Il manuale CYBER.VET.EU

Improving Cybersecurity readiness of the European Vocational education and training sector

2020-1-DE02-KA226-VET-008327

TANDEM PLUS NETWORK con la collaborazione del consorzio di CYBER.VET.EU

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

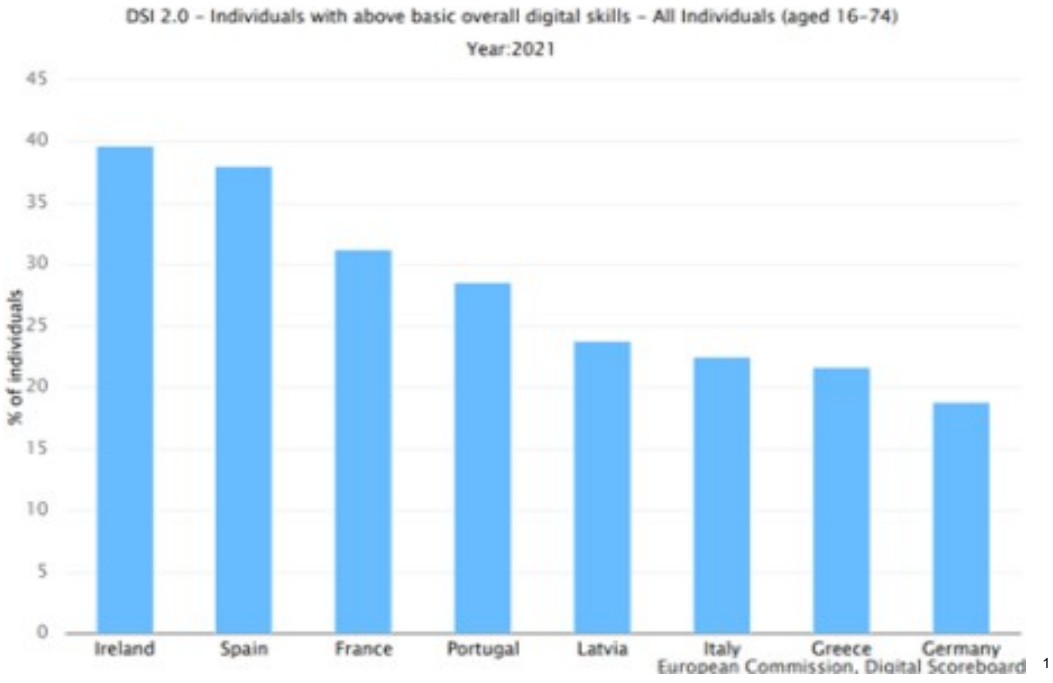
Indice

a) L'implementazione del Progetto CYBER.VET.EU

L'Unione Europea sta affrontando una sfida epocale rappresentata dalla pandemia di Covid-19. Molti settori sono fortemente colpiti da queste crisi e l'istruzione è sicuramente uno di questi.

Sempre più utenti sono ora costretti a utilizzare lezioni o formazione online, quindi l'importanza di riconoscere le minacce quotidiane alla nostra sicurezza è ora più importante che mai. Questo tema è riconosciuto come fondamentale anche dalla Commissione Europea che ogni anno organizza un Mese Europeo della Cyber Security, il cui sito web include già del materiale didattico e specifiche campagne di sensibilizzazione come il "Get cyber skilled" del 2018 .

Il progetto CYBER.EU.VET comprende 8 partner (NGO NEST – Germania (LEADER), MEATH COMMUNITY RURAL AND SOCIAL DEVELOPMENT PARTNERSHIP LIMITED – Irlanda, TANDEM PLUS – A EU network based in France, COFAC COOPERATIVA DE FORMACAO E ANIMACAO CULTURAL CRL- Portogallo, LATVIJAS ASOCIACIJA EIROPAS KOPIENAS STUDIJAM – Lettonia, ASOCIACION EDUCATIVA POR LA
INTEGRACION Y LA IGUALDAD – Spagna, INECIA DIGITAL – Spagna, Extrafondente Open Source – Italia)



[1]

[1] ESMS Indicator Profile (ESMS-IP) Compiling agency: Eurostat, the statistical office of the European Union.

L'obiettivo principale di CYBER.VET.EU è rafforzare la capacità dell'IFP europea di riconoscere e gestire le minacce alla sicurezza informatica (ad esempio attacchi di phishing, botnet, frodi finanziarie e bancarie, frodi di dati) in un contesto storico in cui la formazione online è sempre più utilizzata.

i. Impatto del progetto

Il progetto ha avuto un impatto a livello locale, regionale e nazionale coinvolgendo diversi livelli di parti interessate, offrendo soluzioni su misura per soddisfare le esigenze dei livelli locali, ma allineate a un livello superiore, sviluppando, attraverso il partenariato, materiale formativo applicabile in tutta l'UE e standard.

In particolare, l'impatto sui partecipanti diretti e sui principali gruppi target è stato:

- Educatori VET - Una capacità di insegnamento rafforzata, aggiungendo alle loro competenze una conoscenza delle principali minacce alla sicurezza digitale.
- Educatori e studenti VET - competenze digitali migliorate grazie al materiale di formazione educativa.
- Educatori e studenti dell'IFP: una maggiore consapevolezza delle minacce e dei loro rischi reali, sia economici che sociali.
- Gli istituti di formazione professionale saranno più preparati ad affrontare i rischi di sicurezza informatica con gli strumenti CYBER.VET.EU sia per i loro educatori che per gli studenti.

ii. Target del progetto

Si prevede che il progetto avrà un impatto positivo ea lungo termine sulle diverse parti interessate coinvolte nel progetto, in particolare:

- Studenti VET
- Volontari esperti di sicurezza informatica
- Reti di istituti di formazione professionale
- I responsabili politici

iii. Obiettivi del Progetto

- Il primo obiettivo specifico sarà quello di avere educatori IFP più preparati sulla gestione delle minacce alla sicurezza informatica, dato il loro ruolo centrale nel trasferimento di conoscenze di buone pratiche e competenze ai loro studenti.

- Il secondo obiettivo specifico è quello di aumentare la consapevolezza tra gli insegnanti, gli studenti e i loro parenti dell'IFP sull'importanza di riconoscere tali rischi quotidiani, che possono avere un impattosia economico che sociale su tutti i cittadini europei.
- Il terzo obiettivo specifico è supportare le istituzioni pubbliche e gli istituti di formazione professionaleaffinché siano più pronti ad affrontare questo tipo di sfide, fornendo loro linee guida per le future implementazioni.

iv. Risultati:

- O1: Analisi della ricerca: principali sfide e migliori pratiche per la sicurezza informatica (partner responsabile: ONG NEST BERLIN EV - E10166639)
- O2: materiale di formazione sulla consapevolezza della sicurezza informatica per il settore VET (partner responsabile: INERCIA DIGITAL SL (E10145080,)
- O3: Training for trainers toolkit (partner responsabile INERCIA DIGITAL SL (E10145080)
- O4: Il manuale sulla sicurezza informatica per gli istituti di formazione professionale: buone pratiche, materiale formativo e linee guida per future implementazioni (Partner responsabile TANDEM PLUS - E10103913)

Parallelamente allo sviluppo dei risultati intellettuali, l'altro obiettivo del progetto è diffondere i nostri risultati e risultati in tutta l'UE a potenziali partecipanti, moltiplicatori e parti interessate, per aumentare l'impatto e la rilevanza di CYBER.EU.VET.

v. Cosa è la cybersicurezza?

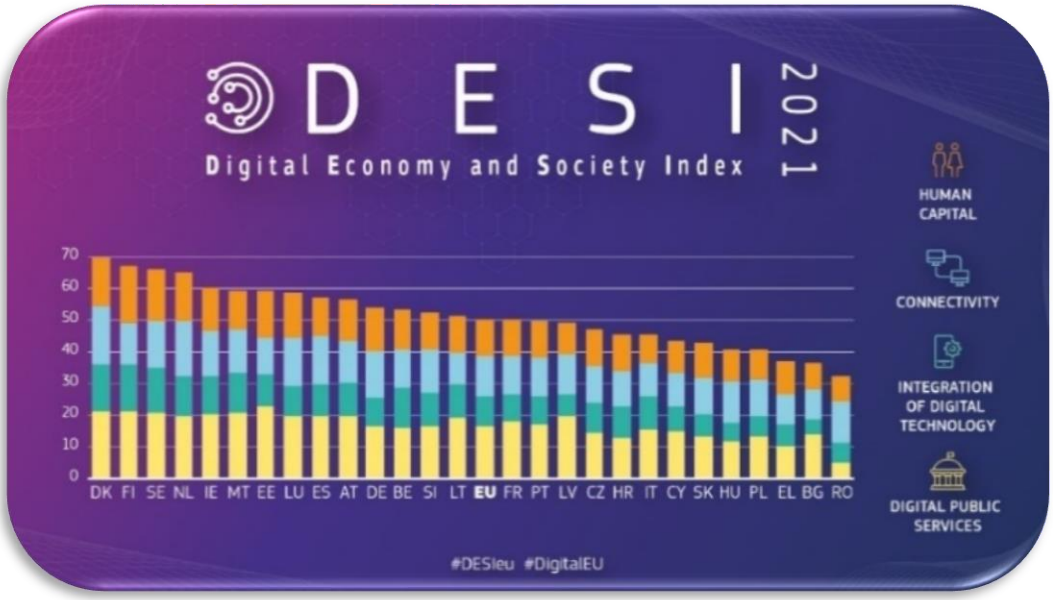
La definizione formale di sicurezza informatica nel diritto dell'UE si trova nel testo dell'EU Cybersecurity Act: "per sicurezza informatica si intendono le attività necessarie per proteggere le reti e i sistemi informativi, gli utenti di tali sistemi e altre persone colpite da minacce informatiche" (art. 2.1).

