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

DiSCVET

TOOLBOX per insegnanti/formatori VET

DiSCVET

Sviluppo delle competenze di sovranità digitale di insegnanti e formatori VET

BBB Bundesverband der Träger beruflicher Bildung (Bildungsverband) e. V. — Germany

MUNDUS Bulgaria — Bulgaria

Greece

VERNIAN rti — Cyprus

MIITR — Slovenia

BK·CON — Germany

petit pas — Italy

Creato da MIITR
maggio 2023

Questo progetto è finanziato con il sostegno della Commissione europea. L'autore è il solo responsabile di questa pubblicazione e la Commissione declina ogni responsabilità sull'uso che potrà essere fatto delle informazioni in essa contenute.
[Numero del progetto: 2020-3-BE05-KA205-003110].

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

1 Contenuti

DiSCVET **TOOLBOX**

PROGETTO: Sviluppo delle competenze di sovranità digitale di insegnanti e formatori VET

Disponibile in: BG, DE, EN, GR, IT, SI!

PERCHÉ?

La sovranità digitale è un nuovo concetto nell'era digitale che suggerisce che le parti dovrebbero avere la sovranità sui propri dati digitali. A livello individuale, la sovranità digitale dimostra la capacità degli individui di possedere i propri dati personali e controllarne l'utilizzo. Le persone spesso fanno fatica ad apprezzare l'importanza della privacy poiché le conseguenze delle violazioni della privacy sono difficili da valutare a causa della loro natura sfuggente.

COSA

Una forma innovativa di contenuti formativi insieme ad una piattaforma di simulazione online

PER CHI

insegnanti/formatori VET, organizzazioni VET, fornitori di istruzione, autorità, esperti/decisori.

DOVE

discvet-hub.eu
discvet.eu
facebook.com/discvet

Include materiale su:

- MGestione delle risorse digitali
- Dati personali e Privacy
- Gestione della sicurezza delle informazioni
- Gestione del rischio
- Gestione delle informazioni e della conoscenza

IO2 Piattaforma online e materiale di formazione

Un materiale di formazione creativo che mira a fornire agli insegnanti/formatori dell'IFP le competenze necessarie per aumentare la loro sovranità digitale e consentire loro di formare gli altri. Il materiale formativo è costituito da un pacchetto di risorse di apprendimento digitale che utilizzano il concetto di micro-apprendimento. Queste pillole di apprendimento digitale presentano varie risorse come giochi interattivi, video di e-learning, case study interattivi, risorse infografiche e altro ancora.

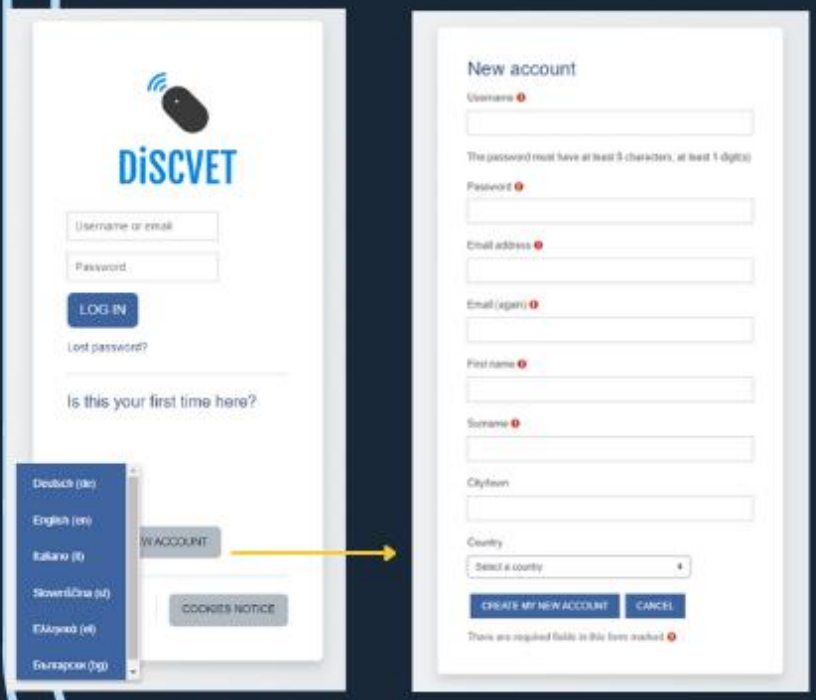
IO3 Esercizi di simulazione

È stata effettuata una transizione sul piano pratico attraverso esercizi di simulazione sulla sovranità digitale nella vita reale, introducendo nuove app, metodi o strumenti e consentendo agli utenti di acquisire esperienza pratica. Grazie a questi esercizi gli utenti saranno in grado di applicare i principi della sovranità digitale e della sicurezza digitale a situazioni pratiche, come attacchi informatici, violazioni della sicurezza, phishing, malware e altro.

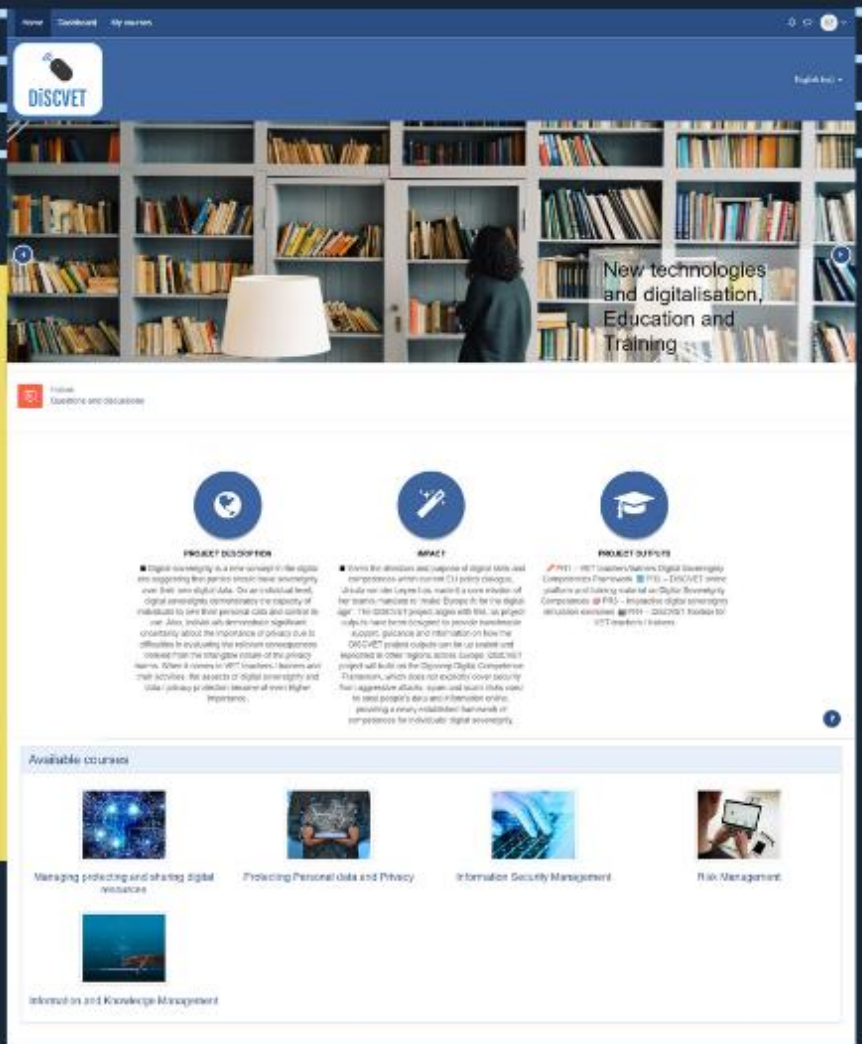
Scopri di più sui risultati, su come utilizzarli, sui test pilota e sulle iniziative nazionali in materia di educazione alla sicurezza digitale! !

Come utilizzare la piattaforma?

(discvet-hub.eu/)



Per accedere ai materiali, gli utenti devono registrarsi sulla piattaforma. Dopo aver fornito tutte le informazioni necessarie per la creazione di un account, riceverai una e-mail di conferma (controlla la tua cartella spam!), che conterrà un link per attivare il tuo account.

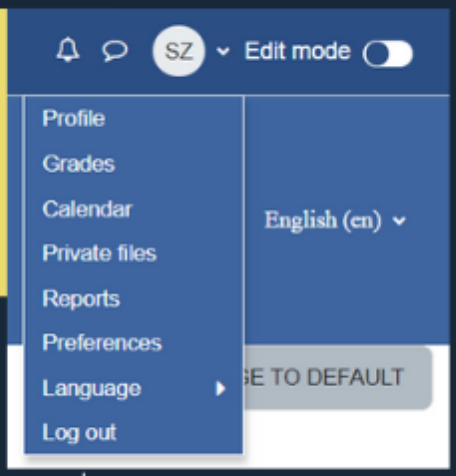


Nella home page puoi trovare informazioni sul progetto e sui 5 corsi disponibili. Per accedere al materiale didattico, fai clic su un corso e premi il pulsante di iscrizione.

Nessuna qualifica necessaria!

Ogni modulo è composto da diverse unità, tutte con una parte di apprendimento teorico (PDF e pillole di apprendimento digitale),e da esercizi di simulazione. Qui è dove metterai alla prova le tue conoscenze acquisite ricevendo un feedback immediato sul tuo punteggio.

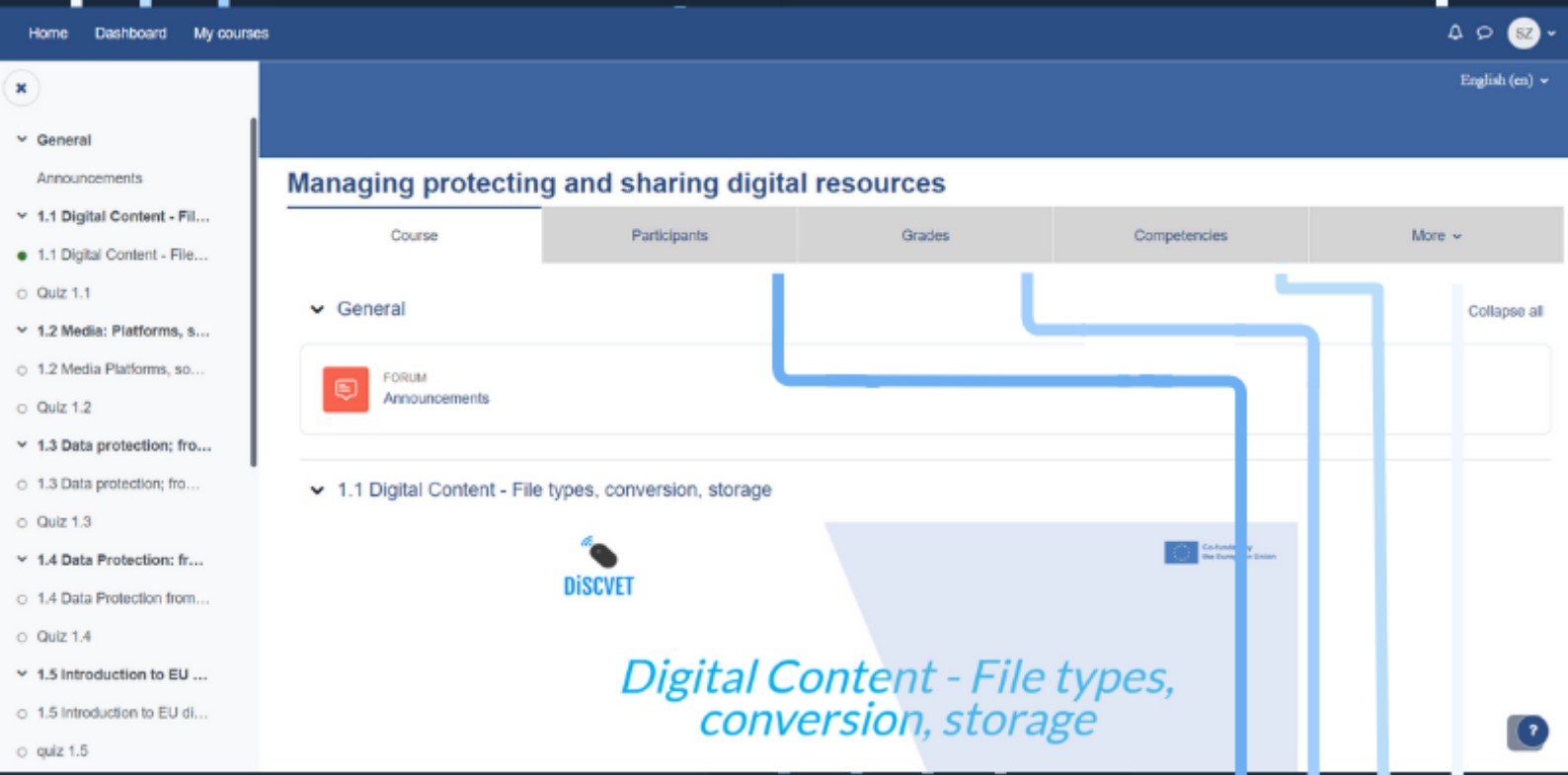
Per accedere al tuo profilo e alle tue impostazioni, clicca in alto a destra sul cerchio luminoso con le tue iniziali. Accanto, puoi trovare le notifiche (simbolo della campana) e le chat (simbolo della bolla della chat).



