LINKS

Co-funded by the European Union

Il quadro delle competenze della sovranità digitale

Co-funded by
the European Union

Questo progetto ha il sostegno della Commissione Europea tramite il programma Erasmus+. Questa pubblicazione riflette solo il punto di vista dell'autore e la Commissione non può essere ritenuta responsabile per qualsiasi uso che possa essere fatto delle informazioni in essa contenute.

Leggi di più su

LINKS

Indice dei Contenuti

Introduzione

Il progetto LINKS mira a sostenere gli operatori giovanili europei nel raggiungere la propria sovranità sui dati e migliorare le proprie competenze in materia di sicurezza digitale attraverso una nuova forma innovativa di contenuti formativi a sostegno della costruzione di competenze digitali.
Durante le fasi iniziali di pianificazione di questo progetto e dell'applicazione, l'analisi delle esigenze ha confermato il fatto che attualmente non esiste un unico quadro di competenze in materia di sovranità e sicurezza digitale per l'Europa.
Il DigComp (Digital Competence Framework) fa riferimento a molte delle abilità e competenze fondamentali e generali relative alla sicurezza digitale nel suo complesso, e questo risultato farà riferimento a questo quadro di competenze esistente, ma è specificamente mirato alla consapevolezza proattiva degli operatori giovanili in tutta Europa delle minacce alla sicurezza digitale attualmente esistenti.
Il Digital Sovereignty Competences Framework definisce le componenti chiave delle competenze necessarie agli animatori giovanili per integrare efficacemente la sovranità digitale e i protocolli di sicurezza nei loro contesti localizzati, nonché per fornire e convalidare un quadro di riferimento dell'UE per lo sviluppo e la valutazione delle competenze di sicurezza digitale. Le competenze in materia di sicurezza digitale sono fortemente legate a competenze digitali generiche e non sono considerate competenze a sé stanti.
Il quadro si rivolge agli animatori giovanili, ma è anche rilevante e di interesse per gli insegnanti, i formatori e gli educatori delle TIC pre-servizio/in servizio, nonché i responsabili politici dell'istruzione e dell'apprendimento permanente, in relazione all'aggiornamento tecnologico e allo sviluppo delle capacità degli individui.
Ci aspettiamo che le ONG di formazione digitale e le organizzazioni di formazione in tutta Europa adottino questo quadro come parte della loro valutazione educativa e attività di insegnamento, che a lungo termine aumenteranno la consapevolezza e incoraggeranno l'integrazione del quadro negli organismi educativi digitali locali, regionali e nazionali nei paesi europei.

Risultati del sondaggio del progetto e focus group

Il Digital Sovereignty Competences Framework si basa sulla metodologia e sui risultati del sondaggio del progetto e dei focus group. Cerca anche di allinearsi con il quadro DigComp che supporta lo sfruttamento e la sostenibilità a lungo termine come quadro di competenze aggiuntivo specifico per il gruppo target.

Il sondaggio del progetto ha aiutato a conoscere l'uso della tecnologia e la protezione dei dati nelle pratiche di lavoro digitale degli operatori giovanili. Gli operatori giovanili hanno bisogno di una maggiore consapevolezza unita ad una buona gestione delle identità digitali, può aiutare a limitare gli eventi causati dalla "disattenzione" dell'utente o dell'organizzazione stessa. Hanno riferito della necessità di impostare e comunicare politiche di sicurezza per il lavoro remoto, sulla regolamentazione dell'uso dei dispositivi personali, sulla protezione dei canali di comunicazione e collaborazione e sulla fornitura di un vigile supporto IT. Hanno raccomandato di rendere i corsi disponibili per un maggior numero di membri del personale e per i giovani, per utilizzare esempi più pertinenti riguardanti compiti specifici, migliorare il networking e condividere esperienze positive e negative online. È importante mantenere l'aggiornamento e in particolare con i nuovi documenti dell'UE.

La maggior parte degli animatori giovanili non hanno ricevuto una formazione mirata, fanno delle scelte sulla sicurezza online in base alle proprie conoscenze. Hanno scritto che è necessario approfondire questi aspetti per la sicurezza delle organizzazioni e degli utenti privati e organizzare una formazione speciale per i responsabili della protezione dei dati.

