

ALTA FORMAZIONE

Corso Specialistico per Professionisti.

TECNOLOGIE DI INTELLIGENZA ARTIFICIALE E DI CYBERSECURITY PER L'INNOVAZIONE E LA COMPETITIVITÀ DELLE ATTIVITÀ PROFESSIONALI.

110 ore tra aula e laboratorio pratico



SISTEMI DI INTELLIGENZA ARTIFICIALE E DI CYBERSECURITY PER L'INNOVAZIONE E LA RESILIENZA DEI SERVIZI PROFESSIONALI.

FINALITÀ

Il corso “Intelligenza Artificiale e Cybersecurity per l’Innovazione Professionale” si propone come un **intervento strategico volto a supportare i professionisti nel processo di transizione digitale, attraverso lo sviluppo di competenze integrate che coniughino innovazione tecnologica, sicurezza e conformità normativa**, favorendo un approccio consapevole, critico e operativo all’utilizzo delle tecnologie digitali avanzate, con particolare riferimento all’Intelligenza Artificiale e alla cybersecurity, intese non come ambiti separati, ma come dimensioni strettamente interconnesse all’interno dei moderni contesti lavorativi. In tale prospettiva il percorso si colloca nell’ambito delle priorità strategiche europee definite dalla Strategic Technologies for Europe Platform (STEP), promuovendo lo sviluppo e la diffusione di tecnologie quali:

- Intelligenza Artificiale (AI), inclusi sistemi basati su modelli generativi e tecniche di automazione dei processi;
- cybersecurity e sicurezza delle infrastrutture digitali;
- gestione e valorizzazione dei dati nei processi professionali.

L’attività formativa, che rafforza le competenze necessarie per l’adozione consapevole e sicura delle tecnologie digitali e pulite favorendo l’innovazione, la competitività e la resilienza dei sistemi professionali, in coerenza con gli obiettivi della stessa piattaforma STEP e con le politiche europee per la transizione digitale, mira a sostenere l’adozione dell’Intelligenza Artificiale come leva di innovazione professionale, supportando i partecipanti nella comprensione delle potenzialità offerte da tali strumenti in termini di automazione, ottimizzazione dei processi e miglioramento della qualità dei servizi, favorendo, di fatto, un cambiamento culturale che consenta ai professionisti di integrare l’AI in modo strategico e responsabile nelle proprie attività. Parallelamente, il corso intende rafforzare la cultura della sicurezza informatica, sviluppando nei partecipanti una maggiore consapevolezza dei rischi digitali e delle implicazioni derivanti da comportamenti non sicuri e, in uno scenario caratterizzato sempre più da una crescente esposizione a minacce informatiche, diventa fondamentale promuovere pratiche corrette di gestione delle informazioni e dei sistemi, al fine di tutelare dati, attività professionali e reputazione. Infine il corso offre gli strumenti necessari per comprendere e applicare i principali riferimenti legislativi europei, quali il GDPR e l’AI Act, favorendo l’adozione di comportamenti conformi e riducendo il rischio di sanzioni o contenziosi. Infine, seppur indirettamente, il percorso contribuisce a sostenere gli obiettivi di sostenibilità, promuovendo l’utilizzo di tecnologie digitali finalizzate all’ottimizzazione dei processi, la riduzione degli sprechi informativi e l’efficientamento delle risorse, in coerenza con i principi dell’Agenda 2030 e del Green Deal europeo.

OBIETTIVI

Obiettivo del percorso è quello di **rafforzare le competenze digitali dei professionisti**, consentendo loro di integrare in modo consapevole, sicuro e conforme alle normative vigenti strumenti di Intelligenza Artificiale

e pratiche di cybersecurity all'interno delle proprie attività lavorative, favorendo un approccio sistemico all'innovazione, in cui l'adozione delle tecnologie sia accompagnata da una corretta gestione dei rischi, dalla tutela dei dati e dal rispetto dei principi normativi stabiliti a livello europeo. In particolare il percorso intende favorire il raggiungimento dei seguenti obiettivi:

1. Acquisizione delle conoscenze strategiche sull'Intelligenza Artificiale.

Il corso si propone di fornire ai partecipanti una comprensione chiara e accessibile dei concetti dell'AI, delle sue principali tipologie e delle applicazioni nei diversi ambiti professionali, con l'obiettivo di ridurre il divario tra innovazione tecnologica e capacità di utilizzo, rendendo l'AI uno strumento concretamente utilizzabile anche da utenti non specialisti.

