti sulla possibile reattività degli studenti al contenuto della lezione, conoscenza generale di base degli argomenti discussi, approcci di mezzi più adatti per la consegna basati sul contenuto dato della lezione e altre esperienze di apprendimento per imparare in generale.

Riportando il punto di vista dei formatori, la conoscenza dei partecipanti alla formazione era elementare, con poche o nessuna informazione sul contenuto, ma tutti hanno mostrato un forte interesse per gli argomenti trattati durante la lezione e si sono detti soddisfatti dell'esplorazione delle risorse di apprendimento attraverso la piattaforma OER. Alla domanda sugli approcci più adatti per l'erogazione della formazione, i mentori hanno dichiarato che la combinazione di argomenti di molti corsi diversi ha portato a migliori risultati e hanno consigliato di utilizzare sia il pilotaggio online che il pilotaggio faccia a faccia con il supporto della piattaforma OER. Inoltre, dopo aver completato le procedure di test e aver visto in prima persona cosa ha funzionato e cosa no, i formatori

Co-funded by the Erasmus+ Programme of the European Union

Con il sostegno di Erasmus+ Programma dell'Unione europea.
Questo documento e il suo contenuto riflettono solo le opinioni degli autori e la Commissione non può essere ritenuta responsabile per qualsiasi uso che possa essere fatto delle informazioni in esso contenute.

sono stati in grado di fornire alcune idee per il miglioramento, dicendo che un buon approccio sarebbe quello di includere un test di valutazione delle conoscenze prima di iniziare i moduli, da un lato, e di utilizzare più scenari di vita reale per coinvolgere gli studenti, d'altra parte.

7. ALCUNI CONSIGLI

Il messaggio che i nostri formatori desiderano trasmettere alle organizzazioni che vogliono implementare i contenuti e gli strumenti Cyber-MSME nel loro percorso professionale è quello di dedicare un po' di tempo a conoscere i materiali di apprendimento e trovare modi per adattarli a vari pubblici di destinazione, in base alle loro esigenze, conoscenze generali sugli argomenti e aree professionali. Inoltre, secondo le note e le raccomandazioni dei formatori, il rapporto di mappatura del progetto mostra statistiche e bisogni in ciascuno dei paesi partner, il che rappresenta un buon punto di partenza per fornire i corsi di formazione.

Tuttavia, anche se queste linee guida, insieme al feedback dei formatori sono un buon punto di partenza per fornire i corsi di formazione, incoraggiamo vivamente tutti i potenziali utenti ad adattare i materiali di apprendimento ai contesti in cui operano e alle persone a cui vengono erogati i corsi di formazione. Si consiglia vivamente ai coach di investire sforzi per coinvolgere gli studenti nell'erogazione del corso e di costruire un ambiente di apprendimento basato sul co-sviluppo e sulla co-creazione del contenuto, in cui viene perseguito l'apprendimento attivo.

8. ALCUNE NOTE FINALI

Mentre il progetto sta volgendo al termine, abbiamo sviluppato due diversi risultati finali per promuovere la scalabilità del progetto, la sua trasferibilità e replicabilità dei suoi

Co-funded by the Erasmus+ Programme of the European Union

Con il sostegno di Erasmus+ Programma dell'Unione europea.
Questo documento e il suo contenuto riflettono solo le opinioni degli autori e la Commissione non può essere ritenuta responsabile per qualsiasi uso che possa essere fatto delle informazioni in esso contenute.

risultati in altri settori pratici, nonché una panoramica delle intuizioni dei partner nel campo della sicurezza informatica e le loro raccomandazioni che desiderano condividere con i responsabili politici e chiunque sia disposto a utilizzare i toolkit e i corsi. Questo documento è una parte di questi risultati, e l'altro documento è rappresentato dal documento programmatico, che è un input al dominio dei decisori politici e (locali) nel campo della sicurezza informatica, della preparazione informatica e della resilienza informatica del settore privato – con particolare riferimento alle micro e piccole e medie imprese – e più in generale, affrontare aspetti quali la competitività delle PMI, l'IFP manageriale, lo sviluppo delle imprese, la digitalizzazione dei cittadini dell'UE in generale.

Co-funded by the Erasmus+ Programme of the European Union

Con il sostegno di Erasmus+ Programma dell'Unione europea.
Questo documento e il suo contenuto riflettono solo le opinioni degli autori e la Commissione non può essere ritenuta responsabile per qualsiasi uso che possa essere fatto delle informazioni in esso contenute.