Ritorna alla pagina iniziale

AAccedi al calendario e alle attività programmate

Corsi a cui sei iscritto e i tuoi progressi [%]



Trova altre persone che partecipano a questo corso

I punteggi dei tuoi esercizi di simulazione

Un elenco delle tue nuove competenze

Descrizione del corso

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

4 Dati raccolti dalle attività pilota

4.1 Metodologia

Lo scopo di questo documento è quello di presentare le risposte raccolte nella fase di sperimentazione pilota dei risultati del progetto. L'attività di test pilota per il progetto DiscVet si è svolta nel periodo che va da Febbraio ad Aprile 2023.

L'obiettivo generale di questo rapporto riassuntivo è registrare il livello percepito di soddisfazione e qualità dei risultati del progetto, nonché la loro utilità, l'essere in grado di concentrarsi sui problemi incontrati e individuare possibili soluzioni al fine di fornire i risultati del progetto nella loro forma finale e versione definitiva.

I risultati del progetto testati sono stati:

- **IO2: piattaforma online DiSCVET e materiale formativo sulle competenze di sovranità digitale**
- **IO3: Sviluppo degli esercizi di simulazione interattiva della sovranità digitale**

I test pilota del risultato di progetto 2 sono stati implementati attraverso un questionario strutturato sotto forma di **Google Form** (per garantire una migliore accessibilità e raggiungibilità del gruppo target); disponibile nell'ALLEGATO I di questo report. Il questionario mirava ad acquisire feedback utili dai partecipanti alle attività pilota, concentrandosi sulla valutazione di diverse caratteristiche del materiale, quali:

- la chiarezza della sua struttura;
- l'efficacia delle risorse digitali che include;
- La facilità di utilizzo e navigazione attraverso la piattaforma;
- La quantità di tempo trascorso nella piattaforma e nelle sue attività/componenti;
- La facilità di inserimento di nuovi dati/informazioni;
- La struttura generale e l'estetica della piattaforma;
- Il collegamento/caricamento dei componenti e/o delle loro pagine.

Il test pilota del risultato numero 3 è stato condotto attraverso un questionario strutturato pertinente, concentrandosi sulla valutazione di diverse caratteristiche degli esercizi di simulazione, quali:

- Pertinenza con l'argomento e le esigenze del gruppo target;
- Facilità d'uso;
- Progetto.

Ai partecipanti è stato chiesto di valutare i diversi aspetti di IO2 e IO3 su una scala da 1 a 5, dove
1 = l'impressione più bassa e insoddisfacente

3 = un'impressione adeguata

5 = l'impressione più alta, molto buona

Nel questionario strutturato è stato incorporato il link alla piattaforma online https://discvet-hub.eu/login/index.php contenente il materiale, al fine di poter monitorare il raggiungimento dei **KPI** previsti per questa attività progettuale.

KPI IO2

KPI 7: Corso di formazione ben definito e materiali che soddisfano le esigenze riconosciute nell'ambito delle attività IO1 (qualitativo) - Strumento di misurazione: valutazione interna da parte dei partner di progetto e valutazione esterna da parte dei membri degli NSAG

KPI 8: Almeno 180 insegnanti/formatori IFP che parteciperanno alle attività pilota (quantitativo) - Strumento di misurazione: numero di persone che si sono registrate nella piattaforma e hanno completato il corso di formazione

KPI 9: 85% di soddisfazione dei partecipanti dalle attività di pilotaggio (quantitativo) - Strumento di misurazione: compilazione di questionari strutturati per la valutazione delle attività di pilotaggio

KPI IO3

KPI 10: Almeno 180 insegnanti/formatori IFP che parteciperanno alle attività pilota (quantitativo) - Strumento di misurazione: numero di persone che si sono registrate nella piattaforma e hanno completato gli esercizi di simulazione

KPI 11: 85% di soddisfazione dalla funzionalità della piattaforma (quantitativo) - Strumento di misurazione: compilazione di questionari strutturati per la valutazione della piattaforma

Ciascun paese partner ha condotto diverse sessioni pilota (online o faccia a faccia), a causa della difficoltà di reclutare 30 partecipanti contemporaneamente.

In **Italia** è stato creato materiale divulgativo per pubblicizzare l'evento e dare istruzioni su come condurre il test pilota. È stata organizzata una sessione in presenza con il coinvolgimento di studenti, insegnanti e parti interessate per testare i risultati del progetto.

In **Bulgaria** si sono svolte complessivamente tre sessioni pilota - 1 di persona e 2 online, con la partecipazione di partecipanti di insegnanti IFP, formatori in Educazione degli adulti e parti interessate.

In **Slovenia** il gruppo target coinvolto nel test pilota era costituito da insegnanti IFP, insegnanti, da istituti VET locali e scuole superiori, nonché da una rete di altre ONG slovene interessate a temi simili, la Camera di commercio e industria locale. Le sessioni di test pilota si sono svolte in momenti separati, secondo la disponibilità dei partecipanti, sono state organizzate 3 sessioni in presenza e 2 sessioni online.

4.2 Risultati

Accesso alla piattaforma E-learning per Paese

Paese	Numero di accessi
Grecia	40
Slovenia	32
Italia	36
Germania	11

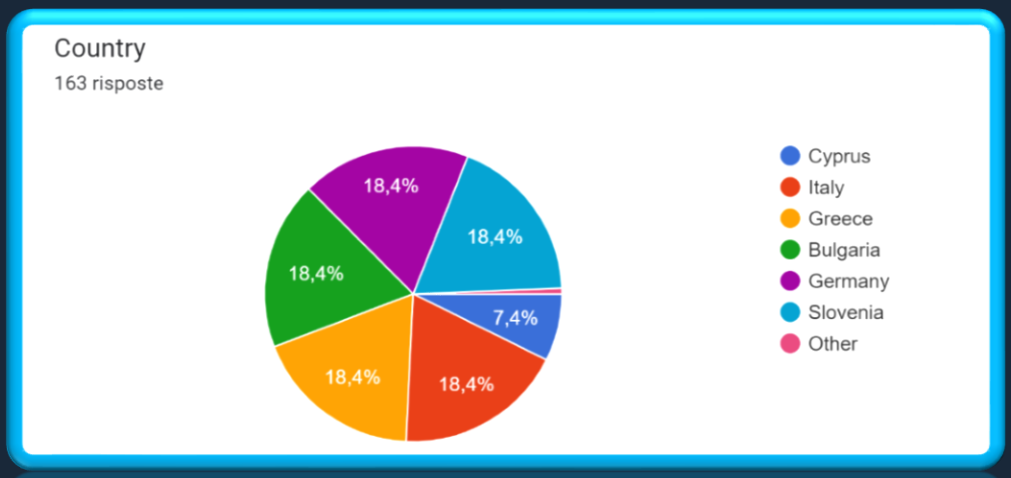
Cipro	23
Bulgaria	35

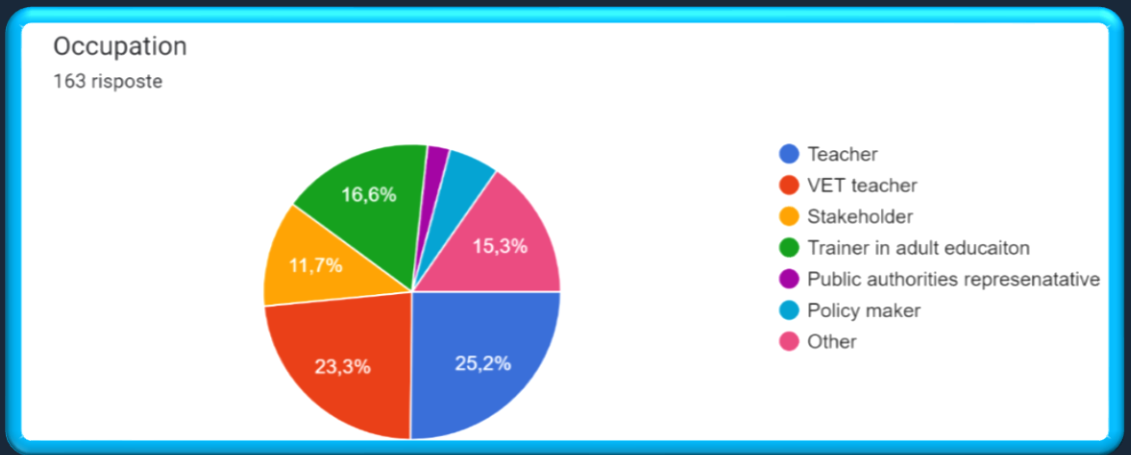
Feedback dei partecipanti.

