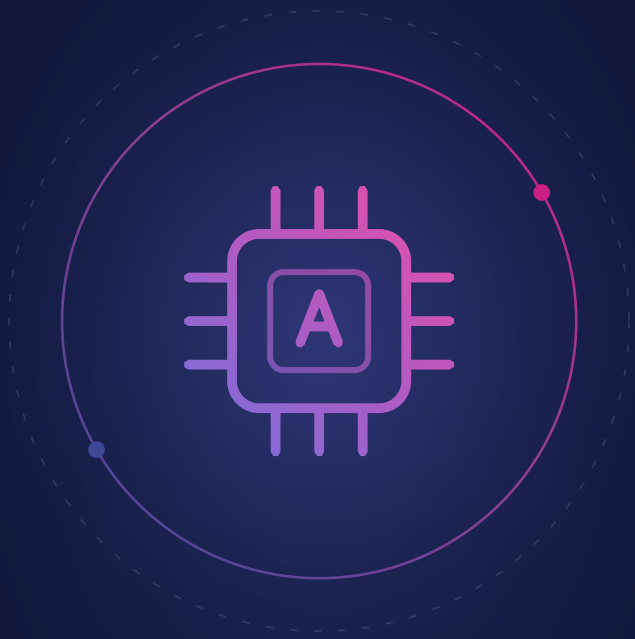
tnsolutions.it
FINE TECHNOLOGY



GUIDA 11 · SVILUPPO E AI

Intelligenza artificiale in azienda: sviluppo su misura, AI locale e MCP

Casi d'uso dell'AI generativa per le PMI, AI in cloud o in locale con Ollama, server per l'AI, Model Context Protocol (MCP), integrazione con gestionali e governance dei dati.

REVISIONE TECNICA **Marco Ursoleo** CEO TN Solutions

Per: Titolari, direzioni, IT Manager e responsabili di processo di PMI, aziende di servizi, studi professionali e startup che vogliono usare l'AI sui propri dati

Versione 1.0 · 14/11/2026

IN QUESTA GUIDA

L'intelligenza artificiale generativa è già entrata in molte aziende, spesso dalla porta di servizio: account personali, documenti incollati in chat pubbliche, nessuna regola. Questa guida spiega come portarla dentro i processi in modo controllato, scegliendo tra cloud e AI locale e collegandola ai sistemi aziendali con il Model Context Protocol.

1. Il problema: AI usata senza progetto 3

2. AI in cloud o AI locale? 4

3. Un server per l'intelligenza artificiale 6

4. MCP: collegare l'AI ai sistemi aziendali 7

5. Sicurezza e governance di AI e MCP 8

6. Sviluppo su misura e integrazione 9

7. Come avviare un progetto AI: passi e checklist 10

A chi è rivolta

Titolari, direzioni, IT Manager e responsabili di processo di PMI, aziende di servizi, studi professionali e startup che vogliono usare l'AI sui propri dati.

Come usarla

Leggi i capitoli nell'ordine, poi compila la checklist finale: le voci con priorità alta sono quelle da affrontare per prime.

Download libero

Questa guida è gratuita e non richiede registrazione. Puoi condividerla con il tuo team.

Contenuti verificati da Marco Ursoleo, CEO di TN Solutions

Revisione tecnica completata il 14/11/2026. TN Solutions opera con sistema di gestione certificato ISO 9001 e ISO/IEC 27001. Per domande su questa guida: info@tnsolutions.it · 02 95 17 550.

1. Il problema: AI usata senza progetto

Molti collaboratori usano già assistenti di intelligenza artificiale per scrivere email, riassumere documenti o generare codice. È un segnale positivo di curiosità, ma senza regole porta tre rischi concreti:

Dati che escono dall'azienda
contratti, offerte, dati di clienti incollati in servizi esterni senza sapere come vengono conservati.

Risultati non verificati
i modelli linguistici possono produrre risposte plausibili ma sbagliate, che finiscono in documenti e comunicazioni.

Valore disperso
ogni persona usa strumenti diversi, i benefici restano individuali e non diventano un miglioramento dei processi.

In sintesi

L'AI dà il massimo quando lavora **sui dati e sui processi dell'azienda**, con regole chiare su cosa può leggere, cosa può fare e chi controlla il risultato. È un progetto di integrazione, non solo l'acquisto di un abbonamento.