Il diritto dell'UE, pur adottando l'approccio della *"protezione delle reti e dei sistemi informativi",* sottolinea anche che la sicurezza informatica protegge non solo i sistemi informativi, ma anche (e forse ancora più importante) le persone, indipendentemente dal fatto che gli utenti di tali sistemi o terzi siano in qualche modo interessati da minacce informatiche.

Nel dicembre 2020 la Commissione europea e il Servizio europeo per l'azione esterna (SEAE) hanno presentato una nuova strategia di sicurezza informatica dell'UE volta a costruire la resilienza alle minacce informatiche e a garantire che i cittadini e le imprese beneficino di tecnologie digitali affidabili.

Il regolamento (UE) 2021/887 che istituisce il Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza e la rete dei centri nazionali di coordinamento istituisce il Centro europeo di competenza sulla cibersicurezza (ECCC) e la rete dei centri nazionali di coordinamento (la "rete") e Stabilisce norme per i centri nazionali di coordinamento (NCC) e per l'istituzione della comunità delle competenze in materia di cibersicurezza.

Il Centro europeo di competenza sulla cibersicurezza aiuta l'UE a rafforzare la leadership dell'UE nella cibersicurezza migliorando la fiducia e la sicurezza, comprese la riservatezza, l'integrità e l'accessibilità dei dati, sostenendo la resilienza e l'affidabilità delle reti e dei sistemi informativi, comprese le infrastrutture critiche e l'hardware e il software di uso comune.



vi. Principali sfide digitali in Europa

- Circa 70 milioni di europei non hanno sufficienti capacità di lettura, scrittura e calcolo
- Il 24% della popolazione dell'UE non ha un diploma di istruzione secondaria superiore
- Il 13% degli europei non ha mai utilizzato Internet

• Il 43% della popolazione dell'UE e il 35% della forza lavoro dell'UE hanno competenze digitali insufficienti
• Il 42% di chi non ha competenze digitali è disoccupato
• Nativi digitali ≠ competenza digitale

vii. Background

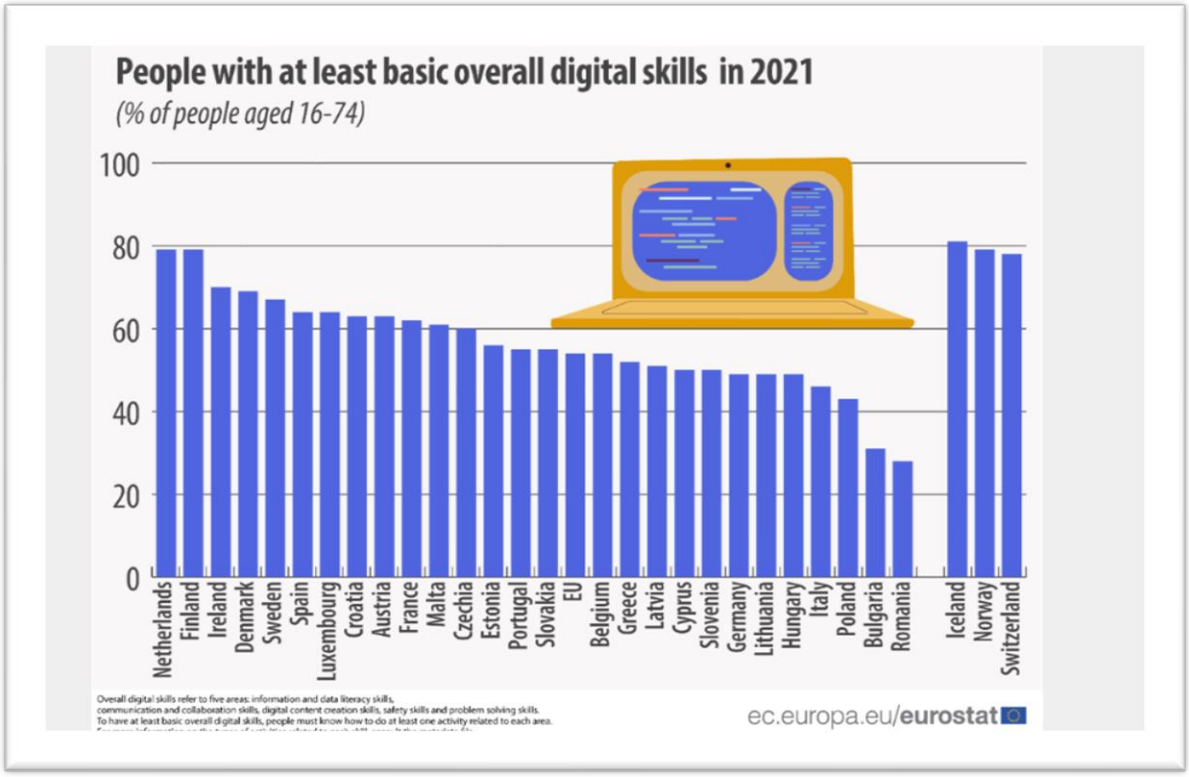
Oltre il 70% delle imprese ha affermato che la mancanza di personale con adeguate competenze digitali è un ostacolo agli investimenti. L'Europa deve inoltre affrontare una carenza di esperti digitali in grado di sviluppare tecnologie all'avanguardia a vantaggio di tutti i cittadini.

Una forte economia digitale alimentata da europei con competenze digitali è fondamentale per l'innovazione, la crescita, l'occupazione e la competitività europea. La diffusione delle tecnologie digitali sta avendo un impatto enorme sul mercato del lavoro e sul tipo di competenze necessarie nell'economia e nella società. Gli Stati membri, le imprese, i fornitori di formazione, la Commissione europea e altre organizzazioni devono collaborare per affrontare il divario di competenze digitali. Per seguire lo sviluppo della transizione digitale e il divario delle competenze digitali, la Commissione pubblica annualmente il DESI [Indicatore delle competenze digitali]. Tiene traccia delle prestazioni digitali degli Stati membri in diverse aree per monitorare i progressi e individuare dove sono necessari ulteriori sforzi.

Nel 2021, il 54% delle persone nell'UE di età compresa tra 16 e 74 anni aveva almeno competenze digitali complessive di base.

Nel 2021, la percentuale di persone di età compresa tra 16 e 74 anni che possedeva almeno competenze digitali complessive di base era più alta nei Paesi Bassi e in Finlandia (entrambi 79%), seguiti dall'Irlanda (70%). La quota più bassa si registra invece in Romania (28%), seguita da Bulgaria (31%) e Polonia (43%).

Gli indicatori delle competenze digitali sono alcuni degli indicatori chiave di prestazione nel contesto del decennio digitale, che definisce la visione dell'UE per la trasformazione digitale. La bussola digitale stabilisce l'obiettivo che l'80% dei cittadini dell'UE di età compresa tra 16 e 74 anni abbia almeno competenze digitali di base entro il 2030.



Torna all'indice ☐

b) Le competenze digitali dei formatori

i. Germania

Il rapporto sui dati sull'IFP (2019) elaborato dall'Istituto federale tedesco per l'istruzione e la formazione professionale (BIBB) ha affermato che "la digitalizzazione rafforzerà i cambiamenti strutturali del mercato del lavoro", indicando la necessità di un cambiamento delle capacità di formazione all'interno dei rispettivi campi.

Come delineato nella Risoluzione della Conferenza permanente dei Ministri dell'Istruzione e degli Affari culturali (2016-2017), l'area della formazione professionale, la promozione delle competenze professionali nel contesto del lavoro digitale e dei processi aziendali è una parte essenziale del competenza degli insegnanti come punto di partenza per le loro attività didattiche.

ii. Irlanda

Una delle strategie chiave dell'Irlanda per quanto riguarda le competenze digitali degli educatori IFP è la strategia digitale nazionale, lanciata nel luglio 2013. La strategia si concentra sull'impegno digitale e sottolinea come l'Irlanda possa trarre vantaggio da una società impegnata digitalmente.
Per quanto riguarda le competenze digitali degli educatori dell'IFP, le prove continuano a evidenziare che esiste un divario crescente tra gli educatori che utilizzano i dispositivi digitali nella loro classe come strumento di apprendimento e quelli che non lo fanno.

iii. Portogallo

Il sistema nazionale delle qualifiche ha riorganizzato l'IFP in un unico sistema in cui i programmi portano a una doppia certificazione. L'IFP per adulti è parte integrante del sistema nazionale delle qualifiche, avendo programmi di istruzione e formazione per adulti e riconoscimento e convalida dell'apprendimento precedente come elementi chiave. Il Portogallo ha compiuto progressi significativi per quanto riguarda il livello di istruzione, ma rimane inferiore alla media dell'UE. Sebbene inferiore al 2015 (73,7%), nel 2019 la quota di persone con basso livello o nessuna qualifica era del 50,2%, la più alta dell'UE.

iv. Italia

Nel campo dell'istruzione gli interventi sono stati realizzati principalmente attraverso l'attuazione del Piano Nazionale Scuola Digitale. Le linee guida del Ministero dell'Istruzione, dell'Università e della Ricerca hanno avviato una strategia complessiva di innovazione per la scuola italiana e per un nuovo posizionamento del suo sistema educativo nell'era digitale. La maggior parte degli interventi per la formazione del personale scolastico è stata rivolta alle scuole primarie e secondarie, che rappresentano

la maggioranza delle scuole in Italia, mentre scarsa attenzione è stata riservata al settore dell'Istruzionee Formazione Professionale (IFP).