Occupazione del gruppo target

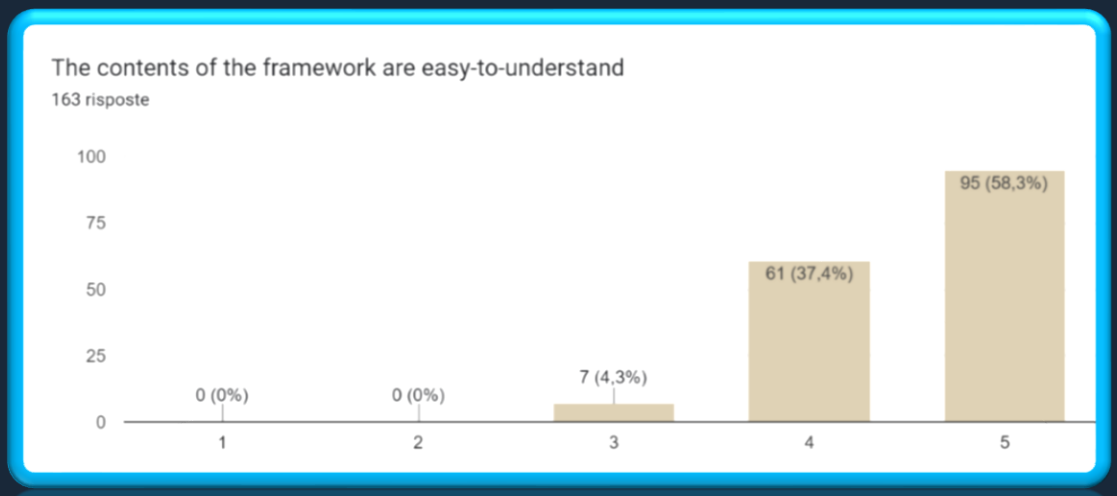
In totale sono state raccolte 163 risposte da tutti i paesi partner, la percentuale più alta che rappresenta l'occupazione del gruppo target è il 25,2% degli insegnanti, seguita dal 23,3% degli insegnanti VET.

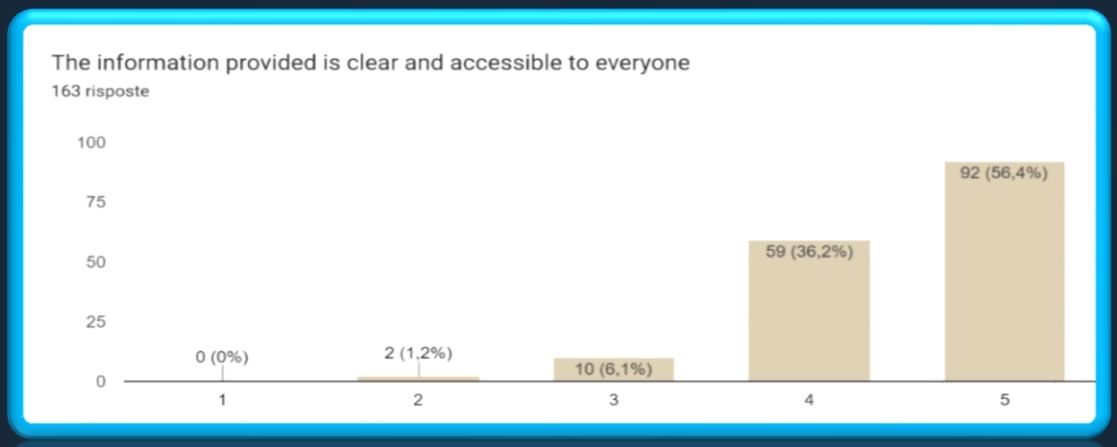
Partecipanti al test pilota registrati da tutti i paesi partner. Una piccola percentuale (1 rispondente) si è registrata dalla Francia.

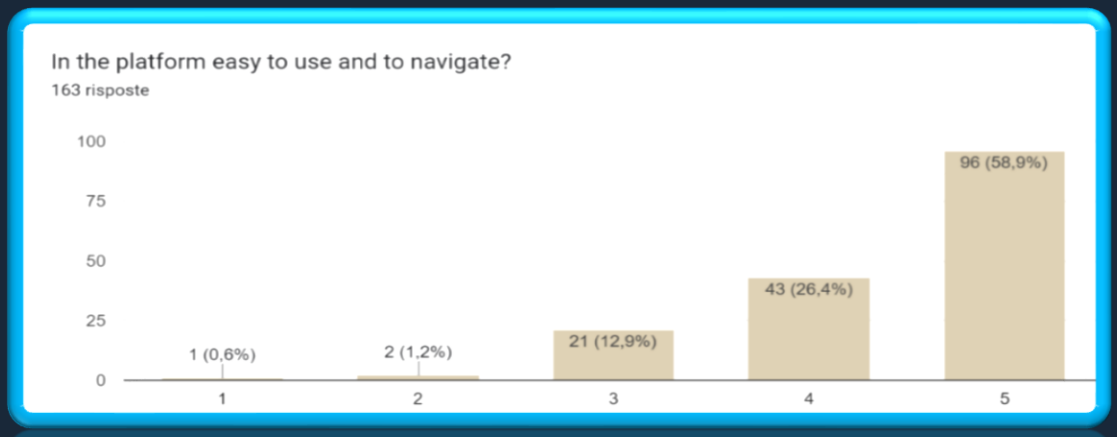




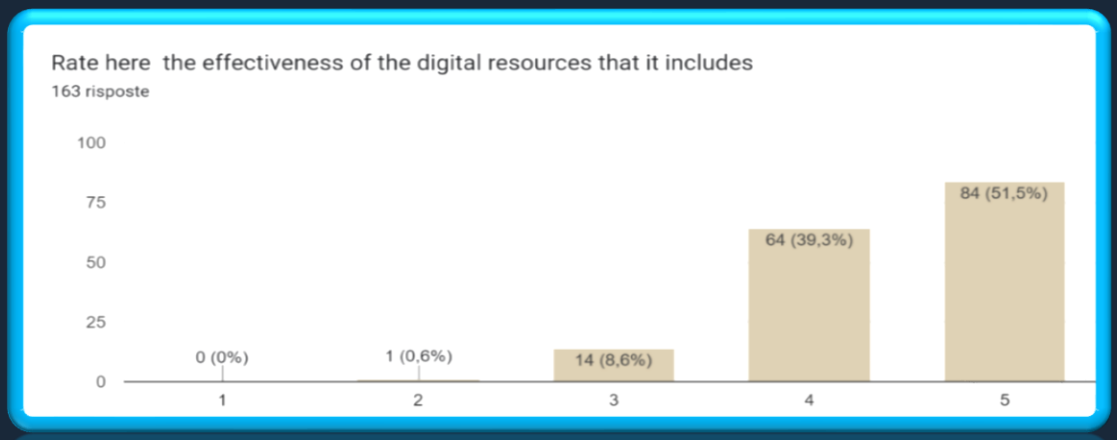
Co-funded by the
Erasmus+ Programme
of the European Union

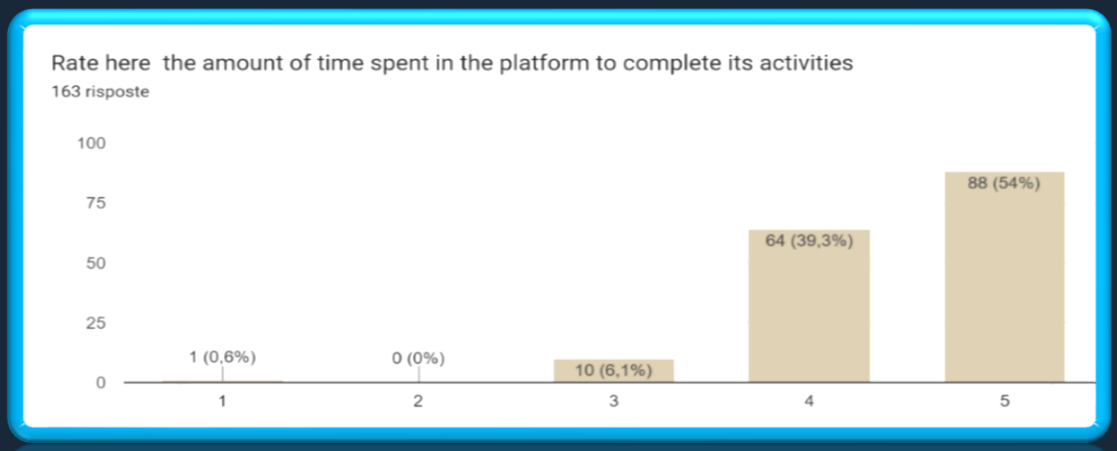


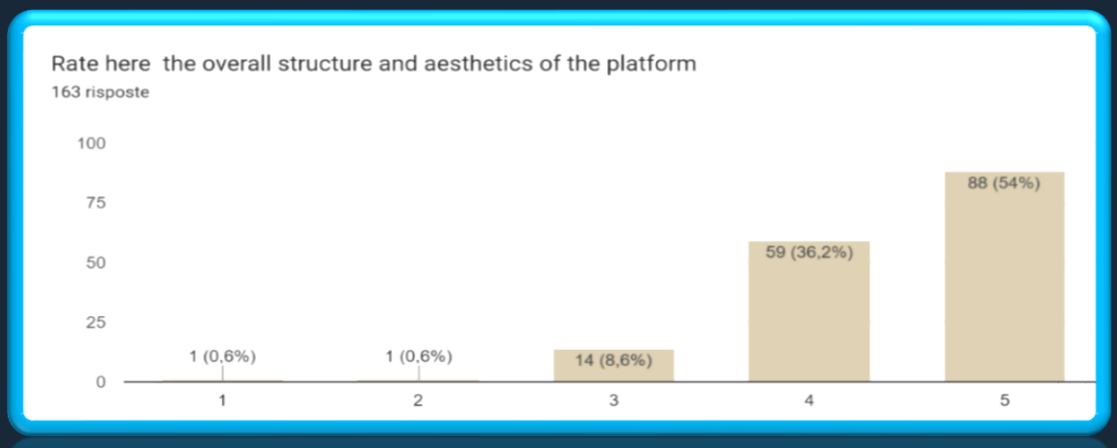




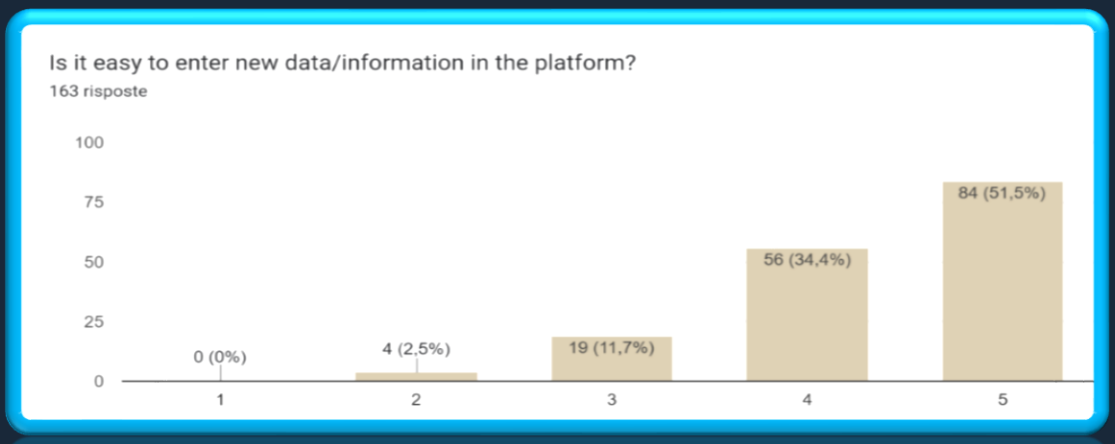
Co-funded by the
Erasmus+ Programme
of the European Union

