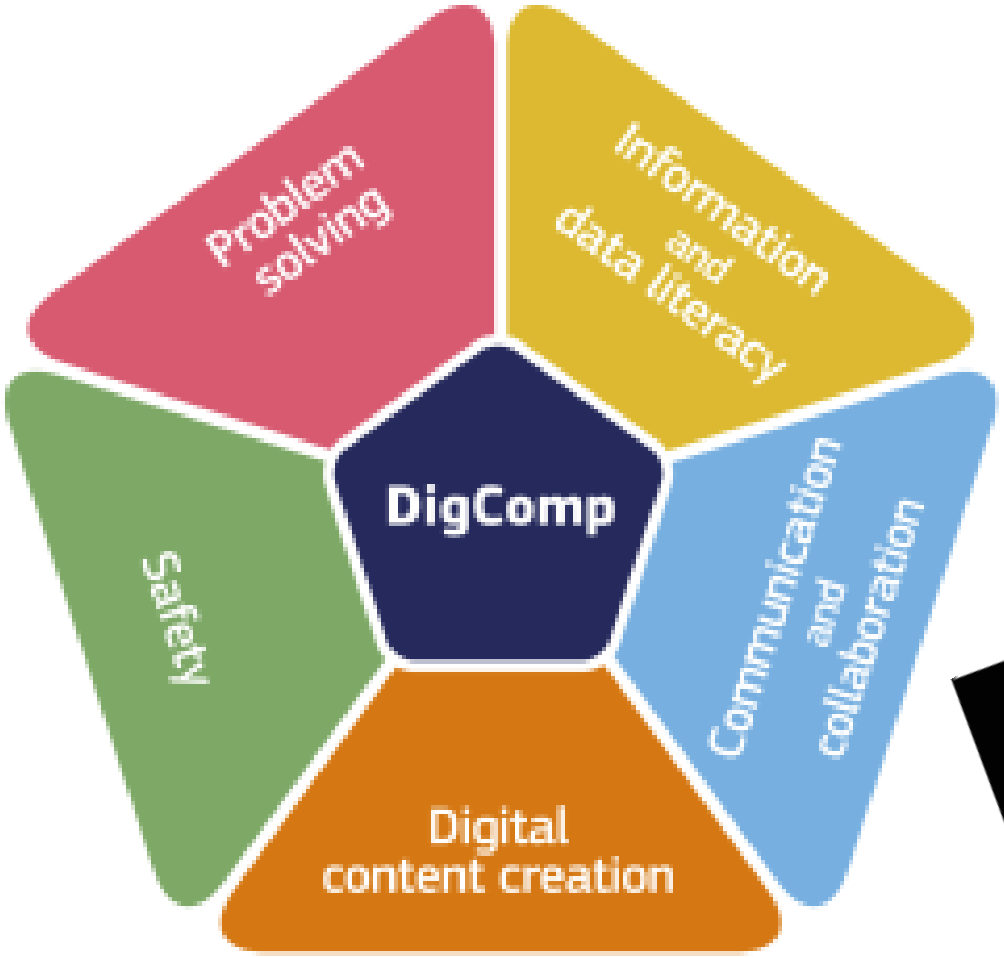
MICROCREDENZIALI PER LA COMUNICAZIONE E LA COLLABORAZIONE
Competenza 2.6: GESTIRE L'IDENTITÀ DIGITALE

DSW
DIGITAL SKILLS WALLET

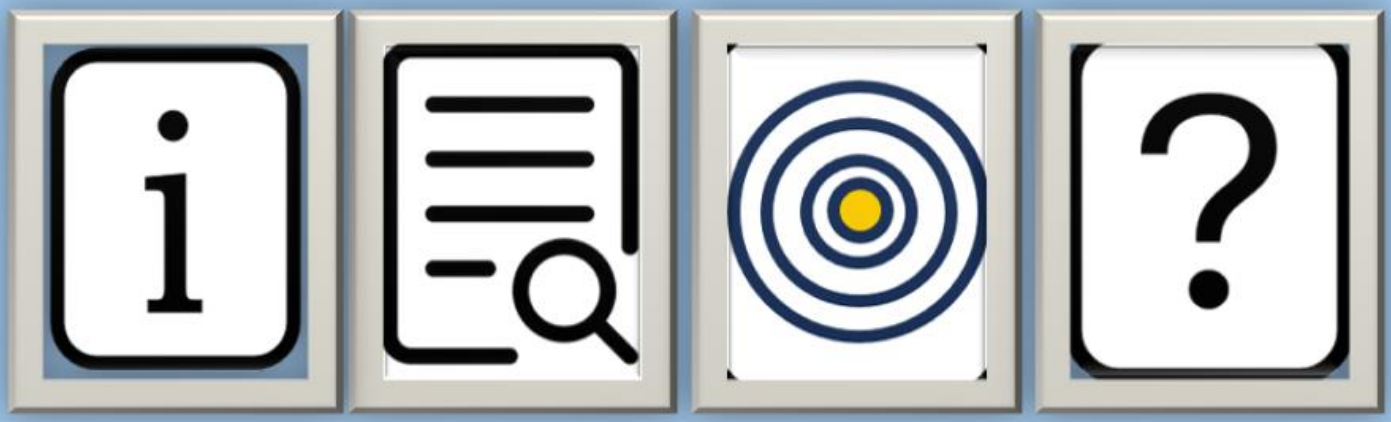
Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.


Problem solving
Information and data literacy
DigComp
Safety
Communication and collaboration
Digital content creation

Sommario

LIVELLO BASE
(FOUNDATION)
(Livello 1 e Livello 2)



Definire l'identità digitale (MC 2.6.A.1)

Informazioni di base

A chi è rivolto il corso	Qualsiasi cittadino
Titolo e codice della microcredenziale	Definire l'identità digitale **Codice: MC 2.6.A.1**
Paese(i)/Regione(i) che hanno contribuito alla pubblicazione	IRLANDA, ITALIA, CIPRO, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Organismo(i) di certificazione	DSW Consortium Numero del progetto: **101087628**
Data di pubblicazione	Dicembre 2023
Quantità di lavoro necessario al conseguimento dei risultati di apprendimento	Minimo 3 – Massimo 5 ore
Livello di competenza necessario al conseguimento della microcredenziale	BASE (FOUNDATION)
Strumento di valutazione	Domande valutate in automatico Numero delle domande: 16 – 20 Percentuale utile al superamento dell'esame: 75%
Modalità di formazione	Online Asincrona
Garanzia di qualità a sostegno della microcredenziale	Revisione paritaria (peer review)

Risultati di apprendimento

Risultati di apprendimento (ref. Level 1 LOs 1.1, 1.2 and 1.3)

- Definire l'identità digitale.
- Descrivere le caratteristiche principali dell'identità digitale.
- Fornire esempi di diverse identità digitali.

Descrizione

Il conseguimento della microcredenziale "Definire l'identità digitale" dimostra che lo studente è in grado di comprendere che l'identità digitale si riferisce alla rappresentazione elettronica di un individuo o di un'organizzazione, e che è un insieme di dati che identificano un utente attraverso la tracciabilità delle sue attività, azioni e contributi digitali su Internet.

Inoltre, questa microcredenziale consentirà agli studenti di descrivere le caratteristiche chiave dell'identità digitale, quali informazioni di identificazione, credenziali di autenticazione, dati di autorizzazione, attributi e caratteristiche, certificati digitali e dati biometrici.

Infine, attraverso questa microcredenziale gli studenti impareranno che le identità digitali possono assumere varie forme attraverso le piattaforme e i servizi online, ad esempio un'identità digitale può essere un account di posta elettronica, un profilo sui social media, una credenziale bancaria online, un ID di e-government, un profilo di gioco, una credenziale per un dispositivo di casa intelligente, un account per servizi di abbonamento e molto altro ancora.

Domande

1. Che cos'è l'identità digitale?
2. Quali sono le caratteristiche principali di un'identità digitale?
3. Cosa sono i dati biometrici?
4. Quali sono alcuni esempi di identità digitali diverse?
5. Un account di servizi di abbonamento è una forma di identità digitale? Spiegate perché.
6. Un profilo di gioco è una forma di identità digitale? Spiegate perché.

Identità digitale: Vantaggi e rischi (MC 2.6.A.2)

Informazioni di base

A chi è rivolto il corso	Qualsiasi cittadino
Titolo e codice della microcredenziale	Digital Identity: Benefits and Risks Code: MC 2.6.A.2
Paese(i)/Regione(i) che hanno contribuito alla pubblicazione	IRLANDA, ITALIA, CIPRO, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Organismo(i) di certificazione	DSW Consortium Numero del progetto: 101087628
Data di pubblicazione	Dicembre 2023
Quantità di lavoro necessario al conseguimento dei risultati di apprendimento	Minimo 1 – Massimo 3 ore
Livello di competenza necessario al conseguimento della microcredenziale	BASE (FOUNDATION)
Strumento di valutazione	Domande valutate in automatico Numero delle domande: 16 – 20 Percentuale utile al superamento dell'esame: 75%
Modalità di formazione	Online Asincrona
Garanzia di qualità a sostegno della microcredenziale	Revisione paritaria (peer review)

Risultati di apprendimento

Risultati di apprendimento (ref. Level 2 LOs 2.4 and 2.5)

- Descrivere i vantaggi dell'identità digitale
- Descrivere i rischi dell'identità digitale

Descrizione

La microcredenziale **"Identità digitale: Benefici e rischi"** indica la capacità degli studenti di descrivere i benefici dell'identità digitale, quali sicurezza e autenticazione, convenienza, protezione della privacy, efficienza e accessibilità e innovazione tecnologica.

Inoltre, questo microcredenziale attesta anche la capacità degli studenti di descrivere i rischi dell'identità digitale, quali problemi di sicurezza, problemi di privacy, mancanza di standardizzazione, sfide normative e legali e innovazione tecnologica.

Domande

1. Quali sono i vantaggi dell'identità digitale?
2. In che modo l'identità digitale è in grado di fornire vantaggi agli utenti?
3. Quali sono i rischi dell'identità digitale?
4. Perché la mancanza di standardizzazione è un rischio dell'identità digitale?
5. Quali sono i problemi di sicurezza legati all'identità digitale?
6. L'innovazione tecnologica è considerata sia un vantaggio che un rischio dell'identità digitale. Spiegatene le ragioni.

Reputazione online (MC 2.6.A.3)

Informazioni di base

A chi è rivolto il corso	Qualsiasi cittadino
Titolo e codice della microcredenziale	Reputazione online **Codice: MC 2.6.A.3**
Paese(i)/Regione(i) che hanno contribuito alla pubblicazione	IRLANDA, ITALIA, CIPRO, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Organismo(i) di certificazione	DSW Consortium Numero del progetto: **101087628**
Data di pubblicazione	Dicembre 2023
Quantità di lavoro necessario al conseguimento dei risultati di apprendimento	Minimo 3 – Massimo 5 ore
Livello di competenza necessario al conseguimento della microcredenziale	BASE (FOUNDATION)
Strumento di valutazione	Domande valutate in automatico Numero delle domande: 16 – 20 Percentuale utile al superamento dell'esame: 75%
Modalità di formazione	Online Asincrona
Garanzia di qualità a sostegno della microcredenziale	Revisione paritaria (peer review)

Risultati di apprendimento

Risultati di apprendimento ref. Level 1 LOs 1.6 and Level 2 LOs 2.7 and 2.8)

- Individuare soluzioni semplici per proteggere la propria reputazione online.
- Chiedere assistenza, quando necessario, per proteggere la propria reputazione online.
- Porre attenzione all'importanza di proteggere la propria reputazione online.

Descrizione

La microcredenziale **"Reputazione online"** insegna agli studenti quali sono i modi per proteggere la propria reputazione online, come ad esempio rivedere e aggiornare le impostazioni della privacy sulle piattaforme di social media, creare profili professionali su piattaforme che non siano associate ai propri account personali su altre piattaforme di social media, evitare di condividere dettagli personali online, mantenere password sicure e uniche e attivare l'autenticazione a due fattori ogni volta che è possibile, essere cauti riguardo ai contenuti che pubblicano sulle piattaforme di social media ed essere cauti riguardo ai gruppi e ai forum a cui si uniscono online.