Dove l'AI generativa è già utile nelle PMI

Area	Esempi di utilizzo	Attenzione a
Documenti	Riassunti, bozze, confronto tra versioni, estrazione di dati da PDF	Verifica umana prima dell'invio
Conoscenza interna	Ricerca in procedure, manuali e storico delle pratiche	Permessi: ognuno deve vedere solo ciò che può già vedere
Assistenza clienti	Bozze di risposta, classificazione dei ticket	Tono, correttezza, escalation a una persona
Vendite e marketing	Schede prodotto, offerte, contenuti	Coerenza con listini e condizioni reali
Sviluppo software	Scrittura e revisione del codice, test, documentazione	Sicurezza del codice e licenze

Approfondisci sul sito TN Solutions: AI generativa per PMI: casi d'uso.

2. AI in cloud o AI locale?

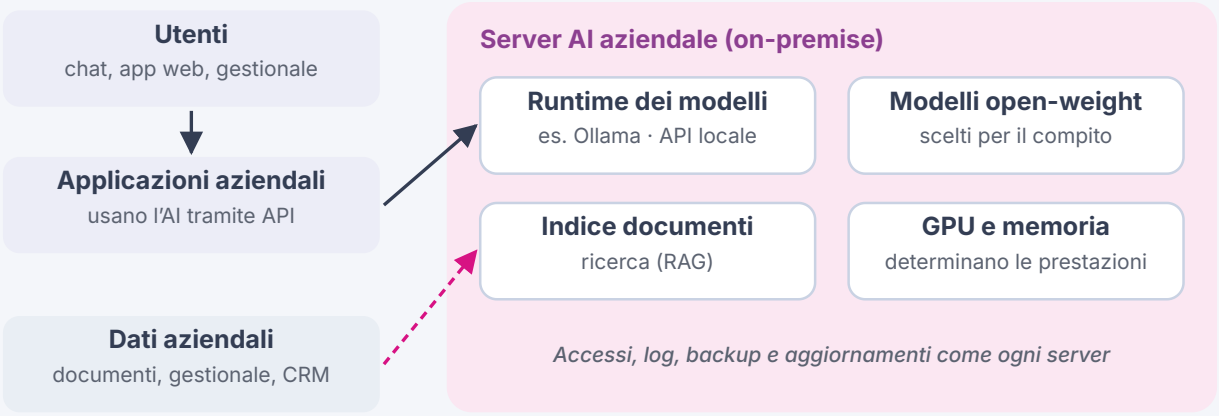
Le soluzioni in cloud offrono i modelli più potenti senza investimenti in hardware. L'**AI locale** esegue invece modelli linguistici "open-weight" su computer o server dell'azienda, così che documenti e richieste non lascino l'infrastruttura.

Criterio	AI in cloud	AI locale (on-premise)
Riservatezza	Dipende da contratto, impostazioni e regione del fornitore	I dati restano nell'infrastruttura aziendale
Qualità dei modelli	Accesso ai modelli più grandi e aggiornati	Modelli aperti, ottimi per molti compiti specifici
Costi	A consumo o per utente, ricorrenti	Investimento in hardware, poi costi prevedibili
Funzionamento offline	No	Sì, anche senza Internet
Gestione	A carico del fornitore	Aggiornamenti, monitoraggio e sicurezza a carico dell'azienda o del partner IT

Spesso la risposta è **ibrida**: modelli locali per i dati più riservati e per i compiti ripetitivi, servizi cloud per i compiti che richiedono le capacità dei modelli più grandi.

Ollama e l'AI locale

Ollama è uno degli strumenti più diffusi per scaricare ed eseguire modelli linguistici in locale. Espone un'interfaccia di programmazione (API) che le applicazioni aziendali possono usare come farebbero con un servizio cloud, e può essere affiancato da interfacce web per la chat. Ne parliamo in dettaglio nell'articolo Ollama, la rivoluzione della tecnologia.



I dati non escono dall'infrastruttura; il cloud resta un'opzione per i compiti più complessi

Schema originale: lo stack di un'AI locale. I modelli girano su un server aziendale, le applicazioni li usano tramite API e accedono ai dati con i permessi dell'utente.