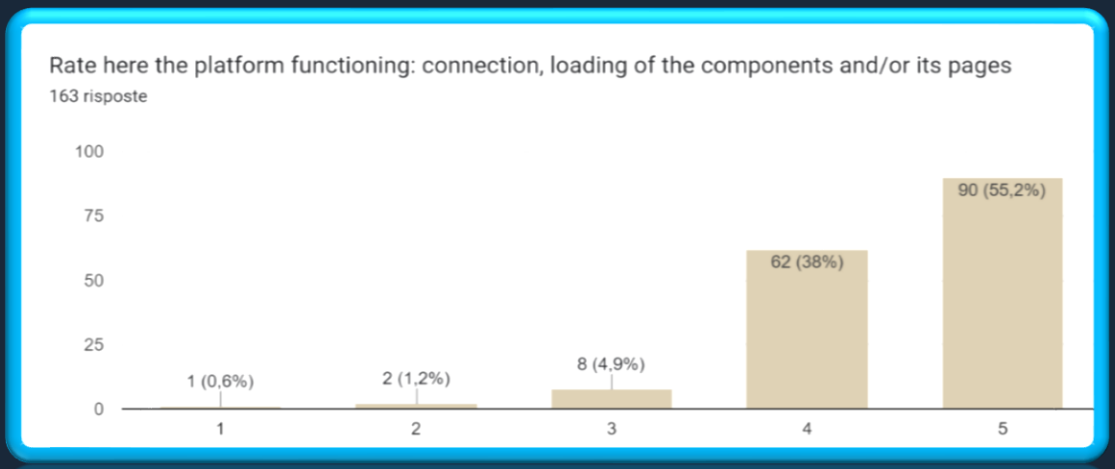


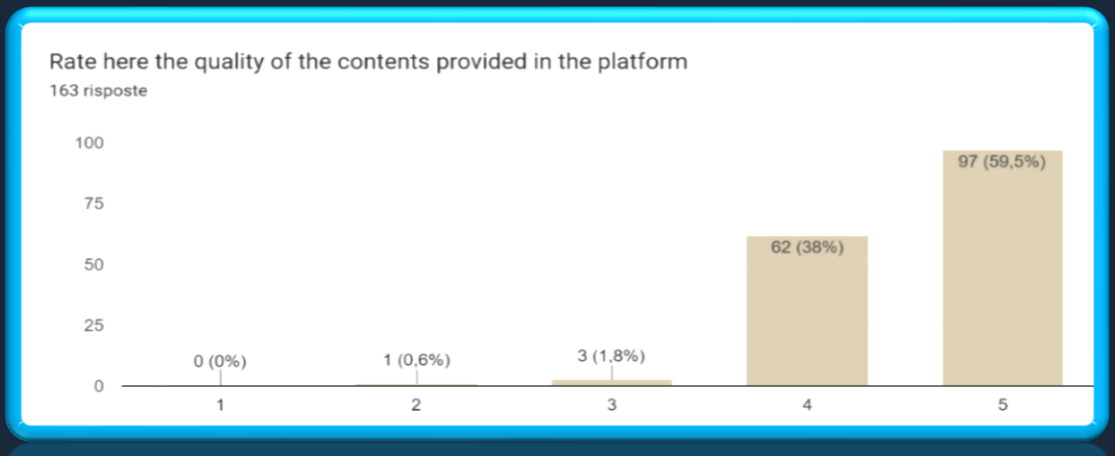


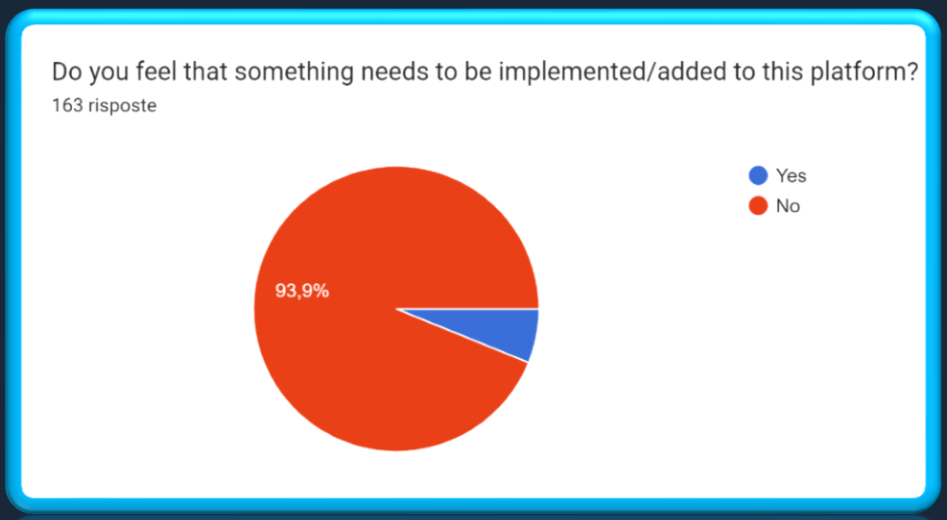


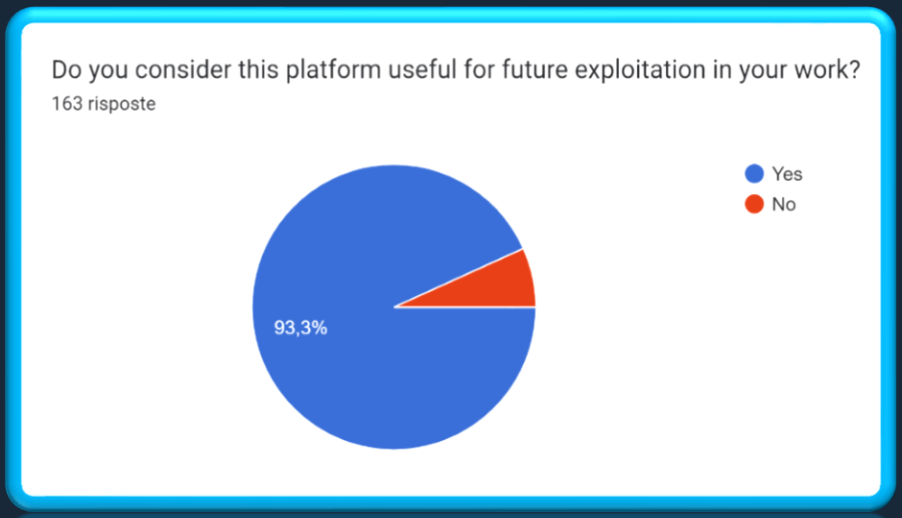
Co-funded by the
Erasmus+ Programme
of the European Union











Come si può vedere dalle figure sopra, che rappresentano le risposte raccolte dopo le sessioni di test pilota in ciascun paese partner, i partecipanti hanno espresso un **alto livello** di soddisfazione valutando i diversi aspetti della piattaforma di e-learning come il suo contenuto, la facilità di utilizzo e navigazione, la qualità dei materiali caricati, il funzionamento della piattaforma, assegnando un punteggio **compreso tra 4 e 5** (dove 5 è il punteggio massimo).

Inoltre, i partecipanti hanno dichiarato l'utilità della piattaforma per l'utilizzo futuro nel loro lavoro. La maggior parte dei partecipanti al test pilota non ha

espresso la necessità di implementare ulteriormente la piattaforma, 10 partecipanti (6,1%) tuttavia, hanno suggerito alcune correzioni specifiche da prendere in considerazione come da feedback riportato di seguito:

- Mancano traduzioni in Sloveno
- domande bulgare mancanti nei quiz
- quando si seleziona una lingua, dovrebbero apparire solo le informazioni in quella lingua
- Altri video informativi

Sebbene il questionario utilizzato per il test pilota abbia mostrato un alto livello di soddisfazione complessiva, vi erano alcuni aspetti da evidenziare e tenere in considerazione per il miglioramento finale della piattaforma e dei suoi contenuti, come visibile in specifici feedback riassunti di seguito.

Riscontro positivo

- *una piattaforma interessante*
- *Bel design e molto utile*
- *credo che questa piattaforma sia facile da capire e da usare, ha anche un'ottima estetica*
- *La piattaforma è molto semplice da usare e può essere facilmente utilizzata.*
- *Molto bene*
- *Penso che questo risultato sia utile*
- *Molto utile e chiara la divisione dei contenuti nella piattaforma*
- *Eccellente*
- *Mi piace che i casi della vita reale siano implementati*
- *La simulazione della vita reale è utile*
- *Mi mancava questa conoscenza*
- *Facile da capire e pratico*
- *La navigazione interattiva e le informazioni raccolte dal sito Web sono state eccellenti*
- *Mi piace molto navigare nel sito Web e ho imparato molte cose nuove su dati e privacy*
- *Userò sicuramente ciò che ho imparato sulla visualizzazione dei dati in futuro e utilizzerò i suggerimenti didattici della piattaforma*
- *Molto interessante e ricco di informazioni che tutti gli insegnanti dovrebbero conoscere*
- *Interessante! Ho imparato molto sull'interattività e sulla gestione dei dati digitali*
- *Il mondo digitale è tutto intorno a noi ed è importante saper gestire i nostri dati e le nostre informazioni! La piattaforma è molto interessante e di facile lettura*

Aspetti da migliorare

- *Si possono trovare alcuni errori grammaticali*
- *È necessaria l'ottimizzazione mobile.*
- *il pulsante indietro glitch, la "pagina slovena" era per lo più in inglese, formato strano, esteticamente sgradevole*
- *Il contenuto sembra utile; tuttavia, il modo in cui viene presentato è a volte scomodo e confuso. In alcuni capitoli sono inclusi il quiz e la presentazione genial.ly, in altri no. Il contenuto in genial.ly e pdf è ripetitivo e poco chiaro.*
- *Non è coerente tra i moduli*
- *Il quiz aveva una formattazione strana (doppi numeri).*
- *Alcuni quiz avevano risposte mancanti, altri avevano domande con diverse risposte corrette al 100% tra cui scegliere, rendendo il quiz un gioco d'ipotesi (es. 5.4)*
- *Le presentazioni hanno impiegato un po' di tempo a caricarsi ma per il resto sono contenuti utili.*
- *Geniallys ha impiegato un po' di tempo per caricarsi. Il contenuto sembra utile; tuttavia, il modo in cui viene presentato è a volte scomodo e confuso. In alcuni capitoli sono inclusi il quiz e la presentazione genial.ly, in altri no. Il contenuto in genial.ly e pdf è ripetitivo e poco chiaro.*

4.3 Conclusione

La fase di sperimentazione pilota si è rivelata complessivamente positiva, avendo evidenziato la soddisfazione della maggior parte dei partecipanti che hanno valutato positivamente i risultati del progetto e la loro utilità.

Allo stesso tempo, sono stati evidenziati aspetti che necessitano di miglioramento e che hanno riguardato principalmente alcuni aspetti legati ai quiz. A tal proposito, i suggerimenti forniti ruotano attorno alla possibilità di "*risolvere prima le questioni più ovvie come la grammatica, i numeri doppi sui quiz, le risposte mancanti ecc., tutte menzionate prima. Quindi passare all'aggiornamento del design del sito (rendendo più piccolo il banner superiore, spostando i moduli verso l'alto, fare un uso migliore della spaziatura e del layout (su tutte le pagine)). Infine, controllare i tempi di caricamento di Geniallys* "

4.4 ALLEGATI

Allegato I - I Questionario test pilota
https://docs.google.com/forms/d/e/1FAIpQLSdLMxrfoPS1RcKhAgGl_Ph0LJceFrdhE5wSCiV01WbhORUE1A/viewform

Allegato II - II IO1 Convalida
https://drive.google.com/drive/folders/1rIvFJQheUiG38Ii7rAG5GxIAyN_e-y0o

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

5 APPROCCIO UE ALLA SICUREZZA DIGITALE

5.1 Approccip generale dell'UE alla cybersicurezza

L'UE ha adottato un approccio globale alla cybersicurezza, con una serie di regolamenti e direttive volti a proteggere l'infrastruttura digitale e i dati personali. Alcuni elementi chiave della strategia di cybersicurezza dell'UE includono:

Il **regolamento generale sulla protezione dei dati (GDPR)**, che stabilisce le regole su come i dati personali devono essere elaborati, archiviati e protetti all'interno dell'UE. Il GDPR si applica a tutte le aziende che operano all'interno dell'UE, nonché a qualsiasi azienda che elabora i dati personali dei cittadini dell'UE.