v. Spagna

L'Agenda Digitale per la Spagna (ADpE, Agenda Digital para España) pubblicata nel 2013, è la tabella di marcia per il raggiungimento degli obiettivi fissati dall'Agenda Digitale per l'Europa nel 2015 e 2020, nonché il raggiungimento di obiettivi specifici per lo sviluppo dell'economia e della società digitale in Spagna. È strutturato attorno a sei obiettivi principali e diversi piani specifici. Il sesto obiettivo riguarda la promozione dell'inclusione e dell'alfabetizzazione digitale e la formazione di nuovi professionisti ICT.

vi. Francia

Osservando il ritmo della formazione sull'uso delle TIC nelle università francesi che la offrono, possiamo vedere che non ci sono politiche chiare e sostenute per la formazione dei formatori sull'uso delle TIC/E. Circa il 58% riferisce solo una sessione di allenamento all'anno rispetto al 7,4% al mese e allo 0,5% alla settimana.
Le statistiche mostrano che la densità della formazione informatica varia da una regione francofona all'altra. Le ragioni di ciò sono diverse, le più significative delle quali sono indubbiamente legate alle istituzioni accademiche e ai loro governi.

vii. Lettonia

Nel 2020, il Ministero dell'Istruzione e della Scienza della Repubblica di Lettonia ha fissato il miglioramento della competenza digitale degli educatori come obiettivo prioritario della competenza professionale, stanziando a tal fine finanziamenti aggiuntivi (0,5 milioni di EUR). La necessità di sensibilizzare gli studenti e gli educatori sulla sicurezza delle informazioni, la protezione della privacy e l'uso di servizi elettronici affidabili (strategia per la sicurezza informatica 2019-2022, area di azioni "Consapevolezza pubblica, istruzione e ricerca").

viii. Grecia

Sebbene l'acquisizione di competenze digitali sia una componente che non dovrebbe essere assente dal kit di strumenti educativi degli educatori dell'IFP, un importante divario può essere identificato monitorando l'attuale sistema educativo in Grecia. Nonostante le numerose riforme del curriculum educativo, le prove suggeriscono che gli educatori non sono sufficientemente dotati di conoscenze TIC e quindi mancano di strumenti e tecniche pedagogici orientati al digitale che potrebbero migliorare il processo di insegnamento (Ministero dell'Istruzione, 2019).

Risultati della ricerca

La ricerca condotta per il progetto CYBER.EU.VET ha rivelato che vi è una mancanza di dati e informazioni sulle competenze e le sfide in materia di sicurezza informatica degli educatori degli istituti di istruzione a livello europeo, nonché che esiste un numero limitato di iniziative incentrate su i problemi di sicurezza informatica all'interno dell'IFP, indicando che il progetto CYBER.EU.VET ha affrontato il tema emergente negli Stati membri. Attualmente, la maggior parte delle attività e dei progetti si concentra sulla sensibilizzazione della popolazione in generale alla sicurezza informatica e sul miglioramento delle competenze digitali complessive degli educatori, che è stata influenzata dal rapido adattamento al processo di lavoro/apprendimento a distanza.

Il consorzio dei partner è poliedrico ed è una chiara espressione di una diversa portata delle competenze digitali in tutta Europa. Tuttavia, a prescindere dalla classifica DESI dei singoli paesi, questo Rapporto di Ricerca del Consorzio può essere utilizzato per trarre indicazioni significative e valide per l'intero contesto europeo. La sensazione di un bisogno di formazione è chiara, anche tra quegli insegnanti VET che sono già stati formati in ICT. Non si rifiuta la necessità della formazione, né si mette in discussione la sua utilità. Notiamo anche che più gli insegnanti si sentono esposti a rischi psicosociali, etici, legali, tecnici o sanitari, più dicono di sentire il bisogno di formazione. Secondo un sondaggio nazionale, più della metà degli insegnanti che si sentono vulnerabili al cyberbullismo ritiene che sia necessaria una formazione. Per loro, la formazione iniziale e continua è un'opportunità per condividere esperienze e analizzare metodi di pratica professionale in questo campo. Si ritiene ancora che l'utilizzo di strumenti digitali nell'istruzione sia un modo per insegnare o un oggetto da insegnare agli studenti piuttosto che parte integrante della loro cultura generale. Dovrebbe essere sviluppata una cultura delle fonti informative e delle pratiche sui

rischi digitali (ricerca e monitoraggio). Va inoltre intensificata la formazione sulle sfide della tecnologia digitale e in particolare sui problemi psicosociali, etici, giuridici e tecnici che possono sorgere nell'uso degli strumenti digitali e che preoccupano i docenti al punto da indurli a rinunciare a ogni uso.

Pertanto, la conoscenza dei rischi digitali può influenzare positivamente le pratiche pedagogiche per educare gli studenti all'alfabetizzazione digitale. Un insegnante con una forte cultura digitale sarà più propenso a utilizzare la tecnologia digitale in classe con i propri alunni ea fare della tecnologia digitale un oggetto di insegnamento-apprendimento. L'evidente influenza della rappresentazione dei rischi non può essere positivamente modificata senza una cultura digitale generale e plurale, complementare a una cultura dell'informazione in senso lato, che eviti di demonizzare l'oggetto tecnico e consenta di sfruttare le potenzialità educative.Non si tratta di educare alla paura, ma di emancipare (e di emanciparsi, anche come insegnante) attraverso una comprensione critica e illuminata del mondo digitale.

Torna all'indice ☐

c) Il toolkit di CYBER.VET.EU

Secondo il Piano per l'istruzione digitale 2021-2027, anche le competenze digitali e le sfide dell'apprendimento hanno la massima priorità nell'agenda europea. La Commissione europea è determinata ad affrontare il divario di competenze digitali e promuovere progetti e strategie per migliorare il livello delle competenze digitali in Europa. Tutti gli europei hanno bisogno di competenze digitali per studiare, lavorare, comunicare, accedere ai servizi pubblici online e trovare informazioni affidabili. Tuttavia, molti europei non dispongono di competenze digitali adeguate. Il Digital Economy and Society Index (DESI) mostra che 4 adulti su 10 e una persona su tre che lavora in Europa non hanno competenze digitali di base. C'è anche una bassa rappresentanza di donne nelle professioni e negli studi legati alla tecnologia, con solo 1 specialista ICT su 6 e 1 laureato in scienze, tecnologia, ingegneria e matematica (STEM) che sono donne.
La Commissione europea ha fissato obiettivi nell'agenda europea per le competenze e nel piano d'azione per l'istruzione digitale per garantire che il 70% degli adulti disponga di competenze digitali di base entro il 2025. Queste iniziative mirano a ridurre il livello di 13-14enni che ottengono risultati inferiori in informatica e alfabetizzazione digitale dal 30% (2019) al 15% nel 2030. La piattaforma europea per le

competenze e le occupazioni digitali è una nuova iniziativa lanciata nell'ambito del programma Connecting Europe Facility. Offre informazioni e risorse sulle competenze digitali, nonché opportunità di formazione e finanziamento.

i. Il Quadro delle competenze digitali JRC/EC

- Quadro delle competenze digitali per i cittadini (DigComp)
- Quadro delle competenze digitali per gli educatori (DigCompEdu)
- Quadro delle competenze digitali per gli enti educativi (DigCompOrg) + strumento di autovalutazione per le scuole (SELFIE)

Perchè tutti questi quadri delle competenze?

- Sviluppo delle capacità per la trasformazione digitale dell'I&T e per affrontare le sfide delle competenze del XXI secolo.
- Quadri di riferimento che forniscono una comprensione complessiva, completa e condivisa: un linguaggio comune.

Di cosa si tratta?

- Modello concettuale, livelli di competenza e moduli di (auto)valutazione.
- Competenza definita come Conoscenze, Abilità e Attitudini.

ii. DigComp 2.2

Più di 250 nuovi esempi di conoscenze, abilità e attitudini per aiutare i fornitori di istruzione e formazione ad aggiornare il loro curriculum DigComp e il materiale del corso per affrontare le sfide odierne.

Uno dei temi chiave dell'aggiornamento DigComp 2.2 è il benessere e la sicurezza. In ogni area ci sono 10-15 affermazioni per competenza per illustrare temi attuali e contemporanei. Non rappresentano un elenco esaustivo di ciò che la competenza stessa comporta e non si riferiscono a livelli di competenza, anche se alcuni sono più complessi di altri, ma sono utili per la pianificazione del curriculum e l'aggiornamento e lo sviluppo del programma di formazione DigComp o del contenuto del corso.

La lista delle competenze DigComp e le aree rimangono le stesse:

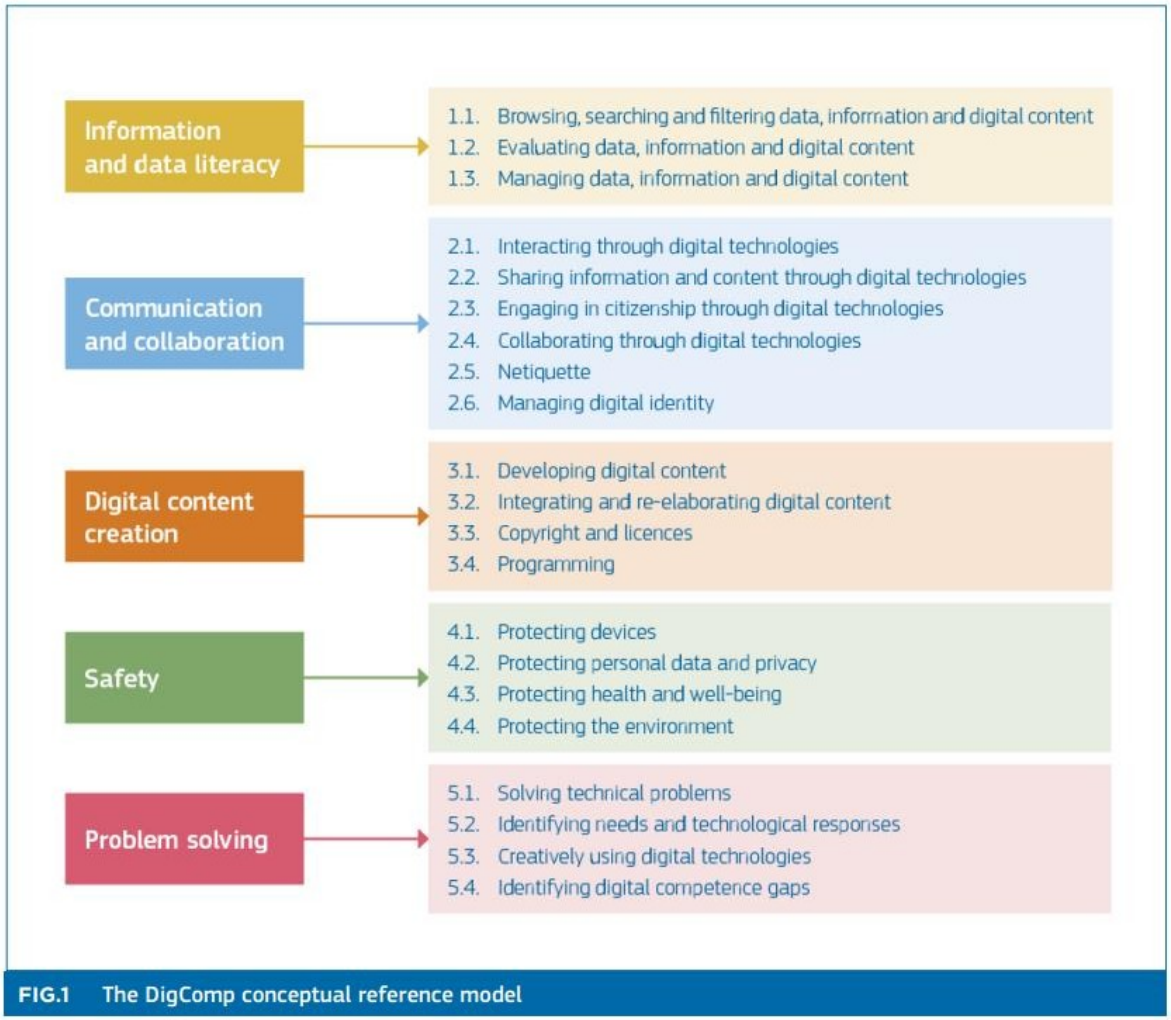


FIG.1 The DigComp conceptual reference model

[2]

[2] European Commission, Joint Research Centre, Vuorikari, R., Kluzer, S., Punie, Y., DigComp 2.2, The Digital Competence framework for citizens : with new examples of knowledge, skills and attitudes, Publications Office of the European Union, 2022, https://data.europa.eu/doi/10.2760/115376

SAFETY: "to protect devices and digital content, and to understand risks and threats in digital environments. To know about safety and security measures and to have a due regard to reliability and privacy."[3]

DIMENSION 1 • COMPETENCE AREA
4. SAFETY

DIMENSION 2 • COMPETENCE
4.1 PROTECTING DEVICES

To protect devices and digital content, and to understand risks and threats in digital environments.

To know about safety and security measures and to have a due regard to reliability and privacy.

DIMENSION 3 • PROFICIENCY LEVEL

FOUNDATION	1	At basic level and with guidance, I can:	• **identify simple** ways to protect my devices and digital content, and • differentiate simple risks and threats in digital environments. • choose simple safety and security measures, and • **identify simple** ways to have due regard to reliability and privacy.
	2	At basic level and with autonomy and appropriate guidance where needed, I can:	• **identify simple** ways to protect my devices and digital content, and • differentiate simple risks and threats in digital environments. • follow simple safety and security measures. • **identify simple** ways to have due regard to reliability and privacy.
INTERMEDIATE	3	On my own and solving straightforward problems, I can:	• **indicate well-defined and routine** ways to protect my devices and digital content, and • differentiate well-defined and routine risks and threats in digital environments, and • **select well-defined and routine** safety and security measures. • **indicate well-defined and routine** ways to have due regard to reliability and privacy
	4	Independently, according to my own needs, and solving well-defined and non-routine problems, I can:	• **organise** ways to protect my devices and digital content, and • **differentiate** risks and threats in digital environments. • **select** safety and security measures. • **explain** ways to have due regard to reliability and privacy.
ADVANCED	5	As well as guiding others, I can:	• **apply different** ways to protect devices and digital content, and • **differentiate a variety** of risks and threats in digital environments. • **apply** safety and security measures. • **employ different** ways to have due regard to reliability and privacy.
	6	At advanced level, according to my own needs and those of others, and in complex contexts, I can:	• **choose the most appropriate** protection for devices and digital content, and • **discriminate** risks and threats in digital environments. • **choose the most appropriate** safety and security measures. • **assess the most appropriate** ways to have due regard to reliability and privacy.
HIGHLY SPECIALISED	7	At highly specialised level, I can:	• **create solutions to complex problems with limited definition** that are related to protecting devices and digital content, managing risks and threats, applying safety and security measures, and reliability and privacy in digital environments. • **integrate my knowledge to contribute to professional practice and knowledge and guide others** in protecting devices.
	8	At the most advanced and specialised level, I can:	• **create solutions to solve complex problems with many interacting factors** that are related to protecting devices and digital content, managing risks and threats, applying safety and security measures, and reliability and privacy in digital environments. • **propose new** ideas and processes to the field.

[4]

iii. DigCompEdu

Il Quadro europeo per la competenza digitale degli educatori (DigCompEdu) è un quadro scientificamente valido che descrive cosa significa per gli educatori essere competenti digitalmente. Fornisce un quadro di riferimento generale per sostenere lo sviluppo di competenze digitali specifiche

[3] Luxembourg: Publications Office of the European Union, 2018 KE-01-18-834-EN-N.pdf
[4] Ibidem

per educatori in Europa. DigCompEdu è rivolto agli educatori a tutti i livelli di istruzione, dalla prima infanzia all'istruzione superiore e per adulti, compresa l'istruzione e la formazione generale e professionale, l'istruzione per bisogni speciali e i contesti di apprendimento non formale.

Il framework DigCompEdu riflette gli sforzi condotti a livello internazionale per acquisire e definire le specifiche competenze digitali di insegnanti e formatori.

L'obiettivo è fornire un quadro per coloro che lavorano nel settore dell'istruzione e dell'istruzione superiore e sono responsabili dello sviluppo di modelli di competenza digitale, ad es. i responsabili politici negli Stati membri, le autorità regionali/locali, le organizzazioni educative, le istituzioni (pubbliche o private) che forniscono servizi di formazione e sviluppo professionale.

Quindi il valore aggiunto del framework DigCompEdu è che fornisce:

- una solida base che possa guidare la politica a tutti i livelli;
- un modello che consenta alle parti interessate locali di passare rapidamente allo sviluppo di un progetto concreto
- strumento, adatto alle loro esigenze, senza dover sviluppare una base concettuale per questo lavoro;
- un linguaggio e una logica comuni che possano favorire la discussione e lo scambio di buone pratiche;
- un punto di riferimento per gli Stati membri e le altre parti interessate per convalidare la preparazione

- approccio comune ai propri strumenti esistenti e futuri e frameworks[5]

iv. COSTRUIRE LE COMPETENZE DIGITALI DEI FOMRATORI IFP IN EUROPA

L'utilizzo o lo sviluppo di quadri o strumenti di autovalutazione è un buon modo per determinare il livello di base di capacità di competenze digitali di un educatore. Da lì, è possibile mappare attività di sviluppo professionale mirate. Legato alla crescente necessità di utilizzare le tecnologie nella loro pratica di insegnamento è il requisito di cambiare la pedagogia per garantire che gli strumenti digitali siano utilizzati in modo efficace non solo nell'insegnamento ma anche nella progettazione e nella valutazione dei corsi. Il quadro europeo per le competenze digitali degli educatori (DigCompEdu) delinea le aree chiave di competenza richieste dagli educatori mentre approfondiscono il loro impegno con l'apprendimento digitale e le pedagogie digitali. Le aree di competenza chiave sono mostrate nella figura seguente (Redecker 2017).

[5] Redecker, C. European Framework for the Digital Competence of Educators: DigCompEdu. Punie, Y. (ed). EUR 28775 EN. Publications Office of the European Union, Luxembourg, 2017, ISBN 978-92-79-73494-6, doi:10.2760/159770, JRC107466

