YBER.EU.VET

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

CYBER.EU.VET

KA226 – Partenariati per la preparazione all'educazione digitale

Progetto n° 2020-1-DE02-KA226-C31C2976

Rapporto del consorzio

Principali sfide per la sicurezza informatica e buone pratiche

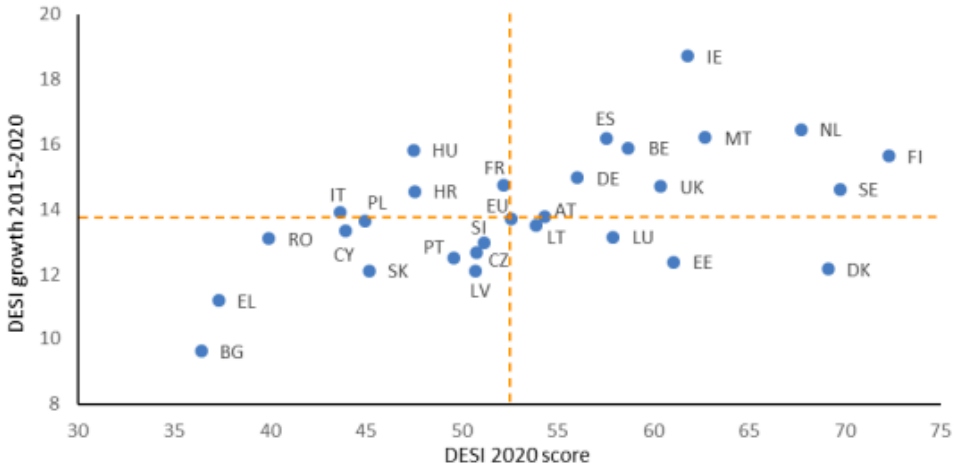
Co-funded by the
Erasmus+ Programme
of the European Union

Sommario

Introduzione

Dal momento che il mondo sta diventando sempre più digitalizzato, è diventato più evidente che la pratica dovrebbe essere combinata con la politica attuale. C'è un'attenzione significativa alle politiche di alfabetizzazione digitale e alla politica di sicurezza informatica nel contesto europeo, tuttavia ci sono meno esempi di iniziative che si ritiene soddisfino questi obiettivi in linea con le politiche sviluppate. Per osservare attentamente quanto le competenze digitali e di cybersecurity siano un tema centrale e divergente, è utile considerare il 2020 Digital Economy and Society Index (DESI).

Come parte del suo quadro generale, DESI monitora le prestazioni digitali complessive dell'Europa e misura il livello di competitività digitale nei paesi dell'UE. Fornendo informazioni sullo stato della digitalizzazione in ciascuno Stato membro, aiuta a identificare le aree di investimento e ulteriori azioni. Verso un futuro digitale su misura per le esigenze delle persone e rispettoso dei valori fondamentali dell'UE, nel febbraio 2020 la Commissione ha presentato una visione per la trasformazione digitale "Shaping Europe's digital future". La relazione DESI 2020 valuta l'economia e la società digitali all'inizio del la pandemia utilizzando i dati del 2019.



Source: DESI 2020, European Commission.

In particolare, questo indice indaga e raccoglie dati su:

- Connettività: la disponibilità di un accesso a Internet veloce e affidabile (comprese le connessioni fisse e mobili) è fondamentale nell'era attuale della fornitura online di servizi sociali ed economici fondamentali;
- Capitale umano: la spina dorsale della società digitale sono le competenze digitali delle persone. Gli utenti di servizi digitali e le persone con mobilità limitata possono svolgere attività di base online attraverso questi dispositivi;

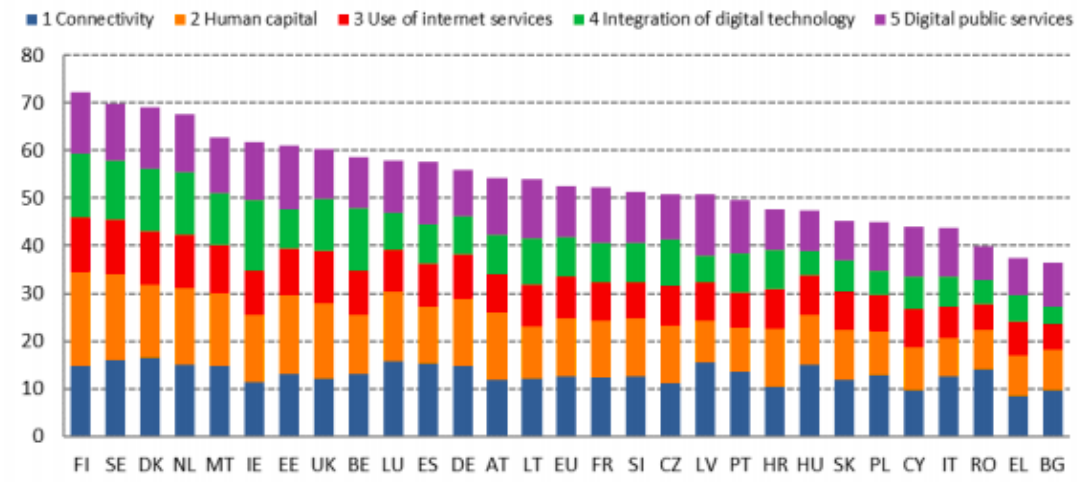
- Uso di Internet: con il progredire della pandemia, sempre più persone hanno utilizzato Internet. Il confinamento generalizzato ha comportato un accesso regolare ai social media e alle piattaforme di intrattenimento, nonché ai servizi di telelavoro e di commercio elettronico;

- Integrazione della tecnologia digitale: le imprese hanno rapidamente adottato nuove modalità di lavoro per adattarsi alle misure del governo che hanno ridotto l'interazione sociale;

- Nel bel mezzo delle misure di allontanamento sociale, è necessario continuare le attività governative per garantire che i servizi pubblici digitali offrano benefici. Saranno necessari solidi servizi pubblici digitali in tutti gli Stati membri per realizzare una strategia di uscita efficace dall'attuale pandemia.

Tale analisi è utile quando si considera il consorzio di partner che i paesi membri si differenziano notevolmente in termini di prestazioni digitali e di sicurezza informatica. In effetti, tre di essi (in ordine di classifica, Irlanda, Spagna e Germania) ottengono un punteggio migliore rispetto alla

media UE, mentre gli altri quattro (Francia, Lettonia, Portogallo e Italia) ottengono risultati inferiori.



Source: DESI 2020, European Commission.

È importante sottolineare che i risultati del DESI 2020 non sembrano confermare una corrispondenza lineare tra il PIL del Paese e la diffusione delle competenze digitali. In effetti, la Spagna, ad esempio, si è classificata come la quinta economia dell'UE solo al decimo posto nell'indice dell'economia e della società digitale. Diverse iniziative sono state recentemente introdotte in alcuni dei paesi che compongono il consorzio per migliorare la digitalizzazione dell'economia e della società. In qualità di paese leader dell'UE per la preparazione al 5G, la Germania ha adottato diverse misure per far progredire la digitalizzazione, comprese iniziative nei settori della sicurezza informatica, del supercalcolo, dell'intelligenza artificiale e della blockchain. Ci sono stati numerosi sforzi per facilitare la digitalizzazione delle imprese e dei servizi pubblici in Francia, compresi gli sforzi per creare un ecosistema per supportare le start-up tecnologiche. Il governo italiano ha adottato nel dicembre 2020 'Italia 2025', un piano quinquennale che pone l'innovazione e la digitalizzazione al centro di un "processo di trasformazione radicale e strutturale del Paese". Nei prossimi anni, queste iniziative - che

richiedono un'attuazione sostenuta nel tempo e che probabilmente richiederanno anche investimenti - potrebbero portare a progressi di questi Stati membri sul DESI.

Un altro aspetto significativo se si considera il livello delle competenze digitali e di cybersecurity riguarda l'impatto della pandemia di COVID-19 su questi temi. Sebbene tale legame tra l'emergenza sanitaria e il numero di attacchi informatici non sia immediatamente chiaro per il grande pubblico, in realtà, il primo ha comportato un aumento del secondo I cybercriminali sono molto flessibili quando si tratta di sfruttare nuovi eventi, poiché noi visto con la recente emergenza sanitaria. Con così tante aziende che nel 2020 passano a nuove strategie digital-first (ad esempio il lavoro a distanza), si sono inavvertitamente aperte a una serie di nuovi vettori di attacco che i criminali hanno rapidamente sfruttato. Tra gli altri, l'evento imprevisto di COVID-19 è stato utilizzato per diffondere tentativi di malware: ad esempio, e-mail a nome dell'Organizzazione mondiale della sanità, indicando che l'allegato include le informazioni più recenti sulla pandemia; collegamenti a grafici che mostrano la diffusione del virus, la cui funzionalità era quella di rubare i dati degli utenti; E-mail dannose alle istituzioni sanitarie riguardanti la consegna di dispositivi di protezione COVID-19 e molti altri.

Nel completare questo rapporto di ricerca del consorzio, abbiamo utilizzato una ricerca a tavolino, che consisteva nell'individuare e raccogliere dati, pubblicazioni, rapporti dell'UE, legislazioni nazionali ed europee seguendo i riferimenti forniti in tutto il rapporto. In particolare, lo studio ha esplorato il tema dell'alfabetizzazione digitale e della sicurezza informatica nei diversi contesti nazionali, con un focus sulla formazione degli insegnanti IFP. Inoltre, questo rapporto di ricerca del consorzio evidenzia alcuni degli attori chiave impegnati nel settore della cibersicurezza, tra cui gli organismi nazionali e l'Agenzia dell'Unione europea per la cibersicurezza (ENISA), che collabora con gli Stati membri e gli organismi dell'UE e assiste l'Europa nella preparazione alle future sfide informatiche.