Necessità del quadro delle competenze della sovranità digitale

C'è una crescente preoccupazione che i cittadini, le imprese e gli Stati membri dell'Unione Europea stiano gradualmente perdendo il controllo sui loro dati, la loro capacità di innovazione e la loro capacità di modellare e applicare la legislazione nell'ambiente digitale. In questo contesto, è cresciuto il sostegno a un nuovo approccio politico volto a rafforzare l'autonomia strategica dell'Europa nel settore digitale.
Le aziende tecnologiche stanno raccogliendo enormi quantità di dati personali e nell'UE è cresciuta la preoccupazione su come i cittadini europei possano recuperare il controllo dei propri dati digitali in un ambiente online che ora è dominato principalmente da aziende tecnologiche non UE.
Poiché l'animazione socioeducativa si sta adattando sempre più al mondo digitale, vediamo che anche gli animatori giovanili stanno adottando nuovi approcci. Sebbene il digitale sia nuovo ed entusiasmante e offra innumerevoli opportunità, richiede comunque una migliore comprensione nel contesto dell'animazione socioeducativa.
Sono necessarie ulteriori azioni per mappare le pratiche, le piattaforme, gli strumenti e i quadri di apprendimento esistenti per l'animazione socioeducativa digitale quando si tratta di competenze di sovranità digitale.
La sovranità digitale è un concetto nuovo nell'era digitale, comunemente intesa come "la capacità degli individui di possedere i propri dati privati e controllarne l'utilizzo".

La pandemia di COVID-19 ha avuto enormi effetti sulla vita quotidiana della maggior parte delle persone. In risposta, la tecnologia è stata adattata per cercare di mitigare questi effetti, offrendo agli individui alternative digitali a molte delle attività quotidiane che non possono più essere completate normalmente. La socializzazione virtuale e gli eventi online sono diventati un luogo comune e hanno fatto molto per impedire alle persone di essere completamente isolate durante il blocco.
Anche l'istruzione online è diventata la normalità in molti luoghi, poiché le scuole e le università si rivolgono alle lezioni online per mantenere l'istruzione degli studenti in pista. Inoltre, poiché le persone hanno orari più flessibili o più tempo libero durante il blocco, c'è stato un aumento significativo del numero di persone che utilizzano strumenti di apprendimento e sviluppo personali come le app per l'apprendimento delle lingue. Anche l'assistenza sanitaria si è rivolta a soluzioni digitali e rendere disponibile online l'assistenza sanitaria sia mentale che fisica è diventata più comune e ha avuto un discreto successo nell'aiutare a mitigare gli effetti negativi della riduzione dell'accesso all'assistenza sanitaria.

Framework pertinenti già esistenti

Vari quadri di competenze pedagogiche digitali sono stati sviluppati per supportare lo sviluppo professionale basato su criteri efficace e significativo degli insegnanti professionisti delle competenze pedagogiche digitali.
I quadri europei pubblicati negli ultimi anni delineano come dovrebbero apparire un'organizzazione educativa digitalmente competente DigCompOrg e il personale docente digitalmente competente DigCompEdu, incoraggiando le organizzazioni a garantire le competenze del proprio personale e a sviluppare soluzioni nazionali per garantire la competenza digitale.
DigCompEdu un framework di competenze digitali e ha come target principalmente professori universitari e membri del personale.
DigComp framework identifica le componenti chiave della competenza digitale in cinque aree:

1. Alfabetizzazione dell'informazione e dei dati: articolare i bisogni informativi, individuare e recuperare dati, informazioni e contenuti digitali. Giudicare la pertinenza della fonte e del suo contenuto. Archiviare, gestire e organizzare dati digitali, informazioni e contenuti.
2. Comunicazione e collaborazione: interagire, comunicare e collaborare attraverso le tecnologie digitali pur essendo consapevoli della diversità culturale e generazionale. Partecipare alla società attraverso i servizi digitali pubblici e privati e la cittadinanza partecipativa. Gestire la propria presenza digitale, identità e reputazione.
3. Creazione di contenuti digitali: creare e modificare contenuti digitali Migliorare e integrare informazioni e contenuti in un corpus di conoscenze esistente comprendendo al contempo come devono essere applicati copyright e licenze. Saper dare istruzioni comprensibili per un sistema informatico.
4. Sicurezza: proteggere dispositivi, contenuti, dati personali e privacy negli ambienti digitali. Tutelare la salute fisica e psicologica e conoscere le tecnologie digitali per il benessere sociale e l'inclusione sociale. Essere consapevoli dell'impatto ambientale delle tecnologie digitali e del loro utilizzo.
5. Risoluzione dei problemi: Identificare bisogni e problemi e risolvere problemi concettuali e situazioni problematiche negli ambienti digitali. Utilizzare gli strumenti digitali per innovare processi e prodotti. Per essere sempre al passo con l'evoluzione digitale.

