Progetti di formazione sull'intelligenza artificiale
ESEMPIO DI PROGETTAZIONE - ISTITUTI TECNICI SIA

1. Dati Generali
Titolo Progetto: Codice Critico: L'Intelligenza Artificiale per i Sistemi Informativi Aziendali e la Sicurezza

Descrizione sintetica del progetto
L'indirizzo SIA forma figure capaci di comprendere, progettare e gestire i sistemi informativi delle imprese, operando su dati, applicazioni, architetture digitali e processi aziendali. In un contesto in cui l'Intelligenza Artificiale generativa è sempre più in grado di produrre codice, strutturare dati, assistere la programmazione e supportare l'organizzazione delle informazioni, il progetto assume un principio centrale: un output generato dall'IA può risultare plausibile o formalmente corretto senza essere, per questo, affidabile, sicuro o adeguato al contesto. L'obiettivo è formare docenti e studenti affinché non siano utenti passivi di tali strumenti, ma soggetti capaci di analizzarne criticamente i risultati, sottoponendoli a verifica tecnica, logica e funzionale. Attraverso un approccio laboratoriale e metodologicamente fondato, il percorso guiderà i partecipanti nell'individuazione di vulnerabilità di sicurezza, bug logici, incoerenze nei dati ed eventuali inefficienze architetturali negli output generati dall'IA, sviluppando competenze di code review, validazione e controllo dei sistemi informativi aziendali. Il progetto mira così a rafforzare una cultura professionale in cui l'IA rappresenta un supporto avanzato alla progettazione e alla gestione dei sistemi, ma non sostituisce la responsabilità tecnica, il controllo umano e la valutazione critica della qualità del software e dei dati.

2. Proposta Progettuale
A. Programmi e Attività Formative
I percorsi per i docenti mirano a consolidare un'alfabetizzazione avanzata sull'Intelligenza Artificiale, con particolare attenzione ai modelli linguistici di grandi dimensioni, al loro funzionamento probabilistico e alle tecniche di prompting e ingegneria delle istruzioni, anche attraverso schemi di strutturazione come Ruolo-Contesto-Task-Vincoli. L'offerta formativa approfondirà le modalità con cui l'IA può essere integrata nella didattica laboratoriale dell'indirizzo come supporto allo sviluppo, alla produzione e alla revisione di codice, alla strutturazione dei dati e all'analisi dei processi dei sistemi informativi aziendali, mantenendo centrale la verifica tecnica e il controllo umano. Verrà inoltre dedicato ampio spazio al quadro normativo ed etico di riferimento, con particolare riguardo all'AI Act, alla protezione dei dati personali, ai limiti strutturali dell'IA e ai rischi connessi alla sicurezza, all'affidabilità e alla correttezza degli output generati. Per il personale amministrativo, saranno previsti moduli specifici sull'automazione sicura dei flussi documentali, sulla gestione delle informazioni e sulla tutela dei dati dell'istituto, nel rispetto della normativa vigente e dei principi di uso responsabile delle tecnologie.
.

B. Percorso per i Formatori
Il programma mira a costituire un nucleo interno di docenti esperti, in grado di diffondere all'interno dell'istituto competenze metodologiche, didattiche e operative sull'uso dell'Intelligenza Artificiale nei sistemi informativi aziendali. I formatori acquisiranno competenze avanzate di red teaming in ambito informatico, inteso come pratica guidata di forzatura dell'errore del modello —

ad esempio attraverso un calcolo errato, un codice con bug o un falso allarme di sicurezza — per poterne analizzare il meccanismo di fallimento, i limiti strutturali e le condizioni di affidabilità. Diventeranno così punti di riferimento per l'istituto, guidando i colleghi nell'adozione di un metodo rigoroso di verifica, validazione e controllo degli output dell'IA, fondato su sicurezza, coerenza logica e supervisione umana consapevole.

C. Laboratori sul campo
I laboratori si svolgeranno esclusivamente in presenza, con un approccio prevalentemente operativo, e saranno orientati alla produzione di output verificabili, validati tecnicamente e non delegati in modo automatico all'IA. Le attività, anche con il coinvolgimento degli studenti, consentiranno di applicare l'Intelligenza Artificiale a situazioni coerenti con il curricolo SIA, mantenendo centrale la verifica logica, la sicurezza e il controllo umano dei risultati generati.