2. Sviluppo di competenze operative nell'utilizzo dell'AI.

Un obiettivo centrale consiste nel permettere ai partecipanti di utilizzare in modo efficace strumenti di Intelligenza Artificiale per attività quotidiane, quali la produzione di contenuti, l'analisi delle informazioni e l'automazione di processi. Ciò implica non solo l'apprendimento tecnico, ma anche la capacità di valutare l'affidabilità dei risultati e di integrare tali strumenti nei flussi di lavoro.

3. Comprensione e gestione dei rischi informatici.

Il percorso mira a sviluppare nei partecipanti la capacità di riconoscere le principali minacce informatiche e di adottare comportamenti adeguati per prevenirle al fine di ridurre la vulnerabilità individuale e organizzativa, promuovendo una maggiore attenzione alla sicurezza nell'uso quotidiano delle tecnologie digitali.

4. Applicazione delle pratiche di cybersecurity.

Oltre alla dimensione teorica, il corso si propone di sviluppare abilità concrete nella gestione della sicurezza informatica, quali la protezione delle credenziali, la gestione sicura dei dati e l'adozione di misure preventive, rendendo i partecipanti autonomi nell'applicazione delle buone pratiche di sicurezza.

5. Conoscenza e applicazione del quadro normativo.

Un ulteriore obiettivo è rappresentato dalla comprensione delle principali normative europee in materia di protezione dei dati e utilizzo dell'AI. I partecipanti saranno guidati nell'interpretazione e nell'applicazione dei principi previsti dal GDPR e dall'AI Act, al fine di garantire comportamenti conformi e responsabili.

6. Sviluppo di una consapevolezza etica e critica.

Il corso intende promuovere una riflessione sulle implicazioni etiche dell'uso delle tecnologie digitali, con particolare riferimento ai temi della trasparenza, della responsabilità e dei bias algoritmici.

7. Potenziamento della competitività professionale.

Il percorso contribuisce al miglioramento della competitività dei professionisti favorendo l'ottimizzazione dei processi lavorativi attraverso l'automazione e l'utilizzo di strumenti di Intelligenza Artificiale e la riduzione dei rischi operativi e reputazionali connessi alla sicurezza informatica, migliorando, di fatto, la qualità e l'efficienza dei servizi erogati, rafforza, così, la capacità dei partecipanti di adattarsi ai continui cambiamenti tecnologici e normativi.

PERCORSO E FABBISOGNO FORMATIVO

Il corso nasce da un fabbisogno sempre più diffuso, all'interno dei contesti professionali, di aggiornare e rafforzare le competenze digitali con particolare riferimento all'utilizzo dell'Intelligenza Artificiale, quale tecnologia abilitante in grado di rendere i processi di lavoro e i servizi erogati rapidi, precisi, controllati, personalizzati e automatizzati, e alla realizzazione di un piano di cybersecurity in grado di garantire a tutte le attività svolte dai professionisti sicurezza, conformità normativa e affidabilità.

Il corso, che si articola in due moduli formativi teorico-pratici e due laboratori applicativi per una durata complessiva di 110 ore, (*Modulo 1 – AI Revolution: come l'intelligenza artificiale cambia il futuro delle Professioni; Laboratorio 1 – AI Lab: strumenti intelligenti per lavorare meglio; Modulo 2 – Cybersecurity: sicurezza e protezione dell'attività professionale; Laboratorio 2 – Cyber Lab: simulazioni e difesa dalle minacce informatiche*) permette di acquisire competenze immediatamente spendibili necessarie per affrontare i cambiamenti tecnologici e normativi in atto, migliorare l'efficienza organizzativa e la competitività professionale.