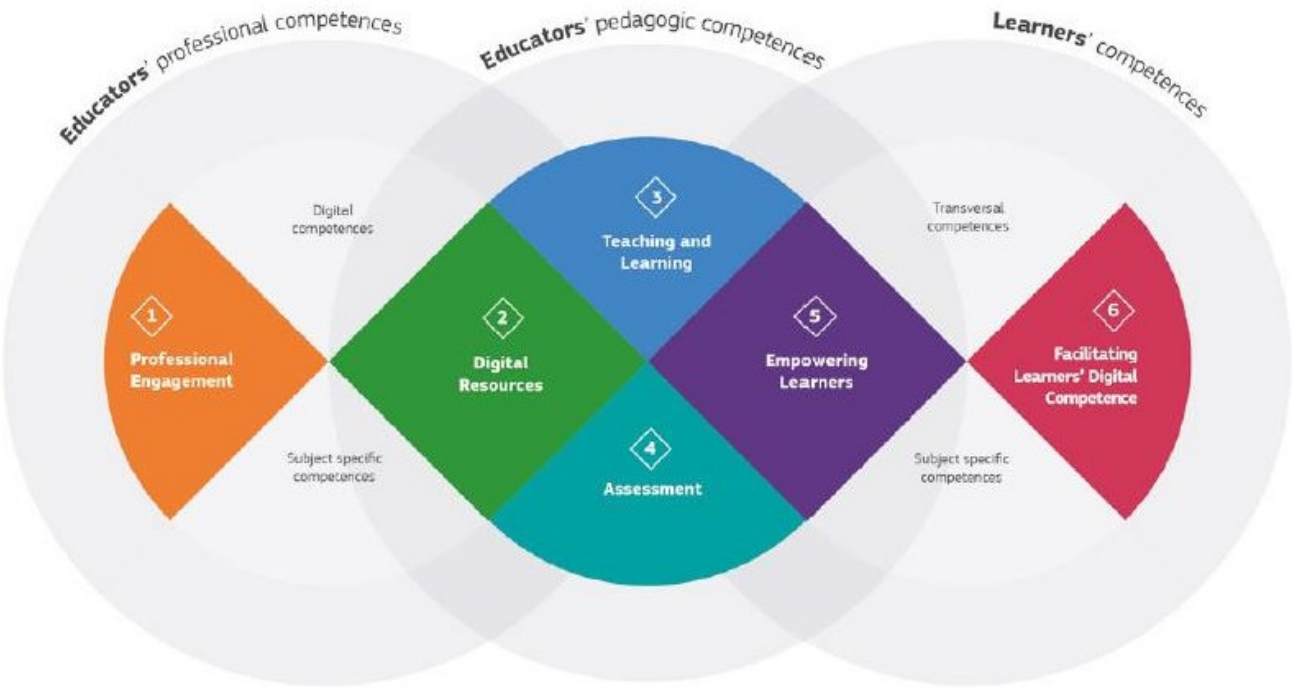


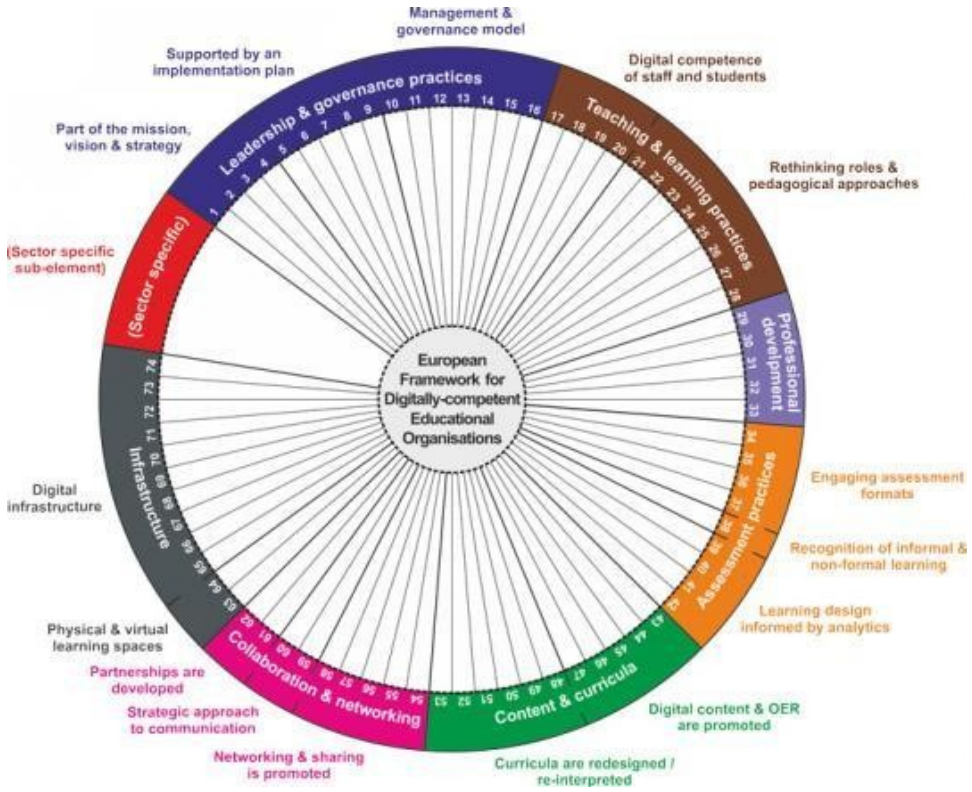
FIGURE 2: DIGCOMPEDU AREAS AND SCOPE

v. DigCompOrg

Diversi framework e strumenti di autovalutazione sono in uso in un certo numero di paesi europei, ma finora non è stato fatto alcun tentativo per sviluppare un approccio paneuropeo alla capacità digitale organizzativa. Un quadro di riferimento europeo che adotti un approccio sistemico può aggiungere valore promuovendo la trasparenza, la comparabilità e l'apprendimento tra pari. Il framework DigCompOrg può essere utilizzato dalle organizzazioni educative (ovvero scuole primarie, secondarie e di formazione professionale, nonché istituti di istruzione superiore) per guidare un processo di auto-

riflessione sui loro progressi verso l'integrazione completa e l'implementazione efficace delle tecnologiedi apprendimento digitale.

Inoltre, può facilitare la trasparenza e la comparabilità tra iniziative correlate in tutta Europa e può anche svolgere un ruolo nell'affrontare la frammentazione e lo sviluppo disomogeneo tra gli Stati membri. Il framework DigCompOrg può anche essere utilizzato come strumento di pianificazione strategica per i responsabili politici per promuovere politiche globali per l'adozione efficace delle tecnologie di apprendimento digitale da parte delle organizzazioni educative a livello regionale, nazionale ed europeo. Può anche essere utilizzato come mezzo per creare consapevolezza sull'approccio sistemico necessario per un uso efficace delle tecnologie di apprendimento digitale.



Gli scopi principali di DigCompOrg sono:

- incoraggiare l'autoriflessione e l'autovalutazione all'interno delle organizzazioni educative mentre approfondiscono progressivamente il loro impegno con l'apprendimento digitale e le pedagogie;
- abilitare i decisori politici (a livello locale, regionale, nazionale e internazionale);
- progettare, implementare e valutare programmi, progetti e interventi politici per l'integrazione delle tecnologie di apprendimento digitale nei sistemi E&T.

vi. SELFIE

SELFIE per l'apprendimento basato sul lavoro (WBL) è uno strumento online gratuito che supporta le scuole e le aziende di istruzione e formazione professionale (IFP) a sfruttare al meglio le tecnologie digitali per l'insegnamento, l'apprendimento e la formazione. SELFIE WBL aiuta le scuole e le aziende a prepararsi per l'era digitale. In questo modo sostiene la transizione digitale, una delle principali priorità politiche della Commissione europea. Questo adattamento di SELFIE ai requisiti specifici di WBL è un passo necessario a supportare gli istituti di formazione professionale.[6]

In totale, sono stati coinvolti nel progetto pilota circa 35.000 partecipanti provenienti da circa 150 scuole di formazione professionale e 250 aziende in Francia, Germania, Ungheria, Polonia, Romania, Georgia, Montenegro e Turchia. I risultati di questi progetti pilota sono disponibili per il download [LINK].[7]

Il Forum europeo dell'istruzione e della formazione tecnica e professionale (EfVET) e la Fondazione
europea per la formazione professionale (ETF) hanno fornito un sostegno inestimabile durante tutto il processo.

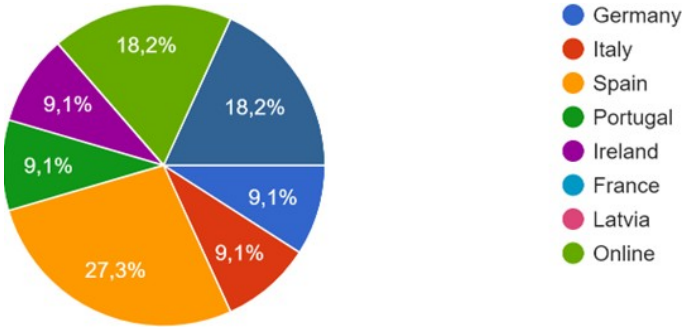
[6] SELFIE for work-based learning | European Education Area (europa.eu)
[7] SELFIE resources | European Education Area (europa.eu)

Torna all'indice ☐

d) Linee guida

Il progetto CYBER.EU.VET ha cercato di contribuire a rafforzare la capacità dell'IFP europea di riconoscere e gestire le minacce alla sicurezza informatica (ad esempio attacchi di phishing, botnet, frodi finanziarie e bancarie, frodi di dati) in un contesto storico in cui la formazione online è sempre più utilizzata.

A tal fine, ha migliorato le capacità e le competenze degli educatori dell'IFP sulla gestione delle minacce alla sicurezza informatica, dato il loro ruolo centrale nel trasferimento di conoscenze di buone pratiche e competenze ai loro studenti, aumentando anche la consapevolezza tra gli insegnanti dell'IFP, gli studenti e le loro famiglie sull'importanza riconoscere tali rischi quotidiani, che possono avere un impatto sia economico che sociale su tutti i cittadini europei. Il progetto si è basato su una circolazione congiunta locale, nazionale e transnazionale di capacità e competenze e su un buon livello di accesso e fruibilità delle informazioni digitali.



Sono state organizzate 8 sessioni di Gamejam con 54 studenti e 15 training nazionali specifici per formatori per discutere i risultati della ricerca, gli strumenti digitali condivisi e quelli nuovi realizzati, scambiando esperienze e riflessioni per sviluppare una sorta di "narrativa collettiva tematica" propedeutica al movimento dall'esplorazione e analisi alla gestione e risoluzione dei problemi digitali.

Questi eventi hanno permesso ai giovani di lavorare insieme e hanno dimostrato che anche le istituzioni percepite come lontane dal cittadino medio (es. Commissione UE) offrono opportunità interessanti per la popolazione giovanile.