1.Ricerca sulle competenze digitali dei formatori professionali

Germania:

• VET Data Report (2019) elaborato dall'Istituto federale tedesco per l'istruzione e la formazione professionale (BIBB), ha incluso la "digitalizzazione" tra le 3 tendenze chiave per le occupazioni della formazione professionale e l'IFP in generale.

• Più specificamente, il Rapporto afferma che “la digitalizzazione rafforzerà i cambiamenti strutturali del mercato del lavoro”, sottolineando la necessità di un cambiamento delle capacità di formazione all'interno dei rispettivi settori. Di conseguenza, in futuro, il mercato del lavoro tedesco ed europeo avrà particolare bisogno di specialisti professionisti altamente qualificati.

• Come delineato nella Risoluzione della Conferenza Permanente dei Ministri dell'Istruzione e degli Affari Culturali (2016-2017) – “Bildung in der digitalen Welt” (Istruzione nel mondo digitale) – nell'area della formazione professionale, la promozione dell'occupazione Le competenze correlate nel contesto del lavoro digitale e dei processi aziendali sono una parte essenziale della competenza degli insegnanti come punto di partenza per le loro attività didattiche.

• Il Ministero federale dell'istruzione e della ricerca (BMBF) e l'Istituto federale per l'istruzione e la formazione professionale (BIBB) si occupano dal 2015 di questioni di ricerca, sviluppo e pratica, relative alla trasformazione digitale del mondo del lavoro e dell'istruzione professionale e formazione.

Irlanda:

• Una delle strategie chiave dell'Irlanda per quanto riguarda le competenze digitali degli educatori dell'IFP è la Strategia Digitale Nazionale che è stata lanciata nel luglio 2013.

• La strategia si concentra sull'impegno digitale e sottolinea come l'Irlanda possa trarre vantaggio da una società impegnata digitalmente.

• La strategia definisce una visione chiara per il progresso digitale dell'Irlanda attraverso l'attuazione di una serie di azioni pratiche per contribuire ad aumentare il numero di cittadini e imprese che si impegnano online attraverso l'industria e le imprese, la formazione dei cittadini, le scuole e l'istruzione.

• 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.

• Molti educatori hanno affermato di ritenere che i dispositivi digitali possano "provocare distrazioni" tra gli studenti. Tuttavia, al contrario, molti educatori ritengono che i dispositivi digitali e le app nelle attività di apprendimento possano potenziare gli studenti e supportarli nell'impegnarsi nelle abilità della vita del 21° secolo come pagare le bollette online o fare domanda per un lavoro.

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.

Italia:

• Nel campo della formazione le azioni sono state realizzate principalmente attraverso l'attuazione del Piano Nazionale Scuola Digitale-PNSD.

• Questo è il documento di indirizzo del Ministero dell'Istruzione, dell'Università e della Ricerca per l'avvio di 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 sono stati rivolti alle scuole primarie e secondarie, che rappresentano la maggioranza delle scuole in Italia, mentre scarsa attenzione è stata data al settore dell'Istruzione e Formazione Professionale (VET).

• A tal proposito, sono stati realizzati progetti per gli Istituti Tecnici Superiori (ITS) di istruzione tecnica post-secondaria con particolare attenzione al rafforzamento delle competenze degli studenti.

• Ad esempio, nel 2019 il progetto “ITS 4.0” ha coinvolto oltre 1.170 studenti ITS e circa 130 aziende partner in 106 progetti di innovazione tecnologica incentrati su tecnologie come stampa 3D, realtà virtuale e big data.

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 il 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. Tra le sue misure specifiche, si possono evidenziare le seguenti misure ai fini di questa analisi:

- aggiornare il Catalogo Nazionale delle Qualifiche Professionali in termini di competenze informatiche e formazione, e inserire tale aggiornamento nelle offerte formative che accreditano le qualifiche professionali;
- massimizzare l'efficienza nella gestione e allocazione dei fondi di formazione per la formazione continua in ambito ICT, sia per i lavoratori del settore pubblico che privato, con particolare attenzione all'utilizzo delle piattaforme di formazione virtuale online;
- destinare parte delle risorse disponibili per la CVET all'acquisizione e all'aggiornamento delle competenze digitali dei professionisti ICT;
- riadeguare la formazione professionale relativa alle TIC includendo, tra le altre azioni, corsi di specializzazione nel mandato educativo;
- promuovere un miglioramento dell'offerta universitaria finalizzata alla formazione dei professionisti ICT attraverso il loro adattamento alle esigenze del mercato, contemplando nuovi profili professionali nel campo dell'ICT e aumentando l'efficienza del sistema.

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.

• L'Agenzia nazionale francese per la sicurezza dei sistemi informativi (ANSSI) ha notato un aumento molto rapido del livello della minaccia informatica in Francia. Proseguendo una traiettoria iniziata nel 2019, il numero di attacchi informatici è esploso: il numero delle vittime si è così moltiplicato per 4 in un anno.

• 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.

• Ulteriori studi per vedere la differenza potrebbero essere condotti in una fase successiva dagli uffici regionali o dai CNF in base alle proprie politiche di educazione digitale locali o regionali.

Lettonia:

• Sebbene attualmente in Lettonia manchino studi di ricerca e dati sulla sicurezza informatica e altre competenze digitali degli educatori nell'IFP e in altre istituzioni educative, è ovvio che la transizione all'apprendimento a distanza, a causa della crisi del covid-19, si è rivelata una grande sfida per molti insegnanti.

• Per quanto riguarda le strategie nazionali, i documenti di programmazione del nuovo periodo di bilancio (2021-2027) evidenziano i seguenti aspetti:

- Lo sviluppo delle competenze digitali nel settore dell'istruzione (Linee guida per la trasformazione digitale 2021-2027) – prevede lo sviluppo delle competenze digitali degli educatori e dei dirigenti delle istituzioni educative, lo sviluppo e l'uso delle competenze digitali nel processo educativo, nonché il sostegno lo sviluppo delle competenze digitali degli adulti occupati;
- Lo sviluppo delle competenze digitali è incluso nel programma di sviluppo delle competenze professionali per gli educatori (Linee guida per lo sviluppo dell'istruzione 2021-2027). 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");
- Lo sviluppo delle competenze digitali della società in generale (Linee guida per lo sviluppo dell'istruzione 2021-2027, Linee guida per la trasformazione digitale 2021-2027) in quanto le competenze digitali sono ora equiparate all'alfabetizzazione e alla matematica in termini di importanza e almeno a livello di base sono necessarie per tutti indipendentemente dal settore di attività (competenze digitali = competenze trasversali). Le misure dovrebbero essere adottate per educare la popolazione alle competenze digitali di base, all'alfabetizzazione mediatica e all'alfabetizzazione informatica, che comprende l'intero insieme di competenze di base, comprese le competenze informatiche;

L'attenzione che è stata prestata al suddetto indice DESI nell'introduzione di questo rapporto di ricerca è giustificata dall'accuratezza con cui ne descrive lo stato dell'arte e il carattere divergente a seconda dei diversi paesi europei. Tale puntualità è confermata anche dai singoli rapporti nazionali relativi alle competenze digitali dei formatori IFP.

Riteniamo che sia particolarmente utile confrontare i due estremi del consorzio, al fine di comprendere in che modo i diversi gradi di competenze digitali influenzino la popolazione nazionale e in particolare gli educatori VET. Prenderemo quindi in considerazione prima l'Irlanda, classificata al 6° posto nella classifica DESI.

Secondo l'Irish Central Statistics Office (CSO), nel 2018 l'89% delle famiglie ha

Accesso a Internet a casa. Inoltre, oltre il 30% di tutti i dati dell'UE è ospitato in Irlanda, poiché molte delle più grandi aziende tecnologiche del mondo hanno sede in Europa. Quando

entrambe le statistiche sono accoppiate, è ovvio che garantire che l'Irlanda sia un paese pronto per la sicurezza informatica è di fondamentale importanza. In questo rapporto nazionale si farà riferimento alla legislazione chiave che esiste in Irlanda sia per quanto riguarda l'alfabetizzazione digitale che

sicurezza informatica. Mentre il mondo continua ad adattarsi alla "convivenza con COVID-19", è necessario garantire che il panorama anti-crimine informatico e i modelli di best practice continuino a influenzare le politiche e le pratiche.

Una delle strategie chiave dell'Irlanda per quanto riguarda le competenze digitali 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. La strategia definisce una visione chiara per il progresso digitale dell'Irlanda attraverso l'attuazione di una serie di azioni pratiche per contribuire ad aumentare il numero di cittadini e imprese che si impegnano online attraverso l'industria e le imprese, la formazione dei cittadini, le scuole e l'istruzione. Nel 2021, il ministro dell'Istruzione Norma Foley, ha annunciato lo sviluppo di una nuova strategia digitale per le scuole primarie. La strategia è impostata per concentrarsi principalmente sull'uso della tecnologia digitale nell'istruzione e migliorare l'apprendimento attraverso l'integrazione della tecnologia nel futuro. Nell'ambito dell'istruzione superiore in Irlanda, uno degli sviluppi più notevoli è una Roadmap per l'apprendimento digitale nell'istruzione superiore: 2015-2017, che è stata sviluppata per supportare un "approccio coordinato e multilivello per promuovere l'alfabetizzazione digitale, le competenze e la fiducia tra gli studenti a livello tutti i livelli di istruzione".

Per quanto riguarda l'istruzione superiore e la formazione, è stato istituito un dipartimento relativamente nuovo per l'istruzione superiore e superiore, la ricerca, l'innovazione e la scienza. All'interno della strategia triennale dei dipartimenti, un'area di interesse chiave riguarda le

competenze digitali, per cui mirano a implementare una nuova strategia decennale per migliorare l'alfabetizzazione, la matematica e le competenze digitali. Inoltre, si concentrano su riformare la formazione delle competenze e investire nella promozione delle competenze digitali. 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.