Inoltre, questa microcredenziale invita gli studenti a richiedere consigli sui modi per proteggere la propria reputazione online, come mantenere password sicure e uniche e attivare l'autenticazione a due fattori ogni volta che è possibile, essere cauti sui contenuti che pubblicano sulle piattaforme di social media ed essere cauti sui gruppi e sui forum a cui si uniscono online.

Infine, il conseguimento di questa microcredenziale dimostra la capacità degli studenti di sensibilizzare gli altri sull'importanza di proteggere la propria reputazione online. Lo studente deve comprendere che la protezione della propria reputazione online è fondamentale per le proprie opportunità professionali, per il proprio personal branding e per la salvaguardia delle proprie informazioni personali, così come anche le aziende dovrebbero proteggere la propria reputazione online, perché questa influisce sulla fiducia e sulla fedeltà dei clienti (ad esempio recensioni positive, testimonianze e una forte presenza digitale possono portare al successo e alla crescita di un'azienda).

Domande

1. Cosa si intende con il termine reputazione online?
2. Sapete indicare dei semplici modi per proteggere la vostra reputazione online?
3. In che modo evitare di condividere dettagli personali aiuta a proteggere la propria reputazione online?
4. Che cosa si intende quando si parla di personal branding?
5. La protezione della reputazione online si riferisce sia alle persone che alle aziende. Spiegate perché.
6. Spiegate l'importanza di proteggere la vostra reputazione online.

Produzione di dati online (MC 2.6.A.4)

Informazioni di base

A chi è rivolto il corso	Qualsiasi cittadino
Titolo e codice della microcredenziale	Produzione di dati online **Codice: MC 2.6.A.4**
Paese(i)/Regione(i) che hanno contribuito alla pubblicazione	IRLANDA, ITALIA, CIPRO, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Organismo(i) di certificazione	DSW Consortium Numero del progetto: **101087628**
Data di pubblicazione	Dicembre 2023
Quantità di lavoro necessario al conseguimento dei risultati di apprendimento	Minimo 2 – Massimo 4 ore
Livello di competenza necessario al conseguimento della microcredenziale	BASE (FOUNDATION)
Strumento di valutazione	Domande valutate in automatico Numero delle domande: 16 – 20 Percentuale utile al superamento dell'esame: 75%
Modalità di formazione	Online Asincrona
Garanzia di qualità a sostegno della microcredenziale	Revisione paritaria (peer review)

Risultati di apprendimento

Risultati di apprendimento (ref. Level 1 LOs 1.9)

- Riconoscere i dati semplici prodotti attraverso strumenti digitali, ambienti e servizi .

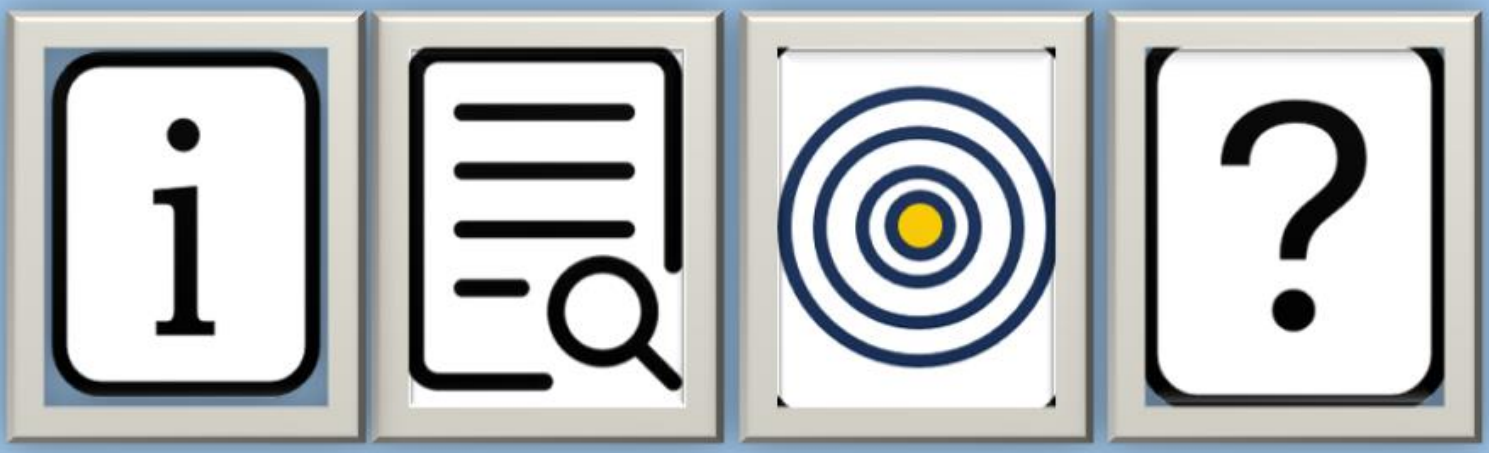
Descrizione

La microcredenziale **"Produrre dati online"** dimostra la capacità degli studenti di riconoscere i dati semplici che vengono prodotti attraverso gli strumenti digitali, gli ambienti e i servizi, come le informazioni personali, i dati sulle attività online, i dati sulle comunicazioni, i dati sulla posizione, i dati sulle transazioni e i dati finanziari (cronologia degli acquisti, transazioni finanziarie, informazioni sui pagamenti), le preferenze e le impostazioni, i dati di autenticazione, le informazioni sui dispositivi, i dati biometrici, le query di ricerca e i cookie e i dati di tracciamento.

Domande

1. Quali tipi di dati vengono prodotti online?
2. Che cos'è la cronologia di navigazione?
3. Quali tipi di dati producete quando fate una ricerca online?
4. Quali sono alcuni esempi di dati personali?
5. Quali sono alcuni esempi di dati sulle attività online?
6. Quali sono alcuni esempi di dati di comunicazione?
7. Quali sono alcuni esempi di dati biometrici?
8. Quali sono alcuni esempi di dati di autenticazione?

LIVELLO INTERMEDIO
(Livello 3 e Livello 4)



Identità digitali di routine (MC 2.6.B.1)

Informazioni di base

A chi è rivolto il corso	Qualsiasi cittadino
Titolo e codice della microcredenziale	Identità digitali di routine **Codice: MC 2.6.B.1**
Paese(i)/Regione(i) che hanno contribuito alla pubblicazione	IRLANDA, ITALIA, CIPRO, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Organismo(i) di certificazione	DSW Consortium Numero del progetto: **101087628**
Data di pubblicazione	Dicembre 2023
Quantità di lavoro necessario al conseguimento dei risultati di apprendimento	Minimo 1 – Massimo 3 ore
Livello di competenza necessario al conseguimento della microcredenziale	INTERMEDIO
Strumento di valutazione	Domande valutate in automatico Numero delle domande: 16 – 20 Percentuale utile al superamento dell'esame: 75%
Modalità di formazione	Online Asincrona
Garanzia di qualità a sostegno della microcredenziale	Revisione paritaria (peer review)

Risultati di apprendimento

Risultati di apprendimento (ref. Level 3 LOs 3.10 and 3.11):

- Distinguere una serie di identità digitali ben definite e di routine.
- Distinguere tra un'identità personale sui social media e un'identità professionale.

Descrizione

Il conseguimento della microcredenziale "Identità digitali di routine" dimostra la capacità degli studenti di distinguere una serie di identità digitali ben definite e di routine, come l'identità personale o professionale sui social media, l'identità di gioco, l'identità di utente di ecommerce, l'identità di piattaforma educativa, l'identità di piattaforma di ricerca di lavoro, l'identità di servizio di abbonamento, ecc.

Inoltre, questa microcredenziale porta gli studenti a comprendere che un'identità personale sui social media può essere utilizzata principalmente per socializzare, connettersi con amici e familiari e condividere esperienze personali. Lo studente deve anche essere in grado di riconoscere i contenuti condivisi da un'identità personale sui social media, come foto e video personali, aggiornamenti casuali, informazioni su hobby e interessi e lo stile di interazione informale.

Infine, questa microcredenziale insegna agli studenti che un'identità professionale può essere utilizzata principalmente per il networking, lo sviluppo della carriera e la presentazione delle capacità e dei risultati relativi a uno specifico settore professionale. Lo studente deve anche essere in grado di riconoscere i contenuti condivisi su un'identità professionale, come i dettagli sull'esperienza lavorativa, i risultati professionali, le capacità, l'istruzione e i riconoscimenti relativi a una carriera specifica e lo stile di interazione formale e incentrato su argomenti professionali.

Domande

1. Quali sono i tipi di identità digitale di routine?
2. Che cos'è l'identità personale sui social media?
3. Che cos'è un'identità professionale sui social media?
4. Qual è lo scopo principale dell'identità personale sui social media? Potete descrivere alcuni dei suoi usi?
5. Qual è lo scopo principale dell'identità professionale sui social media? Potete descriverne alcuni usi?

Costruire un'identità online positiva (MC 2.6.B.2)

Informazioni di base

A chi è rivolto il corso	Qualsiasi cittadino
Titolo e codice della microcredenziale	Costruire un'identità online positiva **Codice: MC 2.6.B.2**
Paese(i)/Regione(i) che hanno contribuito alla pubblicazione	IRLANDA, ITALIA, CIPRO, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Organismo(i) di certificazione	DSW Consortium Numero del progetto: **101087628**
Data di pubblicazione	Dicembre 2023
Quantità di lavoro necessario al conseguimento dei risultati di apprendimento	Minimo 3 – Massimo 5 ore
Livello di competenza necessario al conseguimento della microcredenziale	INTERMEDIO
Strumento di valutazione	Domande valutate in automatico Numero delle domande: 16 – 20 Percentuale utile al superamento dell'esame: 75%
Modalità di formazione	Online Asincrona
Garanzia di qualità a sostegno della microcredenziale	Revisione paritaria (peer review)

Risultati di apprendimento

Risultati di apprendimento (ref. Level 3 LOs 3.12 and 3.13):

- Riconoscere le pratiche di informazione e comunicazione che aiutano un individuo a costruire un'identità online positiva.
- Riconoscere le pratiche di informazione e comunicazione che possono generare un'identità online negativa.

Descrizione

La microcredenziale **"Costruire un'identità online positiva"** dimostra la capacità degli studenti di riconoscere le informazioni e le pratiche di comunicazione che possono aiutare un individuo a costruire un'identità online positiva come, ad esempio, creare e pubblicare contenuti che riflettano positivamente i propri valori e interessi, la condivisione selettiva, promuovere un dialogo costruttivo ed evitare di essere coinvolti in interazioni negative, mantenere un contegno professionale su piattaforme professionali come LinkedIn e rimanere informati sulle tendenze digitali e sulle migliori pratiche.

Inoltre, questa microcredenziale dimostra la capacità degli studenti di riconoscere le informazioni e le pratiche di comunicazione che potrebbero causare un'identità online negativa, come ad esempio l'uso di un linguaggio offensivo o incendiario nelle interazioni online, le molestie online, la condivisione di contenuti che diffondono disinformazione e pettegolezzi, il comportamento inappropriato o non professionale su piattaforme professionali come LinkedIn e l'ignoranza delle tendenze e delle migliori pratiche digitali.

Domande

1. Cosa si intende per identità online positiva?
2. Cosa si intende per identità online negativa?
3. Potete indicare alcune pratiche di informazione e comunicazione che aiutano a costruire un'identità online positiva?
4. Potete citare alcune pratiche di informazione e comunicazione che potrebbero causare un'identità online negativa?
5. Qual è la vostra posizione in merito al dialogo costruttivo e alla diffusione di informazioni errate e notizie false per quanto riguarda il branding dell'identità online?
6. Perché la promozione del dialogo costruttivo è una pratica che aiuta a costruire un'identità online positiva?
7. Perché la diffusione di informazioni e voci errate è una pratica che potrebbe causare un'identità online negativa?

