



Digital-in

DIGITAL SKILLS FOR THE INCLUSION OF DIGITALLY
VULNERABLE GROUPS: A DVGS' NEEDS-BASED
APPROACH TO DIGITAL SKILLS PROVISION
IN ADULT EDUCATION

TEMPLATE DEL MODULO

Curriculum e linee guida metodologiche per il DLC adattate ai
gruppi digitalmente vulnerabili

Deliverable No

4.1.2.

DELIVERABLE INFORMATION

D3.1 –Manual and guidelines for trainers	
Deliverable number	D 4.1.2.
Responsible partner	EMiT Feltrinelli
Due date of deliverable	20/05/2025
Actual submission date	17/12/2025
Version	V.2
Authors	Roberto Minicone, Lucia Zucchella
Contributors	Sofia Nigrelli
Reviewers	Magtel Foundation
Work package number	WP.4
Work package title	Curriculum and methodological guidelines for the DLC adapted to DVGs
Work package leader	NKUA



Dissemination Level		
CO	Confidential, only for members of the consortium including the Commission Services	<input type="checkbox"/>
PU	Public	<input checked="" type="checkbox"/>
PP	Restricted to other programme participants, including the Commission Services	<input type="checkbox"/>
RE	Restricted to a group specified by the consortium including the Commission Services	<input type="checkbox"/>

Nature of the Deliverable		
R	Report	<input type="checkbox"/>
D	Demonstrator	<input checked="" type="checkbox"/>
W	Website, patent filing, etc.	<input type="checkbox"/>
M	Manual	<input type="checkbox"/>

PARTNERS INVOLVED IN THE DELIVERABLE

Participant No.	Name of the Organisation	Short Name	Involved
1	Ethniko kai Kapodistriako Panepistimio Athinon	NKUA	<input checked="" type="checkbox"/>
2	Fundación Magtel	MAGTEL	<input checked="" type="checkbox"/>
3	Ente Morale Giacomo Feltrinelli Per L Incremento Dell Istruzione Tecnica	EMIT	<input checked="" type="checkbox"/>
4	Intercollege	INTERCOLLEGE	<input checked="" type="checkbox"/>



PIANO DEL MODULO

CYBERSECURITY E PROTEZIONE DEI DATI

Unità del modulo:

- **Unità 1. Introduzione alla cybersecurity**
- **Unità 2. Comprendere le minacce informatiche**
- **Unità 3. Politiche e procedure di sicurezza**
- **Unità 4. Introduzione alla protezione dei dati**

4.1 Introduzione alla Cybersecurity

- * Importanza della cybersecurity nell'era digitale
- * Panoramica delle minacce e vulnerabilità più comuni

4.2 Comprendere le minacce informatiche

- * Malware (virus, worm, ransomware, spyware)
- * Attacchi di phishing e social engineering
- * Attacchi Denial of Service (DoS) e Distributed Denial of Service (DDoS)
- * Minacce interne e Advanced Persistent Threats (APT)

4.3 Politiche e procedure di sicurezza

- * Sviluppo di politiche di cybersecurity efficaci
- * Importanza della conformità ai requisiti legali e normativi
- * Buone pratiche di secure coding

4.4 Introduzione alla protezione dei dati

- * Definizione di protezione dei dati
- * Differenza tra dati personali e dati sensibili
- * Impatto delle violazioni dei dati su individui e organizzazioni
- * Regolamento generale sulla protezione dei dati (GDPR)
- * Tendenze emergenti e tecnologie nella protezione dei dati

RISULTATI DI APPRENDIMENTO DEL MODULO

Al termine di questo modulo i partecipanti saranno in grado di:

- * Comprendere perché la cybersecurity è fondamentale nel mondo digitale attuale e riconoscere i principali rischi e vulnerabilità.
- * Identificare le principali minacce informatiche, tra cui malware, phishing, attacchi DoS/DDoS, minacce interne e APT.
- * Comprendere e applicare politiche e procedure efficaci di cybersecurity e i requisiti normativi.
- * Applicare buone pratiche per il secure coding e la protezione dei dati sensibili.
- * Distinguere tra dati personali e dati sensibili e comprendere l'impatto reale delle violazioni dei dati su persone e organizzazioni.
- * Comprendere i principi fondamentali della protezione dei dati e i principali aspetti del GDPR.
- * Rimanere aggiornati sulle tecnologie emergenti nel campo della protezione dei dati.

RISULTATI DI APPRENDIMENTO PER UNITÀ

Unità 1

Dopo aver completato questa unità, il partecipante sarà in grado di:

- * Comprendere il ruolo essenziale della cybersecurity nel mondo digitale contemporaneo.
- * Riconoscere come la cybersecurity protegga le informazioni sensibili e garantisca integrità e disponibilità delle risorse digitali.
- * Comprendere il concetto di rischio informatico e l'importanza delle misure di sicurezza.

Unità 2

Dopo aver completato questa unità, il partecipante sarà in grado di:

- * Comprendere i principi fondamentali per sviluppare politiche efficaci di cybersecurity.
- * Comprendere l'importanza della conformità legale e normativa.
- * Riconoscere normative e standard rilevanti come GDPR, HIPAA e ISO/IEC 27001.

Unità 3

Dopo aver completato questa unità, il partecipante sarà in grado di:

- * Comprendere come sviluppare politiche efficaci di sicurezza informatica.
- * Comprendere il ruolo della conformità normativa nella gestione del rischio informatico.



Unità 4

Dopo aver completato questa unità, il partecipante sarà in grado di:

- * Definire il concetto di protezione dei dati.
- * Distinguere tra dati personali e dati sensibili.
- * Comprendere l'impatto delle violazioni dei dati.
- * Spiegare i principi fondamentali del GDPR.

PAROLE CHIAVE DEL MODULO

Cybersecurity, Minacce informatiche, Malware, Phishing, DoS/DDoS, Insider Threats, APT, Politiche di sicurezza, Compliance, Secure Coding, Protezione dei dati, Dati personali, Dati sensibili, Data breach, GDPR, Tecnologie emergenti.