Al termine del percorso i partecipanti saranno in grado di utilizzare le tecnologie di Intelligenza Artificiale e di Cybersecurity, che permetteranno di automatizzare le attività ripetitive, di supportare decisioni complesse, di prevedere rischi e di personalizzare, in base alle esigenze dei clienti, i servizi che sicuri e protetti, garantiranno prestazioni professionali efficienti e innovative. L'impatto verso i sistemi produttivi, le Istituzioni e i cittadini, sarà evidente in quanto i singoli Professionisti, grazie alle abilità e alle competenze acquisite, aumenteranno la propria competitività, sostenendo, in parallelo, i processi di crescita, resilienza, sostenibilità e innovazione del territorio.

ARTICOLAZIONE DEL CORSO

Il corso è progettato secondo una logica strutturata, progressiva e integrata, finalizzata a garantire l'acquisizione graduale delle competenze in materia di **Intelligenza Artificiale** e **cybersecurity** per arrivare a una piena applicazione operativa nei contesti professionali. I quattro step del percorso non sono concepiti come momenti isolati, ma come parti di un processo formativo unitario, in cui ogni elemento contribuisce al raggiungimento degli obiettivi complessivi. L'integrazione tra Intelligenza Artificiale e cybersecurity rappresenta il filo conduttore della formazione: da un lato, l'AI viene presentata come strumento di innovazione e miglioramento delle performance professionali; dall'altro, la sicurezza informatica viene proposta come condizione imprescindibile per un utilizzo sostenibile e responsabile delle tecnologie digitali.

Modulo 1 - AI Revolution: come l'intelligenza artificiale cambia il futuro delle Professioni - 30 ore

Obiettivi: Il modulo ha l'obiettivo di accompagnare i partecipanti nella comprensione dell'Intelligenza Artificiale per condurli verso una capacità di utilizzo consapevole e operativo degli strumenti. L'intento è

quello di ridurre il divario tra innovazione tecnologica e competenze professionali, fornendo chiavi di lettura semplici ma rigorose. Particolare attenzione è rivolta all'inquadramento dell'AI come leva di innovazione nei contesti lavorativi, evidenziandone le potenzialità in termini di efficienza, automazione e supporto decisionale. Allo stesso tempo, il modulo mira a sviluppare una consapevolezza critica rispetto ai limiti, ai rischi e alle implicazioni etiche, promuovendo un utilizzo responsabile e conforme al quadro normativo europeo, in particolare all'AI Act.

Conoscenze: Definizione di Intelligenza Artificiale e principali caratteristiche; Evoluzione storica dell'AI e principali tappe di sviluppo; Differenze tra: AI simbolica, Machine Learning, Deep Learning; Principi di funzionamento: dati e dataset, addestramento dei modelli, concetto di algoritmo, output e probabilità; Tipologie di sistemi di AI: AI predittiva, AI generativa, sistemi di raccomandazione; Strumenti di AI generativa: generazione di testi (report, email, documenti), generazione di immagini e contenuti multimediali, sintesi e analisi di informazioni; Applicazioni nei contesti professionali: automazione di attività amministrative, supporto alla produzione documentale, gestione della conoscenza, analisi dei dati; Interazione con l'AI: concetto di prompting, strutturazione delle richieste, interpretazione degli output; Limiti e rischi: errori e allucinazioni, bias algoritmici, problemi di affidabilità, dipendenza tecnologica; Aspetti etici: trasparenza, responsabilità, supervisione umana; Normativa: principi dell'AI Act, classificazione dei sistemi AI per rischio, obblighi per utilizzatori e organizzazioni

Abilità: Utilizzare strumenti di AI per: redazione di testi professionali, sintesi di documenti, analisi di contenuti; Formulare prompt efficaci: definizione dell'obiettivo, uso di istruzioni chiare, affinamento delle richieste; Valutare gli output dell'AI: verifica delle informazioni, identificazione di errori, controllo della coerenza; Integrare l'AI nei processi lavorativi: automazione di attività ripetitive, supporto decisionale, ottimizzazione dei tempi; Riconoscere limiti e rischi dell'AI; Applicare principi etici nell'utilizzo degli strumenti