Una sessione di formazione è definita in questa guida come una singola sessione di formazione che si svolge nel corso di un giorno o di una parte di un giorno. Potrebbe durare 30 minuti, un'ora o anche un'intera giornata. Una sessione di formazione potrebbe includere pause durante la giornata e coprire uno o più argomenti. Una sessione potrebbe essere tenuta in un'aula, in un piccolo gruppo con una sola famiglia, o anche individuale. Un programma di formazione, ai fini della presente guida, è una raccolta di sessioni di formazione che completano un ciclo di formazione. Ad esempio, un'agenzia potrebbe offrire un programma di formazione di 8 settimane una volta alla settimana. Il programma di formazione potrebbe quindi essere riavviato per un nuovo gruppo di persone. (Laboratori e Corsi, 2021)

I. Workshop

Questa guida segue un quadro per aumentare la consapevolezza degli studenti sulle minacce digitali, che si basa su conoscenze, abilità e competenze. Allo stesso modo, i supervisori del programma e gli insegnanti/formatori migliorano le loro conoscenze, abilità e attitudini per essere più efficaci. Questa sezione esamina le conoscenze, le abilità e gli atteggiamenti di insegnanti e formatori.

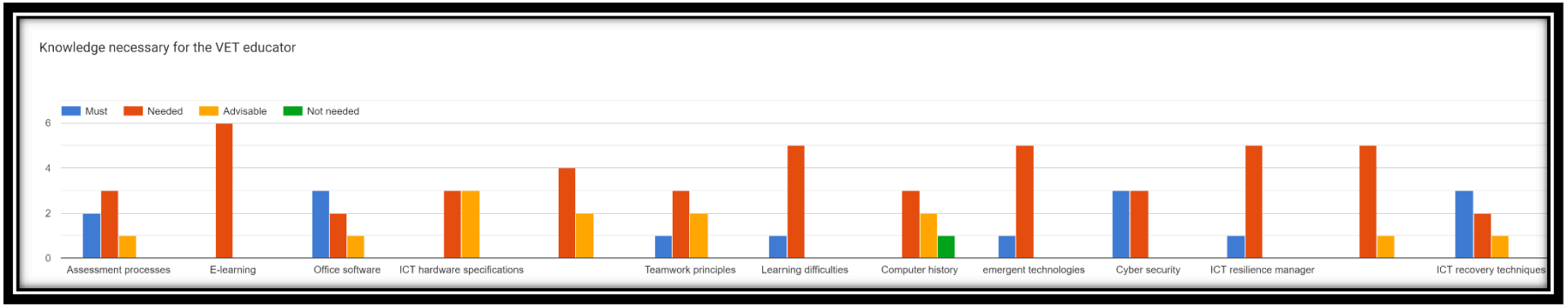
Conoscenze, abilità e attitudini sono le basi di una formazione efficace. I formatori efficaci hanno conoscenze, abilità e atteggiamenti riguardo alla formazione e agli argomenti che insegnano, e i programmi e le sessioni di formazione che offrono dovrebbero includere conoscenze, abilità e atteggiamenti per i partecipanti che sono focalizzati sull'argomento e sul contenuto.

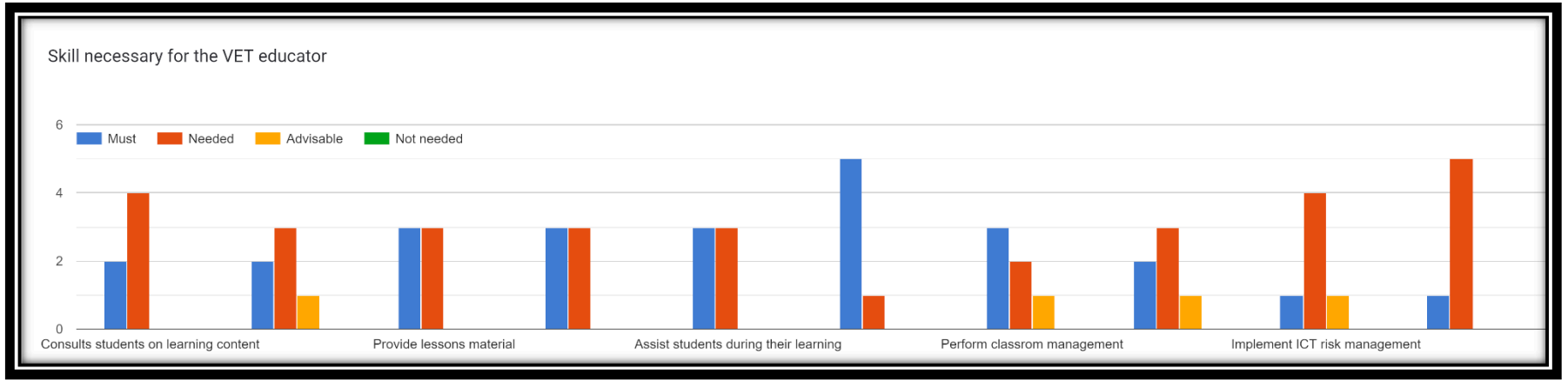
Domanda a te stesso: a chi puoi rivolgerti se hai domande sugli standard e sui contenuti del programma come nuovo professionista IFP?

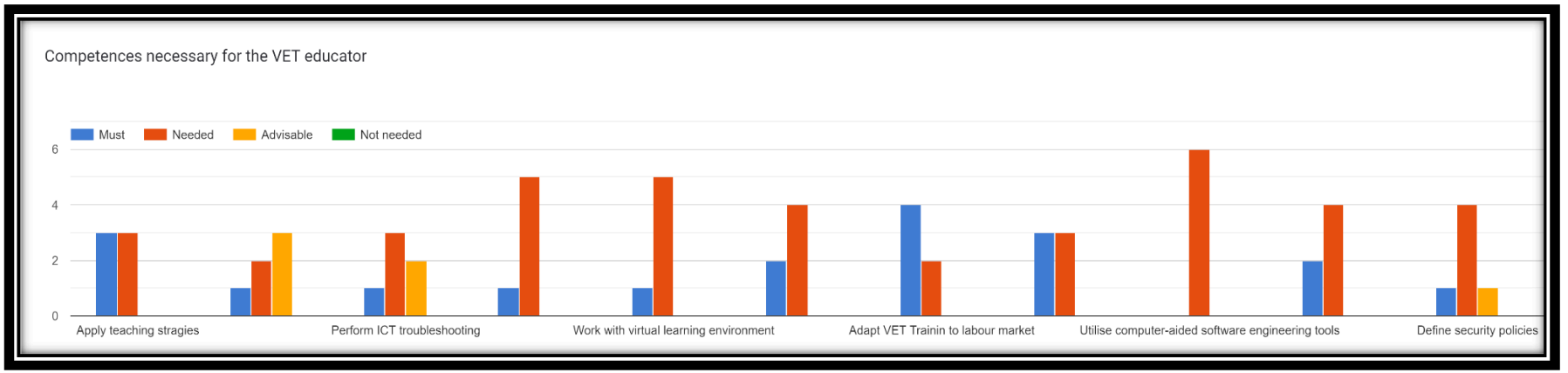
I formatori devono avere un'ampia comprensione dei contenuti principali per rispondere alle domande che possono sorgere. Se un praticante non conosce la risposta a una domanda, è fondamentale che dichiari di non conoscere la risposta, ma la esaminerà e riferirà. I praticanti non dovrebbero fornire informazioni false o inventare risposte per il bene del benessere e della comprensione dei partecipanti. È responsabilità di un formatore condurre ricerche, trovare risposte e seguire i partecipanti per assicurarsi che ricevano informazioni accurate.

Vuoi saperne di più su cosa può fare un insegnante quando affronta la materia?

I seguenti sono esempi di conoscenze, abilità e attitudini appropriate che un formatore efficace dovrebbe possedere secondo i partner del consorzio.







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

Attività: In qualità di insegnante/formatore, quali sono alcuni esempi delle tue conoscenze, abilità e attitudini? Riempi gli spazi vuoti sul grafico. Viene fornito un esempio.

Esempi di conoscenze	Esempi di abilità	Esempi di attitudini
Ho familiarità con la sicurezza informatica e le tecnologie emergenti.	Posso sviluppare materiali didattici digitali e adattare l'insegnamento al gruppo target.	Sono appassionato di rendere le sessioni il più efficaci possibile per i nostri partecipanti e mi impegno a farlo.

- **Conoscenza**: Risultato dell'assimilazione delle informazioni attraverso l'apprendimento. La conoscenza è l'insieme di fatti, principi, teorie e pratiche relative a un campo di studio o di lavoro.
- **Abilità**: Capacità di applicare le conoscenze e utilizzare il know-how per completare compiti e risolvere problemi.
- **Attitudine**: Capacità di applicare adeguatamente i risultati dell'apprendimento in un contesto definito (istruzione, lavoro, sviluppo personale o professionale). [8]

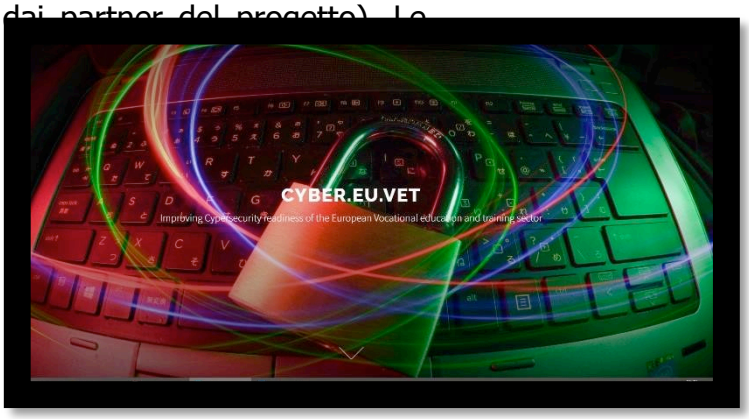
Torna all'indice ↑

[8] The European Qualifications Framework for Lifelong Learning (EQF)

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

II. Il sito web

Il consorzio del progetto ha creato fin dalla prima fase del progetto un sito Web dedicato sviluppato con tecnologie open-source (Wordpress) e un approccio modulare, che potrebbe consentire a nuovi partner di diversi paesi di aggiungere e gestire i propri contenuti (una volta accettati i termini di condizioni stabilite dai partner del progetto). Le piattaforme digitali come CYBER.EU.VET one possono essere aperte in due modi per promuovere l'innovazione e la generazione di valore (Boudreau 2010).