La **direttiva sulla sicurezza delle reti e delle informazioni (direttiva NIS)**, che stabilisce misure di cybersicurezza per i fornitori di infrastrutture critiche, compresi i settori dell'energia, dei trasporti e della sanità. Richiede a questi fornitori di segnalare gravi incidenti di sicurezza alle autorità nazionali.

Il **Cybersecurity Act**, che crea un quadro per l'istituzione di sistemi di certificazione della cybersicurezza a livello dell'UE per prodotti, servizi e processi digitali.

La **strategia dell'UE per la cybersicurezza**, che è un piano globale per migliorare la cybersicurezza in tutta l'UE. Comprende iniziative per rafforzare la cooperazione tra gli Stati membri, promuovere la ricerca e l'innovazione e rafforzare l'infrastruttura di sicurezza informatica dell'UE.

5.2 Piano d'azione per l'educazione digitale

In Europa, c'è un crescente riconoscimento dell'importanza dell'educazione digitale nella preparazione delle persone per il futuro. La Commissione europea ha lanciato un nuovo piano d'azione per l'istruzione digitale, che mira a promuovere l'uso della tecnologia nell'istruzione e migliorare le competenze digitali tra i cittadini europei. Il piano comprende iniziative volte a fornire a tutte le scuole l'accesso a Internet ad alta velocità, aumentare l'uso di strumenti digitali nell'insegnamento e nell'apprendimento e sostenere lo sviluppo di tecnologie educative innovative. Il piano si concentra anche sul miglioramento delle competenze digitali degli insegnanti e sulla promozione di opportunità di apprendimento permanente per tutti i cittadini. Investendo nell'educazione digitale, l'Unione europea spera di promuovere la crescita economica, l'inclusione sociale e la cittadinanza digitale in tutta la regione.

Il Piano prevede 13 azioni, 3 delle quali sono direttamente correlate all'istruzione e alla formazione digitale:

Azione 5 (Piani di trasformazione digitale per gli istituti di istruzione e formazione) - mira a sostenere gli sforzi di trasformazione digitale attraverso progetti di cooperazione Erasmus+, crea accademie per insegnanti per lo sviluppo e la collaborazione e introduce uno strumento di autovalutazione online chiamato SELFIE per gli insegnanti per identificare le aree di miglioramento.

Azione 6 (Linee guida etiche sull'uso dell'IA e dei dati nell'insegnamento e nell'apprendimento per gli educatori) - C'è una crescente necessità di comprendere il potenziale dell'IA e di aumentare la consapevolezza dei possibili rischi in quanto potrebbe trasformare l'istruzione e la formazione, così come le nostra vite quotidiane. Le linee guida forniscono supporto pratico e guida per l'uso dell'IA, aiutano nell'insegnamento e nell'apprendimento, suggeriscono migliori sistemi di supporto per i processi amministrativi e presentano considerazioni etiche.

Azione 7 (Linee guida comuni per insegnanti ed educatori): l'istruzione e la formazione sono fondamentali per coltivare le capacità di pensiero critico dei cittadini necessarie per navigare nel mondo online, date le sue caratteristiche uniche come algoritmi, "bolle di informazioni" e "camere dell'eco". Pertanto, sostenere insegnanti ed educatori con orientamenti ed esempi pratici è essenziale per promuovere l'alfabetizzazione digitale e combattere la disinformazione. Le linee guida offrono suggerimenti pratici e piani di attività per gli insegnanti della scuola primaria e secondaria, indipendentemente dalle loro conoscenze in materia di educazione digitale, e sono integrate da una relazione finale che delinea i risultati e le raccomandazioni principali del gruppo di esperti.

Nel complesso, il piano d'azione per l'istruzione digitale è una strategia globale per promuovere l'educazione digitale e migliorare le competenze digitali in tutta Europa. Riconosce l'importanza della tecnologia nella preparazione degli studenti per il futuro e nella promozione della crescita economica e dell'inclusione sociale.

5.3 Framework contenenti competenze di sicurezza digitale

La crescita esponenziale delle tecnologie digitali ha sottolineato la necessità di sicurezza digitale. L'importanza di sviluppare e migliorare le competenze in materia di sicurezza digitale è menzionata nei quadri di competenze delle tecnologie digitali come il quadro di competenze digitali europee, noto come DigComp 2.2, e il quadro di competenze digitali europeo per gli educatori, noto come DigCompEdu.

Il **quadro DigComp** consente ai cittadini europei di comprendere meglio cosa si intende per competenza digitale e come valutare e sviluppare la propria competenza digitale. I cinque domini principali nel quadro delle competenze sono l'alfabetizzazione informativa e dei dati, la comunicazione e la collaborazione, la creazione di contenuti digitali, la sicurezza e la risoluzione dei problemi.

Il **framework DigCompEdu** descrive cosa significa per gli educatori essere digitalmente competenti ed è diretto a tutti gli educatori a tutti i livelli di istruzione. Il

quadro descrive 22 competenze che sono organizzate in sei aree. Queste aree sono impegno professionale, risorse digitali, insegnamento e apprendimento, valutazione, responsabilizzazione degli studenti e facilitazione delle competenze digitale degli studenti.

5.4 Finanziare la ricerca e l'innovazione per l'apprendimento digitale

L'UE finanzia la ricerca e l'innovazione nel campo della cybersicurezza e della tecnologia digitale attraverso programmi come Orizzonte Europa, Programma Europa digitale e CEF (Connecting Europe Facility). Quest'ultimo supporta l'infrastruttura di sicurezza informatica e i team di risposta agli incidenti. InvestEU finanzia importanti catene di cybersicurezza nel settore privato. Horizon Europe, uno dei più importanti programmi di finanziamento per la sicurezza informatica, finanzia soluzioni innovative di difesa informatica, con l'obiettivo di supportare le PMI, le simulazioni e proteggere i dati critici. Questi programmi collaborano con il Centro europeo di competenza industriale, tecnologica e di ricerca sulla cybersicurezza, un gruppo di esperti e organizzazioni per la diffusione della cybersicurezza in tutti i paesi.

5.5 Risorse e strumenti utili (BBB)

La quarta rivoluzione industriale ha portato rapidi sviluppi nei campi delle nuove tecnologie, della comunicazione e dell'automazione. Questi sviluppi hanno portato alla transizione verso un contesto digitale nell'occupazione e nell'istruzione. La pandemia ha accelerato questa transizione creando un maggiore bisogno di formazione a distanza e di lavoro. Ciò ha creato nuove dinamiche e sfide con l'uso universale e diffuso degli strumenti digitali (piattaforme, siti web, ecc.).

In tale contesto, l'UE ha riconosciuto lo slancio e ha adottato il piano d'azione per l'istruzione digitale (2021-2027), che definisce gli obiettivi della Commissione europea per conseguire un'istruzione digitale efficace, inclusiva e accessibile in tutta l'Unione europea. In particolare, l'UE ha creato una serie di strumenti digitali per facilitare le operazioni dell'UE, le questioni relative alla formazione e la comunicazione tra organizzazioni e individui in tutta l'UE. I principali strumenti digitali lanciati dall'UE sono:

Portale dell'istruzione scolastica . Si tratta di un "catalogo online", dove è possibile consultare materiali didattici, partecipare a corsi online e accedere a risorse formative per gli insegnanti e, più in generale, per le persone interessate all'istruzione scolastica in Europa. School Education Gateway include pubblicazioni, esercitazioni, materiali didattici creati dalle istituzioni dell'UE, progetti finanziati dall'UE, corsi online gratuiti, webinar e le ultime notizie relative alla politica e all'istruzione scolastica europea.

eTwinning . La piattaforma è rivolta al personale scolastico dei paesi europei, per permettere a docenti e presidi di comunicare tra loro, per creare una rete che permetta lo sviluppo di collaborazioni, condivisioni e progetti utili per il sistema scolastico europeo. eTwinning mira a promuovere la collaborazione tra le scuole in Europa attraverso l'uso delle tecnologie dell'informazione e della comunicazione: attraverso la piattaforma, infatti, il personale scolastico può comunicare, scambiare risorse e creare progetti in 30 lingue.

Angolo dell'apprendimento . Questa è una piattaforma rivolta sia agli studenti che agli insegnanti. A seconda della fascia di età, agli studenti vengono forniti diversi materiali, inclusi giochi, concorsi e libri di attività, che consentono loro di conoscere diversi aspetti dell'Unione europea, dalle leggi all'ambiente e alla storia. Per gli insegnanti, la piattaforma è una buona fonte per trovare materiali didattici dedicati agli studenti delle scuole primarie o secondarie.

Supporto, apprendimento avanzato e opportunità di formazione per i giovani (Skip-Youth). Si tratta di una rete di sette centri, ognuno dei quali lavora su un'area prioritaria nel campo della gioventù. Nello specifico, la piattaforma fornisce risorse per l'apprendimento dei giovani, corsi di formazione e opportunità di networking.

Piattaforma elettronica per l'apprendimento degli adulti in Europa (EPALE). Si tratta di una comunità online europea, multilingue e aperta, a cui possono aderire professionisti dell'educazione degli adulti di tutta Europa. La piattaforma offre l'opportunità di implementare le competenze digitali attraverso corsi online gratuiti, accesso a esempi di buone pratiche nell'apprendimento degli adulti e risorse di e-learning.

Self-reflection on Effective Learning by Fostering the use of Innovative Educational Technologies (SELFIE) è uno strumento gratuito progettato per aiutare le scuole a integrare le tecnologie digitali nell'insegnamento, nell'apprendimento e nella valutazione. SELFIE ha una solida base nella ricerca ed è stato sviluppato sulla base del quadro della Commissione europea sulla promozione dell'apprendimento nell'era digitale nelle organizzazioni educative.

6 CONTESTO NAZIONALE

6.1 Slovenia

Negli ultimi anni la Slovenia ha lavorato attivamente per migliorare la sua infrastruttura digitale e di sicurezza informatica. Il paese ha riconosciuto l'importanza della sicurezza informatica come componente essenziale della sicurezza nazionale e ha sviluppato varie iniziative per migliorare le sue capacità di sicurezza informatica. Le capacità nazionali di sicurezza informatica della Slovenia

e i loro ruoli sono definiti a livello operativo: SI-CERT è la risorsa nazionale della garanzia della sicurezza informatica e il MORS è responsabile nel campo della difesa e della protezione contro i disastri naturali e di altro tipo (compresa la protezione delle risorse critiche infrastrutture), la polizia garantisce la sicurezza informatica nel contesto della sicurezza pubblica e della lotta contro la criminalità informatica, l'Agenzia slovena per l'intelligence e la sicurezza (SOVA) conduce il controspionaggio e l'emergente SIGOVCERT è responsabile della sicurezza informatica nella pubblica amministrazione. Nel campo del coinvolgimento sono inclusi anche altri portatori di interesse, come gli operatori di infrastrutture critiche nel settore pubblico e privato.