3. Un server per l'intelligenza artificiale

Le prestazioni dell'AI locale dipendono soprattutto dalla **memoria della GPU** (VRAM): determina quali modelli si possono caricare e quanti utenti si possono servire insieme. Modelli più piccoli o "quantizzati" (compressi con una perdita di qualità contenuta) funzionano anche su hardware più modesto.

Scenario	Esigenza tipica	Indicazioni
Prova di fattibilità	Pochi utenti, un caso d'uso	Workstation con una GPU adeguata, modelli compatti
Reparto o team	Decine di richieste al giorno	Server dedicato, GPU con molta memoria, monitoraggio
Uso aziendale esteso	Più casi d'uso e utenti contemporanei	Più GPU o più nodi, bilanciamento, alta disponibilità

Prima di acquistare hardware conviene fare una **prova con i propri documenti e casi d'uso**: misurare qualità delle risposte e tempi aiuta a dimensionare correttamente l'investimento. La guida Come creare un server per le intelligenze artificiali approfondisce le scelte hardware.

> ⚠ **L'AI locale va gestita come ogni altro server**
>
> Un server AI contiene spesso copie dei documenti aziendali e indici di ricerca. Va protetto con accessi controllati, aggiornamenti, backup e monitoraggio, come descritto nelle Guide 2, 3 e 4 della collana.

Vuoi provare l'AI sui tuoi documenti?

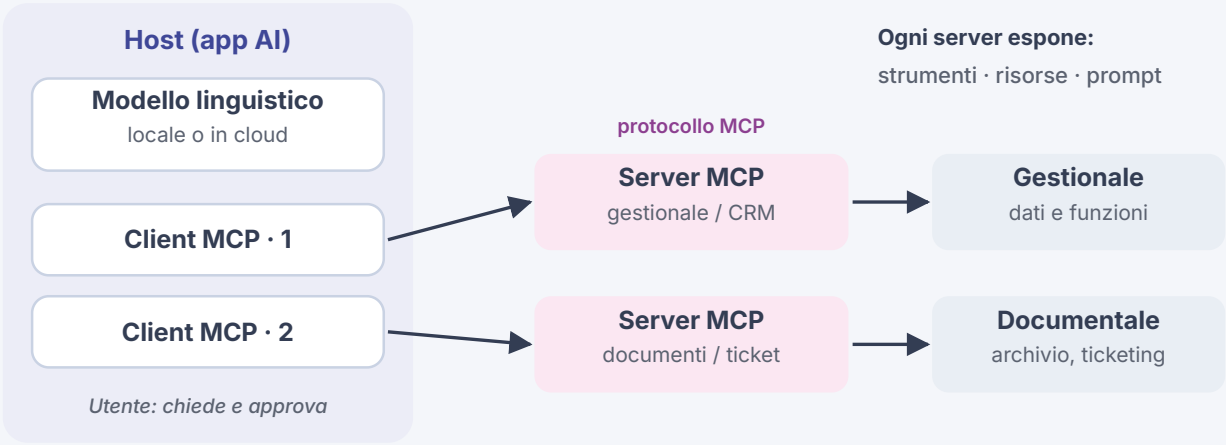
Con una prima telefonata gratuita possiamo individuare un caso d'uso pilota e capire se ha senso partire in cloud, in locale o in modo ibrido.

Richiedi una prima consulenza telefonica gratuita →

4. MCP: collegare l'AI ai sistemi aziendali

Un modello linguistico da solo conosce solo ciò che ha imparato durante l'addestramento e ciò che gli viene scritto nella richiesta. Per essere utile in azienda deve poter **leggere dati aggiornati** (un ordine, una pratica, un ticket) e, in alcuni casi, **eseguire azioni** (creare un appuntamento, aggiornare una scheda).

Il **Model Context Protocol (MCP)** è uno standard aperto, introdotto da Anthropic nel 2024, che definisce come le applicazioni di AI si collegano a strumenti e fonti di dati esterne. Invece di sviluppare un'integrazione diversa per ogni combinazione di modello e software, si espone ogni sistema aziendale una volta sola tramite un **server MCP**, utilizzabile da più assistenti e modelli compatibili.



Schema originale: architettura MCP semplificata. L'applicazione AI (host) usa client MCP per parlare con i server MCP che espongono i sistemi aziendali.

I componenti, in parole semplici

Host
l'applicazione con cui l'utente lavora (un assistente AI, un ambiente di sviluppo, un'app aziendale).