Molti educatori hanno affermato di ritenere che i dispositivi digitali possano "provocare distrazioni" tra gli studenti. Tuttavia, al contrario, molti educatori ritengono che i dispositivi digitali e le app nelle attività di apprendimento possano potenziare gli studenti e supportarli nell'impegnarsi nelle abilità della vita del 21° secolo come pagare le bollette online o fare domanda per un lavoro. Un'ultima strategia intergovernativa che vale la pena notare dal punto di vista irlandese è l'iniziativa Future Jobs Ireland del 2018, che enfatizza una filosofia di apprendimento permanente. Nell'ambito dei suoi cinque temi chiave, il secondo si concentra su “innovazione e tecnologia, compresa la preparazione alla transizione verso l'economia digitale”. La strategia è al centro delle discussioni sulla necessità di ulteriori ricerche e investimenti nell'area dell'alfabetizzazione digitale.

Una comprensione e un apprezzamento così condivisi dei mezzi digitali confermano l'Irlanda come un paese leader in termini di integrazione della tecnologia digitale. Tra l'altro, tale integrazione risulta essere una delle questioni principali per il contesto italiano.
In Italia, meno della metà della popolazione ha competenze digitali di base e la percentuale di specialisti ICT, che costituisce solo l'1% dei laureati italiani, è ancora al di sotto della media UE, sebbene sia aumentata negli ultimi anni. Inoltre, i dati dell'OCSE Teaching and Learning International Survey (2013) vedono l'Italia al primo posto per i fabbisogni di formazione ICT dei propri insegnanti. Almeno il 36% degli insegnanti italiani ha dichiarato di non essere

sufficientemente preparato per l'insegnamento digitale, rispetto a una media OCSE del 17%, a dimostrazione della necessità di una formazione specifica.

Negli ultimi anni, in termini di risposta politica, l'Italia ha incorporato misure sulle competenze digitali in diverse strategie settoriali. Nel campo della formazione, le azioni sono state realizzate principalmente attraverso l'attuazione del Piano Nazionale Scuola Digitale (PNSD), documento di indirizzo del Ministero dell'Istruzione, dell'Università e della Ricerca per l'avvio di un percorso complessivo strategia di innovazione per la scuola italiana e per un nuovo posizionamento del suo sistema educativo nell'era digitale. È un pilastro fondamentale de La Buona Scuola (legge 107/2015), una visione operativa che riflette la posizione del Governo rispetto alle più importanti sfide di innovazione del sistema pubblico e, al centro di questa visione, ci sono le l'innovazione del sistema scolastico e le opportunità dell'educazione digitale. Le aree di intervento individuate dal PNSD sono: accesso, spazi e ambienti di apprendimento, amministrazione digitale, identità digitale, competenze degli studenti, imprenditorialità e mercato del lavoro, contenuti digitali, formazione del personale. Su quest'ultimo punto, il PNSD sostiene che la formazione degli insegnanti deve essere incentrata sull'innovazione didattica, tenendo conto delle tecnologie digitali come supporto per l'implementazione di nuovi paradigmi educativi e la progettazione operativa delle attività. Gli obiettivi di questa azione sono:

- Rafforzare la preparazione del personale in materia di competenze digitali, raggiungendo l'intera comunità scolastica;
- Promuovere il legame tra innovazione educativa e tecnologie digitali;
- Sviluppare standard efficaci, sostenibili e continuativi nel tempo per la formazione all'innovazione educativa;
- Rafforzare la formazione all'innovazione educativa a tutti i livelli (iniziale, in entrata, in servizio).

Al fine di favorire la formazione dei docenti in materie informatiche, è stato sottoscritto un Protocollo d'Intesa con gli enti di formazione e sono state previste risorse finanziarie per facilitare la partecipazione ai corsi, quali:

- Protocollo d'Intesa n. 785 del 22 gennaio 2021 tra il Ministero dell'Istruzione e Cisco Programma di formazione "Innovare e valorizzare le competenze digitali nella scuola" e "Docenti connessi e sicuri".
- Protocollo d'Intesa n. 4 del 28 ottobre 2020 tra il MIUR e S.O.S. Il Telefono Azzurro Onlus per lo svolgimento di attività didattiche e formative congiunte per promuovere l'educazione alla cittadinanza digitale e l'uso consapevole delle tecnologie digitali, dei social media e dei corsi di formazione per gli insegnanti.

Finora, la maggior parte degli interventi per la formazione del personale scolastico sono stati rivolti alle scuole primarie e secondarie, che rappresentano la maggioranza delle scuole in Italia, mentre scarsa attenzione è stata data al settore dell'Istruzione e Formazione Professionale (IFP). A tal proposito, sono stati realizzati progetti per gli Istituti Tecnici Superiori (ITS) di istruzione tecnica post-secondaria con particolare attenzione al rafforzamento delle competenze degli studenti. Ad esempio, nel 2019 il progetto “ITS 4.0” ha coinvolto oltre 1.170 studenti ITS e circa 130 aziende partner in 106 progetti di innovazione tecnologica incentrati su tecnologie come stampa 3D, realtà virtuale e big data.

Un altro strumento che contribuirà all'acquisizione di competenze digitali è incluso nel Piano Nazionale di Ripresa e Resilienza (PNRR), che fa parte del programma Next Generation EU, un pacchetto da 750 miliardi di euro, di cui quasi la metà di cui è costituito da sovvenzioni, concordate dall'Unione Europea in risposta alla crisi pandemica. Il PNRR promuoverà lo sviluppo delle competenze digitali del personale scolastico per incoraggiare un approccio accessibile,

inclusivo e intelligente all'educazione digitale. Lo scopo principale è la creazione di un ecosistema di competenze digitali, in grado di accelerare la trasformazione digitale dell'organizzazione scolastica e dei processi di apprendimento e insegnamento, in linea con il quadro di riferimento europeo per le competenze digitali DigComp 2.1 (per gli studenti) e DigCompEdu (per gli insegnanti). L'attuazione di questa linea di azione è assicurata dal Ministero dell'Istruzione e coinvolgerà circa 650.000 persone tra docenti e personale scolastico e oltre 8.000 istituzioni educative. Il governo intende rafforzare l'istruzione professionale, in particolare il sistema di formazione professionale terziaria (ITS) e l'istruzione STEM, con una forte priorità sulla parità di genere.

I suddetti contesti rappresentano due diversi contesti nazionali. Per avere un'indicazione più vicina al quadro generale europeo, può essere utile analizzare il panorama delle competenze digitali in Francia, un paese che sulla scala DESI è molto vicino e immediatamente successivo alla media europea.

L'Agenzia nazionale francese per la sicurezza dei sistemi informativi (ANSSI) ha notato un aumento molto rapido del livello della minaccia informatica in Francia. Proseguendo una traiettoria iniziata nel 2019, il numero di attacchi informatici è esploso: il numero delle vittime si è così moltiplicato per 4 in un anno. Ciò è particolarmente preoccupante, soprattutto in un contesto in cui è probabile che qualsiasi attacco informatico abbia un impatto esacerbato a causa della crisi sanitaria. La scarsa consapevolezza dei rischi informatici, la mancanza di controllo sui sistemi informativi, il mancato rispetto delle misure di igiene informatica, la carenza di esperti di sicurezza informatica e, in una certa misura, l'aumento della superficie di attacco dovuto al diffuso utilizzo del telelavoro, sono tutte debolezze sfruttate dai criminali informatici. Le campagne di attacco che hanno colpito la Francia nel 2020 hanno interrotto con successo molte attività commerciali e causato perdite finanziarie significative. L'uso massiccio di servizi digitali in outsourcing, spesso meno sicuri, è una pratica diffusa che gli aggressori non

mancano di sfruttare. Le statistiche mostrano che la densità della formazione informatica varia da una regione francofona all'altra. Ci sono diverse ragioni per questo. Tra questi, il più significativo è senza dubbio quello relativo alle istituzioni accademiche e ai loro governi. Ulteriori studi per vedere la differenza potrebbero essere condotti in una fase successiva dagli uffici regionali o dai CNF secondo le proprie politiche di educazione digitale locale o regionale. Le statistiche sulla formazione mostrano che anche i fabbisogni tematici che sono stati oggetto di workshop formativi variano da una regione all'altra. La frequenza tematica in tal senso dipende anche da fattori endogeni legati alla domanda e all'offerta in funzione delle esigenze e dei livelli di avanzamento nei campi dell'ICT/E e dell'ODL dei partner locali.

2. Ricerca sui principali rischi e minacce informatiche nei Paesi partner

Germania:

• Per analizzare lo specifico contesto tedesco e tracciare un'analisi dei bisogni, è particolarmente significativa la revisione del Barometro digitale 2020, un sondaggio online rappresentativo di privati cittadini sulla sicurezza informatica, condotto congiuntamente dal BSI e dalla Commissione per la prevenzione della criminalità della polizia statale e federale tedesca.

• Negli ultimi anni, nel panorama tedesco ed europeo, la criminalità informatica è stata la causa principale dei recenti attacchi informatici. Il rapporto BSI 2020 ha confermato fughe di dati e vulnerabilità critiche riscontrate nei prodotti software e hardware. Questa ricerca ha inoltre rilevato un aumento dei crimini informatici di massa contro cittadini privati, imprese commerciali e altre istituzioni che utilizzano malware.

• La vulnerabilità più comune sfruttata dal malware è una vulnerabilità nel sistema host. Nel caso di prodotti software o hardware, le vulnerabilità possono essere trovate nei gateway, come quelli che operano tra uffici o reti di produzione, oppure possono essere causate da errori umani nell'ingegneria sociale.

• Questo grado di digitalizzazione non è privo di rischi e pericoli. Un intervistato su quattro ha riferito di essere stato vittima di un crimine informatico nell'ultimo anno. Il tasso complessivo di criminalità informatica nel 2020 rimane costante. Lo shopping online e l'accesso di terze parti agli account online sono i tipi più comuni di frode che colpiscono le vittime (44%) e (30%), rispettivamente.