Risultati attesi: Al termine del modulo, i partecipanti saranno in grado di comprendere il funzionamento e le potenzialità dell'Intelligenza Artificiale, utilizzando strumenti di base in modo autonomo e consapevole. Saranno inoltre in grado di integrare tali strumenti nelle proprie attività professionali, migliorando l'efficienza e la qualità del lavoro. Inoltre, i partecipanti svilupperanno una capacità critica nell'interpretazione dei risultati prodotti dall'AI e una maggiore consapevolezza delle implicazioni etiche e normative, operando in coerenza con i principi introdotti dall'AI Act.

Laboratorio 1 – AI Lab: strumenti intelligenti per lavorare meglio - 25 ore

OBIETTIVI

Il laboratorio è finalizzato allo sviluppo di competenze operative nell'utilizzo di strumenti di Intelligenza Artificiale, con particolare riferimento all'applicazione nei processi professionali. L'obiettivo è quello di rendere i partecipanti autonomi nell'utilizzo consapevole dell'AI per l'automazione delle attività, la produzione di contenuti e il supporto alle decisioni, in coerenza con le tecnologie digitali avanzate riconducibili alla piattaforma STEP.

SESSIONI DI LAVORO

Sessione 1 – Utilizzo degli strumenti di Intelligenza Artificiale

- Introduzione operativa agli strumenti di AI generativa;
- utilizzo guidato per la produzione di contenuti (email, documenti, report);
- analisi delle funzionalità e dei limiti.

Sessione 2 – Tecniche di prompting e ottimizzazione degli output

- Definizione degli obiettivi;
- costruzione di prompt efficaci;
- raffinamento delle richieste;
- valutazione della qualità e affidabilità degli output;
- gestione degli errori e dei bias.

Sessione 3 – Integrazione nei processi professionali

- Applicazione dell'AI in casi simulati;
- automazione di attività ripetitive;
- utilizzo dell'AI come supporto decisionale;
- integrazione nei flussi di lavoro.

RISULTATI ATTESI

Al termine del laboratorio i partecipanti saranno in grado di utilizzare strumenti di Intelligenza Artificiale in modo autonomo e consapevole, formulare richieste efficaci, valutare criticamente gli output e integrare tali tecnologie nei processi professionali, contribuendo all'efficientamento delle attività e al miglioramento della qualità del lavoro.

Modulo 2 – Cybersecurity: sicurezza e protezione dell'attività professionale – 30 ore

Obiettivi: Il modulo ha l'obiettivo di sviluppare nei partecipanti una solida cultura della sicurezza informatica, fondamentale per operare in contesti digitalizzati. L'intento è quello di fornire strumenti per riconoscere, prevenire e gestire le principali minacce informatiche, riducendo il rischio di incidenti e violazioni dei dati. Particolare attenzione è rivolta alla protezione dei dati personali e alla conformità normativa, con riferimento al GDPR, al fine di rendere i partecipanti consapevoli delle proprie responsabilità e capaci di adottare comportamenti corretti nella gestione delle informazioni.

Conoscenze: Principi della cybersecurity: riservatezza, integrità, disponibilità; Architettura dei sistemi digitali: dispositivi, reti, cloud; Tipologie di minacce: phishing, social engineering, malware, ransomware, attacchi informatici; Vulnerabilità: fattore umano, errori operativi, configurazioni non sicure; Misure di sicurezza: password sicure, autenticazione a più fattori, aggiornamenti software, antivirus; Sicurezza delle reti: Wi-Fi, connessioni pubbliche, accessi remoti; Protezione dei dati: trattamento dei dati personali,

classificazione dei dati, sicurezza delle informazioni; Normativa: principi del GDPR, diritti degli interessati, obblighi dei titolari; Gestione del rischio: identificazione delle minacce, valutazione del rischio, mitigazione

