|  |  |  |  |
| --- | --- | --- | --- |
| **Denominazione Modulo/Area di Attività (ADA 4): Sicurezza Digitale** | | | |
| **Nr. Scheda Formativa 11/15** | **Livello di padronanza 4** | | **Durata complessiva 11 ore** |
| **Obiettivi formativi** | | L’obiettivo del modulo è riportato di seguito in elenco:   * Conoscere la terminologia di base della cyber security e i principali criteri di valutazione di un piano personale di sicurezza digitale. * Saper applicare i criteri di valutazione del rischio in base alle proprie caratteristiche di uso dei dispositivi digitali." * "Acquisire la padronanza del proprio ambiente di lavoro e applicare adeguate misure di sicurezza. * Capacità di distinguere il campo di applicazione dei dati in possesso e capacità di applicare i migliori modelli di monitoraggio per la sicurezza e conservazione dei dati. * "Essere in grado di applicare e rispondere ai livelli di autorizzazione di raccolta, uso, elaborazione dei dati, in linea con la vigente normativa Europea e specifica. * Essere in grado di selezionare contenuti in base all'affidabilità delle fonti, dati, informazioni raccolte." * Saper riconoscere la conformità di un software o dispositivo * "Saper distinguere le varie tecnologie a supporto delle attività ludico/sociali e le loro applicazioni nel mondo del lavoro. * Saper riconoscere gli effetti di una dipendenza digitale " * Saper identificare e costruire soluzioni/offerte considerando opzioni di mercato non proprietarie. | |
| **Unità didattiche** | | **Contenuti/argomenti** | |
| **Il mondo digitale e l'orientamento del cybernauta (3 ore)** | | * Orientamento sulla rete e sul web * Cenni sulla tutela dello scambio dati online * Livelli di protezione online * Cenni sull'assessment di protezione personale * Hacker, cracker e criminali informatici * Malware, virus, rootkit e RAT * Spyware, adware, scareware * Che cos'è Phishing, Vishing e SMShing - * Spamming e doxing * Ingegneria sociale: truffe, trucchi e frodi * Darknets, Dark Markets e Exploit kit * La scelta del sistema operativo - principali Sistemi Operativi a confronto:   1. Microsoft Windows   2. Linux   3. MacOS | |
| **Consapevolezza dell'identità personale e digitale: quadro normativo e sua applicazione (4 ore)** | | * Funzioni hash/firme digitali * Crittografia end-to-end (E2EE) * Come vengono realmente attaccati la sicurezza e la crittografia * Introduzione alla configurazione di un ambiente di test utilizzando macchine virtuali * Adeguamento agli attuali standard di sicurezza digitale" * Mappatura dei dati * Monitoraggio dei dati * Quadro normativo Europeo:   1. GDPR,   2. Cybersecurity ACT,   3. Direttiva NIS   4. IPR e Open Resources" | |
| **Benessere digitale: dal design all'uso degli ambienti digitali (2 ore)** | | * Sicurezza d'uso dei dispositivi digitali in ambiente di lavoro, personale e ludico * Conformità dei software/dispositivi e certificazioni: le norme * Realtà Virtuale * Realtà Aumentata * Metaverso * Impatti su salute mentale, Inclusione vs Isolamento * Difesa del benessere psicofisico dalle nuove dipendenze | |
| **Sostenibilità Digitale (2 ore)** | | * Evoluzione degli ambienti, soluzioni a confronto * Riuso del software e tecnologie open source * Orientamento e progettazione di soluzioni tailor made | |
| **Modalità di erogazione (in presenza / FAD) e metodologie didattiche** | | * Lezione frontale e FAD. * Discussione guidata. * Esercitazioni. * Sessioni di traning on the job. | |
| **Attestato finale** | | * Attestato di messa in trasparenza delle competenze | |

|  |
| --- |
|  |