Nonostante i risultati, due terzi degli intervistati hanno espresso il desiderio di maggiori informazioni sulla prevenzione del furto di dati (66%). I consigli richiesti più spesso consistono in suggerimenti pratici come modi per garantire password sicure per più account online (59%),

seguiti da consigli su quale software è più adatto per proteggere gli account online (52%) e consigli sui pro e contro dei gestori di password (49%).

Irlanda:

• Le minacce alla sicurezza informatica in Irlanda continuano ad aumentare, con il più recente attacco alla sicurezza informatica avvenuto nel 2021 contro l'Ireland Health Service Executive (HSE) che ha e continua ad avere effetti devastanti sul sistema sanitario irlandese.

• L'Irlanda ospita oltre il 30% dei dati dell'UE a causa del numero di centri di sicurezza informatica con sede nel paese. Sebbene ciò offra molte opportunità, si traduce anche in un aumento del livello di minaccia del crimine informatico. Poiché l'Irlanda è una democrazia liberale aperta, è considerata particolarmente vulnerabile ai cosiddetti attacchi di tipo "hack and leak".

• La seconda strategia nazionale per la sicurezza informatica dell'Irlanda 2019-2024 è stata lanciata nel tentativo di aumentare la preparazione alla sicurezza informatica del paese. Gli obiettivi chiave della strategia sono:

- Per garantire la prontezza della sicurezza informatica dell'Irlanda e rispondere e gestire gli incidenti di sicurezza informatica, compresi quelli riguardanti la sicurezza nazionale,
- Per proteggere e gestire qualsiasi interruzione dei servizi che coinvolgono infrastrutture nazionali critiche da attacchi informatici,
- Per far crescere e sviluppare ulteriormente il settore della sicurezza informatica in Irlanda ed essere pronti per il cyber,
- Per implementare la migliore tecnologia e misure disponibili a livello internazionale nelle imprese irlandesi,
- Aumentare la consapevolezza e sviluppare le competenze tra le organizzazioni e i privati in merito alla sicurezza informatica.

• Nel 2018 è stato lanciato un piano d'azione per la sicurezza online che contiene venticinque azioni nell'ambito di cinque obiettivi principali incentrati sulla legislazione sui reati in materia di

criminalità informatica, rimozione di materiale illegale e dannoso e promozione della sicurezza online.

Portogallo:

I principali argomenti di sicurezza digitale da garantire sono:

o Livello base

- Identificare l'esposizione dell'infrastruttura e delle applicazioni scolastiche nell'ambiente online e adottare misure di mitigazione del rischio (sia strutturali che comportamentali);
- Identificare e mitigare le vulnerabilità;
- Identificare le informazioni personali su Internet che possono essere utilizzate per un attacco;
- Acquisire un insieme di comportamenti adeguati nell'uso del cyberspazio;

o Livelli intermedio e avanzato:

- Ambienti tecnici di programmazione della sicurezza
- Ingegneria sociale
- Esplorare le fonti di dati aperti
- Reti senza fili
- Crittografia e password

Italia:

• Il problema di sicurezza più diffuso negli ultimi tre anni in Italia è il phishing delle password, indicato dal 48% dei manager italiani, contro il 36% dei manager europei. Inoltre, il 28% dei manager italiani ha problemi legati all'accesso e all'identità (in linea con la percentuale europea) seguiti dal problema del malware basato sull'ingegneria sociale (24%).

• Inoltre, solo il 42% delle persone tra i 16 ei 74 anni ha competenze digitali di base e la percentuale di laureati in materie informatiche e ICT è molto bassa rispetto ai dati europei.

• Il Governo affronta le competenze digitali in “Italia 2025”, strategia quinquennale per l'innovazione e la digitalizzazione lanciata nel 2019. In particolare, la strategia include “Repubblica Digitale”, iniziativa promossa e coordinata dal Ministero per l'Innovazione Tecnologica e la Digitalizzazione.

• L'iniziativa mira a costruire un'alleanza tra le organizzazioni pubbliche e private ei cittadini, invitandoli ad agire concretamente per promuovere le competenze digitali. Si concentra su tre linee di azione:

- potenziamento delle competenze digitali di base;
- promuovere il miglioramento delle competenze e la riqualificazione della forza lavoro;
- sviluppare competenze in materia di TIC e tecnologie emergenti.

• Un ulteriore passo avanti verrà compiuto con "Italia digitale 2026" che si pone cinque ambiziosi obiettivi da raggiungere nei prossimi anni:

- Diffondere l'identità digitale, facendo in modo che sia utilizzata dal 70% della popolazione;
- Colmare il divario di competenze digitali, con almeno il 70% della popolazione digitalizzata

capace;

- Portare circa il 75% delle PA italiane all'utilizzo dei servizi cloud;
- Raggiungere almeno l'80% dei servizi pubblici essenziali forniti online;
- Raggiungere, in collaborazione con il Mise, il 100% delle famiglie e delle imprese italiane con reti ultrabroadband.

Spagna:

• La strategia di attivazione spagnola per l'occupazione 2017-20 mira a consolidare la ripresa economica promuovendo programmi e risorse di sicurezza informatica per gli istituti di formazione professionale per affrontare le sfide del mercato del lavoro presente e futuro derivanti dalla globalizzazione e dalla digitalizzazione. Stabilisce gli interventi che devono essere realizzati, sia a livello statale che regionale, dai Servizi Pubblici per l'Impiego (SPI);

• In termini quantitativi, uno degli obiettivi è la formazione in competenze digitali di almeno 225.000 giovani: il 75% in competenze di base e il 25% in competenze digitali avanzate, che rappresentano rispettivamente il 40% e il 38% della popolazione giovane sotto i 30 anni .

o supporto all'avvio di progetti basati sulla tecnologia per giovani donne, fornendo un consulente per consigliare queste imprenditrici sul loro piano aziendale e offrendo servizi di monitoraggio;

o azioni di formazione specifica per le giovani donne delle zone rurali nelle tecnologie ICT e nei nuovi settori del futuro, sfruttando le possibilità delle nuove tecnologie e con formatori e tutor, compreso l'insegnamento online;

o promozione dell'imprenditorialità, del lavoro autonomo e delle nuove opportunità di lavoro offerte dall'economia digitale e dalle diverse formule dell'economia sociale e dell'economia delle piattaforme digitali, nell'ambito delle politiche di attivazione occupazionale;

o migliorare la visibilità delle best practice sviluppate per comprendere quali sono i principali temi di sicurezza digitale.

• Programma Operativo Nazionale Occupazione Giovanile (budget 39 milioni di euro). A titolo esemplificativo, il Programma prevede un percorso formativo sulla Trasformazione Digitale per l'occupazione.

• Il Progetto, realizzato da EOI con la partnership di Google, è finalizzato a migliorare l'occupabilità dei giovani che hanno abbandonato la scuola fin dalla tenera età, hanno perso il lavoro o hanno difficoltà a trovare la prima occupazione.

Francia:

• I ministri dell'istruzione superiore del mondo francofono si sono riuniti il 5 giugno 2015 a Parigi su iniziativa congiunta della Francia, dell'OIF (Organisation internationale de la francophonie) e dell'AUF (Agence universitaire de la francophonie) per esaminare lo stato della e prospettive per lo sviluppo digitale dell'università francofona e dello spazio VET.

• Lo scopo principale di questo lavoro è stato quello di contribuire all'elaborazione di una strategia francofona per la formazione dei formatori nel campo dell'educazione digitale e di valutare le esigenze formative e le aspettative dei gruppi target interessati, e quindi determinare cosa è necessario per soddisfare queste esigenze e aspettative, in particolare in termini di servizi, contenuti e competenze.

• Secondo lo studio "Étude sur l'identification des besoins en training tic/e dans les pays francophones du sud, 2016", i bisogni degli insegnanti-ricercatori sono fortemente contrassegnati da una tendenza unanime verso la formazione in ICT/E e il capacity building legati all'educazione digitale (80,4%).

• I rischi digitali sono molto presenti nelle rappresentazioni dei giovani insegnanti, che facilmente trasmettono il discorso dei media. I tre rischi che gli insegnanti sentono di affrontare più personalmente sono tecnici (66,20%), etici e legali (55,80%) e informativi (54,70%).

Lettonia:

• Secondo la strategia nazionale per la sicurezza informatica 2019-202215, il cyberspazio lettone continua a subire minacce su larga scala: phishing, estorsioni e malware, tentativi di hackerare sistemi, reti e siti Web, attacchi denial-of-service (DoS) a sistemi informativi critici così come e-mail fraudolente e campagne di ingegneria sociale per recuperare dati personali o di autenticazione per screditare una specifica persona, azienda o istituzione o per commettere reati.

• Sia in Europa che in Lettonia, sono diventati di attualità i seguenti incidenti: tentativi di estorsione di denaro rivolti principalmente a istituzioni finanziarie o società del settore privato (gli aggressori hanno eseguito una serie di attacchi di prova, minacciando di sospendere il funzionamento dei siti Web aziendali o di altre risorse mediante attacchi fino a 2 Tb/s).

• Alla fine del 2021, frodi, malware e vulnerabilità continuano ad essere attivi: account WhatsApp rubati tramite codici di attivazione richiesti dagli account compromessi dell'elenco dei contatti della persona; una nuova ondata di e-mail di ricatto (sextortion) – minacciano di distribuire materiale compromettente, se l'utente dell'e-mail non farà un riscatto.

• L'anno 2020 con i suoi cambiamenti globali ha dimostrato che per gli educatori dell'IFP e di altri istituti di istruzione è importante avere maggiori conoscenze/competenze sul lavoro remoto sicuro quando si organizzano lezioni online e si utilizzano strumenti digitali (e-mail, WhatsApp, apprendimento piattaforma, ecc.) nonché di essere a conoscenza delle truffe e delle frodi di attualità, soprattutto sui social media, per sensibilizzare i propri alunni e studenti.