INIZIATIVA 1	
Nome	Sicuro su Internet
Posizione	Nazionale
Durata	2011 -
Descrizione	SI-CERT ha sensibilizzato la nazione e gestito un programma educativo "Sicuri su Internet". Questa iniziativa si rivolge al grande pubblico con contenuti specifici per piccole imprese, artigiani e ditte individuali per sensibilizzare all'uso sicuro di Internet. Il progetto è finanziato dal Ministero dell'Istruzione , della Scienza e dello Sport e partecipa anche alle campagne del mese europeo della sicurezza informatica.
Risultati/impatto	Finora, l'iniziativa ha collaborato con diverse organizzazioni e istituzioni, come: Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione, Centro europeo dei consumatori, Agenzia per le reti e i servizi di comunicazione della Repubblica di Slovenia, Commissario per l'informazione della RS, Ufficio per la proprietà intellettuale , Associazione delle banche della Slovenia, Associazione dei consumatori della Slovenia.
Collegamento alla fonte	https://www.varninainternetu.si/

INIZIATIVA 2

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

Nome	Safer Internet Center Slovenia
Posizione	Nazionale
Durata	2005 -
Descrizione	Safer Internet Center (SIC) Slovenia è il progetto nazionale che promuove e garantisce un Internet migliore per i bambini. Il progetto è cofinanziato dall'Agenzia esecutiva europea per la salute e il digitale (HaDEA); in Slovenia il sostegno finanziario arriva anche dall'Ufficio governativo per la sicurezza delle informazioni. Il progetto è gestito da un consorzio di partner coordinato dalla Facoltà di scienze sociali dell'Università di Lubiana, dalla Rete accademica e di ricerca slovena (ARNES), dall'Associazione slovena degli amici della gioventù (ZPMS) e dalla Youth Information and Counseling Centro della Slovenia (MISSS). Dal 2005 SAFE.SI opera come punto nazionale di sensibilizzazione per bambini e ragazzi sull'uso sicuro di internet e dei dispositivi mobili. Le loro attività sono rivolte a quattro gruppi target: bambini, adolescenti, genitori e professionisti (insegnanti, assistenti sociali, animatori giovanili, ecc.). La missione della campagna di sensibilizzazione è quella di informare i giovani utenti di Internet e mobile su come proteggersi dai rischi e utilizzare il web e le altre nuove tecnologie in modo sicuro e responsabile.
Risultati/impatto	SAFE.si incoraggia la cooperazione con le parti interessate slovene e le istituzioni della sfera pubblica e privata, per rendere i bambini e gli adolescenti più sicuri online e per proteggerli da potenziali pericoli e rischi. Ha collaborato con l'Agenzia per le reti e i servizi di comunicazione della Repubblica di Slovenia, l'Associazione per la pediatria, il Ministero dell'istruzione, della scienza e dello sport (preparazione di un piano d'azione per la digitalizzazione dell'istruzione), ecc.
Collegamento	https://safe.si/

alla fonte	

SUGGERIMENTI DI VALUTAZIONE E IMPLEMENTAZIONE

Oltre alle iniziative menzionate, la Slovenia ha contribuito ai sistemi nazionali di sicurezza informatica attraverso programmi di istruzione superiore (ad es. Facoltà di informatica e scienze dell'informazione) e corsi sulla sicurezza informatica a tutti i livelli di istruzione, nonché i risultati di organizzazioni di ricerca. Le associazioni professionali hanno avviato miglioramenti e assistenza per sensibilizzare i vari gruppi target (ad es. Camera di commercio e industria della Slovenia, ISACA, SI-CERT). Sebbene la Slovenia abbia compiuto sforzi per educare i suoi cittadini sulla sicurezza digitale, c'è ancora spazio per miglioramenti.

Per migliorare il livello di conoscenza tra i cittadini, la Slovenia potrebbe attuare iniziative offline, come una promozione nelle scuole primarie e secondarie. La sicurezza digitale potrebbe diventare una parte obbligatoria del curriculum scolastico per garantire che i bambini siano istruiti sui rischi per la sicurezza online fin dalla tenera età. Le iniziative dovrebbero essere estese a gruppi target più ampi, come gli adulti e le imprese. In Slovenia è stata sviluppata una strategia di sicurezza informatica, ma senza un piano d'azione per attuarla.

6.2 Grecia

In Grecia, il digitale e la sicurezza informatica sono diventati sempre più importanti negli ultimi anni poiché il paese è diventato più dipendente dalla tecnologia e da Internet. Il governo greco ha adottato misure per rafforzare le misure di sicurezza informatica e proteggere le infrastrutture critiche, come i sistemi energetici e di trasporto del paese. Nel 2019, il ministero greco per la politica digitale ha lanciato una nuova strategia nazionale per la sicurezza informatica, che comprende una serie di iniziative per migliorare la sicurezza informatica nei settori pubblico e privato. La strategia si concentra su quattro aree chiave: protezione, rilevamento, risposta e ripristino. Include misure come il miglioramento della sicurezza delle infrastrutture critiche, lo sviluppo di campagne di sensibilizzazione sulla sicurezza informatica e il miglioramento della capacità del paese di rispondere alle minacce informatiche. Il governo greco ha inoltre istituito un'autorità nazionale per la sicurezza informatica, responsabile del coordinamento degli sforzi di sicurezza informatica nei settori pubblico e privato. L'autorità lavora per identificare e mitigare i rischi di sicurezza informatica, sviluppare politiche e regolamenti sulla sicurezza informatica e fornire guida e supporto a organizzazioni e individui.

INIZIATIVA 1	
Nome	Strategia nazionale per la sicurezza informatica
Posizione	Nazionale, settore pubblico
Durata	2019 -
Descrizione	La strategia nazionale per la sicurezza informatica della Grecia è stata lanciata nel 2019 dal ministero della politica digitale, delle telecomunicazioni e dell'informazione. La strategia mira a migliorare la sicurezza informatica nei settori pubblico e privato e a proteggere le infrastrutture critiche dalle minacce informatiche. La strategia si basa su quattro pilastri principali: protezione, rilevamento, risposta e ripristino. Questi pilastri sono supportati da una serie di iniziative, tra cui: Rafforzare la sicurezza delle infrastrutture critiche Sviluppare la consapevolezza della sicurezza informatica Migliorare la capacità del Paese di rispondere alle minacce informatiche Promuovere la cooperazione internazionale La strategia nazionale per la cybersicurezza include anche obiettivi e tempistiche specifiche per l'attuazione delle sue iniziative. Nel complesso, la strategia rappresenta un approccio globale al miglioramento della sicurezza informatica in Grecia e alla protezione dalle minacce informatiche.
Risultati/impatto	Migliore consapevolezza della sicurezza informatica Sicurezza rafforzata delle infrastrutture critiche: Funzionalità avanzate di risposta agli incidenti Maggiore cooperazione internazionale Nel complesso, la strategia nazionale per la cybersicurezza ha avuto un impatto positivo sulla cybersicurezza in Grecia. Sebbene ci sia ancora del lavoro da fare per affrontare le minacce e le sfide in

	corso, la strategia ha contribuito a sensibilizzare sui rischi per la sicurezza informatica, migliorare la sicurezza delle infrastrutture critiche, migliorare le capacità di risposta agli incidenti e promuovere la cooperazione internazionale.
Collegamento alla fonte	https://www.trade.gov/market-intelligence/greece-cyber-security-strategy

INIZIATIVA 2	
Nome	Autorità nazionale per la sicurezza informatica
Posizione	Nazionale, settore pubblico
Durata	2019 -
Descrizione	La National Cybersecurity Authority (NCA) è un'agenzia governativa greca responsabile del coordinamento e dell'attuazione delle politiche e delle iniziative di sicurezza informatica nei settori pubblico e privato. L'ANC è stata istituita nel 2019 nell'ambito della strategia nazionale per la cybersicurezza della Grecia. Le principali responsabilità dell'ANC includono: Sviluppo e attuazione di politiche e regolamenti sulla sicurezza informatica: l'ANC è responsabile dello sviluppo di politiche e regolamenti per migliorare la sicurezza informatica in diversi settori in Grecia. Coordinamento degli sforzi di sicurezza informatica: l'ANC lavora per coordinare gli sforzi di sicurezza informatica tra diverse agenzie governative, nonché con organizzazioni del settore privato e partner internazionali. Identificazione e attenuazione dei rischi di cybersicurezza: l'ANC è responsabile dell'identificazione e dell'attenuazione dei rischi di cybersicurezza, compresi quelli relativi alle infrastrutture critiche. Fornire guida e supporto: la NCA fornisce guida e supporto a organizzazioni e individui sulle migliori

	pratiche di sicurezza informatica e sulla risposta agli incidenti.
Risultati/impatto	Poiché l'autorità nazionale per la cybersicurezza (ANC) in Grecia è stata istituita nel 2019, è ancora relativamente presto per valutare appieno i risultati e l'impatto delle sue attività. Tuttavia, dalla sua istituzione si sono verificati diversi sviluppi degni di nota che suggeriscono che l'ANC sta esercitando un impatto positivo sulla cybersicurezza in Grecia. L'ANC ha svolto un ruolo nell'aumentare la consapevolezza dei rischi per la sicurezza informatica e delle migliori pratiche in Grecia, attraverso campagne di sensibilizzazione pubblica, programmi di formazione e altre iniziative. Ciò ha contribuito a migliorare il livello generale di sicurezza informatica nel paese. Nel complesso, dalla sua istituzione nel 2019, l'ANC ha compiuto passi importanti nel miglioramento della sicurezza informatica in Grecia. Anche se c'è ancora del lavoro da fare per affrontare le attuali sfide alla sicurezza informatica, l'ANC ha avuto un impatto positivo e sta svolgendo un ruolo fondamentale nella protezione della Grecia contro minacce informatiche.
Collegamento alla fonte	https://www.concordia-h2020.eu/consortium/national-cyber-authority-ncsa/

SUGGERIMENTI DI VALUTAZIONE E IMPLEMENTAZIONE

Anche se la Grecia ha compiuto progressi nella sensibilizzazione sulla sicurezza digitale tra i suoi cittadini, c'è ancora spazio per miglioramenti. Ecco alcune possibili soluzioni per migliorare il livello di conoscenza e consapevolezza della sicurezza digitale in Grecia, con particolare attenzione a come altri paesi/istituzioni possono implementare iniziative simili:

INIZIATIVE EDUCATIVE: una possibile soluzione è aumentare l'enfasi sulla sicurezza digitale nelle istituzioni educative, come scuole e università. I governi e le istituzioni possono sviluppare e attuare programmi educativi che insegnino ai giovani competenze e pratiche di sicurezza informatica di base. Questi programmi possono anche rivolgersi agli adulti che potrebbero non aver avuto l'opportunità di conoscere la sicurezza digitale in precedenza nel loro percorso.

CAMPAGNE DI SENSIBILIZZAZIONE PUBBLICA: i governi possono organizzare campagne di sensibilizzazione pubblica per aumentare la consapevolezza sull'importanza della sicurezza digitale e per fornire indicazioni su come proteggersi online. Queste campagne possono assumere forme diverse, come poster, pubblicità e post sui social media.

CERTIFICAZIONI DI CYBERSECURITY: Un'altra soluzione è stabilire certificazioni di sicurezza informatica che le persone possono ottenere dopo aver completato un corso di formazione. Queste certificazioni possono fornire agli individui una qualifica riconosciuta che dimostri le loro conoscenze e competenze in materia di sicurezza informatica.