Esiste un modello di riferimento concettuale DigComp in cui 21 competenze sono pertinenti a queste aree. Ulteriori dimensioni delineano livelli di competenza, conoscenza, abilità e atteggiamenti e casi d'uso.

Il quadro delle competenze digitali per gli animatori giovanili

Sulla base del sondaggio e dell'analisi dei quadri esistenti, i partner di questo progetto hanno deciso di concentrarsi su quattro argomenti di sicurezza di DigiComp e aggiungere anche le competenze necessarie per gli operatori giovanili. Ecco le competenze del framework DigiComp:

4.1 Dispositivi di protezione

Per proteggere dispositivi e contenuti digitali e per comprendere i rischi e le minacce negli ambienti digitali. Conoscere le misure di sicurezza e protezione e tenere in debito conto l'affidabilità e la privacy.

4.2 Protezione dei dati personali e della privacy

Per proteggere i dati personali e la privacy negli ambienti digitali. Comprendere come utilizzare e condividere le informazioni di identificazione personale pur essendo in grado di proteggere se stessi e gli altri dai danni. Comprendere che i servizi digitali utilizzano una "Informativa sulla privacy" per informare su come vengono utilizzati i dati personali.

4.3 Tutela della salute e del benessere

Essere in grado di evitare rischi per la salute e minacce al benessere fisico e psicologico durante l'utilizzo delle tecnologie digitali. Essere in grado di proteggere se stessi e gli altri da possibili pericoli negli ambienti digitali (es. cyberbullismo). Essere consapevoli delle tecnologie digitali per il benessere sociale e l'inclusione sociale.

4.4 Tutela dell'ambiente

Essere consapevoli dell'impatto ambientale delle tecnologie digitali e del loro utilizzo.

https://joint-research-centre.ec.europa.eu/digcomp/digital-competence-framework_en#ref-4-safety

Quando si definiscono le competenze digitali di base per gli animatori giovanili, è utile pensare alle caratteristiche sia universali (competenze DigComp per i cittadini) che specifiche (attività quotidiane nell'animazione socioeducativa) dell'apprendimento pratico risultante.

Competenze per la protezione dei dati personali e della privacy

* competenze tecniche nel campo delle tecnologie digitali,
* la capacità di utilizzare le tecnologie digitali in modo significativo per lavorare, studiare e altre attività quotidiane,
* la capacità di valutare criticamente le tecnologie digitali;
* conoscere le regole di base in materia di sicurezza online;
* capire come funziona online;
* capire cos'è e come funziona l'e-marketing;
* comprendere la privacy ed essere a conoscenza dei diritti di proprietà intellettuale;
* sapere come implementare le misure di sicurezza;
* sviluppare l'autoefficacia utilizzando le tecnologie digitali.

Competenze per i dispositivi di protezione

Proteggi il computer e lo smartphone con un software di sicurezza potente e aggiornato. Se il computer o il telefono è stato infettato da software dannoso, altre misure di protezione sono di scarso aiuto perché i criminali potrebbero già possedere la chiave di tutte le azioni online. È importante anche essere sicuri che tutti gli aggiornamenti del sistema operativo siano installati. Gli operatori giovanili dovrebbero prendersi cura di tutti i propri dispositivi. Devono essere aggiornati, con un software antivirus efficiente. Vari produttori rilasciano aggiornamenti che non solo migliorano le funzionalità, ma risolvono anche eventuali falle di sicurezza che potrebbero mettere a rischio i dispositivi. Come regola generale di sicurezza, è consigliabile non utilizzare nessun altro computer o dispositivo per attività che richiedono di "accedere" a uno qualsiasi dei servizi che utilizzi..

Imparare a individuare spam e truffe

TSebbene alcuni siano facili da identificare, altri tentativi di phishing in un'e-mail, sui siti di social network o sui siti Web possono sembrare molto legittimi. L'unico modo per non cadere mai in una truffa di phishing è non fare mai clic su un collegamento che è stato inviato. Se l'e-mail dice che proviene da una banca e ha tutti i loghi corretti e conosce il nome, potrebbe provenire dalla banca reale o potrebbe non esserlo. Invece di utilizzare il collegamento fornito, trovare il sito Web e utilizzare un motore di ricerca può aiutare a prevenire la truffa. In questo modo l'utente saprà se è arrivato sul sito legittimo e non su un sito falso simulato..