Sebbene il collegamento tra la pandemia di COVID-19 e il numero di attacchi informatici non sia immediatamente chiaro per il grande pubblico, in realtà il primo ha determinato un aumento del secondo. I criminali informatici sono molto flessibili quando si tratta di sfruttare nuovi eventi, come abbiamo visto con la recente emergenza sanitaria. Con così tante aziende che quest'anno sono passate a nuove strategie digital-first (ad esempio il lavoro a distanza), si sono inavvertitamente aperte a una serie di nuovi vettori di attacco che i criminali hanno rapidamente sfruttato.

Gli uffici nazionali offrono una prospettiva poliedrica sui principali temi del digitale e della cybersecurity. Mentre l'apprendimento a distanza diventa la nuova normalità, i criminali informatici stanno trovando nuovi modi per sfruttare tecniche come phishing, ransomware, ingegneria sociale e altro ancora per lanciare i loro attacchi. Ecco alcuni dei rischi più critici incontrati.

1. Accesso remoto sicuro

Poiché l'apprendimento a distanza prende il posto dell'insegnamento fisico, studenti e insegnanti hanno bisogno di accedere a strumenti di apprendimento online situati principalmente nel cloud, ad esempio applicazioni di condivisione di file, e-mail, applicazioni e talvolta devono accedere alle risorse sulla rete scolastica da remoto. Se l'accesso remoto non è protetto, gli hacker possono penetrare nel sistema e assumere il controllo dell'intera rete.

2. Accesso ai dati sensibili

Le istituzioni educative contengono un tesoro di dati sensibili che possono essere venduti sul dark web. I dati personali di studenti, insegnanti, ex studenti e personale amministrativo, nonché i dati sensibili relativi alla ricerca e alla proprietà intellettuale di una scuola, possono essere un vero tesoro da vendere o riscattare per un hacker. È quindi essenziale implementare

l'accesso basato sull'identità, consentendo agli utenti autorizzati di accedere solo alle risorse di cui hanno bisogno per svolgere il proprio lavoro.

3. Malware

Il passaggio alla didattica a distanza significa che molti dispositivi connessi alla rete scolastica sono BYOD (Bring Your Own Device). È difficile sapere se i dispositivi e le applicazioni utilizzate sono correttamente aggiornati con le patch e se l'antivirus stesso è aggiornato. A meno che questi dispositivi remoti non si connettano tramite una VPN, è necessario assicurarsi che siano protetti prima che possano accedere alle risorse sulla rete di formazione. È importante implementare funzionalità di protezione Web avanzate in grado di identificare e bloccare le più recenti minacce Web.

4. Phishing

Gli attacchi di social engineering e phishing sono i principali rischi per la sicurezza informatica per i centri di formazione francesi. Formatori e insegnanti o membri del personale che vengono indotti con l'inganno a fare clic su collegamenti dannosi possono consentire ai criminali informatici di accedere alla rete della scuola e a risorse preziose. Il modo migliore per contrastare gli attacchi di social engineering e phishing è attraverso la sensibilizzazione e la formazione degli utenti. Formare e testare gli utenti con attacchi simulati aiuterà a creare una cultura positiva di consapevolezza della sicurezza e li renderà meno vulnerabili a varie truffe online.

5. Frode

Per quanto riguarda le frodi, l'anno 2020 è stato segnalato come molto intenso, compresi gli attacchi di ingegneria sociale. Tra i tentativi di frode più attivi vi sono le campagne estorsive, in cui gli hacker affermano di aver violato il dispositivo di un utente e di aver ottenuto materiale

compromettente per il quale è stato fissato un riscatto; lotterie fraudolente per conto di marchi noti, che offrono di vincere gli smartphone più recenti o altri premi preziosi.

È stata osservata una nuova tendenza: l'estorsione di e-mail con la minaccia di fuga di dati. In molte occasioni, le aziende sono state prese di mira. Pubblicità ingannevoli sui social media – utilizzando i nomi di personaggi famosi a loro insaputa, invitavano gli utenti di Internet a investire in criptovalute. I truffatori hanno anche fatto telefonate e cercato di convincere le persone a investire. In alcuni casi, sono stati osservati ripetuti tentativi fraudolenti in cui alle vittime di frodi finanziarie è stato offerto aiuto per recuperare le risorse perdute.

Truffe telefoniche - falsificando i numeri di telefono di diversi istituti di credito e fingendosi rappresentanti di banca, truffatori, utilizzando la scarsa conoscenza del pubblico su metodi di autenticazione aggiuntivi, risorse finanziarie defraudate da diverse migliaia di utenti, causando perdite totali per centinaia di migliaia agli istituti di credito lettoni . L'adattamento degli hacker alla necessità di iniziare il lavoro a distanza - considerando le esigenze delle aziende di passare rapidamente a una condizione di lavoro a distanza e l'implementazione della circolazione dei documenti elettronici, gli hacker hanno sfruttato la situazione per ad es. alcuni contabili aziendali hanno ricevuto e-mail a nome del direttore o di un altro dipendente per effettuare un pagamento urgente o modificare il conto paghe.

L'interferenza nella corrispondenza commerciale delle aziende - compromettendo le e-mail delle aziende o dei loro partner di collaborazione, ha consentito agli aggressori di scegliere un momento adatto per inviare a una delle parti una fattura con un account modificato.

Numerosi internauti sono stati bersaglio di messaggi truffa con link scorciatoia (ej.uz), utilizzati per mascherare l'effettiva destinazione del link, per conto delle istituzioni statali in merito allo stato di emergenza e alla situazione epidemiologica nel Paese.

Falsi negozi online: durante le festività natalizie è stata osservata un'attività particolarmente elevata per mezzo di pubblicità sui social media e a causa delle restrizioni covid-19 che hanno costretto le aziende a vendere i loro prodotti online.

Può essere utile utilizzare alcuni dati riportati dai rapporti nazionali. Ad esempio, in Francia i rischi digitali sono molto presenti nelle rappresentazioni dei giovani insegnanti, che trasmettono facilmente il discorso dei media. I tre rischi che gli insegnanti sentono di affrontare più personalmente sono tecnici (66,20%), etici e legali (55,80%) e informativi (54,70%). I rischi psicosociali, cognitivi e socioeconomici sembrano preoccuparli meno. Esiste una discrepanza sistematica tra le rappresentazioni dei rischi per se stessi rispetto a quelle per gli alunni. Infatti, i tre rischi che gli insegnanti avvertono maggiormente per i propri alunni sono quello psicosociale (69,95%), informativo (70,75%) e tecnico (62,80%). Gli insegnanti quindi avvertono la stessa vulnerabilità dei loro studenti rispetto ai rischi tecnici, ma considerano i loro studenti più esposti a problemi legati in particolare a molestie o false informazioni. L'amplificazione dei rischi per gli studenti può essere spiegata dal fatto che gli insegnanti li percepiscono come molto vulnerabili. Un'insegnante in formazione ha descritto i suoi alunni di quarta elementare come molto vulnerabili, abbastanza ingenui, non necessariamente consapevoli del potenziale pericolo delle reti.

Il rapporto dell'Ufficio federale tedesco per la sicurezza delle informazioni (BSI) ha rilevato che diverse campagne hanno sfruttato la confusione e la paura create da COVID-19, tra cui campagne di malware e phishing, frodi del CEO e truffe. Inoltre, il BSI ha affermato che tali eventi potrebbero aver aumentato le possibilità di successo per tali attacchi a causa delle paure, delle preoccupazioni e delle insicurezze associate a tali eventi. Negli ultimi anni, nel panorama tedesco ed europeo, la criminalità informatica è stata la causa principale dei recenti attacchi informatici. Per analizzare lo specifico contesto tedesco e tracciare un'analisi dei bisogni, è particolarmente significativa la revisione del Barometro Digitale 2020, un sondaggio online rappresentativo di privati cittadini sulla sicurezza informatica, condotto congiuntamente dal BSI e dalla Commissione per la prevenzione della criminalità della polizia statale e federale tedesca. La transizione digitale sta modellando attivamente la nostra vita quotidiana, dallo shopping

online ai dispositivi indossabili (come bracciali per il monitoraggio del fitness, smartwatch o occhiali intelligenti), nuovi schemi di pagamento e identificazione.

Tuttavia, questo grado di digitalizzazione non è privo di rischi e pericoli. Un intervistato su quattro ha riferito di essere stato vittima di un crimine informatico nell'ultimo anno. Il tasso complessivo di criminalità informatica nel 2020 rimane costante. Lo shopping online e l'accesso di terze parti agli account online sono i tipi più comuni di frode che colpiscono le vittime (44%) e (30%), rispettivamente. La maggior parte degli intervistati nel sondaggio conosceva le recenti raccomandazioni sulla sicurezza informatica per prevenire il crimine informatico. Queste raccomandazioni sono generalmente seguite solo quando ha senso che la persona lo faccia (41%) o che abbia appena appreso di un particolare consiglio (39%). La ricerca mostra che le persone che sono già state vittime più volte hanno maggiori probabilità di ascoltare i consigli solo quando si presenta un problema (33%), anche se ne erano già consapevoli. Alla fine, nonostante i risultati, due terzi degli intervistati hanno espresso il desiderio di maggiori informazioni sulla prevenzione del furto di dati (66%). I consigli richiesti più spesso consistono in suggerimenti pratici come modi per garantire password sicure per più account online (59%), seguiti da consigli su quale software è più adatto per proteggere gli account online (52%) e consigli sui pro e contro dei gestori di password (49%).