- **Sviluppo assistito e Code Review:** Utilizzo dell'IA come copilota per la stesura di funzioni complesse. Gli studenti dovranno eseguire una *code review* sistematica per intercettare vulnerabilità (es. *SQL injection*, *buffer overflow*, input non sanitizzati) e proporre interventi di *refactoring*.
- **Database e Data Analysis:** L'IA genererà query complesse per interrogare database relazionali didattici. Gli allievi dovranno testarne le performance, verificare i filtri e confrontare il risultato algoritmico con versioni ottimizzate manualmente.
- **Cybersecurity e Architetture:** Analisi di log di sistema per rilevare anomalie (es. tentativi di accesso sospetti). Verrà valutata la capacità dell'IA di distinguere minacce reali da falsi positivi. Inoltre, si richiederà all'IA di progettare architetture web, di cui gli studenti dovranno criticare le scelte di *design* e la scalabilità.
- **Project Work Finale:** Sviluppo di un modulo software o applicazione sicura assistita dall'IA. Il progetto dovrà essere accompagnato dalla "Dichiarazione metodologica", un documento in cui il partecipante ricostruisce il percorso seguito nell'interazione con l'IA, esplicita i prompt utilizzati, motiva le scelte tecniche compiute, segnala gli errori individuati e corretti e documenta i criteri adottati per validare gli output, dimostrando di aver sviluppato un metodo di lavoro consapevole e non un semplice uso strumentale della tecnologia.

D. Conformità alle Linee Guida e Framework
Il progetto si sviluppa in coerenza con i principali riferimenti europei e nazionali richiamati dall'Avviso. Per la formazione dei docenti assume come riferimento il framework DigCompEdu, con particolare attenzione all'aggiornamento metodologico e tecnologico, alla progettazione di risorse digitali, all'integrazione delle tecnologie nei processi di insegnamento e apprendimento e allo sviluppo delle competenze digitali degli studenti. Le attività proposte sono inoltre coerenti con DigComp 3.0, soprattutto per quanto riguarda uso critico e responsabile delle tecnologie, valutazione delle informazioni, sicurezza e integrazione delle competenze connesse all'Intelligenza Artificiale. Il progetto si raccorda inoltre con le Linee guida per l'introduzione dell'IA nelle istituzioni scolastiche, promuovendo un approccio consapevole, sicuro e fondato sulla supervisione umana, con le Linee guida per l'insegnamento dell'educazione civica, attraverso una particolare attenzione alla cittadinanza digitale, alla protezione dei dati personali, alle implicazioni etiche e sociali dell'IA e, in modo specifico, alla cybersecurity, al rilevamento delle minacce, alla gestione dei falsi positivi e alla responsabilità nell'uso dei sistemi informativi. Il progetto si collega infine alle Linee guida per le discipline STEM, valorizzando

programmazione, analisi dei dati, problem solving, sicurezza dei sistemi e lettura critica dei processi di automazione.

3. Aspetti Tecnici e Diffusione

E. Software e Privacy I laboratori adotteranno piattaforme basate su modelli linguistici generativi di livello avanzato, mantenendo un approccio agnostico rispetto ai fornitori commerciali per evitare logiche di *vendor lock-in* e insegnare il funzionamento strutturale delle tecnologie. I sistemi prescelti saranno integrati nel cloud d'istituto utilizzando licenze protette (*enterprise*). Sarà garantito il rigoroso rispetto della normativa Privacy (GDPR), istruendo gli studenti sull'obbligo di sanitizzare e anonimizzare dataset, porzioni di codice o log di rete prima di sottoporli all'analisi dell'intelligenza artificiale.

F. Modalità di Diffusione La disseminazione seguirà una strategia multilivello a cascata. L'azione dei formatori interni sarà affiancata dalla piattaforma Academy dedicata, che ospiterà materiali di approfondimento, risorse asincrone**,** tutorial per il *prompting* informatico e librerie di codice validato. Poiché l'indirizzo SIA ha un forte legame con il tessuto produttivo, i risultati del progetto — in particolare le metodologie di audit dell'IA e le Dichiarazioni Metodologiche elaborate nei *Project Work* — verranno condivisi in seminari aperti al territorio, coinvolgendo aziende IT locali, *stakeholder* e le famiglie, posizionando l'istituto come centro di eccellenza per l'innovazione tecnologica responsabile.