Certo, le piattaforme digitali, e in questo caso specifico la piattaforma concepita come Open Educational Resource, possono essere ulteriormente sfruttate per attività di follow-up. Questo nuovo sistema consente di mettere in relazione il mondo fisico tradizionale con un'interfaccia digitale in grado di connettere e organizzare la domanda e l'offerta di uno strumento o di un servizio in un unico spazio virtuale. Queste piattaforme creano reti che connettono persone e servizi nel tempo.

L'integrità della rete è legata non solo ai fattori dell'infrastruttura informativa, alla sua sicurezza e al flusso di dati all'interno della rete, ma anche ai cambiamenti sociali e ambientali che interferiscono con le componenti umane.

Per questo motivo, è stata organizzata una campagna di eventi moltiplicatori per diffondere e pubblicizzare gli strumenti tecnologici e il manuale CYBER.EU.VET sviluppati.
Questa campagna aveva anche l'obiettivo di aumentare la consapevolezza tra gli insegnanti, gli studenti e i loro parenti dell'IFP sull'importanza di riconoscere tali rischi quotidiani, che possono avere un impatto sia economico che sociale su tutti i cittadini europei.

Sistemi ICT che sfruttano l'emergente "effetto rete" combinando social media online aperti, creazione di conoscenza distribuita e dati provenienti da ambienti reali

Karhu, Gustafsson, and Lyytinen: *Exploiting and Defending Open Digital Platforms*
Information Systems Research, 2018, vol. 29, no. 2, pp. 479–497, © 2018 The Author(s)

Table 1. Two Forms of Platform Openness and Related Resources

Platform openness	Boundary resources	Shared resources	Actor who shares	Type of sharing	Platform owner's rationale
Access openness	API, app store	Complement, e.g., apps	Complementor	Shared for distribution	Generate network effects, and extract value from complementarities
Resource openness	Open-source license	Platform core, e.g., AOSP	Platform owner	Shared IPR	Strategic forfeiture of IPR while recovering costs from somewhere else

al fine di creare

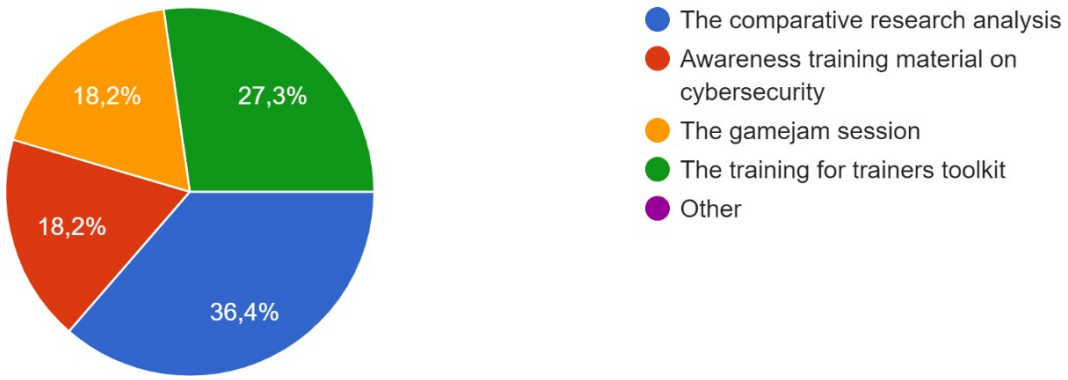
consapevolezza dei problemi e delle possibili soluzioni che richiedono sforzi collettivi, abilitando nuove forme di innovazione sociale.

III. Il parere dei professionisti

I partner e i professionisti che sono stati coinvolti nel progetto CYBER.EU.VET hanno affermato di aver beneficiato dei loro obiettivi di ricerca con una migliore comprensione della percezione degli studenti di sicurezza informatica nel contesto locale ed europeo. Gli scambi tra stakeholder così diversi tra loro sono stati un'opportunità per acquisire prospettive e approcci diversi a questioni condivise e per imparare a tradurli in un linguaggio più comune. Nelle parole del nostro partner: "È stato molto utile saperne di più sull'attuale stato dell'arte nel campo della sicurezza informatica e delle principali minacce informatiche nei paesi partner. È interessante anche conoscere e poter seguire le tendenze in termini di attacchi informatici che sembrano essere molto simili in ogni Paese". L'81,8% dei partner ha dichiarato di voler utilizzare in futuro il materiale condiviso o creato all'interno del progetto CYBER.VET.EU, il 36,4% a livello locale, il 36,4% a livello nazionale e il 27,3% a livello internazionale, attraverso sessioni di formazione e workshop, forum e, naturalmente, social media.

Il contesto dei paesi che partecipano al progetto è molto diverso l'uno dall'altro, anche se come paesi europei condividono alcune somiglianze. La sicurezza informatica è molto mutevole poiché le minacce sono diverse nel tempo. Pertanto, è interessante che i risultati ottenuti siano aggiornati sia dai formatori che dai ricercatori in modo che siano validi nel momento in cui vengono utilizzati.

Significativo il grafico che mostra quali strumenti condivisi sono stati più utili per gli operatori dei diversi servizi degli 8 consorziati:



IV. Note conclusive

Il manuale CYBER.EU.VET è stato progettato per assistere i formatori VET e gli operatori digitali nell'utilizzo degli strumenti per la sicurezza informatica, nonché istruzioni su come utilizzare il materiale CYBER.EU.VET elencato nell'appendice. Fornisce suggerimenti su come organizzare la formazione, nonché raccomandazioni operative per consentire ai professionisti di fornire agli studenti le conoscenze e gli strumenti di cui hanno bisogno per riconoscere le minacce alla sicurezza informatica. Questo e-book è stato progettato a beneficio degli insegnanti VET, degli studenti VET, delle famiglie degli studenti e degli istituti VET a livello internazionale o locale. I professionisti (o operatori del caso/dirigenti) che forniscono formazione e orientamento, supervisori o coordinatori della formazione e coloro che forniscono orientamento, come volontari, stagisti, altro personale di supporto al reinsediamento, altri fornitori di servizi e membri della comunità, possono tutti trarne vantaggio . Una maggiore consapevolezza dei rischi causati da frodi di dati, malware e altre minacce alla sicurezza online, a tutti i livelli, dalla gestione dell'istituto di formazione professionale alle famiglie dello studente, è un passo fondamentale per difendere i cittadini dell'UE dai danni causati dalle minacce alla sicurezza informatica, in modo momento già caratterizzato da una crisi epocale.

Questo e-book contiene diversi suggerimenti che speriamo inducano gli insegnanti e gli operatori del programma IFP a ripensare gli obiettivi della loro formazione e come potrebbero migliorare la qualità dell'istruzione, sviluppando modalità innovative di e-learning.

e) Appendice

I. Glossario

II. La guida CYBER.EU.VET – linee guida per future implementazioni

I. GLOSSARIO

DATI

Una sequenza di uno o più simboli a cui è stato attribuito un significato da specifici atti di interpretazione (i dati non hanno significato intrinseco). I dati possono essere analizzati o utilizzati nel tentativo di acquisire conoscenze o prendere decisioni. I dati digitali sono rappresentati utilizzando il sistema numerico binario di uno (1) e zeri (0) in contrasto con la sua rappresentazione analogica. [9]

COMUNICAZIONE DIGITALE

Comunicazione utilizzando la tecnologia digitale. Esistono varie modalità di comunicazione, ad es. comunicazione sincrona (comunicazione in tempo reale, ad esempio tramite skype o chat video o Bluetooth) e asincrona (comunicazione non simultanea, ad esempio email, sms) utilizzando ad esempio modalità one-to-one, one-to-many o many-to-many.[10]

COMPETENZA DIGITALE

La competenza digitale può essere ampiamente definita come l'uso fiducioso, critico e creativo delle TIC per raggiungere obiettivi relativi al lavoro, all'occupabilità, all'apprendimento, al tempo libero, all'inclusione e/o alla partecipazione nella società.[11]

CONTENUTO DIGITALE

Qualsiasi tipo di contenuto esistente sotto forma di dati digitali codificati in un formato leggibile da una macchina e che possono essere creati, visualizzati, distribuiti, modificati e archiviati utilizzando tecnologie digitali. Esempi di contenuti digitali includono: pagine Web e siti Web, social media, dati e database, audio digitale, come mp3 ed e-book, immagini digitali, video digitali, videogiochi, programmi per computer e software. Per il framework DigCompEdu, il contenuto digitale è suddiviso in risorse digitali e dati.[12]

AMBIENTE DIGITALE

un contesto, o un "luogo", abilitato dalla tecnologia e dai dispositivi digitali, spesso trasmessi su Internet o altri mezzi digitali, ad es. rete di telefonia mobile. Le registrazioni e le prove dell'interazione di un individuo con un ambiente digitale costituiscono la loro impronta digitale. In DigComp, il termine ambiente digitale viene utilizzato come sfondo per azioni digitali senza nominare una tecnologia o uno strumento specifico.