Infine, un'altra prospettiva significativa è offerta dall'Irlanda e dalle minacce alla sicurezza informatica verificatesi nel 2021. Un attacco massiccio e coordinato iniziato nel maggio 2021, ha interrotto il servizio sanitario e i sistemi informatici in tutto il paese, ha rubato i dati personali di un'alta percentuale di pazienti e continua a chiedere un riscatto per la restituzione dei dati. In risposta, l'Health Service Executive (HSE) ha dovuto chiudere i sistemi IT degli ospedali e dei servizi sanitari per proteggersi da ulteriori furti di dati. Molti servizi sono stati interrotti e sono trapelate informazioni personali e mediche. Tuttavia, va notato che non ci sono prove a sostegno dell'acquisizione che si siano verificate ulteriori truffe che coinvolgono le informazioni

delle persone. L'Irlanda ospita oltre il 30% dei dati dell'UE a causa del numero di centri di sicurezza informatica con sede nel paese. Sebbene ciò offra molte opportunità, si traduce anche in un aumento del livello di minaccia del crimine informatico. Poiché l'Irlanda è una democrazia liberale aperta, è considerata particolarmente vulnerabile ai cosiddetti attacchi di tipo "hack and leak". In generale, questi attacchi sono visti come motivati politicamente e sono incentrati sulla disinformazione e sulle "notizie false" utilizzate come tentativo di destabilizzare lo Stato.

Molte persone coinvolte nel settore della sicurezza informatica chiedono maggiori investimenti in enti governativi come il National Cyber Security Centre (NCSC) in Irlanda. Altre minacce/rischi che continuano a prevalere sono i rischi posti alle Infrastrutture Nazionali Critiche (CNI), ai sistemi e ai dati del settore pubblico che sono stati brevemente delineati nei paragrafi precedenti. Nuove problematiche che cominciano ad emergere sono quelle legate alla diffusione delle tecnologie 5G. Anche se questo darà origine a nuove tecnologie e servizi, la sicurezza informatica deve essere in prima linea mentre molti paesi iniziano ad adattarsi.

Al di fuori di una prospettiva nazionale e aziendale, i crimini di sicurezza informatica continuano a verificarsi in modo prolifico su base giornaliera tra la persona media. Spesso non vengono segnalati alle forze dell'ordine con solo il cinque percento dei crimini informatici presumibilmente denunciati alla polizia in Irlanda nel 2019. Inoltre, un rapporto del 2019 commissionato da Microsoft in Irlanda rileva che i dipendenti sono ancora considerati l'"anello debole" nella sicurezza sistema a causa della mancanza di formazione sulla sicurezza, della scarsa gestione delle password, dell'uso di dispositivi personali con dati relativi al lavoro e di potenziali violazioni del regolamento generale sulla protezione dei dati dell'UE.

3. Buone pratiche relative a programmi per la sicurezza informatica e risorse per gli istituti di formazione professionale nei Paesi partne

Come specificato nell'introduzione, il progetto Cyber.EU.VET coinvolge un consorzio poliedrico e diversificato. Per quanto riguarda le competenze digitali e di sicurezza informatica, i paesi partner del consorzio si comportano con diversi gradi di efficacia, come perfettamente descritto dall'indice DESI. L'analisi accademica e la valutazione delle buone pratiche è stata parte integrante del lavoro di ricerca svolto a livello nazionale da ciascun partner del consorzio del progetto. Questa ricerca ha avuto come linea guida comune un'analisi dei bisogni delle problematiche dell'IFP a livello locale e nazionale. Nello svolgimento di questo lavoro, i sette partner nazionali hanno condiviso alcune difficoltà relative alla ricerca di iniziative di formazione e sicurezza informatica specificamente progettate per gli insegnanti IFP. Sebbene ciò abbia reso questo compito piuttosto difficile, ha anche mostrato ancora più chiaramente l'importanza e la necessità di sviluppare progetti in questo settore. Ha poi confermato lo spirito estremamente innovativo del progetto CYBER.EU.VET. Ecco una raccolta delle buone pratiche più rilevanti trovate da ciascun partner.

3.1 Germania – Iniziativa VET 4.0

L'IFP 4.0 è un'iniziativa ombrello, sviluppata in collaborazione dal Ministero federale dell'Istruzione e della ricerca (BMBF) e dall'Istituto federale per l'istruzione e la formazione professionale (BIBB) dal 2016, che ha riunito un'ampia gamma di progetti nell'ambito di tre pilastri principali. Il pilastro 2 di questa iniziativa globale (che è ancora in corso) è interamente dedicato all'"alfabetizzazione digitale/competenza mediatica" e mira a definire le competenze mediatiche, che dovrebbero essere considerate un requisito di accesso e una competenza

chiave in tutte le professioni nell'IFP (per apprendisti, insegnanti e formatori). I programmi di finanziamento per attrezzare meglio i centri di formazione e per sostenere le piccole e medie imprese (PMI) in vista della digitalizzazione completano questo approccio di promozione delle competenze mediatiche nell'IFP. Attraverso lo speciale programma di digitalizzazione ÜBS (71), il BMBF e il BIBB stanno contribuendo ad accelerare la digitalizzazione dei processi nella formazione degli apprendisti nel contesto della "VET 4.0". Il programma speciale si compone di due linee di finanziamento:

1) Il finanziamento è fornito per l'acquisto di attrezzature digitali selezionate (dispositivi digitali, macchine, sistemi e software, come tecnologie per la casa intelligente, 21 robot industriali, stampanti 3D e supporti digitali per l'insegnamento e l'apprendimento, come tablet e touchscreen), al fine di modernizzare la formazione degli apprendisti, in particolare per quelli formati dalle PMI;

2) Il programma finanzia anche 8 progetti pilota nei centri di competenza che identificano gli impatti della digitalizzazione sui profili dell'attività professionale e determinano i requisiti e le conseguenze che ne derivano per la qualificazione del personale qualificato e della formazione del personale. In una seconda fase, sviluppano concetti innovativi di insegnamento e apprendimento per l'IFP 4.0 e li diffondono come moltiplicatori. L'obiettivo è garantire che i risultati siano trasferibili e che vi sia un'ampia gamma di applicazioni.

Di seguito sono riportati alcuni esempi dei suddetti progetti pilota:

● "Digital Media in VET", che terminerà nel 2022 e che è composto da diversi sottoprogrammi con diverse priorità di finanziamento, sta finanziando progetti nazionali di formazione digitale che sviluppano nuovi scenari di apprendimento e moderni corsi di formazione iniziale e continua che promuovono l'acquisizione di competenze sui media digitali ;

● "Qualification Initiative Digital Change - Q 4.0", che dal 2018 finanzia lo sviluppo e la sperimentazione di ulteriori concetti di formazione per i formatori VET in azienda. Il progetto si compone di due sottoprogetti: 1) seminari MIKA (Media e Competenza IT per la formazione del personale) per promuovere la competenza pedagogica di base sui media, lo sviluppo e la sperimentazione di moduli di formazione continua per rafforzare le competenze di base sui media e sull'IT del personale di formazione; 2) Q 4.0 NETWORK volto ad adattare il processo di formazione al cambiamento digitale, tenendo conto anche delle differenze regionali e settoriali. In entrambi i progetti, il risultato finale potrebbe essere un prototipo di un'offerta di seminari testata che potrebbe essere messa a disposizione del personale IFP a livello nazionale;

● "Digitalizzazione II" dal 2018 per identificare strategie per progettare processi di apprendimento che utilizzino il potenziale dei media digitali per supportare un apprendimento di successo, sia per individui che per gruppi.

3.2 Francia - Internet Sans Crainte

(Poiché in questo specifico paese mancano buone pratiche nel campo dell'IFP, questo caso di studio è stato selezionato come pratica che soddisfa i vincoli richiesti ma non riguarda specificamente il settore dell'IFP).

Di fronte ai continui casi di cyberbullismo, dipendenza da Internet, pericolosi incontri in rete e alle loro tragiche conseguenze per i giovanissimi studenti, si è reso necessario richiamare l'attenzione di tutti sui diritti e sui limiti del comportamento online e, soprattutto, presentare Internet come strumento di arricchimento e intrattenimento libero da pericoli. Creata nel 2000, pioniera della pedagogia digitale ed esperta di comunicazione pubblica giovanile, Tralalere è un produttore leader di programmi educativi crossmediali: cartoni animati per produzioni

multimediali, serious games, app mobili, eBook ecc. In particolare, Tralalere ha ideato e diretto il programma nazionale sensibilizzazione ai rischi su Internet: www.internetsanscrainte.fr.

Gestito da Tralalere dal 2008, Internet Sans Crainte è il programma nazionale per aiutare i giovani a ottenere un migliore controllo sulle loro vite digitali. In termini concreti, Internet Sans Crainte offre un centinaio di risorse chiavi in mano gratuite per aiutare insegnanti, educatori e genitori a sostenere i giovani dai 6 ai 18 anni nel loro per aiutare insegnanti, educatori e genitori a guidare i giovani dai 6 ai 18 anni verso un mondo illuminato e uso responsabile degli schermi e della tecnologia digitale. Internet Sans Crainte offre anche consulenza e competenza su come supportare i giovani nella loro educazione digitale attraverso schede tematiche. Tralalere e Internet Sans Crainte coordinano inoltre Safer Internet France, programma nazionale ed europeo per la protezione dei minori su Internet, insieme alla linea Net Ecoute (e15 Enfance) e Point de contact. In questa veste, Internet Sans Crainte organizza il Safer Internet Day in Francia, una giornata mondiale per sensibilizzare i giovani a utilizzare meglio Internet. Questo programma è sostenuto dalla Commissione Europea come parte della rete Inhope/Insafe, che comprende 38 Paesi.

BENEFICIARI

Internet Sans Crainte, offre tutto l'anno risorse digitali adattate a diversi tipi di pubblico,

Compreso:

- Mediatori educativi (insegnanti, animatori, bibliotecari, ecc.);
- Genitori e famiglie;
- Istituzioni e associazioni.

3.3 Irlanda – Cybersafe Kids

(Poiché in questo specifico paese esiste una mancanza di buone pratiche nel campo dell'IFP, è stata selezionata una pratica che soddisfi i vincoli richiesti ma non riguardi specificamente il settore dell'IFP).