Client MCP
il componente dell'host che gestisce la connessione con ciascun server.

Server MCP
un piccolo servizio che espone a un sistema (gestionale, documentale, ticketing, database) tre tipi di capacità: **strumenti** (azioni), **risorse** (dati da leggere) e **prompt** (istruzioni predefinite).

Locale o remoto
un server MCP può girare sullo stesso computer dell'utente o essere pubblicato in rete. Con l'AI locale, modello, host e server MCP restano tutti dentro l'infrastruttura aziendale.

5. Sicurezza e governance di AI e MCP

Collegare l'AI ai sistemi aziendali aumenta il valore, ma anche la superficie di rischio. Le regole di base:

Rischio	Contromisura
L'AI vede dati a cui l'utente non ha accesso	Il server MCP usa l'identità e i permessi dell'utente, non un super-account
Azioni indesiderate	Strumenti in sola lettura dove possibile; conferma umana per le azioni che modificano dati
Istruzioni malevole nascoste nei contenuti (prompt injection)	Separare dati e istruzioni, limitare gli strumenti disponibili, verificare gli output
Server MCP di terze parti non verificati	Usare solo server noti, revisionati e aggiornati; inventario dei server installati
Mancanza di tracciabilità	Log delle richieste e delle azioni eseguite, conservati e consultabili

Regole e normative

Il trattamento di dati personali con sistemi di AI resta soggetto al GDPR. Il Regolamento europeo sull'intelligenza artificiale (AI Act, Reg. UE 2024/1689) introduce obblighi graduali in base al livello di rischio dei sistemi e al ruolo di chi li sviluppa o li utilizza. Quali obblighi si applicano a un caso specifico va verificato con i propri consulenti; dal punto di vista tecnico, una **policy interna sull'uso dell'AI** è il primo passo concreto.

> **Cosa scrivere in una policy sull'AI**
>
> Quali strumenti sono approvati; quali dati non possono mai essere inseriti in servizi esterni; chi verifica i risultati prima dell'uso; come si segnalano errori o incidenti; chi approva nuovi collegamenti ai sistemi aziendali.

> **Approfondimento: MCP e RAG**
>
> La **RAG** (Retrieval-Augmented Generation) recupera passaggi pertinenti da un archivio di documenti e li fornisce al modello per rispondere. MCP è più ampio: oltre a leggere dati permette di invocare strumenti e compiere azioni. Le due tecniche spesso convivono: un server MCP può anche offrire la ricerca nella base documentale.

6. Sviluppo su misura e integrazione

L'AI produce valore quando è inserita nei flussi di lavoro esistenti, non quando resta una chat separata. Per questo i progetti di AI sono spesso, prima di tutto, **progetti di sviluppo software**:

- **API e integrazioni** tra gestionale, CRM, documentale e assistente AI;
- **server MCP su misura** per esporre in modo controllato i sistemi aziendali;
- **applicazioni web** che incorporano funzioni AI (ricerca, classificazione, bozze) nelle schermate già usate dal personale;
- **automazioni** che preparano il lavoro e lasciano la decisione finale a una persona.

Approfondisci i servizi di sviluppo software, CRM su misura e intelligenza artificiale per le aziende.

HECTOR, L'ECOSISTEMA AI DI TN SOLUTIONS

TN Solutions sviluppa internamente l'ecosistema Hector. Hector-ai è l'assistente che risponde in linguaggio naturale solo sui dati e sui contenuti dell'azienda, con modelli open source eseguiti sull'infrastruttura Hector Cluster sotto il controllo di TN Solutions. Completano l'ecosistema Hector Biz, il gestionale per le PMI, e Hector Lis, il monitoraggio di sicurezza H24. Approfondisci la piattaforma Hector.

7. Come avviare un progetto AI: passi e checklist

1. **Scegliere un caso d'uso circoscritto**, con un beneficio misurabile (tempo risparmiato, errori ridotti).
2. **Mappare i dati necessari** e chi può accedervi.
3. **Decidere l'architettura**: cloud, locale o ibrida, in base a riservatezza, costi e qualità richiesta.
4. **Realizzare un pilota** con un gruppo ristretto di utenti e con i documenti reali.
5. **Misurare** qualità delle risposte, tempi e soddisfazione; correggere.
6. **Estendere** solo dopo aver definito policy, permessi, log e responsabilità.