Abilità: Riconoscere attacchi informatici: email sospette, link malevoli, tentativi di phishing; Applicare misure di sicurezza: gestione password, uso MFA, protezione dispositivi, Gestire dati in sicurezza:

archiviazione corretta, condivisione controllata, protezione informazioni; Utilizzare strumenti digitali in modo sicuro; Adottare comportamenti preventivi; Applicare principi normativi nella gestione dei dati

Risultati attesi: Al termine del modulo, i partecipanti saranno in grado di riconoscere le principali minacce informatiche e di adottare comportamenti adeguati per prevenirle, riducendo significativamente il livello di rischio nelle proprie attività professionali. Saranno inoltre in grado di gestire dati e informazioni in modo sicuro e conforme alla normativa vigente, in particolare al GDPR, contribuendo a rafforzare la sicurezza complessiva dei contesti organizzativi in cui operano.

Laboratorio 2 – Cyber Lab: simulazioni e difesa dalle minacce informatiche – 25 ore

OBIETTIVI

Il laboratorio è finalizzato allo sviluppo di competenze pratiche nella prevenzione e gestione dei rischi informatici, attraverso l'analisi e la simulazione di scenari realistici. L'obiettivo è quello di rafforzare la capacità dei partecipanti di riconoscere le minacce, adottare misure di sicurezza e gestire correttamente dati e informazioni, in coerenza con i principi di sicurezza e resilienza digitale previsti dalle tecnologie STEP.

SESSIONI DI LAVORO

Sessione 1 – Analisi delle minacce e riconoscimento dei rischi.

- Simulazioni di attacchi informatici (phishing, social engineering);
- analisi di email sospette;
- individuazione di vulnerabilità nei comportamenti e nei sistemi.

Sessione 2 – Applicazione delle misure di sicurezza.

- Gestione delle credenziali e autenticazione;
- utilizzo di strumenti di protezione;
- sicurezza delle reti e dei dispositivi;
- applicazione di buone pratiche nella gestione dei dati.

Sessione 3 – Gestione degli incidenti e prevenzione.

- Simulazione di gestione di incidenti informatici;
- definizione di semplici procedure di risposta;
- creazione di policy di sicurezza;
- strategie di prevenzione e mitigazione del rischio.

RISULTATI ATTESI

Al termine del laboratorio i partecipanti saranno in grado di riconoscere le principali minacce informatiche, adottare comportamenti sicuri, proteggere dati e dispositivi e gestire situazioni di rischio in modo consapevole, contribuendo alla sicurezza e alla continuità operativa nei contesti professionali.

METODOLOGIA D'INTERVENTO

La metodologia adottata è il risultato di una progettazione attenta alle caratteristiche dei destinatari, agli obiettivi dell'intervento e alla natura delle competenze da sviluppare. In particolare, trattandosi di professionisti si è scelto di adottare un **approccio metodologico capace di coniugare accessibilità, gradualità e forte orientamento alla pratica**, strutturando un modello integrato di apprendimento che combina **momenti teorici, attività applicative ed esperienze laboratoriali**, con l'obiettivo di accompagnare i partecipanti in un percorso progressivo di acquisizione delle competenze. La complementarità tra formazione in presenza e laboratorio pratico è stata progettata in modo funzionale agli obiettivi didattici: le attività in presenza sono orientate all'approfondimento, al confronto e alla sistematizzazione delle conoscenze mentre i laboratori privilegiano le dimensioni esperienziali e fattuale, in cui è richiesta una maggiore interazione operativa, combinazione, questa, che consente di ottimizzare i tempi, migliorare l'efficacia dell'apprendimento e rispondere alle esigenze organizzative dei partecipanti. L'intervento, dunque, si configura come un sistema articolato e coerente, capace di **integrare teoria e pratica, apprendimento individuale e collaborativo**, funzionale allo sviluppo di competenze operative e all'acquisizione di una consapevolezza critica, elementi, questi, indispensabili per affrontare in modo efficace e responsabile le sfide poste dall'innovazione tecnologica e dalla sicurezza digitale.