Cybersafe Kids come progetto è iniziato nel 2015 ed è ora diventato un ente di beneficenza riconosciuto finanziato da una serie di fondi filantropici irlandesi come The Ireland Funds. Cybersafe Kids offre una serie di programmi di formazione incentrati sulla sicurezza informatica nelle scuole di tutto il paese d'Irlanda. La visione di Cybersafe Kids è per un mondo in cui i bambini utilizzino la tecnologia in modo sicuro, positivo e di successo. Le principali parti interessate di Cybersafe Kids sono le scuole partecipanti in tutta l'Irlanda (gli studenti, gli insegnanti, i presidi e i tutori), le università di ricerca partner, i finanziatori dell'ente di beneficenza e il team coinvolto nella realizzazione dei programmi. L'obiettivo principale dell'ente di beneficenza è promuovere, promuovere e fornire istruzione e formazione a bambini, genitori e insegnanti della comunità per garantire una navigazione sicura e responsabile nel mondo online. Per quanto riguarda l'impatto, ad oggi Cybersafe Kids ha raggiunto 24.000 bambini di età compresa tra 8 e 13 anni attraverso i loro programmi scolastici. Solo nel 2020, i programmi hanno collaborato con 5.986 bambini e 1.554 genitori in 56 scuole in Irlanda. Inoltre, è stato distribuito un sondaggio online anonimo che ha raccolto dati da 3.764 bambini di età compresa tra 8 e 12 anni riguardo al loro uso online. Secondo la Relazione degli Amministratori (2019) le principali aree di impatto includevano le seguenti:

- La realizzazione di un programma educativo e il lancio di un progetto di misurazione del cambiamento comportamentale in collaborazione con l'Università di Dublino e il Comitato per i bambini ei giovani (CYPSC);

- Hosting di una forte campagna "Safe Internet Day";

● Lancio di contenuti e risorse online rivolti ai genitori di bambini più piccoli (dai 2 ai 10 anni). Negli anni precedenti è stato pubblicato materiale per bambini più grandi;

● Sviluppo di una serie di "richieste" politiche che mirano a incidere sulla politica generale del paese per quanto riguarda la sicurezza informatica.

3.4 Spagna – SPACE: competenze per professionisti nelle scuole contro il cyberbullismo

CONTESTO

La diffusione capillare e l'utilizzo delle nuove tecnologie è connesso al fenomeno del cyberbullismo. Nel 2009 in tutta Europa circa il 18% dei giovani europei di età compresa tra 13 e 19 anni è stato vittima di bullismo/molestie/persecuzione tramite Internet e telefoni cellulari, le percentuali attuali variavano dal 10% al 52%. Il Parlamento europeo sottolinea che il cyberbullismo è aumentato tra i bambini di età compresa tra 11 e 16 anni dal 7% nel 2010 al 12% nel 2014.

ESIGENZE DEI GRUPPI TARGET

Il progetto SPACE risponde ai bisogni formativi degli insegnanti delle scuole, al fine di far loro acquisire competenze per prevenire/contrastare il cyberbullismo. Infatti, nonostante gli Stati membri dell'UE abbiano avviato molte iniziative e progetti per prevenire e contrastare il cyberbullismo, questo sembra essere in crescita: trattandosi di un fenomeno nuovo, manca un sistema organico di conoscenze, competenze e azioni educative strutturate che assicurino agli insegnanti l'acquisizione delle la conoscenza delle sue dinamiche, la padronanza delle tecnologie digitali per un uso sicuro del Web e le competenze per progettare azioni di prevenzione, informazione e formazione.

OBIETTIVI

Molte risorse e contenuti sul cyberbullismo sono stati sviluppati da scuole e istituzioni; tuttavia si trattava di iniziative isolate, non raccolte in un unico spazio web e quindi non valorizzate. SPACE ha raccolto questa sfida e ha sviluppato un MOOC - corso aperto online gratuito - sul cyberbullismo per insegnanti scolastici e una Biblioteca digitale pubblica multilingue di risorse educative aperte sul cyberbullismo. Scopi principali del progetto:

- mappare e descrivere le competenze necessarie per prevenire e contrastare il cyberbullismo;
- sviluppare una biblioteca digitale di OER sul cyberbullismo, con funzioni di ricerca avanzate;
- sviluppare un MOOC per insegnanti scolastici sul cyberbullismo, utilizzando le OER precedentemente recuperate ed etichettate;
- potenziare e migliorare negli insegnanti coinvolti la competenza digitale, vale a dire sicurezza informatica, rischio web e net etiquette;
- supportare gli insegnanti nell'acquisizione delle competenze per intervenire in caso di cyberbullismo a scuola e per progettare e realizzare attività informative e formative con i propri studenti.

PARTECIPANTI

Il principale gruppo target coinvolto nel progetto è rappresentato dagli insegnanti delle scuole (livelli ISCED2 e ISCED3). I gruppi target indiretti erano dirigenti scolastici e personale non docente; studenti; genitori; autorità scolastiche e decisori. 139 insegnanti sono stati coinvolti nella sperimentazione MOOC e 300 hanno partecipato agli eventi Multiplier organizzati nei paesi partner. La Biblioteca digitale pubblica ha ricevuto oltre 8.000 visite durante il ciclo di vita del progetto.

ATTIVITÀ

Il progetto ha avuto una durata di 24 mesi, durante i quali si sono svolte le seguenti attività:

- realizzazione di una mappa delle competenze e di un modello MOOC;

● progettazione e sviluppo di una biblioteca digitale online sul cyberbullismo;

● recupero, catalogazione e identificazione delle OER sul cyberbullismo e implementazione di tali risorse nella biblioteca digitale;

● impostazione e personalizzazione di una piattaforma CMS per ospitare il MOOC;

● progettazione, sviluppo e test di un MOOC multilingue sul cyberbullismo;

● creazione di un Toolkit con indicazioni, linee guida e raccomandazioni sul sistema e sugli strumenti SPACE;

● realizzazione di 10 Eventi Moltiplicatori nei paesi partner e una conferenza finale;

● realizzazione di 4 riunioni consortili;

● divulgazione attraverso la realizzazione di un sito web, brochure, presentazioni, partecipazione come reporter invitato alla Fiera DIDACTA di Firenze, articoli su riviste e quotidiani.

IMPATTO

Il progetto ha prodotto un impatto positivo, promuovendo la consapevolezza del cyberbullismo, una maggiore conoscenza delle sue dinamiche e delle modalità di prevenzione e contrasto, e sviluppando un insieme multidimensionale di conoscenze e competenze nel gruppo di insegnanti europei coinvolti. Gli insegnanti e le organizzazioni coinvolte nella sperimentazione hanno acquisito competenze per prevenire e contrastare il cyberbullismo, competenze digitali specialistiche su cybersecurity, web risk e net etiquette, sviluppato abilità strategiche e competenze metodologico-didattiche migliorando la propria professionalità docente, hanno a disposizione strumenti più efficaci per svolgere attività di informazione e formazione per i propri studenti per prevenire il cyberbullismo.

3.5 Lettonia - Programma "Accrescimento delle competenze digitali degli insegnanti relative all'utilizzo di ambienti digitali per l'insegnamento"

OBBIETTIVO

Lo scopo del programma è quello di migliorare la competenza digitale degli educatori - insegnare tecnologie e strumenti che aiuteranno gli educatori a organizzare il loro processo lavorativo in modo più efficiente. Il programma è implementato dal 2014 dal Ministero dell'Istruzione e della Scienza della Repubblica di Lettonia.

BENEFICIARI

Il contenuto dei corsi nel 2020 è progettato per:

- gruppi di gestione delle istituzioni educative;
- educatori delle scuole professionali (IFP) e generali;
- insegnanti della scuola primaria;
- insegnanti di scuola materna;
- insegnanti di varie materie (matematica, lingua lettone, informatica, ingegneria, design e tecnologia, fisica, chimica e biologia).

DESCRIZIONE

Nel 2020, il Ministero dell'Istruzione e della Scienza ha posto il miglioramento delle competenze digitali degli educatori come obiettivo prioritario della competenza professionale, stanziando ulteriori finanziamenti. Il programma offre corsi gratuiti per educatori con diversi livelli di conoscenza che rappresentano varie materie (il loro campo di specializzazione, vedere la sezione Beneficiari). Gli esecutori dei corsi hanno sviluppato compiti di apprendimento dettagliati, hanno attratto leader di gruppo - consulenti per garantire un regime di

apprendimento favorevole per gli educatori. Il contenuto dei corsi è progettato in conformità con i requisiti del moderno ambiente di apprendimento.

RISULTATI RAGGIUNTI

4339 educatori hanno frequentato a lungo (con il diritto concesso di lavorare come insegnante di informatica) e brevi corsi di sviluppo delle competenze professionali (2014-2020).

INNOVAZIONE

L'approccio innovativo ostacola l'organizzazione del processo: ogni partecipante al corso può apprendere il

contenuti a un ritmo e un tempo conveniente per loro. Durante il corso vengono analizzate le tecnologie e gli strumenti che possono essere utilizzati nel processo di studio al fine di promuovere la collaborazione e semplificare l'organizzazione del processo di studio/processo di lavoro dei docenti.

3.6 Portogallo

Nonostante alcune iniziative ad hoc, non sono state individuate azioni di formazione nel settore della sicurezza informatica per l'IFP. Sul mercato sono stati identificati solo diversi corsi di istruzione superiore, post-laurea o di natura aziendale, quindi la formazione in cybersecurity per l'IFP dovrebbe essere una priorità fondamentale per sostenere il futuro più cybersafe del nostro Paese, ovvero in grado di garantire la sicurezza personale e aziendale.

Il Centro Nazionale per la Cybersecurity, con la missione di promuovere la condivisione delle conoscenze e una cultura nazionale della Cybersecurity, ha sviluppato il Programma di Sensibilizzazione e Formazione in Cybersecurity, attraverso il quale si intende massificare la formazione e la sensibilizzazione dei cittadini e dei dipendenti delle organizzazioni per i pericoli

della l'uso disinformato del cyberspazio, realizzando azioni di sensibilizzazione e formazione sulla Cybersecurity in diverse parti del Paese, da nord a sud, passando per le isole, con il supporto di partner, ma nulla diretto agli Istituti di Formazione Professionale.