Checklist AI, AI locale e MCP

Prima di portare l'AI nei processi aziendali	
☐ Policy interna sull'uso dell'AI condivisa con il personale	Alta
☐ Elenco dei dati che non possono essere inviati a servizi esterni	Alta
☐ Caso d'uso pilota con obiettivo misurabile	Alta
☐ Scelta motivata tra cloud, AI locale o soluzione ibrida	Alta
☐ Accessi dell'AI basati sui permessi dell'utente	Alta
☐ Conferma umana per le azioni che modificano dati	Alta
☐ Inventario dei server MCP e delle integrazioni attive	Media
☐ Log delle richieste e delle azioni eseguite	Media
☐ Server AI locale protetto, aggiornato e incluso nel backup	Media
☐ Verifica degli obblighi GDPR e AI Act con i consulenti	Media
☐ Formazione degli utenti su limiti e verifica dei risultati	Media
☐ Revisione periodica di costi, qualità e casi d'uso	Bassa

COME LAVORIAMO

Dal download alla soluzione, senza impegno nei primi passi

1 Download gratuito

Hai scaricato questa guida senza registrazione: usala per una prima autovalutazione.

2 Telefonata gratuita

Un incaricato TN Solutions ascolta le tue esigenze e ti aiuta a capire le priorità. È conoscitiva e senza impegno.

3 Audit avanzato (facoltativo, a pagamento)

Se serve un'analisi approfondita, con sopralluogo concordato, ricevi prima un preventivo dedicato. L'audit parte solo dopo che hai accettato il preventivo.

4 Proposta commerciale

Ricevi una proposta per i soli servizi necessari, con priorità e fasi di intervento.

Parla con noi
Prima telefonata gratuita e senza impegno

02 95 17 550 · info@tnsolutions.it · www.tnsolutions.it

Chi è TN Solutions

System integrator B2B con sede a Melzo (MI), operativo in Lombardia e da remoto su tutto il territorio nazionale. Dal 2001 progettiamo, integriamo e gestiamo infrastrutture IT per PMI, studi professionali, aziende di servizi, startup e imprese manifatturiere. L'azienda è guidata da **Marco Ursoleo**, CEO di TN Solutions.

Il sistema di gestione aziendale di TN Solutions è certificato **ISO 9001** (qualità) e **ISO/IEC 27001** (sicurezza delle informazioni). Le certificazioni riguardano i processi dell'azienda, non i singoli prodotti di terze parti citati in questa guida.

Servizi collegati a questa guida

Intelligenza artificiale per le aziende
/it/intelligenza-artificiale/

Sviluppo software
/it/sviluppo-software/

Server per le AI in locale: guida pratica per PMI
/it/creare-un-server-per-le-ai-in-locale/

Ollama: AI locale per le aziende
/it/ollama-la-rivoluzione-della-tecnologia/

AI generativa per PMI: casi d'uso
/it/ai-generativa-per-pmi-casi-uso/

Ecosistema Hector
/it/ecosistema-hector/

PROSSIMO PASSO

Vuoi capire come migliorare l'infrastruttura IT della tua azienda?

TN Solutions può aiutarti a valutare le esigenze, individuare le priorità e progettare la soluzione più adatta.

Richiedi una prima consulenza telefonica gratuita →

tnsolutions.it/it/contatti/

> Vuoi capire quali processi possono beneficiare dell'AI, in cloud o in locale? Parliamone in una prima telefonata gratuita.

TELEFONO 02 95 17 550

EMAIL info@tnsolutions.it

SITO WEB www.tnsolutions.it

SITO WEB

CONTATTI

tnsolutions.it
FINE TECHNOLOGY

TN Solutions · Viale Svezia 3, 20066 Melzo (MI) · 02 95 17 550 · info@tnsolutions.it · www.tnsolutions.it

Contenuto realizzato con il supporto dell'intelligenza artificiale. Revisione e supervisione tecnica: Marco Ursoleo, CEO TN Solutions.

TN Solutions — Guide tecniche per le imprese · Guida 11 · Versione 1.0 · 14/11/2026. Le informazioni hanno carattere divulgativo e non sostituiscono un'analisi tecnica specifica. Le tabelle economiche sono esempi illustrativi, non offerte né medie di mercato. I marchi citati appartengono ai rispettivi titolari.