Comprendere e manipolare i dati prodotti online (MC 2.6.B.3)

Informazioni di base

A chi è rivolto il corso	Qualsiasi cittadino
Titolo e codice della microcredenziale	Comprendere e manipolare i dati prodotti online **Codice: MC 2.6.B.3**
Paese(i)/Regione(i) che hanno contribuito alla pubblicazione	IRLANDA, ITALIA, CIPRO, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Organismo(i) di certificazione	DSW Consortium Numero del progetto: **101087628**
Data di pubblicazione	Dicembre 2023
Quantità di lavoro necessario al conseguimento dei risultati di apprendimento	Minimo 3 – Massimo 5 ore
Livello di competenza necessario al conseguimento della microcredenziale	INTERMEDIO
Strumento di valutazione	Domande valutate in automatico Numero delle domande: 16 – 20 Percentuale utile al superamento dell'esame: 75%
Modalità di formazione	Online Asincrona
Garanzia di qualità a sostegno della microcredenziale	Revisione paritaria (peer review)

Risultati di apprendimento

Risultati di apprendimento (ref. Level 3 LOs 3.14 and Level 4 LOs 4.15, 4.16):

- Descrivere il tipo di dati prodotti attraverso strumenti, ambienti e servizi digitali.
- Manipolare i dati prodotti attraverso strumenti, ambienti e servizi digitali.
- Sensibilizzare su quali siano i dati da produrre sull'identità digitale.

Descrizione

La microcredenziale **"Comprendere e manipolare i dati prodotti online"** attesta l'ampia conoscenza degli studenti dei dati prodotti online, come quelli relativi alle informazioni personali, alle firme digitali, alle informazioni di contatto, alla biometria, alla cronologia del browser e ai cookie, alla cronologia delle transazioni, alle preferenze e agli interessi, ai metadati delle comunicazioni, ai dati di autenticazione e autorizzazione e alle registrazioni del consenso dato.

Inoltre, questa microcredenziale dimostra la capacità degli studenti di manipolare i dati prodotti attraverso strumenti, ambienti e servizi digitali. Ad esempio, per quanto riguarda le informazioni personali, lo studente sarà in grado di riconoscere quando è necessario aggiungere informazioni come l'indirizzo di casa o il numero di telefono.

Infine, questa microcredenziale porterà gli studenti a sensibilizzare gli altri su quali dati si debbano produrre nell'ambito dell'identità digitale, ad esempio i dati relativi alle informazioni personali dovrebbero essere evitati a meno che non sia assolutamente necessario (ad esempio, l'indirizzo di casa, i numeri di telefono), i dati relativi alle informazioni finanziarie dovrebbero essere condivisi con cautela (ad esempio, i numeri dei conti bancari, i dettagli delle carte di credito, i PIN delle carte), mentre i dati relativi all'ubicazione dovrebbero essere evitati a meno che non sia necessario per proteggere la propria sicurezza fisica e la propria privacy.

Domande

1. Nominate un tipo di dati prodotti online.
2. Si possono manipolare i dati relativi alle informazioni personali? Spiegate come.
3. Si possono manipolare i dati relativi alle informazioni di contatto? Spiegate come.
4. È possibile manipolare i dati relativi alla posizione? Spiegate come.
5. Perché è importante manipolare i dati prodotti online?

Creazione e gestione di profili per scopi personali o professionali (MC 2.6.B.4)

Informazioni di base

A chi è rivolto il corso	Qualsiasi cittadino
Titolo e codice della microcredenziale	Creazione e gestione di profili per scopi personali o professionali **Codice: MC 2.6.B.4**
Paese(i)/Regione(i) che hanno contribuito alla pubblicazione	IRLANDA, ITALIA, CIPRO, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Organismo(i) di certificazione	DSW Consortium Numero del progetto: **101087628**
Data di pubblicazione	Dicembre 2023
Quantità di lavoro necessario al conseguimento dei risultati di apprendimento	Minimo 1 – Massimo 3 ore
Livello di competenza necessario al conseguimento della microcredenziale	INTERMEDIO
Strumento di valutazione	Domande valutate in automatico Numero delle domande: 16 – 20 Percentuale utile al superamento dell'esame: 75%
Modalità di formazione	Online Asincrona
Garanzia di qualità a sostegno della microcredenziale	Revisione paritaria (peer review)

Risultati di apprendimento

Risultati di apprendimento (ref. Level 3 LOs 3.17 and 3.18):

- Creare profili in ambienti digitali per scopi personali o professionali.
- Gestire i profili in ambienti digitali per scopi personali o professionali.

Descrizione

La microcredenziale **"Creare e gestire profili per scopi personali o professionali"** dimostra la capacità degli studenti di creare un profilo attraverso la corretta compilazione dei dati del profilo, tra cui la biografia, le informazioni di contatto, l'istruzione, l'esperienza lavorativa e qualsiasi altro dettaglio rilevante.

Inoltre, questa microcredenziale dimostra la capacità degli studenti di gestire il proprio profilo nell'ambiente digitale per scopi personali o professionali attraverso aggiornamenti regolari, impostazione della privacy, presentazione delle capacità, ricerca di approvazione, revisione e pulizia dei profili digitali, ecc.

Domande

1. Quali informazioni includereste nel vostro profilo digitale?
2. Descrivete le attività da intraprendere per garantire che il vostro profilo rimanga aggiornato e interessante.
3. Come potete migliorare il vostro profilo digitale?
4. Distinguete tra un profilo digitale da utilizzare per uso personale e per uso professionale.

Strategie per proteggere la propria reputazione online (MC 2.6.B.5)

Informazioni di base

A chi è rivolto il corso	Qualsiasi cittadino
Titolo e codice della microcredenziale	Strategie per proteggere la propria reputazione online **Codice: MC 2.6. B.5**
Paese(i)/Regione(i) che hanno contribuito alla pubblicazione	IRLANDA, ITALIA, CIPRO, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Organismo(i) di certificazione	DSW Consortium Numero del progetto: **101087628**
Data di pubblicazione	Dicembre 2023
Quantità di lavoro necessario al conseguimento dei risultati di apprendimento	Minimo 1 – Massimo 3 ore
Livello di competenza necessario al conseguimento della microcredenziale	INTERMEDIO
Strumento di valutazione	Domande valutate in automatico Numero delle domande: 16 – 20 Percentuale utile al superamento dell'esame: 75%
Modalità di formazione	Online Asincrona
Garanzia di qualità a sostegno della microcredenziale	Revisione paritaria (peer review)

Risultati di apprendimento

Risultati di apprendimento (ref. Level 3 LOs 3.19)

- Presentare diverse strategie per proteggere la propria reputazione online.

Descrizione

La microcredenziale **"Strategie per proteggere la propria reputazione online"** fornisce agli studenti diverse strategie per proteggere la propria reputazione online, come ad esempio monitorare la propria presenza online cercando regolarmente il proprio nome, impostare gli avvisi sul proprio browser, regolare le impostazioni della privacy sulle piattaforme dei social media, essere cauti riguardo alle informazioni condivise online, utilizzare password forti ed essere cauti riguardo ai contenuti che si pubblicano online.

Domande

1. Indicare alcune strategie per proteggere la propria reputazione online.
2. Come si può monitorare la propria presenza online? Fornite alcuni esempi.
3. Perché la regolazione della privacy sulle piattaforme di social media è una strategia per proteggere la propria reputazione online?
4. Descrivete le informazioni che si possono condividere online e quelle che non si dovrebbero condividere online.
5. Sapete indicare alcune impostazioni della privacy che possono essere modificate?

Metadati nelle immagini condivise (MC 2.6.B.6)

Informazioni di base

A chi è rivolto il corso	Qualsiasi cittadino
Titolo e codice della microcredenziale	Metadati nelle immagini condivise **Codice: MC 2.6. B.6**
Paese(i)/Regione(i) che hanno contribuito alla pubblicazione	IRELAND, ITALY, CYPRUS, GREECE, ROMANIA http://dsw.projectsgallery.eu
Organismo(i) di certificazione	DSW Consortium Project Number: **101087628**
Data di pubblicazione	Dec 2023
Quantità di lavoro necessario al conseguimento dei risultati di apprendimento	3-5 Hours
Livello di competenza necessario al conseguimento della microcredenziale	INTERMEDIATE
Strumento di valutazione	Automatically marked Questions Number of Questions: 16 – 20 Passing Score: 75%
Modalità di formazione	Online Asynchronous
Garanzia di qualità a sostegno della microcredenziale	Peer Review

Risultati di apprendimento

Risultati di apprendimento (ref. Level 3 LOs 3.20 and Level 4 LOs 4.21)

- Descrivere il tipo di metadati inclusi nelle immagini condivise.
- Descrivere i modi in cui è possibile modificare i metadati di un'immagine condivisa.

Descrizione

La microcredenziale **"Metadati nelle immagini condivise"** mostra agli studenti quali tipi di metadati sono inclusi nelle immagini condivise, come i dati EXIF (Exchangeable Image File Format), i dati IPTC (International Press Telecommunications Council), i dati XMP (Extensible metadata platform), i dati informativi sui file, nonché la capacità degli studenti di riconoscere i metadati che possono essere modificati.

Infine, questa microcredenziale dimostra la capacità degli studenti di descrivere i modi in cui è possibile modificare i metadati di un'immagine condivisa, ad esempio utilizzando strumenti e siti web online (Metapicz), utilizzando software specializzati (Exif Pilot, Adobe Lightroom), su Windows e MacOS e utilizzando software di editing delle immagini (Photoshop, GIMP).

Domande

1. Che tipo di metadati sono inclusi nelle immagini condivise?
2. Cosa comprendono i dati EXIF?
3. Cosa comprendono i dati IPTC?
4. Quali tipi di metadati possono essere modificati?
5. Quali strumenti digitali si possono utilizzare per modificare i metadati?
6. Descrivete il processo che seguireste per modificare i metadati utilizzando uno strumento digitale.
7. Descrivere la procedura da seguire per modificare i metadati su Windows..

Gestire più identità digitali: Vantaggi e rischi (MC 2.6.B.7)

Informazioni di base

A chi è rivolto il corso	Qualsiasi cittadino
Titolo e codice della microcredenziale	Gestire più identità digitali: Vantaggi e rischi **Codice: MC 2.6. B.7**
Paese(i)/Regione(i) che hanno contribuito alla pubblicazione	IRLANDA, ITALIA, CIPRO, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Organismo(i) di certificazione	DSW Consortium Numero del progetto: **101087628**
Data di pubblicazione	Dicembre 2023
Quantità di lavoro necessario al conseguimento dei risultati di apprendimento	Minimo 4 – Massimo 6 ore
Livello di competenza necessario al conseguimento della microcredenziale	INTERMEDIO
Strumento di valutazione	Domande valutate in automatico Numero delle domande: 16 – 20 Percentuale utile al superamento dell'esame: 75%
Modalità di formazione	Online Asincrona
Garanzia di qualità a sostegno della microcredenziale	Revisione paritaria (peer review)

Risultati di apprendimento

Risultati di apprendimento (ref. Level 4 LOs 4.22 and 4.23)

- Identificare i vantaggi della gestione di una o più identità digitali tra sistemi, applicazioni e servizi digitali.
- Identificare i rischi della gestione di una o più identità digitali attraverso sistemi, applicazioni e servizi digitali.

Descrizione

La microcredenziale **"Gestire più identità digitali: Benefici e rischi"** dimostra la capacità degli studenti di identificare i benefici della gestione di una o più identità digitali, come l'accesso e la comodità, la personalizzazione, l'autenticazione efficiente, i servizi personalizzati e il networking professionale, nonché la capacità degli studenti di identificare i rischi della gestione di una o più identità digitali, come le minacce alla sicurezza, le preoccupazioni per la privacy, la frammentazione dell'identità, le violazioni dei dati, i danni alla reputazione, le sfide di autenticazione e la mancanza di controllo.

Domande

1. Quali sono i vantaggi della gestione di una o più identità digitali attraverso sistemi, applicazioni e servizi digitali?
2. Quali sono i rischi della gestione di una o più identità digitali attraverso sistemi, applicazioni e servizi digitali?
3. Perché l'accesso e la praticità sono un vantaggio nella gestione di una o più identità digitali attraverso sistemi, applicazioni e servizi digitali?
4. Perché la mancanza di controllo è un rischio nella gestione di una o più identità digitali attraverso sistemi, applicazioni e servizi digitali?
5. Perché i danni alla reputazione sono un rischio quando si gestiscono una o più identità digitali attraverso sistemi, applicazioni e servizi digitali?

LIVELLO AVANZATO
(Livello 5 e Livello 6)

Identità digitale coerente (MC 2.6.C.1)

Informazioni di base

A chi è rivolto il corso	Qualsiasi cittadino
Titolo e codice della microcredenziale	Identità digitale coerente **Codice: MC 2.6.C.1**
Paese(i)/Regione(i) che hanno contribuito alla pubblicazione	IRLANDA, ITALIA, CIPRO, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Organismo(i) di certificazione	DSW Consortium Numero del progetto: **101087628**
Data di pubblicazione	Dicembre 2023
Quantità di lavoro necessario al conseguimento dei risultati di apprendimento	Minimo 3 – Massimo 5 ore
Livello di competenza necessario al conseguimento della microcredenziale	AVANZATO
Strumento di valutazione	Domande valutate in automatico Numero delle domande: 16 – 20 Percentuale utile al superamento dell'esame: 75%
Modalità di formazione	Online Asincrona
Garanzia di qualità a sostegno della microcredenziale	Revisione paritaria (peer review)

Risultati di apprendimento

Risultati di apprendimento (ref. Level 6 LOs 6.24, 6.25 and 6.26):

- Spiegare l'espressione "identità digitale coerente in tutti i social media".
- Spiegare perché si dovrebbe avere un'identità digitale coerente in tutti i social media.
- Creare un'identità digitale coerente in tutti i social media.

Descrizione

La microcredenziale **"Identità digitale coerente"** insegna agli studenti a spiegare l'espressione "identità digitale coerente in tutti i social media", che si riferisce al mantenimento di una presenza online uniforme su diverse piattaforme. Ciò include l'uso di nomi utente uguali o simili, immagini di profilo e una strategia di branding personale o professionale standardizzata, nonché la capacità degli studenti di giustificare il motivo per cui si dovrebbe avere un'identità digitale coerente in tutti i social media al fine di creare un marchio personale riconoscibile che rappresenti la persona su diversi canali online.

Inoltre, questa microcredenziale dimostra la capacità degli studenti di creare un'identità digitale coerente.

Domande

1. Cosa si intende per identità digitale coerente in tutti i social media?
2. Quali sono le caratteristiche principali di un'identità digitale coerente?
3. Quali sono le principali ragioni per cui si dovrebbe avere un'identità digitale coerente?
4. Descrivete le strategie attraverso le quali si può raggiungere la coerenza della propria identità digitale.
5. Quali elementi di branding si possono utilizzare per ottenere coerenza nella propria identità digitale.

Modificare i metadati (MC 2.6.C.2)

Informazioni di base

A chi è rivolto il corso	Qualsiasi cittadino
Titolo e codice della microcredenziale	Modificare i metadati **Codice: MC 2.6.C.2**
Paese(i)/Regione(i) che hanno contribuito alla pubblicazione	IRLANDA, ITALIA, CIPRO, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Organismo(i) di certificazione	DSW Consortium Numero del progetto: **101087628**
Data di pubblicazione	Dicembre 2023
Quantità di lavoro necessario al conseguimento dei risultati di apprendimento	Minimo 4 – Massimo 6 ore
Livello di competenza necessario al conseguimento della microcredenziale	AVANZATO
Strumento di valutazione	Domande valutate in automatico Numero delle domande: 16 – 20 Percentuale utile al superamento dell'esame: 75%
Modalità di formazione	Online Asincrona
Garanzia di qualità a sostegno della microcredenziale	Revisione paritaria (peer review)

Risultati di apprendimento

Risultati di apprendimento (ref. Level 6 LOs 6.27 and 6.28):

- Selezionare una foto che si desidera caricare su una specifica piattaforma di social media e modificarne i metadati utilizzando un software specifico.
- Sottolineare l'importanza di modificare i metadati per proteggere la propria privacy.

Descrizione

La microcredenziale **"Modificare i metadati"** dimostra la capacità degli studenti di selezionare una foto che desiderano caricare su una specifica piattaforma di social media e di modificarne i metadati utilizzando uno specifico strumento o software digitale. Questa microcredenziale dimostra anche la loro capacità a sottolineare l'importanza di modificare i metadati per proteggere la propria privacy, ad esempio modificando o rimuovendo le informazioni relative al luogo, all'ora e alla data in cui la foto è stata scattata, l'individuo può evitare di rivelare i propri spostamenti e le informazioni sulle proprie attività.

Domande

1. Indicare due software che possono essere utilizzati per modificare i metadati di un'immagine.
2. Selezionate un software e descrivete il processo di modifica dei metadati di un'immagine.
3. Quale tipo di metadati può essere modificato?
4. Come può un individuo mantenere l'anonimato modificando i metadati?
5. Come si può ridurre il rischio di essere rintracciati modificando i metadati?
6. Spiegare l'importanza di modificare i metadati di un'immagine.

Gestire più identità digitali (MC 2.6.C.3)

Informazioni di base

A chi è rivolto il corso	Qualsiasi cittadino
Titolo e codice della microcredenziale	Gestire più identità digitali **Codice: MC 2.6.C.3**
Paese(i)/Regione(i) che hanno contribuito alla pubblicazione	IRLANDA, ITALIA, CIPRO, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Organismo(i) di certificazione	DSW Consortium Numero del progetto: **101087628**
Data di pubblicazione	Dicembre 2023
Quantità di lavoro necessario al conseguimento dei risultati di apprendimento	Minimo 4 – Massimo 6 ore
Livello di competenza necessario al conseguimento della microcredenziale	AVANZATO
Strumento di valutazione	Domande valutate in automatico Numero delle domande: 16 – 20 Percentuale utile al superamento dell'esame: 75%
Modalità di formazione	Online Asincrona
Garanzia di qualità a sostegno della microcredenziale	Revisione paritaria (peer review)

Risultati di apprendimento

Risultati di apprendimento (ref. Level 5 LOs 5.29 and 5.30):

- Gestire una o più identità digitali attraverso i sistemi digitali
- Considerare i vantaggi e i rischi della gestione di una o più identità digitali attraverso sistemi, app e servizi digitali.

Descrizione

La microcredenziale **" Gestire più identità digitali"** dimostra l'abilità degli studenti di poter gestire una o più identità digitali attraverso i sistemi digitali. Dopo aver conseguito questa microcredenziale gli studenti saranno anche in grado di elencare i vantaggi della gestione di una o più identità digitali attraverso i sistemi digitali, le app e i servizi, come ad esempio la creazione di un marchio personale e di una reputazione professionale, il mantenimento delle opportunità di rete, il miglioramento della comunicazione efficiente, l'adattamento più facile ai cambiamenti, l'aumento della visibilità e altro ancora.

Domande

1. Cosa si intende per gestione di una o più identità digitali attraverso i sistemi digitali?
2. Fornite un esempio di gestione di una o più identità digitali attraverso i sistemi digitali.
3. Quali sistemi, app e servizi digitali utilizzereste per gestire le identità digitali multiple?
4. Quali sono i vantaggi della gestione di una o più identità digitali?
5. Come si può ottenere una comunicazione efficiente quando si gestiscono più identità digitali?

Controllare, gestire o cancellare i dati raccolti dai sistemi online (MC 2.6.C.4)

Informazioni di base

A chi è rivolto il corso	Qualsiasi cittadino
Titolo e codice della microcredenziale	Controllare, gestire o cancellare i dati raccolti dai sistemi online **Codice: MC 2.6.C.4**
Paese(i)/Regione(i) che hanno contribuito alla pubblicazione	IRLANDA, ITALIA, CIPRO, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Organismo(i) di certificazione	DSW Consortium Numero del progetto: **101087628**
Data di pubblicazione	Dicembre 2023
Quantità di lavoro necessario al conseguimento dei risultati di apprendimento	Minimo 1 – Massimo 3 ore
Livello di competenza necessario al conseguimento della microcredenziale	AVANZATO
Strumento di valutazione	Domande valutate in automatico Numero delle domande: 16 – 20 Percentuale utile al superamento dell'esame: 75%
Modalità di formazione	Online Asincrona
Garanzia di qualità a sostegno della microcredenziale	Revisione paritaria (peer review)

Risultati di apprendimento

Risultati di apprendimento (ref. Level 6 LOs 6.31):

- Utilizzare strategie per controllare, gestire o cancellare i dati raccolti dai sistemi online.

Descrizione

La microcredenziale **"Controllare, gestire o cancellare i dati raccolti dai sistemi online"** dimostra che gli studenti sono in grado di utilizzare in modo efficace le strategie per controllare, gestire o cancellare i dati raccolti dai sistemi online, come cancellare regolarmente i cookie e la cache, esercitare il diritto di richiedere la cancellazione dei propri dati dalle piattaforme online, utilizzare password forti e l'autenticazione a due fattori, verificare regolarmente le app connesse ed educare se stessi.

Domande

1. Definite le strategie per controllare, gestire o cancellare i dati raccolti dai sistemi online.
2. Come si cancellano i cookie e la cache?
3. È possibile richiedere la cancellazione dei dati da una piattaforma online? Qual è la procedura da seguire?
4. Perché l'utilizzo dell'autenticazione a due fattori è una buona strategia da seguire?
5. Come ci si può formare per essere efficienti nel controllo, nella gestione e nella cancellazione dei dati raccolti dai sistemi online?

Utilizzare diverse strategie per proteggere la propria reputazione online (MC 2.6.C.5)

Informazioni di base

A chi è rivolto il corso	Qualsiasi cittadino
Titolo e codice della microcredenziale	Utilizzare diverse strategie per proteggere la propria reputazione online **Codice: MC 2.6.C.5**
Paese(i)/Regione(i) che hanno contribuito alla pubblicazione	IRLANDA, ITALIA, CIPRO, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Organismo(i) di certificazione	DSW Consortium Numero del progetto: **101087628**
Data di pubblicazione	Dicembre 2023
Quantità di lavoro necessario al conseguimento dei risultati di apprendimento	Minimo 3 – Massimo 5 ore
Livello di competenza necessario al conseguimento della microcredenziale	AVANZATO
Strumento di valutazione	Domande valutate in automatico Numero delle domande: 16 – 20 Percentuale utile al superamento dell'esame: 75%
Modalità di formazione	Online Asincrona
Garanzia di qualità a sostegno della microcredenziale	Revisione paritaria (peer review)

Risultati di apprendimento

Risultati di apprendimento (ref. Level 5 LOs 5.32 and 6.33):

- Saper mettere in atto diverse strategie per proteggere la propria reputazione online.
- Spiegare le strategie più appropriate per proteggere la propria reputazione online.

Descrizione

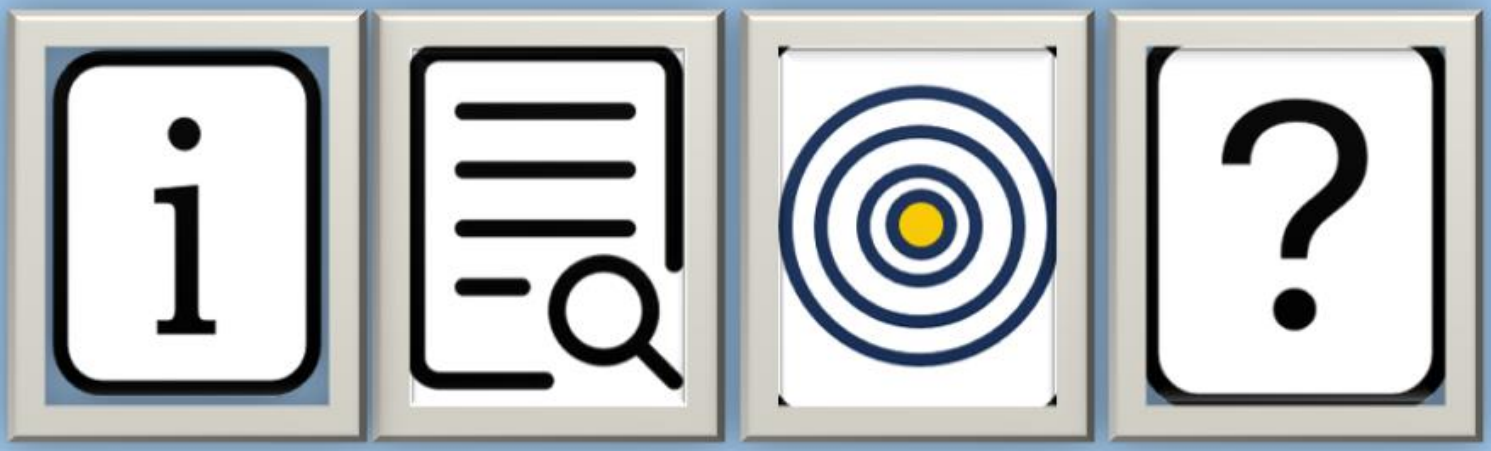
La microcredenziale **"Utilizzare diverse strategie per proteggere la propria reputazione online"** dimostra la padronanza da parte degli studenti di diverse strategie per proteggere la propria reputazione online, come cercare il proprio nome e le sue varianti sui motori di ricerca, impostare avvisi nel proprio browser per ricevere notifiche su menzioni o aggiornamenti relativi alla propria presenza online, regolare l'impostazione della privacy sulle piattaforme di social media per controllare chi può vedere le proprie informazioni personali, utilizzare password sicure e uniche per i vari account online, attivare l'autenticazione a due fattori quando possibile, considerare il tipo di contenuti che si condividono online per evitare di pubblicare contenuti controversi o offensivi.

Questa microcredenziale dimostra anche la capacità degli studenti di poter spiegare le strategie più appropriate per proteggere la propria reputazione online, come le impostazioni della privacy, il monitoraggio regolare online, gli account online sicuri, la condivisione dei contenuti e il galateo online.

Domande

1. Presentare le strategie per proteggere la propria reputazione online.
2. Descrivete i passaggi da seguire per impostare gli avvisi in due browser al fine di ricevere notifiche su menzioni o aggiornamenti relativi alla vostra presenza online.
3. Cosa si intende quando si parla di monitoraggio online regolare?
4. Come si proteggono gli account online? Descrivete i contenuti che si possono condividere online e quelli che non si devono condividere online.

LIVELLO ESPERTO
(Livello 7 e Livello 8)



Affrontare problemi complessi legati all'identità digitale e alla protezione della propria reputazione online (MC 2.6.D.1)

Informazioni di base

A chi è rivolto il corso	Qualsiasi cittadino
Titolo e codice della microcredenziale	Affrontare problemi complessi legati all'identità digitale e alla protezione della propria reputazione online. **Codice: MC 2.6.D.1**
Paese(i)/Regione(i) che hanno contribuito alla pubblicazione	IRLANDA, ITALIA, CIPRO, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Organismo(i) di certificazione	DSW Consortium Numero del progetto: **101087628**
Data di pubblicazione	Dicembre 2023
Quantità di lavoro necessario al conseguimento dei risultati di apprendimento	Minimo 3 – Massimo 5 ore
Livello di competenza necessario al conseguimento della microcredenziale	ESPERTO
Strumento di valutazione	Domande valutate in automatico Numero delle domande: 16 – 20 Percentuale utile al superamento dell'esame: 75%
Modalità di formazione	Online Asincrona
Garanzia di qualità a sostegno della microcredenziale	Revisione paritaria (peer review)

Risultati di apprendimento

Risultati di apprendimento (ref. Level 7 LOs 7.34 and 7.35):

- Spiegare perché la creazione di soluzioni a problemi complessi legati all'identità digitale richiede un approccio strategico.
- Spiegare perché la creazione di soluzioni a problemi complessi legati alla protezione della propria reputazione online richiede un approccio strategico.

Descrizione

La microcredenziale **"Affrontare i problemi complessi legati all'identità digitale e alla protezione della propria reputazione online"** dimostra la capacità degli studenti di spiegare perché affrontare i problemi complessi legati all'identità digitale richiede un approccio strategico che enfatizza ragioni come l'interconnessione dei sistemi, la diversità degli stakeholder, la conformità normativa, le preoccupazioni relative alla sicurezza e alla privacy, la tecnologia in rapida evoluzione, le considerazioni globali, la complessità dell'ecosistema e le considerazioni etiche.

Inoltre, questa microcredenziale dimostra la capacità di chi apprende di spiegare perché affrontare i problemi complessi legati alla protezione della propria reputazione online richieda un approccio strategico, enfatizzando ragioni quali la diversità delle piattaforme e dei canali, il monitoraggio continuo, la diversità degli stakeholder, le considerazioni legali, l'integrazione della tecnologia, la necessità di costruire la reputazione in modo proattivo, la necessità di adattarsi al cambiamento.

Domande

1. Per quali ragioni affrontare i problemi complessi legati all'identità digitale richiede un approccio strategico?
2. Indicate alcuni stakeholder chiave che dobbiamo prendere in considerazione quando affrontiamo problemi complessi legati all'identità digitale. In che modo gli stakeholder sono legati alla complessità dei problemi legati all'identità digitale?
3. Per quali ragioni affrontare i problemi complessi legati alla protezione della propria reputazione online richiede un approccio strategico?
4. In che modo le considerazioni legali possono essere collegate alla protezione della propria reputazione online?
5. Spiegate perché è necessario costruire la reputazione in modo proattivo.

Guidare gli altri nella gestione di una o più identità e proteggere la propria reputazione online. (MC 2.6.D.2)

Informazioni di base

A chi è rivolto il corso	Qualsiasi cittadino
Titolo e codice della microcredenziale	Guidare gli altri nella gestione di una o più identità e proteggere la propria reputazione online. **Codice: MC 2.6.D.2**
Paese(i)/Regione(i) che hanno contribuito alla pubblicazione	IRLANDA, ITALIA, CIPRO, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Organismo(i) di certificazione	DSW Consortium Numero del progetto: **101087628**
Data di pubblicazione	Dicembre 2023
Quantità di lavoro necessario al conseguimento dei risultati di apprendimento	Minimo 5 – Massimo 8 ore
Livello di competenza necessario al conseguimento della microcredenziale	ESPERTO
Strumento di valutazione	Domande valutate in automatico Numero delle domande: 16 – 20 Percentuale utile al superamento dell'esame: 75%
Modalità di formazione	Online Asincrona
Garanzia di qualità a sostegno della microcredenziale	Revisione paritaria (peer review)

Risultati di apprendimento

Risultati di apprendimento (ref. Level 7 LOs 7.36 and 7.37):

- Guidare gli altri nella gestione di una o più identità digitali.
- Guidare gli altri nella protezione della propria reputazione online.

Descrizione

La microcredenziale **"Guidare gli altri nella gestione di una o più identità e proteggere la propria reputazione online"** dimostra la capacità degli studenti di condurre workshop su come gestire una o più identità, incluse sessioni su come impostare la privacy, come rivedere e ripulire, come aggiornare regolarmente e come mostrare le capacità.

Inoltre, questa microcredenziale dimostra la capacità degli studenti di condurre workshop su come proteggere la propria reputazione online, comprese sessioni sulle impostazioni della privacy, sul monitoraggio online regolare, sugli account online sicuri, sulla condivisione dei contenuti e sul galateo online.

Domande

1. Definire l'importanza di guidare gli altri nella gestione di una o più identità digitali.
2. Descrivete i principali risultati di un workshop che organizzereste sulle impostazioni della privacy.
3. Descrivete i principali risultati di un workshop che organizzereste su come rivedere e ripulire la vostra identità digitale.
4. Descrivete i principali risultati dell'apprendimento di un workshop che organizzereste su aggiornamenti regolari e capacità di mostrare le identità digitali.
5. Elaborate l'importanza di guidare gli altri nella protezione della propria reputazione online.
6. Descrivete i principali risultati di un workshop che organizzereste sul galateo online.

Ricerca di un nome negli ambienti online e modifica delle configurazioni utente (MC 2.6.D.3)

Informazioni di base

A chi è rivolto il corso	Qualsiasi cittadino
Titolo e codice della microcredenziale	Ricerca di un nome negli ambienti online e modifica delle configurazioni utente **Codice: MC 2.6.D.3**
Paese(i)/Regione(i) che hanno contribuito alla pubblicazione	IRLANDA, ITALIA, CIPRO, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Organismo(i) di certificazione	DSW Consortium Numero del progetto: **101087628**
Data di pubblicazione	Dicembre 2023
Quantità di lavoro necessario al conseguimento dei risultati di apprendimento	Minimo 3 – Massimo 5 ore
Livello di competenza necessario al conseguimento della microcredenziale	ESPERTO
Strumento di valutazione	Domande valutate in automatico Numero delle domande: 16 – 20 Percentuale utile al superamento dell'esame: 75%
Modalità di formazione	Online Asincrona
Garanzia di qualità a sostegno della microcredenziale	Revisione paritaria (peer review)

Risultati di apprendimento

Risultati di apprendimento (ref. Level 7 LOs 7.38 and Level 8 LOs 8.39):

- Condurre una ricerca online di nomi di persone o famiglie.
- Modificare le configurazioni degli utenti per abilitare, impedire o moderare il tracciamento, la raccolta o l'analisi dei dati da parte del sistema AI.

Descrizione

La microcredenziale **"Ricerca di un nome in ambienti online e modifica delle configurazioni utente"** dimostra la capacità degli studenti di condurre una ricerca di un nome individuale o di famiglia in ambienti online al fine di ispezionare la propria impronta digitale. Inoltre, questa microcredenziale dimostra la capacità degli studenti di modificare le configurazioni dell'utente attraverso l'uso di app, software e piattaforme digitali, al fine di abilitare, impedire o moderare il tracciamento, la raccolta o l'analisi dei dati da parte del sistema di intelligenza artificiale.

Domande

1. Che cos'è l'impronta digitale?
2. Elaborare l'importanza di condurre una ricerca individuale negli ambienti online al fine di ispezionare la propria impronta digitale?
3. Descrivete i passi da seguire per condurre una ricerca individuale negli ambienti online al fine di controllare la propria impronta digitale?
4. Potete spiegare l'importanza di modificare le configurazioni degli utenti per abilitare, prevenire o moderare il tracciamento, la raccolta o l'analisi dei dati da parte del sistema di intelligenza artificiale?
5. Descrivete i passaggi da seguire per modificare le configurazioni dell'utente al fine di abilitare, prevenire o moderare il tracciamento, la raccolta o l'analisi dei dati da parte del sistema di intelligenza artificiale.
6. Che cos'è l'opzione di opt-out? Fornite degli esempi.

Proporre nuove idee relative alla gestione dell'identità digitale e alla protezione della propria reputazione online (MC 2.6.D.4)

Informazioni di base

A chi è rivolto il corso	Qualsiasi cittadino
Titolo e codice della microcredenziale	Proporre nuove idee relative alla gestione dell'identità digitale e alla protezione della propria reputazione online **Codice: MC 2.6.D.4**
Paese(i)/Regione(i) che hanno contribuito alla pubblicazione	IRLANDA, ITALIA, CIPRO, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Organismo(i) di certificazione	DSW Consortium Numero del progetto: **101087628**
Data di pubblicazione	Dicembre 2023
Quantità di lavoro necessario al conseguimento dei risultati di apprendimento	Minimo 1 – Massimo 3 ore
Livello di competenza necessario al conseguimento della microcredenziale	ESPERTO
Strumento di valutazione	Domande valutate in automatico Numero delle domande: 16 – 20 Percentuale utile al superamento dell'esame: 75%
Modalità di formazione	Online Asincrona
Garanzia di qualità a sostegno della microcredenziale	Revisione paritaria (peer review)

Risultati di apprendimento

Risultati di apprendimento (ref. Level 8 LOs 8.40 and 8.41):

- Proporre nuove idee nel campo della gestione delle identità digitali.
- Proporre nuove idee nel campo della protezione della propria reputazione online.

Descrizione

La microcredenziale **"Proporre nuove idee relative alla gestione di un'identità digitale e alla protezione della propria reputazione online"** dimostra la capacità degli studenti di proporre diverse idee relative alla gestione delle identità digitali, come le piattaforme di identità decentralizzate, l'autenticazione biometrica, la verifica dell'identità guidata dall'IA, le tecnologie che preservano la privacy e le piattaforme di identità collaborative.

Inoltre, questa microcredenziale dimostra la capacità degli studenti di proporre diverse idee relative alla protezione della propria reputazione online, come sistemi basati su blockchain per la verifica dell'identità, app personalizzate per la privacy e la sicurezza e strumenti di gestione delle crisi basati sull'intelligenza artificiale.

Domande

1. Come si può sfruttare l'intelligenza artificiale per prevedere i rischi legati all'identità?
2. Come si può sfruttare l'intelligenza artificiale per implementare in modo proattivo misure di sicurezza per prevenire potenziali minacce?
3. Elaborare idee come la condivisione dell'identità basata sul consenso, che consente agli individui di concedere autorizzazioni per un periodo di tempo specifico e limitato, avendo così il controllo sulle proprie informazioni personali.
4. In che modo la combinazione della biometria potrebbe contribuire a sistemi accurati di verifica dell'identità?
5. Elaborare l'idea di un'autenticazione anonima ma sicura, che permetta agli utenti di accedere ai servizi senza rivelare la propria identità completa.

APPENDICE 1: RISULTATI DI APPRENDIMENTO PER L'AREA DI COMPETENZA: GESTIONE DELL'IDENTITÀ DIGITALE

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them

COMPETENZA: COMUNICAZIONE E COLLABORAZIONE (2)		
AREA DI COMPETENZA 2.6: GESTIONE DELL'IDENTITÀ DIGITALE		
Creare e gestire una o più identità digitali, essere in grado di proteggere la propria reputazione, gestire i dati che si producono attraverso diversi strumenti digitali, ambienti e servizi.		
1	A livello base e con la guida, sono in grado di:	• Identificare un'identità digitale • descrivere i modi più semplici per proteggere la mia reputazione online • riconoscere i dati semplici che si producono attraverso gli strumenti digitali, gli ambienti o i servizi
2	A livello di base e con autonomia e una guida appropriata, se necessario, sono in grado di:	• Identificare un'identità digitale • descrivere i modi più semplici per proteggere la propria reputazione online • riconoscere i dati semplici che si producono attraverso gli strumenti digitali, ambienti o servizi
3	Da solo e risolvendo problemi semplici, posso:	• determinare una serie di identità digitali ben definite e di routine • definire modi ben definiti e di routine per proteggere la propria reputazione online • definire dati ben definiti che si producono abitualmente attraverso strumenti, ambienti o servizi digitali
4	In modo indipendente, in base alle mie esigenze, e risolvendo problemi ben definiti e non di routine, posso:	• mostrare una varietà di identità digitali specifiche • discutere di modi specifici per proteggere la propria reputazione online, • manipolare i dati che vengono prodotti attraverso strumenti, ambienti o servizi digitali
5	Oltre a guidare gli altri, sono in grado di:	• utilizzare una varietà di identità digitali • applicare modi diversi per proteggere la propria reputazione online • utilizzare i dati che si producono attraverso strumenti, ambienti o servizi digitali
6	A livello avanzato, in base alle mie esigenze e a quelle degli altri, e in contesti complessi, posso:	• individuare le diverse identità digitali • spiegare i modi più appropriati per proteggere la propria reputazione • modificare i dati che si producono attraverso strumenti, ambienti o servizi digitali
7	A livello altamente specializzato, posso:	• creare soluzioni a problemi complessi con una definizione limitata, legati alla gestione delle identità digitali e alla protezione della reputazione online delle persone • integrare le proprie conoscenze per contribuire alle pratiche e alle conoscenze professionali e guidare gli altri nella gestione dell'identità digitale

8	A livello più avanzato e specializzato, posso:	• creare soluzioni per risolvere problemi complessi con molti fattori interagenti che sono legati alla gestione delle identità digitali e alla protezione della reputazione online delle persone • proporre nuove idee e processi al settore.

INTRODUZIONE:

La comunicazione e la collaborazione si riferiscono alle capacità e alle competenze necessarie per comunicare e collaborare efficacemente nell'ambiente digitale.

Si tratta della capacità di utilizzare la comunicazione e la collaborazione con un pubblico specifico e in un contesto specifico o di esprimere opinioni in pubblico.

La comunicazione e la collaborazione si ottengono identificando che cos'è un'identità digitale ed essendo in grado di creare e gestire una o più identità attraverso i sistemi, le applicazioni e i servizi digitali e identificando e applicando varie strategie per proteggere la propria reputazione, come ad esempio rivedere e aggiornare le impostazioni sulla privacy, creare profili professionali che non siano associati a un profilo personale, evitare di condividere dettagli personali online, mantenere password sicure e uniche e prestare attenzione ai contenuti che si pubblicano sulle piattaforme di social media e ai gruppi e ai forum a cui si partecipa online.

Infine, ma non meno importante, la comunicazione e la collaborazione attraverso la gestione dell'identità digitale e la protezione della propria reputazione online sono uno strumento potente per creare soluzioni a problemi complessi, per guidare gli altri nella gestione dell'identità digitale e per proporre nuove idee e processi al settore.

PREREQUISITI:

Per sviluppare le capacità di comunicazione e di collaborazione, servono come prerequisiti diverse aree di conoscenza. Queste includono:

1. **Alfabetizzazione informatica di base:** gli individui devono avere una comprensione fondamentale delle operazioni al computer, della gestione dei file e dell'uso del software per muoversi in modo efficace sulle piattaforme digitali.
2. **Conoscenza di Internet:** La competenza nell'uso dei browser internet, dei motori di ricerca e la comprensione dei principi di sicurezza online sono essenziali per una comunicazione digitale sicura ed efficace.
3. **Adattabilità alle nuove tecnologie:** Disponibilità e volontà di imparare e adattarsi a nuovi strumenti e tecnologie digitali che emergono in un panorama digitale in rapida evoluzione.

BASE/FOUNDATION (LIVELLO 1 e LIVELLO 2)

AREA DI COMPETENZA 2.6: GESTIONE DELL'IDENTITÀ DIGITALE

COMPETENZA: CREARE E GESTIRE UNA O PIÙ IDENTITÀ DIGITALI, ESSERE IN GRADO DI PROTEGGERE LA PROPRIA REPUTAZIONE, GESTIRE I DATI CHE SI PRODUCONO ATTRAVERSO DIVERSI STRUMENTI DIGITALI, AMBIENTI E SERVIZI.

LIVELLO: 1 – BASE/FOUNDATION

A livello base e con una guida, sono in grado di:

- definire un'identità digitale
- descrivere semplici modi per proteggere la propria reputazione online
- riconoscere semplici dati che si producono attraverso strumenti digitali, ambienti o servizi **LIVELLO: 2 – BASE/FOUNDATION**

A livello di base, in autonomia e con una guida appropriata, se necessario, sono in grado di:

- definire un'identità digitale
- descrivere i modi più semplici per proteggere la propria reputazione online
- riconoscere i semplici dati che si producono attraverso strumenti digitali, ambienti o servizi

Risultati di apprendimento	Level	K – S – A	Descrizione
1. Definire l'identità digitale.	L1	K	Riconoscere che l'identità digitale si riferisce alla rappresentazione elettronica di un individuo o di un'organizzazione. Un'identità digitale è un insieme di informazioni, attributi e credenziali associate a un individuo o a un'organizzazione che possono essere riconosciuti e verificati nell'ambiente online. Riconoscere inoltre che un'identità digitale si riferisce a un insieme di dati che identificano un utente attraverso il tracciamento delle sue attività digitali, delle sue azioni e dei suoi contributi su Internet o sui servizi digitali (ad esempio, le

			pagine visualizzate, la cronologia degli acquisti, i dati personali, la posizione geografica e altro ancora).
2. Descrivere le caratteristiche principali dell'identità digitale.	L1	K	Elencare alcune caratteristiche dell'identità digitale come le informazioni di identificazione (ad esempio, dati personali come nome, cognome, data di nascita, indirizzo, ecc.), le credenziali di autenticazione (ad esempio, combinazioni di nome utente e password, PIN, dati biometrici o qualsiasi altro fattore di autenticazione), i dati di autorizzazione (ad esempio, determinare quali azioni o risorse l'entità è autorizzata ad accedere), gli attributi e le caratteristiche (ad esempio, informazioni aggiuntive che descrivono gli interessi, le affiliazioni o le preferenze dell'entità), certificati digitali (ad esempio, firme digitali o certificati emessi da autorità fidate per convalidare e verificare l'autenticità dell'identità digitale) e dati biometrici (ad esempio, caratteristiche biologiche o comportamentali uniche, come le impronte digitali e il riconoscimento facciale, utilizzate per verificare un'identità).
3. Fornire esempi di diverse identità digitali.	L1	K	Lo studente deve essere in grado di riconoscere che le identità digitali possono assumere varie forme su piattaforme e servizi online e che hanno scopi diversi. Un'identità digitale può essere un account di posta elettronica, un profilo su varie piattaforme di social media (Facebook, Instagram, X (ex Twitter)), contenente informazioni personali, post e connessioni, una credenziale bancaria online contenente una combinazione di nome utente, password e misure di sicurezza aggiuntive, un ID di e-government per l'accesso ai servizi governativi, un profilo di gioco in cui gli utenti possono creare identità digitali associate ai loro account di gioco, mostrando risultati, classifiche e le loro personalità nel gioco. Un'identità digitale può essere anche una credenziale per dispositivi smart home, associata a dispositivi smart home, che consente agli utenti di controllare e monitorare i dispositivi con l'uso di strumenti digitali e un account per servizi di abbonamento, per accedere a servizi basati su

			abbonamento come le piattaforme di streaming, contenente la cronologia delle visualizzazioni, le preferenze e le impostazioni dell'account.
4. Descrivere i vantaggi dell'identità digitale.	L2	K	Descrivere i vantaggi dell'identità digitale come la sicurezza e l'autenticazione (le piattaforme di identità digitale migliorano la sicurezza attraverso l'uso dell'autenticazione a più fattori, della biometria, ecc.), la convenienza (un'identità digitale consente transazioni e interazioni online più efficienti su varie piattaforme digitali come l'e-banking, l'e-commerce, ecc.), la protezione della privacy (gli individui hanno il controllo su quali informazioni condividere e su chi è il loro pubblico), l'efficienza e l'accessibilità (gli individui possono facilmente accedere alla loro identità digitale da qualsiasi luogo e in qualsiasi momento) e l'innovazione tecnologica (l'identità digitale serve come elemento fondante per le tecnologie emergenti come la blockchain e l'IA).
5. Descrivere i rischi dell'identità digitale	L2	K	Descrivere i rischi dell'identità digitale, come i problemi di sicurezza (un'identità digitale ha maggiori probabilità di ricevere minacce informatiche, attacchi di phishing e malware), i problemi di privacy (gli individui condividono contenuti online che possono essere raccolti e utilizzati contro la loro volontà), la mancanza di standardizzazione (mancano protocolli e politiche standardizzate tra le varie piattaforme e ambienti digitali), le sfide normative e legali (la non conformità con le protezioni dei dati e le normative sulla privacy può portare a conseguenze legali e sanzioni finanziarie) e l'innovazione tecnologica (i sistemi obsoleti possono diventare vulnerabili alle minacce alla sicurezza quando si cerca di soddisfare nuove esigenze tecnologiche).
6. Identificare i modi più semplici per proteggere la propria reputazione online.	L1	K	Elencare i semplici modi in cui un individuo può proteggere la propria reputazione online, come ad esempio rivedere e aggiornare le impostazioni della privacy sulle piattaforme di social media, creare profili professionali su piattaforme che non siano associate ai propri account personali su altre piattaforme di social media, evitare di condividere dettagli personali online (ad esempio, indirizzi o numeri di telefono), mantenere password sicure e uniche e

			attivare l'autenticazione a due fattori ogni volta che è possibile, essere cauti riguardo ai contenuti che si pubblicano sulle piattaforme di social media ed essere cauti riguardo ai gruppi e ai forum a cui si partecipa online.
7. Chiedere assistenza quando è necessario per proteggere la propria reputazione online.	L2	K	Chiedere indicazioni su come proteggere la propria reputazione online, come ad esempio mantenere password sicure e uniche e attivare l'autenticazione a due fattori ogni volta che è possibile, prestare attenzione ai contenuti che si pubblicano sulle piattaforme di social media e prestare attenzione ai gruppi e ai forum a cui si partecipa online.
8. Concentrarsi sull'importanza di proteggere la propria reputazione online.	L2	A	Sensibilizzare sull'importanza di proteggere la propria reputazione online. Lo studente deve essere in grado di riconoscere che la protezione della propria reputazione online è fondamentale per le proprie opportunità professionali; ad esempio, i datori di lavoro spesso conducono controlli sul passato dei potenziali candidati, quindi una presenza digitale pulita e professionale può aumentare le possibilità di ottenere un lavoro. La vostra presenza online contribuisce anche al vostro personal branding, ad esempio gestire con attenzione il vostro profilo online sui social media vi permette di modellare il modo in cui gli altri vi percepiscono e vi consente di costruire una rete e delle connessioni forti. La cybersecurity e la privacy, la protezione della vostra reputazione online, implicano la salvaguardia delle vostre informazioni personali. Le aziende devono anche proteggere la propria reputazione online, perché la reputazione online influisce sulla fiducia e sulla fedeltà dei clienti; ad esempio, recensioni positive, testimonianze e una forte presenza digitale possono portare al successo e alla crescita di un'azienda.
9. Riconoscere i dati semplici che si producono attraverso	L1	K	Elencare i dati semplici che si producono attraverso gli strumenti digitali, gli ambienti e i servizi, come i dati personali (nome, data di nascita, indirizzo, numero di telefono), i dati relativi all'attività online (cronologia di navigazione,

strumenti digitali, ambienti e servizi.			query di ricerca, interazioni con i siti web), i dati di comunicazione (e-mail, messaggi, registri delle chiamate), i dati relativi all'ubicazione (dati GPS, check-in, cronologia delle posizioni), i dati relativi alle transazioni e ai finanziamenti (cronologia degli acquisti, transazioni finanziarie, informazioni di pagamento), preferenze e impostazioni (impostazioni personalizzate, preferenze, configurazioni), dati di autenticazione (nomi utente, password, token di autenticazione), informazioni sul dispositivo (tipo di dispositivo, sistema operativo, dettagli del browser), dati biometrici (impronte digitali, riconoscimento facciale), query di ricerca (termini e parole chiave inseriti nei motori di ricerca) e cookie e dati di tracciamento.

INTERMEDIO (LIVELLO 3 e LIVELLO 4)

AREA DI COMPETENZA 2.6: GESTIONE DELL'IDENTITÀ DIGITALE

COMPETENZA: CREARE E GESTIRE UNA O PIÙ IDENTITÀ DIGITALI, ESSERE IN GRADO DI PROTEGGERE LA PROPRIA REPUTAZIONE, GESTIRE I DATI CHE SI PRODUCONO ATTRAVERSO DIVERSI STRUMENTI DIGITALI, AMBIENTI E SERVIZI.

LIVELLO: 3 – INTERMEDIO

Da solo e messo di fronte a problemi semplici, sono in grado di:

- determinare una serie di identità digitali ben definite e di routine
- determinare modi ben definiti e di routine per proteggere la mia reputazione online
- determinare dati ben definiti che si producono abitualmente attraverso strumenti, ambienti o servizi digitali

LIVELLO: 4 – INTERMEDIO

In modo indipendente, in base alle mie esigenze e affrontando problemi limitati e non abituali, sono in grado di:

- mostrare una varietà di identità digitali specifiche
- discutere di modi specifici per proteggere la mia reputazione online,
- modificare i dati che si producono attraverso gli strumenti digitali, gli ambienti o i servizi

Risultati di apprendimento	Level	K – S – A	Descrizione
10. Riconoscere una serie di identità digitali ben definite e di routine.	L3	K	Riconoscere una serie di identità digitali ben definite e di routine, come l'identità personale o professionale sui social media, l'identità di gioco, l'identità di utente di e-commerce, l'identità di piattaforma educativa, l'identità di piattaforma di ricerca di lavoro, l'identità di servizio di abbonamento, ecc.

11. Distinguere tra un'identità personale sui social media e un'identità professionale.	L3	K	Riconoscere che un'identità personale sui social media è usata principalmente per socializzare, connettersi con amici e familiari e condividere esperienze personali. Lo studente deve anche essere in grado di riconoscere i contenuti condivisi su un'identità personale sui social media, come foto e video personali, aggiornamenti casuali, informazioni su hobby e interessi e lo stile di interazione informale. Riconoscere che un'identità professionale è usata principalmente per fare networking, sviluppare la propria carriera e mostrare capacità e risultati relativi a un campo professionale specifico. Lo studente deve anche essere in grado di riconoscere i contenuti condivisi su un'identità professionale, come i dettagli sull'esperienza lavorativa, i risultati professionali, le capacità, l'istruzione e i riconoscimenti relativi a una carriera specifica e lo stile di interazione formale e incentrato su argomenti professionali.
12. Riconoscere le pratiche di informazione e comunicazione che aiutano un individuo a costruire un'identità online positiva.	L3	K	Riconoscere le pratiche di informazione e comunicazione che possono aiutare un individuo a costruire un'identità online positiva, come ad esempio creare e pubblicare contenuti che riflettano positivamente i propri valori e interessi, condividere in modo selettivo, promuovere un dialogo costruttivo ed evitare di essere coinvolti in interazioni negative, mantenere un contegno professionale su piattaforme professionali come LinkedIn e rimanere informati sulle tendenze digitali e sulle migliori pratiche.
13. Riconoscere le pratiche di informazione e comunicazione che possono causare un'identità online negativa.	L3	K	Riconoscere le pratiche di informazione e comunicazione che potrebbero causare un'identità online negativa, come ad esempio l'uso di un linguaggio offensivo o incendiario nelle interazioni online, le molestie online, la condivisione di contenuti che diffondono disinformazione e voci, il comportamento inappropriato o poco professionale su piattaforme professionali come LinkedIn e l'ignoranza delle tendenze e delle buone pratiche digitali.

14. Descrivere il tipo di dati che si producono attraverso strumenti digitali, ambienti e servizi.	L3	K	Lo studente deve essere in grado di comprendere che attraverso strumenti digitali, ambienti e servizi, si producono dati relativi alle proprie informazioni personali, firme digitali, informazioni di contatto, dati biometrici, cronologia del browser e cookie, cronologia delle transazioni, preferenze e interessi, metadati di comunicazione, dati di autenticazione e autorizzazione e registrazioni del consenso dato.
15. Manipolare i dati che si producono attraverso strumenti digitali, ambienti e servizi.	L4	S	Lo studente deve essere in grado di manipolare i dati che si producono attraverso gli strumenti digitali, l'ambiente e i servizi, ad esempio per quanto riguarda le informazioni personali, lo studente deve essere in grado di riconoscere quando è necessario aggiungere informazioni come l'indirizzo di casa o il numero di telefono e quando non è necessario; nei casi in cui non è necessario, lo studente deve essere in grado di manipolare i dati, non includendoli o includendo un insieme diverso di dati.
16. Sensibilizzare su quali dati si producono sull'identità digitale.	L4	S	Informare circa i dati che si producono sull'identità digitale, ad esempio i dati relativi alle informazioni personali dovrebbero essere evitati a meno che non sia assolutamente necessario (ad esempio, l'indirizzo di casa, i numeri di telefono), i dati relativi alle informazioni finanziarie dovrebbero essere condivisi con cautela (ad esempio, i numeri dei conti bancari, i dettagli delle carte di credito, i PIN delle carte), i dati relativi all'ubicazione dovrebbero essere evitati a meno che non sia necessario per proteggere la propria sicurezza fisica e la propria privacy. Per quanto riguarda i dati relativi ai contenuti, lo studente deve essere cauto nell'esprimere opinioni o convinzioni sensibili, nelle piattaforme in cui c'è interazione con altre persone.
17. Creare profili in ambienti digitali per scopi personali o professionali.	L3	S	Lo studente può creare un profilo compilando in modo completo i dettagli del profilo, tra cui la biografia, le informazioni di contatto, l'istruzione, l'esperienza lavorativa e qualsiasi altro dettaglio rilevante.
18. Gestire profili in ambienti digitali per scopi personali o professionali.	L3	S	Lo studente è in grado di gestire il proprio profilo nell'ambiente digitale per scopi personali o professionali attraverso aggiornamenti regolari, insieme alle impostazioni sulla privacy, mostrando le proprie capacità, cercando di ottenere

			l'approvazione, revisionando e ripulendo i profili digitali, ecc.
19. Presentare diverse strategie per proteggere la propria reputazione online.	L3	K	Lo studente deve essere in grado di presentare diverse strategie per proteggere la propria reputazione online come, ad esempio, monitorare la propria presenza online cercando regolarmente il proprio nome e le sue varianti sui motori di ricerca per vedere quali informazioni sono disponibili, impostare gli avvisi sul proprio browser per ricevere notifiche quando il proprio nome viene citato online. Regolare le impostazioni della privacy sulle piattaforme di social media, prestare attenzione alle informazioni condivise online, utilizzare password forti e prestare attenzione ai contenuti pubblicati online.
20. Descrivere il tipo di metadati inclusi nelle immagini condivise.	L3	K	Descrivere il tipo di metadati inclusi nelle immagini condivise, come ad esempio: • **Dati EXIF (Exchangeable Image File Format)**, che includono le impostazioni della fotocamera, le informazioni sul momento in cui è stata scattata la foto, ad esempio otturatore, velocità, apertura, ISO e lunghezza focale. La data e l'ora in cui la foto è stata scattata e la posizione geografica della foto. • **Dati IPTC (International Press Telecommunications Council),** che includono una breve descrizione della foto, parole chiave o tag associate all'immagine e dettagli sul proprietario del copyright e sui diritti di utilizzo. • **Dati XMP (Extensible metadata platform),** che includono informazioni aggiuntive rispetto ai dati EXIF e IPTC. • **Dati di informazione sul file**, che includono il nome e la dimensione del file e il formato in cui l'immagine è stata salvata (JPEG, PNG).
21. Descrivere i modi in cui è possibile modificare i metadati di un'immagine condivisa.	L4	S	Riconoscere i metadati che possono essere modificati, ad esempio: • **Dati EXIF (Exchangeable Image File Format),** è possibile modificare informazioni come data, ora e insieme delle impostazioni della fotocamera.

			• **Dati IPTC (International Press Telecommunications Council),** per modificare informazioni come la modifica delle didascalie, le parole chiave e le informazioni sul copyright. • **Dati XMP (Extensible metadata platform),** è possibile modificare i metadati estesi. Descrivere i modi in cui è possibile modificare i metadati di un'immagine condivisa, ad esempio utilizzando strumenti e siti web online (Metapicz), utilizzando software specializzati (Exif Pilot, Adobe Lightroom), su Windows e MacOS e utilizzando software di editing delle immagini (Photoshop, GIMP).
22. Identificare i vantaggi della gestione di una o più microcredenziali attraverso sistemi, applicazioni e servizi digitali.	L4	K	Identificare i vantaggi della gestione di una o più identità digitali, come l'accesso e la comodità, la personalizzazione, l'autenticazione efficiente, i servizi personalizzati e il networking professionale.
23. Identificare i rischi della gestione di una o più identità digitali attraverso sistemi, applicazioni e servizi digitali.	L4	K	Identificare i rischi legati alla gestione di una o più identità digitali, come le minacce alla sicurezza, i problemi di privacy, la frammentazione delle identità, le violazioni dei dati, i danni alla reputazione, le difficoltà di autenticazione e la mancanza di controllo.

AVANZATO (LIVELLO 5 e LIVELLO 6)

AREA DI COMPETENZA 2.6: GESTIONE DELL'IDENTITÀ DIGITALE

COMPETENZA: CREARE E GESTIRE UNA O PIÙ IDENTITÀ DIGITALI, ESSERE IN GRADO DI PROTEGGERE LA PROPRIA REPUTAZIONE, GESTIRE I DATI CHE SI PRODUCONO ATTRAVERSO DIVERSI STRUMENTI DIGITALI, AMBIENTI E SERVIZI.

LIVELLO: 5 – AVANZATO

Oltre a guidare gli altri, sono in grado di:

- utilizzare una varietà di identità digitali
- applicare diversi modi per proteggere la propria reputazione online
- utilizzare i dati che si producono attraverso strumenti digitali, ambienti e servizi

LIVELLO: 6 – AVANZATO

A livello avanzato, in base alle mie esigenze e a quelle degli altri, e in contesti complessi, sono in grado di:

- determinare le identità digitali multiple
- spiegare i modi più appropriati per proteggere la propria reputazione
- modificare i dati che si producono attraverso strumenti digitali, ambienti o servizi

Risultati di apprendimento	Level	K – S – A	Descrizione
24. Spiegare l'espressione "identità digitale coerente in tutti i social media".	L6	K	Spiegare l'espressione "identità digitale coerente in tutti i social media" come al mantenimento di una presenza online uniforme su diverse piattaforme. Ciò include l'utilizzo di nomi utente uguali o simili, immagini del profilo e una strategia di branding personale o professionale standardizzata.
25. Giustificare perché si dovrebbe avere un'identità	L6	S	Spiegare perché si dovrebbe avere un'identità digitale coerente su tutti i social media per creare un marchio personale riconoscibile che rappresenti la persona su diversi canali online. La coerenza rappresenta professionalità,

digitale coerente in tutti i social media.			fiducia e credibilità, facilità nel trovare la persona, coinvolgimento su tutte le piattaforme.
26. Creare un'identità digitale coerente in tutti i social media.	L6	S	Creare un'identità digitale coerente su tutti i social media utilizzando un nome utente uguale o simile, disegnando un'immagine del profilo unificata, componendo una biografia unificata, mantenendo elementi di branding coerenti come colori, caratteri e loghi su tutti i profili dei social media, collegandosi ad altri profili, mantenendo uno stile e un tono coerenti sui post, ma adattando il contenuto per adattarlo alle caratteristiche uniche di ogni piattaforma mantenendo il messaggio principale coerente, aggiornando le modifiche su tutte le piattaforme.
27. Selezionare una foto che si vuole caricare su una specifica piattaforma di social media e modificarne i metadati utilizzando un software specifico.	L6	S	Selezionare un'immagine che si desidera caricare su una specifica piattaforma di social media e modificarne i metadati utilizzando un software specifico. Lo studente deve essere in grado di scaricare e installare Exif Pilot, aprire l'immagine nel software, individuare i campi dei metadati e apportare le modifiche. Lo studente deve anche essere in grado di utilizzare Adobe Lightroom, selezionare e aprire l'immagine nel modulo libreria e accedere al pannello dei metadati. Se si utilizza Windows, lo studente deve essere in grado di fare clic con il tasto destro del mouse sull'immagine, selezionare proprietà, andare su dettagli e fare clic su rimuovi proprietà e informazioni personali.
28. Porre attenzione sull'importanza di modificare i metadati per proteggere la propria privacy.	L6	A	Porre l'accento sull'importanza di modificare i metadati per proteggere la propria privacy, ad esempio modificando o rimuovendo le informazioni relative al luogo, all'ora e alla data in cui è stata scattata la foto, l'individuo può evitare di divulgare i propri spostamenti e le informazioni sulle proprie attività. Modificando i metadati, l'individuo può controllare quali informazioni

			vengono condivise e ridurre al minimo il rischio di essere tracciato senza il suo consenso. Modificando i metadati, l'individuo può mantenere l'anonimato.
29. Gestire una o più identità digitali attraverso i sistemi digitali.	L5	S	Essere in grado di gestire una o più identità digitali attraverso i sistemi digitali, ad esempio accedere tramite Facebook, o qualsiasi altro fornitore di autenticazione di terze parti, significa utilizzare le credenziali esistenti di un social media o di un servizio esterno per accedere a un sito web, a un'applicazione o a un servizio digitale. Questo metodo di autenticazione semplifica il processo di accesso per gli utenti e offre una comoda alternativa alla creazione e al ricordo di un nuovo insieme di credenziali per ogni piattaforma.
30. Valutare i vantaggi e i rischi della gestione di una o più identità digitali attraverso sistemi, applicazioni e servizi digitali.	L5	K	Essere in grado di elencare i vantaggi della gestione di una o più identità digitali attraverso i sistemi, le app e i servizi digitali, come la creazione di un marchio personale e di una reputazione professionale, il mantenimento delle opportunità di rete, il miglioramento della comunicazione efficiente, l'adattamento più facile ai cambiamenti, l'aumento della visibilità e altro ancora.
31. Utilizzare strategie per controllare, gestire o cancellare i dati raccolti dai sistemi online.	L6	S	Utilizzare strategie per controllare, gestire o cancellare i dati raccolti dai sistemi online, come cancellare regolarmente i cookie e la cache, esercitare il diritto di richiedere la cancellazione dei propri dati dalle piattaforme online, utilizzare password forti e l'autenticazione a due fattori, verificare regolarmente le app collegate ed educare se stessi.
32. Applicare diverse strategie per proteggere la propria reputazione online.	L5	S	Lo studente deve essere in grado di applicare diverse strategie per proteggere la propria reputazione online, come ad esempio cercare il proprio nome e le sue varianti nei motori di ricerca, impostare avvisi nel proprio browser per ricevere notifiche su menzioni o aggiornamenti relativi alla propria presenza online, regolare le impostazioni della privacy sulle piattaforme di social media per controllare chi può vedere le proprie informazioni personali, utilizzare password

			sicure e uniche per i vari account online, attivare l'autenticazione a due fattori ogni volta che è possibile, considerare il tipo di contenuti che si condividono online per evitare di pubblicare contenuti controversi o offensivi.
33. Spiegare le strategie più appropriate per proteggere la propria reputazione online.	L6	K	Lo studente deve essere in grado di spiegare le strategie più appropriate per proteggere la propria reputazione online, come ad esempio: • Impostazioni della privacy: Regolare le impostazioni della privacy su piattaforme di social media, siti web e altri account online per controllare chi può visualizzare le informazioni personali. • Monitoraggio online regolare: Monitorare regolarmente la presenza online cercando il proprio nome online. • Protezione degli account online: Rafforzare le misure di sicurezza per gli account online utilizzando password sicure e uniche e l'autenticazione a due fattori. Cambiare la password ogni pochi mesi. • Condivisione dei contenuti: Prestare attenzione ai contenuti che si condividono online, compresi testi, e-mail, foto e video. • Galateo online: Praticare un buon galateo online trattando gli altri con rispetto ed evitando di fare commenti offensivi o infiammatori.

ESPERTO (LIVELLO 7 e LIVELLO 8)

AREA DI COMPETENZA 2.6: GESTIONE DELL'IDENTITÀ DIGITALE

COMPETENZA: CREARE E GESTIRE UNA O PIÙ IDENTITÀ DIGITALI, ESSERE IN GRADO DI PROTEGGERE LA PROPRIA REPUTAZIONE, GESTIRE I DATI CHE SI PRODUCONO ATTRAVERSO DIVERSI STRUMENTI DIGITALI, AMBIENTI E SERVIZI.

IVELLO: 7 – ALTAMENTE SPECIALIZZATO

A livello di alta specializzazione, sono in grado di:

- creare soluzioni a problemi complessi con una definizione limitata, legati alla gestione delle identità digitali e alla protezione della reputazione online delle persone
- integrare le proprie conoscenze per contribuire alle pratiche e alle conoscenze professionali e guidare gli altri nella gestione delle identità digitali

LIVELLO: 8 – ALTAMENTE SPECIALIZZATO

Al livello più avanzato e specializzato, sono in grado di:

- trovare soluzioni per risolvere problemi complessi, con molti fattori interagenti, legati alla gestione delle identità digitali e alla protezione della reputazione online delle persone.
- proporre nuove idee e procedure al settore.

Risultati di apprendimento	Level	K – S – A	Descrizione
34. Spiegare perché la creazione di soluzioni a problemi complessi legati all'identità digitale richiede un approccio strategico.	L7	K	La creazione di soluzioni a problemi complessi legati all'identità digitale richiede un approccio strategico. Ciò è dovuto a diversi motivi, quali l'interconnessione dei sistemi (la gestione dell'identità digitale spesso coinvolge più sistemi interconnessi), la diversità degli stakeholder (tra cui individui, aziende, enti governativi e fornitori di servizi), la conformità normativa (la raccolta, l'archiviazione e l'utilizzo dei dati digitali sono accompagnati da quadri legali e normativi), problemi di sicurezza e privacy (la gestione di più identità digitali

			coinvolge informazioni sensibili e la sicurezza e la privacy sono spesso richieste), la rapida evoluzione della tecnologia, le considerazioni globali (le identità digitali spesso trascendono i confini nazionali), la complessità dell'ecosistema (le identità digitali possono includere entità pubbliche e private) e le considerazioni etiche (le soluzioni devono riflettere specifici standard etici).
35. Spiegare perché la creazione di soluzioni a problemi complessi legati alla protezione della propria reputazione online richiede un approccio strategico.	L7	K	La creazione di soluzioni a problemi complessi legati alla protezione della propria reputazione online richiede un approccio strategico. Ciò è dovuto a diverse ragioni, come la diversità delle piattaforme e dei canali (la reputazione online si estende su varie piattaforme di social media, siti web e altro), il monitoraggio continuo, la diversità degli stakeholder (tra cui clienti, dipendenti, concorrenti e pubblico), le considerazioni legali (gestire la propria reputazione online può comportare aspetti legali come la diffamazione, la proprietà intellettuale, ecc.), l'integrazione della tecnologia (essere in grado di utilizzare e gestire strumenti digitali per il monitoraggio e la modifica), la necessità di costruire la reputazione in modo proattivo, la necessità di adattarsi al cambiamento.
36. Guidare gli altri nella gestione di una o più identità digitali.	L7	S	Condurre workshop su come gestire una o più identità, comprese lezioni su come impostare la privacy, come revisionare e ripulire, come aggiornare regolarmente e come mostrare le capacità.
37. Guidare gli altri nella protezione della propria reputazione online.	L7	S	Condurre workshop su come proteggere la propria reputazione online, includendo lezioni sulle impostazioni della privacy, sul monitoraggio online regolare, sulla sicurezza degli account online, sulla condivisione dei contenuti e sul galateo online.

38. Condurre una ricerca del nome di una persona o di una famiglia in ambienti online.	L7	S	Condurre una ricerca del nome individuale o di famiglia in ambienti online per verificare la propria impronta digitale negli ambienti online. • Lo studente deve essere in grado di seguire i seguenti passaggi: • Cercare il nome completo della famiglia dell'individuo o qualsiasi altra informazione rilevante in diversi motori di ricerca (Google, Yahoo, Bing). • Cercare il nome in varie piattaforme di social media (Facebook, Instagram, X (ex Twitter), LinkedIn). • Accedere ai database dei registri pubblici online. • Accedere ai registri giudiziari online o ai database legali.
39. Modificare le configurazioni degli utenti per abilitare, impedire o moderare il tracciamento, la raccolta o l'analisi dei dati da parte del sistema di IA.	L8	S	Lo studente deve essere in grado di modificare le configurazioni dell'utente attraverso l'uso di app, software e piattaforme digitali al fine di abilitare, impedire o moderare il tracciamento, la raccolta o l'analisi dei dati da parte del sistema di intelligenza artificiale. Lo studente deve essere in grado di seguire i seguenti passaggi: • Controllare le impostazioni dell'account, in particolare quelle relative alla privacy, alla raccolta dei dati e ad altre configurazioni. • Esplorare le sezioni relative alla privacy, alla sicurezza e all'utilizzo dei dati su diverse piattaforme. • Esaminare i termini di servizio e le politiche sulla privacy. • Opt-out di qualsiasi funzione di raccolta o analisi dei dati. Lo studente deve essere in grado di accedere alle impostazioni del proprio dispositivo telefonico e di rinunciare all'opzione di localizzazione.

40. Proporre nuove idee nel campo della gestione delle identità digitali.	L8	S	Proporre diverse idee relative alla gestione delle identità digitali, come piattaforme di identità decentralizzate, autenticazione biometrica, verifica dell'identità guidata dall'intelligenza artificiale, tecnologie di conservazione della privacy e piattaforme di identità collaborative.
41. Proporre nuove idee nel campo della protezione della propria reputazione online.	L8	S	Proporre diverse idee relative alla protezione della propria reputazione online, come un sistema basato sulla blockchain per la verifica dell'identità, app personalizzate per la privacy e la sicurezza e strumenti di gestione delle crisi basati sull'intelligenza artificiale.

Project Coordinator:

EdiTC EDUCATION & INFORMATION TECHNOLOGY CENTRE

Partners:

DIMITRA educational organization

UNIVERSITAS GALATIENSIS

UNIVERSITÀ TELEMATICA INTERNAZIONALE UNINETTUNO

CYPRUS COMPUTER SOCIETY

MMC Mediterranean Management Centre

MTU Ollscoil Teicneolaíochta na Mumhan Munster Technological University

DSW DIGITAL SKILLS WALLET

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.