---

9 Modified from: en.wikipedia.org/wiki/Data_(computing)

[10] Source: *DigComp Framework* https://ec.europa.eu/jrc/digcomp

[11] *Ibidem*

[12] Redecker, C. European Framework for the Digital Competence of Educators: DigCompEdu. Punie, Y. (ed). EUR 28775 EN. Publications Office of the European Union, Luxembourg, 2017, ISBN 978-92-79-73494-6, doi:10.2760/159770, JRC107466

SERVIZIO DIGITALE
consente a un utente (cittadino, consumatore) di creare, elaborare, archiviare o accedere a dati in forma digitale e di condividere o interagire con dati in forma digitale caricati o creati dallo stesso o da altri utenti di tale servizio (Direttiva (UE) 2019/770).

TECNOLOGIA DIGITALE
Qualsiasi prodotto che può essere utilizzato per creare, visualizzare, distribuire, modificare, archiviare, recuperare, trasmettere e ricevere informazioni elettronicamente in forma digitale. Ad esempio, personal computer e dispositivi (ad esempio desktop, laptop, netbook, tablet, smartphone, PDA con funzioni di telefonia mobile, console per videogiochi, lettori multimediali, lettori di e-book), televisione digitale, robot.[13]

STRUMENTI DIGITALI
Tecnologie digitali utilizzate per un determinato scopo o per svolgere una particolare funzione, ad es. elaborazione delle informazioni, comunicazione, creazione di contenuti, sicurezza o risoluzione di problemi.[14]

CONTENUTI EDUCATIVI
Contenuti (digitali) pertinenti, in un modo o nell'altro, al contesto educativo. Questo termine è più ampio di "risorsa educativa" in quanto comprende anche contenuti marginali al processo didattico, ad es. comunicazione con studenti, genitori, colleghi; contenuto amministrativo, ecc.[15]

RISORSE EDUCATIVE
Risorse (digitali e non) progettate e destinate ad essere utilizzate per scopi didattici.[16]

ALFABETIZZAZIONE MEDIATICA
si riferisce alle abilità, conoscenze e capacità di comprensione che consentono ai cittadini di utilizzare i media in modo efficace e sicuro. Per consentire ai cittadini di accedere alle informazioni e di utilizzare, valutare criticamente e creare contenuti multimediali in modo responsabile e sicuro, i cittadini devono possedere competenze avanzate di alfabetizzazione mediatica. L'alfabetizzazione mediatica non dovrebbe limitarsi all'apprendimento di strumenti e tecnologie, ma dovrebbe mirare a dotare i cittadini delle capacità di pensiero critico necessarie per esercitare il giudizio, analizzare realtà complesse e riconoscere la differenza tra opinione e fatto. [17]

RISORSE EDUCATIVE OPEN-SOURCE
Materiali per l'insegnamento, l'apprendimento e la ricerca su qualsiasi supporto, digitale o di altro tipo, che sono di dominio pubblico o sono stati rilasciati con una licenza aperta che consente l'accesso, l'uso, l'adattamento e la ridistribuzione gratuiti da parte di altri senza restrizioni o con restrizioni limitate. [18]

AUTO-VALUTAZIONE
L'autovalutazione implica la capacità di essere un giudice realistico delle proprie prestazioni. I sostenitori dell'autovalutazione suggeriscono che abbia molti vantaggi, ad esempio: fornisce un feedback tempestivo ed efficace e consente agli studenti di valutare rapidamente il proprio apprendimento; consente agli istruttori di comprendere e fornire un rapido feedback sull'apprendimento; promuove l'integrità accademica attraverso l'autovalutazione dei progressi nell'apprendimento da parte degli studenti; promuove le capacità di pratica riflessiva e di autocontrollo; sviluppa l'apprendimento autoregolato; aumenta la motivazione degli studenti; migliora la soddisfazione dalla

[13] Modified from source: http://www.tutor2u.net/business/ict/intro_what_is_ict.htm
[14] *Ibidem*
[15] *Ibidem*
[16] *Ibidem*
[17] Source: the EU's Audiovisual Media Services Directive (2018)
[18] Source: UNESCO definition http://www.unesco.org/new/en/communication-and-information/access-to-knowledge/open-educational-resources/what-are-open-educational-resources-oers/

partecipazione a un ambiente di apprendimento collaborativo; aiuta gli studenti a sviluppare una gamma di competenze personali e trasferibili per soddisfare le aspettative dei futuri datori di lavoro.[19]

INCLUSIONE SOCIALE
Il processo di miglioramento delle condizioni per individui e gruppi di prendere parte alla società (da parte della Banca Mondiale). L'inclusione sociale mira a consentire alle persone povere ed emarginate di trarre vantaggio dalle crescenti opportunità globali. Garantisce che le persone abbiano voce in capitolo nelle decisioni che riguardano la loro vita e che godano di pari accesso a mercati, servizi e spazi politici, sociali e fisici.[20]

AMBIENTE STRUTTURATO
dove i dati risiedono in un campo fisso all'interno di un record o di un file, ad es. database relazionali e fogli di calcolo. La risposta/soluzione tecnologica si riferisce al tentativo di utilizzare la tecnologia (e/o l'ingegneria) per risolvere un problema.

Bibliografia

Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)

Ala-Mutka, K. (2011). Mapping Digital Competence: Towards a Conceptual Understanding. (JRC Technical Notes No. JRC67075). IPTS.

Baron G.-L. et Baudé J. (1992), L'intégration de l'informatique dans l'enseignement et la formation des enseignants, Tours: EPI - INRP.

BIBB (2016), "Economy 4.0 needs Education 4.0", Strengthening the media competence of training staff and trainees.

https://doi.org/10.13140/RG.2.2.18046.00322
Brodnik, A., Csizmadia, A., Futschek, G., Kralj, L., Lonati, V., Micheuz, P., & Monga, M. (2021). Programming for All: Understanding the Nature of Programs. ArXiv:2111.04887 [Cs].

http://arxiv.org/abs/2111.04887
Buisán García,M.; Valdés, F. (2017), La industria Conectada 4.0., Revista de economía, No 898.

Bihouix P, Mauvilly, K (2016), Le Désastre de l'école numérique, Le Seuil.

Carretero, S., Vuorikari, R., & Punie, Y. (2017). DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use. Publica-tions Office of the European Union.
https://data.europa.eu/doi/10.2760/38842

Cyber Ireland, (2021), Cyber Security Skills Report 2021: National Survey: https://www.cyberireland.ie/wp-content/uploads/2021/02/Cyber-Ireland-Skills-Report2021.pdf (accessed on 3rd July, 2021).

[19] Source: *Cornell University Centre for Teaching Excellence* http://www.cte.cornell.edu/

[20] Source: *DigComp Framework* https://ec.europa.eu/jrc/digcomp

EFVET (2021), Digital Balance: Balancing Digital Competences and Wellbeing.

European Commission. (2022). Translations of DigComp 2.0 in the European Skills, Competences and Occupa-tions classification (ESCO). Publications Office of the Eu-ropean Union. DOI:10.2767/316971

European Union. (2018). Council Recommenda-tion of 22 May 2018 on key competences for lifelong learning (ST/9009/2018/INIT).

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:O-J.C_.2018.189.01.0001.01.ENG
Ferrari, A. (2012). Digital competence in practce: An anal-ysis of frameworks. Publications Office of the European Union.

https://data.europa.eu/doi/10.2791/82116

Ferrari, A. (2013). DIGCOMP: A framework for developing and understanding digital competence in Europe. Publi-cations Office. doi:10.2788/52966

Ferrari, A., Brecko, B., & Punie, Y. (2014). DIGCOMP: a Framework for Developing and Understanding DigitalCompetence in Europe. ELearning Papers, 38, 1–14.

Ferrari, A., Punie, Y., & Redecker, C. (2012). Understand-ing digital competence in the 21st century: An analysis of current frameworks. In EC-TEL 2012: 21st Century Learning for 21st Century Skills (pp. 79–92).

Government of Latvia, (2020), Digital Transformation Guidelines 2021-2027.

Huismann, A. (2020), Vocational education and training for the future of work: Germany, Cedefop ReferNet thematic perspectives series.

Information Technology Security Incident Response Institution, (2021), CERT.LV Annual Report 2020.

Izglītības un zinātnes ministrija (2017), Informatīvais ziņojums "Priekšlikumi konceptuāli jaunas kompetencēs balstītas izglītības prasībām atbilstošas skolotāju izglītības nodrošināšanai Latvijā.

Izglītības un zinātnes ministrija (2020), Pedagogiem nodrošināta iespēja bez maksas pilnveidot digitālās prasmes.

Janssen, J., & Stoyanov, S. (2012). Online Consultation on Experts' Views on Digital Competence. Publications Office of the European Union. https://publications.jrc.ec.europa.eu/repository/handle/JRC73694

Kampylis, P, Punie, Y & Devine, J 2015, Promoting effective digital-age learning: a European framework for digitally competent educational organisations, Publications Office of the European Union, Luxembourg

Microsoft Digital Defense Report. https://www.microsoft.com/de/security/business/security-intelligence-report

Ministry of Education, University and Research, Government of Italy (2021), Innovare e potenziare le competenze digitali nella scuola, Memorandum of Understanding n. 785 of 22 January 2021

Ministry of Technological Innovation and Digital Transition (2020), 2025 – Strategia per l'innovazione tecnologica e la digitalizzazione del Paese.

OECD. (2014). Assessing problem-solving skills in PISA 2012. In PISA 2012 Results: Creative Problem Solv-ing (Volume V): Students' Skills in Tackling Real-Life Problems. OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264208070-6-en

Vuorikari, R., Punie, Y., Carretero Gomez, S., & Van den Brande, L. (2016). DigComp 2.0: The Digital Competence Framework for Citizens. Update Phase 1: the Conceptu-al Reference Model. Publications Office of the European Union. https://publications.jrc.ec.europa.eu/repository/handle/JRC101254

YBER.VET.EU

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

Disclaimer

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

QR code del documento:

Torna all'indice ☐