Utilizzo di siti Web affidabili quando si effettuano acquisti

Se un utente non conosce la reputazione di un'azienda da cui desidera acquistare, è importante studiare il sito prima di farlo. Chiedi "Come vengono esaminati da altri utenti?", "Utilizzano una connessione sicura e crittografata per informazioni personali e finanziarie?"

Stare allerta

Diffidare del WiFi pubblico e pensarci due volte prima di entrare in una rete non protetta. Esistono strumenti che possono aiutare un utente ad avere più privacy e protezione durante l'attività di navigazione da altri utenti e dai siti Web stessi su reti WiFi pubbliche.

Rimanere al sicuro online

Il mondo online è diventato un ambiente in così rapida evoluzione che i suggerimenti di oggi potrebbero essere obsoleti domani. Gli operatori giovanili devono essere consapevoli del fatto che il contenuto che consumano (e talvolta può essere davvero molto) deve essere filtrato. È importante essere un po' sospettosi. È relativamente facile falsificare le cose su Internet. È molto facile pubblicare su Internet qualcosa che non è del tutto vero o solo un mucchio di bugie. Dovremmo prestare particolare attenzione a non credere a tutto ciò che vediamo e leggiamo su Internet. Come buon consiglio, dovremmo scavare più a fondo per distinguere ciò che è vero e ciò che non lo è nel caso in cui abbiamo anche il minimo dubbio su qualcosa. Cerca di essere critico sulle cose online e quindi minimizza il rischio connesso a qualsiasi attività online.

Condivisione delle informazioni sui social network

“La condivisione delle informazioni descrive lo scambio di dati tra varie organizzazioni, persone e tecnologie” (Techopedia). Esistono diversi tipi di condivisione delle informazioni:

- Informazioni condivise da individui (come un video condiviso su Facebook o YouTube);
- Informazioni condivise dalle organizzazioni (come il feed RSS di un bollettino meteorologico online)
- Informazioni condivise tra firmware/software (come gli indirizzi IP dei nodi di rete disponibili o la disponibilità di spazio su disco)

Tutti i social network (o la maggior parte di essi) consentono agli utenti di creare profili dettagliati quanto desiderano. In alcuni casi, questa procedura aiuta gli utenti a trovare altri utenti con interessi comuni e così via. Sui social media come Facebook è possibile modificare le impostazioni sulla privacy in modo da controllare quali informazioni sono pubbliche e quali informazioni sono conservate solo per gli “amici”. È importante sapere, tuttavia, che il social network stesso dispone di queste informazioni indipendentemente dall'impostazione della privacy.

Di solito le persone condividono età, sesso, famiglia, altri interessi, background educativo e dettagli relativi al proprio impiego. Pubblicare immagini o "status" è un modo rapido per mostrare sentimenti, situazioni e condividere informazioni. La maggior parte dei social network sono progettati per farlo nel modo più rapido possibile. Essere consapevoli di quali sono le cose che un utente sta condividendo è davvero importante. La condivisione espone le informazioni che consentono agli inserzionisti di tenere traccia delle preferenze e dei gusti dei potenziali consumatori.

GDPR

Il GDPR è stato applicato a tutti i membri dell'UE e del SEE dal 25 maggio 2018. Ha sostituito l'odierna legislazione in materia di privacy nei paesi membri attualmente soggetti alla Direttiva UE 95/46. Il GDPR è più dettagliato e preciso in alcune aree e tiene conto delle sfide nel mondo digitale in rapida evoluzione, che comportano rischi per la privacy degli interessati.

Riferimenti

DProtezione dei dati e privacy online https://europa.eu/youreurope/citizens/consumers/internet-telecoms/dataprotection-online-privacy/index_en.htm
Techopedia https://www.techopedia.com/definition/24839/information-sharing

Linee guida dettagliate sulla configurazione del computer e sulla creazione di un utente https://www.wikihow.com/Use-a-Computer
Diritti alla privacy
https://www.privacyrights.org/consumer-guides/social-networking-privacy-how-be-safe-secure-and-social