DESTINATARI

Il percorso formativo è rivolto all'intera platea di **professionisti appartenenti a tutti i settori economici e professionali**, accomunati dalla necessità di confrontarsi con i processi di trasformazione digitale e con l'introduzione crescente di tecnologie basate sull'Intelligenza Artificiale. La scelta di un target così ampio è motivata dalla natura pervasiva delle tecnologie oggetto del corso: l'Intelligenza Artificiale e la cybersecurity non rappresentano infatti ambiti specialistici circoscritti, ma competenze ormai indispensabili in qualsiasi contesto professionale.

SEDE DI SVOLGIMENTO

Il Corso si svolgerà a **Potenza** c/o la sede della New Form in via Alberobello, 7, tuttavia in fase di avvio, per assicurare la piena efficacia della formazione e la continuità lavorativa dei professionisti coinvolti, potrà essere individuata anche una **sede diversa**.

QUOTA DI PARTECIPAZIONE

La quota di partecipazione è di € **5.000,00** comprensiva del materiale didattico.

DURATA

L'intero percorso avrà la durata complessiva di **110 ore**. L'attività sarà avviata il **18 giugno 2026** e si concluderà entro il **30 novembre 2026**. Eventuali modifiche saranno comunicate tempestivamente agli iscritti. Il calendario definitivo delle lezioni sarà comunicato in fase di avvio.

ISCRIZIONI

Il corso prevede una presenza massima di **25 iscritti**. In caso di numero maggiore la New Form valuterà in autonomia l'eventuale accesso all'aula degli iscritti in esubero. L'iscrizione va effettuata compilando la domanda di ammissione secondo le modalità di seguito riportate:

- **on site**, recandosi presso la sede della NEW FORM sita in via Alberobello, 7 - Potenza;
- **on line**, compilando il modulo di iscrizione presente sul sito www.newformpotenza.it;

INFORMAZIONI

Per informazioni, approfondimenti e chiarimenti, al numero **0971.21184**, è a disposizione un help desk attivo dal lunedì al venerdì (09.00 - 12.30 / 15.00 - 19.00). E' inoltre possibile contattarci al numero **340.8469035** o inviando una mail a: master@newformpotenza.it. Tutte le informazioni sono presenti sul nostro sito: www.newformpotenza.it

Corso Specialistico per Professionisti

TECNOLOGIE DI INTELLIGENZA ARTIFICIALE E DI CYBERSECURITY PER L'INNOVAZIONE E LA COMPETITIVITÀ DELLE ATTIVITÀ PROFESSIONALI.



New Form è Ente di formazione accreditato presso il MIUR ai sensi del D. M. n° 90/2003 – protocollo n° AOODPIT.852 del 30/07/2015 per la formazione del personale scolastico ed autorizzato all'utilizzo del BONUS SCUOLA

New Form è Ente di formazione accreditato presso la Regione Basilicata con D.D. n. 1702 del 08/11/2023 per la formazione e l'erogazione dei servizi al lavoro

New Form è ente certificato ai sensi della normativa UNI EN ISO 9001:2000.

New Form è Ente Gestore dell'Istituto Universitario per Mediatori Linguistici della Basilicata istituito dal Ministero dell'Istruzione, dell'Università e della Ricerca con Decreto Ministeriale n. 1931 del 1 agosto 2017 (*G.U. n. 197 del 24/08/2017*) ed è abilitato al rilascio della Laurea in Mediazione Linguistica e Culturale.

New Form è Ente Gestore della Scuola di Specializzazione in Psicoterapia della Basilicata istituita dal Ministero dell'Istruzione, dell'Università e della Ricerca con Decreto Ministeriale del 21 settembre 2017 (*G.U. n. 237 del 10/10/2017*) ed è abilitata al rilascio del Diploma quadriennale post-laurea per l'esercizio dell'attività di Psicoterapeuta.

0971.21184 / 340.8469035 / master@newformpotenza.it

WWW.NEWFORMPOTENZA.IT