3.7 Italia – "Docenti connessi e sicuri"

CONTESTO

Il programma ha l'obiettivo generale di realizzare azioni volte a innovare e rafforzare le competenze digitali nelle scuole. Nello specifico, il programma mira a migliorare le competenze e le conoscenze degli insegnanti in merito alle nuove esperienze di didattica digitale integrata, al funzionamento e ai benefici dell'Internet of Things e all'importanza della sicurezza informatica. Il programma è promosso nell'ambito del nuovo protocollo d'intesa tra il Ministero dell'Istruzione (Italia) e Cisco.

GRUPPI TARGET.

I beneficiari del programma sono docenti delle scuole italiane di qualsiasi ordine e grado.

ATTIVITÀ.

Il programma di formazione offerto da Cisco ai docenti si compone di 3 webinar a cui sono collegati 3 corsi di approfondimento. La partecipazione all'intero programma è totalmente gratuita.

1. Un mondo digitale connesso Webinar "DAD e nuove esperienze di didattica digitale integrata" tenuto da personale Cisco o Partner Cisco e linkato corso online "Get Connected". Tempo stimato per il completamento: 30 ore Panoramica del corso: il corso ti insegna a sviluppare conoscenze digitali di base. La struttura del corso,

particolarmente interattiva, crea un ambiente facilmente accessibile per un pubblico che si avvicina per la prima volta al mondo dell'informatica.

2. Cittadini digitali consapevoli: Webinar “Smart City e Internet of Things: nuovi servizi digitali per i cittadini” tenuto da personale Cisco o Partner Cisco e correlato corso online “Introduzione all'Internet of Things (IoT)”. Tempo stimato per il completamento: 20 ore Panoramica del corso: Il corso Introduzione all'IoT (Internet of Things) introduce gli insegnanti alle tecnologie che supportano l'IoT e alle opportunità generate dal crescente numero di connessioni di rete tra persone, processi, dati e cose.

3. Sicurezza informatica: Webinar “Come proteggersi dalle minacce di rete” tenuto da personale Cisco o Partner Cisco e linkato corso online “Introduzione alla Cybersecurity”. Tempo stimato per il completamento: 20 ore. Panoramica del corso: Il corso Introduzione alla sicurezza informatica analizza le tendenze nel mondo IT, le minacce e il fatto di essere in totale sicurezza nel cyberspazio, proteggendo i dati personali.

IMPATTO.

Poiché il progetto si è concluso il 3 giugno, i numeri relativi ai docenti formati sono ancora in fase di elaborazione. Tuttavia, il progetto è innovativo perché combina la formazione legata alla tecnologia con l'imprenditoria digitale, ma anche con la programmazione.

Conclusioni

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.

Tuttavia, le iniziative esistenti sono complete e si sono dimostrate efficaci (vedere la sezione Buone Pratiche). 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 utilizzo.

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.

Bibliografia

ADEI (2017), *El trabajo del futuro*. Technical Note.

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

Andries B. et Beigbeder I. (coordonné par) (1993), *La culture scientifique et technique pour les professeurs des écoles*, Paris: Hachette éducation, CNDP.

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

Baron G.-L. et Bruillard É. (2000), *Technologies de l'information et de la communication dans l'éducation : Quelles compétences pour les enseignants?,* Éducation et Formation, No 56.

Baron G.-L. et Bruillard É. (sous la direction) (2002), *Les technologies en éducation: perspectives de recherche et questions vives*, Actes du Symposium international francophone, Paris : INRP, IUFM de Basse-Normandie, MSH.

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

Blanco, R., Fontrodona, J., Poveda, C. (2017), *La industria 4.0: el estado de la cuestión,* Revista Economía Industrial, No 406.

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.

Capelle, C., Cordier, A., Lehmans, A., (2018), *Usages numériques en éducation : l'influence de la perception des risques par les enseignants*, Open Edition Journals.

Carrizosa Prieto, E (2018), *Lifelong learning e industria 4.0. Elementos y requisitos para optimizar el aprendizaje en red.*, Revista internacional y comparada de relaciones laborales y derecho del empleo. Vol. 6, No 1.

Central Statistics Office (CSO) (2018), Information Society Statistics – Households: https://www.cso.ie/en/releasesandpublicatons/er/isshh/informationsocietystatisticshouseholds2018/ (accessed on 6th July, 2021).

CEFEDOP, (2021), *Vocational education and training in Portugal*, EU Agenda.

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).

Database of National Education Opportunities – Niid.lv, study programmes in cybersecurity

Department of Education and Skills, Government of Ireland (2015), *Digital Strategy for Schools (2015-2020)-Enhancing Teaching, Learning and Assessment.*

Department of Education and Skills, Government of Ireland (2017), *Higher Education System Performance Framework 2018-2020.*

Department of Enterprise, Trade and Employment (2018), *Future Jobs Ireland – Preparing Now for Tomorrow's Economy.*

Department of Further and Higher Education, Research, Innovation and Science, Government of Ireland (2021), *Statement of Strategy 2021-2023.*

Department of Justice (2021). Cybercrime: www.justice.ie/en/jelr/pages/cybercrime (accessed on 2nd July, 2021).

Department of Tourism, Culture, Arts, Gaeltach, Sport and Media (2019), *Action Plan for Online Safety 2018 – 2019.*

Dig8tal (2020), *Is German Cybersecurity ready for 2021?,* https://dig8ital.com/resources/library/is-german-cyber-security-ready-for-2021

Erasmus+ project DIG4VET (Digital Tools for Learning and Validation in VET and WBL: Training Program
for VET Teachers, Trainers and Potential I-Coaches)

Escuela de organizacion industrial, *Activa industria 4.0.*

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

European Commission (2020), *Italy in the Digital Economy and Society Index.*

European Commission (2020), *Latvia in the Digital Economy and Society Index.*

Federal Office For Information Security, (2019),*The State of IT Security in Germany in 2019.*

Federal Office For Information Security, (2020), *The State of IT Security in Germany in 2020.*

Federal Office For Information Security, (2020). *Digitalbarometer: Bürgerbefragung zur Cyber-Sicherheit.*

Government of Ireland (2018), *National Cyber Security Strategy 2019-2024.*

Government of Italy (2020), *Piano Nazionale di Ripresa e Resilienza -PNRR.*

Government of Latvia, (2019), *Informative report, Cybersecurity Strategy of Latvia.*

Government of Latvia, (2020), *Education Development Guidelines 2021-2027 "Future Skills for the Future Society".*

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

Guir R. (2002), *Pratiquer les TICE : Former les enseignants et les formateurs à de nouveaux usages*, Bruxelles: De Boeck et Larcier.

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.*

Joseph, V. (2020). *Vocational education and training for the future of work: France*, Cedefop ReferNet thematic perspectives series.

Kultusministerkonferenz (2016), "*Bildung in der digitalen Welt: Strategie der Kultusministerkonferenz"*

Lardellier P., Moatti, D. (2014), *Les ados pris dans la Toile. Des cyberaddictions aux techno-dépendances*, Paris: Éditions Le Manuscrit, Coll. « Addictions : Plaisir, Passion, Possession »

Latvian Safer Internet Centre (Project-platform "Drossinternets.lv"): https://drossinternets.lv/

LIKTA (Latvian Information and Communication Technologies Association): https://likta.lv/digitalasparmainas-izglitiba/

Likumi.lv, Noteikumi par pedagogiem nepieciešamo izglītību un profesionālo kvalifikāciju un pedagogu profesionālās kompetences pilnveides kārtību. https://likumi.lv/ta/id/301572-noteikumi-par-pedagogiem-nepieciesamo-izglitibu-un-profesionalo-kvalifikaciju-un-pedagogu-profesionalas-kompetences-pilnveides

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

Ministry of Education, University and Research, Government of Italy, *Piano Nazionale Scuola Digitale – PNSD.*

Ministry of Education, University and Research, Government of Italy, (2018), *La Buona Scuola* (Law No. 107/2015)

Ministry of Education, University and Research, Government of Italy (2020), *Accordo di collaborazione per lo svolgimento di attività didattiche e formative congiunte per promuovere l'educazione alla cittadinanza digitale e l'utilizzo consapevole delle tecnologie digitali e dei social media*, Memorandum of Understanding n. 4 of 28 October 2020.

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 Industry, Trade and Tourism, Government of Spain, Industria Conectada 4.0, Agenda Digital para Espana.

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

Mokhtar Ben Henda (2016), *Identification des besoins en formation tic/e dans les pays francophones du sud. Étude réalisée par: Initiatives pour le Développement numérique de l'espace universitaire francophone francophone*, [Rapport de recherche] Agence universitaire de la Francophonie.

National Centre for Vocational Education Research, (2020), *Teaching digital skills: Implications for VET educators - good practice guide.*

OECD (2021), Going Digital in Latvia

OECD, (2018), TALIS - The OECD Teaching and Learning International Survey TALIS - OECD Teaching and Learning International Survey

Pridzans, Dzerviniks (2019), *The Topicality of Educators' Digital Competence Development*, SOCIETY. INTEGRATION. EDUCATION Proceedings of the International Scientific Conference. Volume V, May 24th -25th.

Principes et organisation de la deuxième année de la formation des enseignants stagiaires en IUFM, (2002). La circulaire du 4 avril 2002 parue au Bulletin officiel n° 15 du 11 avril 2002.

Saldus Technical School, Study Programme Civil Security and Defence: https://www.saldustehnikums.lv/izglitibas-iespejas/profesijas/profesionala-videja

Stolterman, E (2004), *Information Technology and the Good Life*, International Federation for Information Processing Digital Library; Information Systems Research. Volume 143.

Télé-enseignement : *les 5 risques majeurs en matière de cybersécurité* – Sophos News

Thélot C. (sous la direction) (2004), *Pour la réussite de tous les élèves, rapport officiel de la Commission du débat national sur l'avenir de l'École*, Paris : La documentation Française.

YBER.EU.VET

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.

E' possibile risalire al documento attraverso il seguente QR code: