

**Piano Emergo 2021**  
**Bando MI272**  
**Costituzione del Catalogo dei corsi di formazione finanziabili attraverso i**  
**voucher “Cittadinanza Digitale”**

**MODULO C - SCHEDA DESCRITTIVA CORSO DI FORMAZIONE**  
*(da ripetere per ciascun corso di formazione candidato a Catalogo)*

Titolo	Gestione della sicurezza informatica
Classificazione in formazione base/avanzata	Formazione avanzata
Prerequisiti ( <i>competenze e abilità già acquisite o titolo di studio indispensabili per affrontare efficacemente il corso</i> )	<p>Titolo di istruzione secondaria di secondo grado  <i>Oppure</i>  Assolvimento del diritto-dovere all’istruzione e alla formazione professionale o proscioglimento, e conoscenze informatiche di livello intermedio secondo la classificazione DiGComp2.1 (corrispondente al livello 3 e livello 4).  Le conoscenze informatiche saranno accertate - in assenza di evidenze documentali - tramite test d’ingresso standardizzato sul modello Digital Skills Assesment Tool  <a href="https://europa.eu/europass/digitalskills/screen/home">https://europa.eu/europass/digitalskills/screen/home</a></p>
Destinatari ( <i>tipo di disabilità</i> )	PSICHICA - FISICA - SENSORIALE
Indicazione del gruppo classe di riferimento ( <i>min 5-max 12 allievi</i> )	10 ALLIEVI
Durata (n. ore) <i>Formazione base: min 8 ore - max 25 ore</i> <i>Formazione avanzata: min 8 ore - Max 250 ore</i>	220 ore
Classificazione del corso per aree tematiche Dig. Comp. (Tabella 1)	<ol style="list-style-type: none"> <li>1. Alfabetizzazione su informazioni e dati <ol style="list-style-type: none"> <li>1.2 <i>Valutare dati, informazioni e contenuti digitali</i></li> </ol> </li> <li>2. Comunicazione e collaborazione <ol style="list-style-type: none"> <li>2.1 <i>Interagire attraverso le tecnologie digitali</i></li> </ol> </li> <li>4. Sicurezza <ol style="list-style-type: none"> <li>4.1 <i>Proteggere i dispositivi</i></li> <li>4.2 <i>Proteggere i dati personali e la privacy</i></li> <li>4.3 <i>Proteggere la salute e il benessere</i></li> <li>4.4 <i>Proteggere l’ambiente</i></li> </ol> </li> </ol>

	<p>5. Risolvere i problemi</p> <p>5.1 Risolvere problemi tecnici</p> <p>5.2 Individuare fabbisogni e risposte tecnologiche</p>
<p>Principali <i>obiettivi formativi e contenuti</i> del corso</p>	<p>Il corso mira a fornire le competenze necessarie per controllare e proteggere il sistema informativo dell'organizzazione, assicurando che i rischi legati alla sicurezza siano analizzati e gestiti per i dati e le informazioni interne.</p> <p>1) Analisi delle prestazioni dei sistemi IT</p> <ul style="list-style-type: none"> <li>• Sicurezza informatica</li> <li>• Sistemi di prevenzione degli attacchi alla rete</li> </ul> <p>1) Analisi dei livelli di sicurezza</p> <ul style="list-style-type: none"> <li>• Principi di programmazione sicura</li> <li>• Sicurezza dei sistemi operativi</li> <li>• Sicurezza delle applicazioni web</li> <li>• Sicurezza delle basi di dati</li> <li>• Sicurezza delle reti senza fili</li> </ul>
<p>Correlazione della/e competenza/e acquisibile/i attraverso il corso con i profili professionali individuati dal QRSP (<i>solo formazione avanzata</i>)</p>	<p>Il corso prevede l'acquisizione delle seguenti competenze:</p> <ul style="list-style-type: none"> <li>- Effettuare la revisione delle prestazioni del sistema IT in uso;</li> <li>- Valutare il grado di sicurezza informatica del sistema sviluppato.</li> </ul> <p>Tali competenze sono correlate alla figura di Specialista per la sicurezza informatica (ICT security specialist) presente nel QRSP della Regione Lombardia  Referenziazione: livello EQF 5</p>
<p>Metodologia didattica proposta (tecniche e strumenti), anche in relazione al target specifico individuato</p>	<p>Sarà privilegiata una modalità di formazione in presenza di tipo laboratoriale con l'utilizzo di PC e altra strumentazione ritenuta idonea per l'erogazione dei contenuti. Ci riserviamo la formazione in remoto, in modalità sincrona, al gruppo partecipante, nel caso di impossibilità da parte degli utenti di frequentare il corso in presenza. Rilascio materiale didattico prodotto e condiviso con i partecipanti durante il corso di formazione.</p>
<p>Efficacia potenziale del corso in termini di innalzamento dell'autonomia della persona (<i>formazione di base</i>) o di miglioramento delle chance occupazionali (<i>formazione avanzata</i>)</p>	<p>Le competenze relative alla figura di ICT security specialist e più in generale del cyber security expert, sono estremamente richieste dal mercato del lavoro, per un valore assoluto di fabbisogno di personale che va dalle 30mila alle 40 mila unità nel breve e medio periodo.  Fonte: Previsione dei fabbisogni occupazionali e professionali in Italia a medio termine (2022-2026) - Sistema Informativo Excelsior</p>
<p>Patentino, certificazione o</p>	<p>Attestato di acquisizione delle competenze (GEFO) e attestato di frequenza.</p>

attestazione acquisibili al termine del corso	In caso di mancata acquisizione di una competenza piena, attestazione delle conoscenze e delle abilità acquisite tra quelle che definiscono la competenza e attestato di frequenza.
---	---

Ente erogatore del corso	ACCADEMIA DA VINCI
Sede di erogazione del corso (indirizzo)	Via A. Cechov, n.50 MILANO
Contatti per iscrizione (riferimento): mail	politicheattive@ig-samsic.eu
Contatti per iscrizione (riferimento): telefono	0282902532

Tabella 1 – Aree tematiche di riferimento – Dig. Comp.

## **1. Alfabetizzazione su informazioni e dati**

1.1 Navigare, ricercare e filtrare dati, informazioni e contenuti digitali

1.2 Valutare dati, informazioni e contenuti digitali

1.3 Gestire dati, informazioni e contenuti digitali

**Accesso digitale** – Tutti gli utenti devono avere gli stessi diritti digitali e uguale accesso alle tecnologie. L'obiettivo dei cittadini digitali è impedire l'esclusione digitale che rende difficile la crescita della società utilizzando questi strumenti;

## **2. Comunicazione e collaborazione**

2.1 Interagire attraverso le tecnologie digitali

2.2 Condividere informazioni attraverso le tecnologie digitali

2.3 Esercitare la cittadinanza attraverso le tecnologie digitali

2.4 Collaborare attraverso le tecnologie digitali

2.5 Netiquette

**Netiquette** - Tenere un corretto codice di condotta nell'uso delle tecnologie è una questione complessa. Ma esiste un galateo digitale normalmente presente nei forum, nelle community e nei social network. Tali norme e regolamenti garantiscono il rispetto altrui un po' come richiesto dalle situazioni in cui interagiamo con altre persone dal vivo;

2.6 Gestire l'identità digitale

## **3. Creazione di contenuti digitali**

3.1 Sviluppare contenuti digitali

3.2 Integrare e rielaborare contenuti digitali

3.3 Copyright e licenze

3.4 Programmazione

## **4. Sicurezza**

4.1 Proteggere i dispositivi

4.2 Proteggere i dati personali e la privacy

4.3 Proteggere la salute e il benessere

*4.4 Proteggere l'ambiente*

**5. Risolvere i problemi**

*5.1 Risolvere problemi tecnici*

*5.2 Individuare fabbisogni e risposte tecnologiche*

*5.3 Utilizzare in modo creativo le tecnologie digitali*

*5.4 Individuare divari di competenze digitali*