COLLABORAZIONE CON IL SETTORE PRIVATO: i governi possono collaborare con le organizzazioni del settore privato per fornire formazione e supporto ai cittadini sulla sicurezza digitale. Ad esempio, le società di telecomunicazioni possono fornire indicazioni sull'utilizzo sicuro di Internet ai propri clienti.

COOPERAZIONE INTERNAZIONALE: i paesi possono collaborare a iniziative per migliorare la sicurezza digitale. Ciò può includere la condivisione di informazioni sulle minacce informatiche e sulle migliori pratiche, esercitazioni congiunte di formazione e risposte coordinate agli incidenti informatici.

6.3 Italia

L'Italia ha compiuto passi significativi verso il miglioramento della sua posizione complessiva in materia di sicurezza digitale/informatica. Il paese ha riconosciuto l'importanza della sicurezza informatica e sta adottando varie iniziative per migliorare le sue capacità di sicurezza informatica. Nel 2021 è stata istituita la National Cybersecurity Agency (ACN) che mira ad aumentare la cyber security nazionale e la resilienza per lo sviluppo digitale del Paese, raggiungere l'autonomia strategica nazionale ed europea nel settore digitale, promuovere corsi di formazione specifici per lo sviluppo della forza lavoro del settore, sostenere campagne di sensibilizzazione, promuovere una diffusa cultura della cybersecurity e sviluppare azioni e progetti internazionali per un ciberspazio globale sicuro. Il governo ha anche introdotto la National Cybersecurity Strategy (NCS), che mira a rafforzare la resilienza digitale del paese e le capacità contro le minacce informatiche. Si concentra sulla protezione delle infrastrutture critiche, la condivisione delle informazioni, la ricerca e lo sviluppo, la formazione e l'istruzione.

INIZIATIVA 1	
Nome	Strategia Cloud Italia

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

Posizione	Per la Pubblica Amministrazione italiana
Durata	15/12/2021 -
Descrizione	La Strategia Cloud Italia, realizzata dal Dipartimento per la Trasformazione Digitale e dall'Agenzia Nazionale per la Cybersecurity (ACN), contiene le linee guida strategiche per il percorso di migrazione dei dati e dei servizi digitali della Pubblica Amministrazione verso il cloud, attraverso un sistema di classificazione dei dati a 3 livelli . Strategico: dati e servizi la cui compromissione potrebbe avere un impatto sulla sicurezza nazionale. Critico: dati e servizi la cui compromissione potrebbe arrecare pregiudizio al mantenimento di funzioni rilevanti per la società, la salute, la sicurezza e il benessere economico e sociale del Paese. Ordinario: dati e servizi la cui compromissione non determina l'interruzione dei servizi dello Stato o, comunque, pregiudizio per il benessere economico e sociale del Paese. Con l'obiettivo di guidare e promuovere l'adozione sicura, controllata e completa delle tecnologie cloud da parte del settore pubblico, in linea con i principi di tutela della privacy e con le raccomandazioni delle istituzioni europee e nazionali.
Risultati/impatto	Le infrastrutture digitali saranno più affidabili e sicure e la Pubblica Amministrazione potrà rispondere in modo organizzato agli attacchi informatici, garantendo continuità e qualità nell'utilizzo dei dati e dei servizi.
Collegamento alla fonte	https://www.acn.gov.it/

INIZIATIVA 2	
Nome	Safer Internet Center - Generazioni connesse
Posizione	Nazionale

Durata	1/07/2016 -
Descrizione	Il progetto Safer Internet Center (SIC) - Connected Generations è cofinanziato dalla Commissione Europea nell'ambito del programma Europa Digitale, è coordinato dal Ministero dell'Istruzione e del Merito ed è membro di un network promosso dalla Commissione Europea sulla piattaforma online "Better Internet for Kids" gestito da European Schoolnet, in stretta collaborazione con INSAFE (rete che riunisce tutte le SIC europee) e Inhope (rete che riunisce tutte le hotline europee). La Missione Educativa di SIC è fornire informazioni, consulenza e supporto a bambini, ragazzi, genitori, insegnanti ed educatori per facilitare la segnalazione di materiale illegale online. L'obiettivo generale è quello di sviluppare servizi con contenuti innovativi e di qualità superiore al fine di garantire ai giovani utenti la sicurezza online considerando, allo stesso tempo, l'investimento connesso come un'opportunità 'virtuosa' per la crescita 'sociale' ed economica dell'intera comunità .
Risultati/impatto	Fornire supporto e consulenza per aumentare la consapevolezza dei pericoli online.
Collegamento alla fonte	https://www.generazioniconnesse.it/site/it/safer-internet-centre/

SUGGERIMENTI DI VALUTAZIONE E IMPLEMENTAZIONE

In Italia ci sono diverse iniziative in tema di cybersecurity. È stata inoltre sviluppata una Strategia Nazionale di Cybersecurity 2022-2026 finalizzata alla pianificazione, al coordinamento e all'attuazione di misure volte a rendere il Paese più sicuro e resiliente. Tale strategia prevede il raggiungimento di 82 misure entro il 2026. Un valido suggerimento potrebbe essere quello di inserire nei piani educativi scolastici le materie della sicurezza online e delle lezioni di cybersecurity, non lasciandole solo alla discrezionalità di corsi aggiuntivi, attività extrascolastiche o curricula delle scuole in cui si studia materie relative alla formazione informatica.

6.4 Cipro

Secondo OCECPR "La visione della strategia di sicurezza informatica di Cipro è il funzionamento delle tecnologie dell'informazione e della comunicazione a Cipro con i necessari livelli di sicurezza a vantaggio di ogni utente". L'obiettivo principale della strategia è sviluppare e mantenere un ambiente elettronico sicuro e protetto a Cipro per tutte le imprese ei cittadini, sviluppando politiche nell'ambito della cooperazione tra tutte le autorità competenti. In questa direzione, Cipro ha approvato una serie di azioni che sono state promosse a livello nazionale, come la creazione di un quadro per la sicurezza e l'integrità delle infrastrutture informatiche e la sensibilizzazione di tutte le parti interessate e della società cipriota sulle questioni di sicurezza rilevanti e la formazione di gruppi di risposta alle emergenze informatiche (CCERT/CSIRT). Inoltre, Cipro si impegna a contribuire alla collaborazione europea e internazionale nella risposta alle minacce nel cyberspazio.

INIZIATIVA 1	
Nome	Centro nazionale di coordinamento per la cybersicurezza (NCCC-CY) per la Repubblica di Cipro
Posizione	Nazionale
Durata	21 dicembre 2021 -
Descrizione	L'autorità per la sicurezza digitale (DSA) è stata designata come NCCC-CY da una decisione del Consiglio dei ministri di Cipro nel dicembre 2021. Le sue principali responsabilità sono fornire conoscenze e facilitare l'accesso al know-how in materia di sicurezza informatica industriale, tecnologica e questioni di ricerca. Inoltre, è la promozione e l'agevolazione della partecipazione di start-up, PMI e comunità accademiche e di ricerca a livello nazionale a progetti transfrontalieri e ad azioni di cybersicurezza finanziate dai pertinenti programmi dell'Unione. Inoltre, il Centro fornisce assistenza tecnica alle parti interessate supportandole nella fase di candidatura per i progetti gestiti dal Centro di competenza e cerca di stabilire collaborazioni con attività pertinenti a livello nazionale, regionale e locale, come le politiche nazionali in materia di ricerca, sviluppo e innovazione in l'area della

	sicurezza informatica, e in particolare quelle politiche enunciate nella Strategia nazionale per la sicurezza informatica .
Risultati/impatto	Dal 4 maggio 2022 i DSA in collaborazione con la Research and Innovation Foundation - CY sono in grado di attingere e canalizzare i fondi disponibili per la sicurezza informatica a seguito dell'approvazione della sua proposta da parte della Commissione Europea. Perché DSA potesse funzionare in questa direzione, doveva essere valutata in modo approfondito dalla Commissione Europea in termini di capacità di gestione dei fondi in questione. La Commissione Europea ha effettuato la valutazione dopo la presentazione della proposta il 17 febbraio 2022 e l'ha approvata il 4 maggio.
Collegamento alla fonte	https://dsa.cy/it/attività/nccc

SUGGERIMENTI DI VALUTAZIONE E IMPLEMENTAZIONE

Oltre al CCERT, ci sono varie iniziative volte ad aumentare la consapevolezza della sicurezza informatica e promuovere le migliori pratiche. Questi includono l'annuale Cyprus Cybersecurity Challenge, che cerca di identificare e sviluppare i migliori talenti della sicurezza informatica del paese, e l'istituzione della Cyprus Cybersecurity Association, che mira a promuovere la ricerca, l'istruzione e l'innovazione sulla sicurezza informatica. DSA lavora per aumentare la consapevolezza della sicurezza informatica e sviluppare competenze informatiche in vari settori di attività. Organizza corsi di formazione, workshop e webinar e offre sessioni informative per studenti interessati a studiare la sicurezza informatica, le PMI e gli anziani. Il Ministero dell'Istruzione e della Cultura ha anche implementato programmi educativi sulla cybersicurezza nelle scuole. Questi programmi mirano a fornire agli studenti le conoscenze e le competenze necessarie per proteggersi online e aumentare la consapevolezza sulle minacce informatiche.

Tuttavia, vi è ancora margine di miglioramento nel settore della sicurezza informatica/digitale a Cipro. In particolare, si potrebbero dedicare maggiori risorse ai programmi di istruzione e formazione sulla cybersicurezza, in particolare per le PMI, che potrebbero essere più vulnerabili agli attacchi informatici. Inoltre, una maggiore collaborazione tra il governo, il mondo accademico e il settore privato potrebbe contribuire a rafforzare la posizione complessiva della sicurezza informatica del paese.

6.5 Bulgaria

La Bulgaria ha compiuto progressi nel miglioramento della cybersicurezza con una strategia nazionale per la cybersicurezza, una legge sulla protezione dei dati personali e una direttiva NIS. L'Agenzia statale per la governance elettronica coordina le politiche e fornisce formazione. CERT Bulgaria rileva e risponde alle minacce, mentre il Cybersecurity Competence Center mira a promuovere le competenze. Le sfide includono la carenza di professionisti qualificati, la scarsa consapevolezza pubblica e i recenti attacchi informatici.

INIZIATIVA 1	
Nome	Agenzia statale per l'e-government (SEGA)
Posizione	Nazionale, settore pubblico
Durata	2016 -
Descrizione	La State e-Government Agency (SEGA) è responsabile della governance elettronica del paese e delle politiche di sicurezza informatica. L'agenzia si coordina con altri enti governativi e fornisce formazione sulla sicurezza informatica ai dipendenti del settore pubblico.
Risultati/impatto	SAEG ha lavorato per migliorare le capacità di sicurezza informatica del paese promuovendo comunicazioni elettroniche sicure, implementando misure di sicurezza delle informazioni e conducendo controlli regolari dei sistemi informativi del governo.
Collegamento alla fonte	https://www2.e-gov.bg/en/about_us

INIZIATIVA 2	
Nome	Programma educativo nazionale sulla sicurezza informatica

Posizione	Scuole superiori nazionali (dal 7° al 12° grado)
Durata	2016 -
Descrizione	Questo programma è rivolto agli studenti dalla settima alla dodicesima elementare e si concentra sulla sensibilizzazione sui rischi della sicurezza informatica, sulla promozione di comportamenti sicuri e responsabili online e sull'incoraggiamento degli studenti a prendere in considerazione una carriera nella sicurezza informatica. Ha 3 componenti principali: lezioni, esercitazioni e concorsi. L'iniziativa mira a promuovere una cultura della consapevolezza e dell'educazione alla sicurezza informatica in Bulgaria e a contribuire a creare una forza lavoro qualificata nel campo della sicurezza informatica.
Risultati/impatto	Il programma ha contribuito ad aumentare il livello di interesse per l'istruzione e le carriere in materia di cybersicurezza tra i giovani in Bulgaria, incoraggiando nel contempo le organizzazioni nazionali a formare partenariati per rafforzare le capacità di cybersicurezza del paese. Ha inoltre portato alla nascita di una nuova generazione di professionisti della cybersicurezza dotati delle conoscenze e delle competenze necessarie per proteggere l'infrastruttura digitale della Bulgaria.
Collegamento alla fonte	https://ccdcoe.org/uploads/2018/10/Bulgaria_National-program-Digital-Bulgaria-2025_2019_original.pdf

SUGGERIMENTI DI VALUTAZIONE E IMPLEMENTAZIONE

Sebbene la Bulgaria stia adottando le misure necessarie per progredire nella sicurezza informatica, c'è sempre spazio per miglioramenti. Ad esempio, il programma educativo nazionale sulla cybersicurezza potrebbe essere ampliato per raggiungere un pubblico più ampio, compresi gli adulti e le imprese. Detto questo, è una buona idea rivolgersi a un pubblico giovane, poiché sono loro a plasmare il futuro. Questo è qualcosa che anche altri paesi potrebbero implementare. Oltre alle iniziative educative, in Bulgaria sono necessarie politiche e normative di sicurezza informatica più complete per proteggere dalle minacce informatiche. Ciò include leggi e normative

più severe sulla protezione dei dati, nonché migliori standard di sicurezza informatica per le infrastrutture critiche.

6.6 Germania

Le questioni relative all'educazione digitale/cybersecurity sono una priorità per la Germania per essere in grado di affrontare le sfide poste dai nuovi sviluppi nella governance informatica e nella transizione digitale. In particolare, il governo tedesco, in collaborazione con le parti interessate del settore, ha proceduto allo sviluppo di una strategia digitale.

La "Digital Strategy 2025" delinea le priorità del governo tedesco, ovvero sviluppare le competenze digitali e promuovere l'uso di nuovi strumenti per migliorare i processi di digitalizzazione della Germania. La strategia si basa su 10 pilastri importanti per la digitalizzazione, compreso un pilastro incentrato sull'introduzione dell'educazione digitale in tutte le fasi della vita di un individuo.

La strategia digitale tedesca 2025 è stata adottata nel 2016 per 10 anni. Le azioni della Strategia mirano non solo a consentire all'economia tedesca di affrontare le nuove sfide, ma anche a garantire la sua posizione di leader sia in termini di qualità che di tecnologia per i prossimi anni, combinando i tradizionali vantaggi competitivi con la tecnologia più recente, metodi moderni e speciali programmi di sostegno.

INIZIATIVA 1	
Nome	Strategia di sicurezza informatica per la Germania
Posizione	Nazionale
Data	2021

Descrizione	L'8 settembre 2021, il gabinetto federale ha adottato la strategia di sicurezza informatica 2021 per la Germania preparata dal ministro federale dell'interno e della comunità. Fornisce il quadro per la sicurezza informatica nei prossimi cinque anni. La sicurezza informatica è un compito per il presente e uno dei compiti importanti per il futuro. È un'era definita dalle nuove opportunità del mondo digitale, come l'intelligenza artificiale, i dispositivi elettronici connessi e nuovi mezzi di comunicazione innovativi. Per poter sfruttare queste opportunità, è essenziale ridurre al minimo i rischi. La Strategia tedesca per la sicurezza informatica 2021 sostituisce la Strategia tedesca per la sicurezza informatica 2016. La strategia definisce la direzione essenziale a lungo termine della politica di sicurezza informatica del governo federale, suddivisa in principi guida, aree di azione e obiettivi strategici. La strategia per la sicurezza informatica si concentra su quattro aree di azione: società, industria privata, governo e UE/affari internazionali. Nell'ambito di queste aree di azione sono stati fissati un totale di 44 obiettivi strategici.
Risultati/impatto	L'Ufficio federale della sicurezza informatica diventerà un hub per le agenzie federali e statali per lavorare insieme nella prevenzione della criminalità informatica, creando un terzo pilastro nell'architettura globale della sicurezza informatica federale: prenderà il suo posto accanto all'Ufficio federale di polizia criminale (BKA), che già svolge questo ruolo nel settore della polizia tedesca e l'Ufficio federale per la protezione della costituzione, che lo svolge nella comunità dell'intelligence tedesca interna. La strategia rafforza la sovranità digitale e quindi la trasformazione digitale sicura del nostro Paese. L'economia digitale della Germania sarà rafforzata attraverso un sostegno mirato per le tecnologie abilitanti fondamentali e il collegamento in rete con i ricercatori pertinenti. Un approccio "security by

	design" sarà applicato fin dall'inizio alle tecnologie abilitanti emergenti e fondamentali.

INIZIATIVA 2	
Nome	Centri di ricerca sulla sicurezza informatica
Posizione	Nazionale
Data	2011
Descrizione	Il finanziamento della ricerca ha l'obiettivo di finanziare lo sviluppo di nuove idee e tecnologie. Il finanziamento è previsto per progetti in un ampio spettro di aree di ricerca. La gamma copre tutto, dalla ricerca di base nelle scienze naturali, allo sviluppo sostenibile rispettoso dell'ambiente, alle nuove tecnologie, alle tecnologie dell'informazione e della comunicazione, alle scienze della vita, alla progettazione del lavoro, al finanziamento strutturale della ricerca presso gli istituti di istruzione superiore al sostegno all'innovazione e al trasferimento tecnologico. Il Ministero federale dell'istruzione e della ricerca (BMBF) sta finanziando tre Kompetenzzentren für IT-Sicherheitsforschung (Centri di ricerca sulla sicurezza informatica). Singole università eccezionali o istituti di ricerca non universitari vengono finanziati come centri di ricerca per la sicurezza informatica. I centri si concentrano tematicamente e organizzativamente sulle sfide più importanti nel campo della sicurezza IT.
Risultati/impatto	Il compito di questi centri è sviluppare strategie a lungo termine per la sicurezza informatica e realizzare progetti di ricerca correlati per affrontare le sfide attuali e future.

La Germania ha compiuto sforzi significativi per educare i suoi cittadini sulla sicurezza digitale, ma c'è spazio per miglioramenti. Sebbene siano state implementate iniziative come campagne di sensibilizzazione pubblica, programmi scolastici e risorse finanziate dal governo, la natura in continua evoluzione delle minacce digitali richiede sforzi continui.

Per migliorare il livello di conoscenza dei cittadini sulla sicurezza digitale, la Germania può prendere in considerazione le seguenti soluzioni:

- Programmi integrati di formazione per il settore pubblico e privato
- Iniziative del settore pubblico e privato
- Piattaforme di scambio di informazioni
- Campagne di sensibilizzazione
- Per implementare iniziative simili, altri paesi/istituzioni possono:
- Adattare i programmi esistenti: studiare le iniziative di successo della Germania e di altri paesi per adattarle e implementarle nei propri sistemi educativi.
- Lavora con esperti del settore: collabora con esperti del settore locale e professionisti della sicurezza informatica per sviluppare contenuti educativi pertinenti e pratici.
- Promuovere partenariati pubblico-privato: incoraggiare partenariati tra agenzie governative, aziende private e organizzazioni senza scopo di lucro.
- Adatta i canali di comunicazione: utilizza un mix di canali di comunicazione per raggiungere un vasto pubblico.
- Utilizzare una varietà di canali di comunicazione per sfruttare un mix di canali: valutare regolarmente l'efficacia delle iniziative di educazione alla sicurezza digitale.

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

7 Conclusione

L'obiettivo principale del progetto DiscVET era fornire agli insegnanti e ai formatori dell'IFP le competenze necessarie nella sovranità digitale per formare efficacemente gli altri e promuovere un ambiente digitale sicuro. Con un focus sulla creazione di materiali di formazione innovativi ed esercizi di simulazione interattivi, il progetto mira a migliorare la preparazione alla sicurezza digitale dei partecipanti. Tuttavia, la nostra visione si estende oltre questo obiettivo immediato. Miriamo a contribuire all'educazione della generazione di europei più consapevoli e altamente qualificati fornendo agli insegnanti e ai formatori dell'IFP le conoscenze e le competenze necessarie per la sovranità digitale.

Riconoscendo l'importanza delle competenze digitali, degli ambienti digitali sicuri e delle opportunità di apprendimento permanente, l'UE ha adottato un approccio globale alla cybersicurezza, all'istruzione digitale e al finanziamento della ricerca e dell'innovazione. Questo impegno è evidente nelle strategie, nei regolamenti e nelle iniziative dell'UE volte a dotare le persone delle necessarie competenze digitali e promuovere pratiche digitali sicure in tutta Europa.

Per garantire l'efficacia e la qualità del progetto DiscVET, apprezziamo il feedback e la valutazione forniti dai partecipanti. Analizzando attentamente e affrontando eventuali problemi identificati, ci sforziamo di fornire la versione finale e definitiva dei risultati del progetto. Il rapporto di valutazione servirà come risorsa preziosa, guidandoci nel migliorare i risultati del progetto e garantendo l'elevata soddisfazione e l'utilità del progetto tra il gruppo target.

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

8 Bibliografia

- UpGuard: sicurezza informatica delle infrastrutture digitali critiche
  - Estratto da: https://www.upguard.com/blog/cybersecurity-regulations-in-the-european-union#toc-3
- Commissione europea: Apprendimento digitale e TIC nell'istruzione
  - Estratto da: https://digital-strategy.ec.europa.eu/en/policies/digital-learning
- Commissione europea: Piano d'azione per l'educazione digitale - Azione 5
  - Estratto da: https://education.ec.europa.eu/focus-topics/digital-education/action-plan/action-5
- Commissione europea: Piano d'azione per l'educazione digitale - Azione 6
  - Estratto da: https://education.ec.europa.eu/focus-topics/digital-education/action-plan/action-6
- Commissione europea: Piano d'azione per l'educazione digitale - Azione 7
  - Estratto da: https://education.ec.europa.eu/focus-topics/digital-education/action-plan/action-7
- Commissione Europea: DigComp Framework
  - Estratto da: https://joint-research-centre.ec.europa.eu/digcomp/digcomp-framework_en#ref-4-safety
- Christine Redecker: Quadro europeo per la competenza digitale degli educatori: DigCompEdu
  - Estratto da: https://publications.jrc.ec.europa.eu/repository/handle/JRC107466
- UpGuard: Normativa sui Finanziamenti e la Ricerca (Sostegno alla Ricerca e all'Innovazione)
  - Estratto da: https://www.upguard.com/blog/cybersecurity-regulations-in-the-european-union#toc-4
- Francesca Bernasconi: L'educazione digitale secondo l'UE: strumenti utili
  - Estratto da: https://www.elearningnews.it/en/news-C-27/digital-education-according-to-the-eu-useful-tools-AR-1488/