Come costruire le precondizioni perché un sistema agentico possa essere usato nella PA

Recupero documentale assistito (RAG), connettori MCP e modelli linguistici locali per un’IA affidabile nella PA

Gianluigi Cogo - Consulente Formez esperto di innovazione digitale - https://gigicogo.substack.com

AI generica ≠ AI affidabile per la PA

Risposte plausibili, non corrette
I modelli generici producono la risposta più probabile, non quella verificata

Zero tracciabilità
Nella PA serve sempre sapere da dove arriva una risposta: fonte, data, documento

Responsabilità da gestire
L'IA nei processi amministrativi richiede ruoli chiari, controlli e supervisione umana

Dati fuori dal perimetro
Se documenti e dati sensibili finiscono su infrastrutture esterne, emergono problemi di sicurezza e governance.

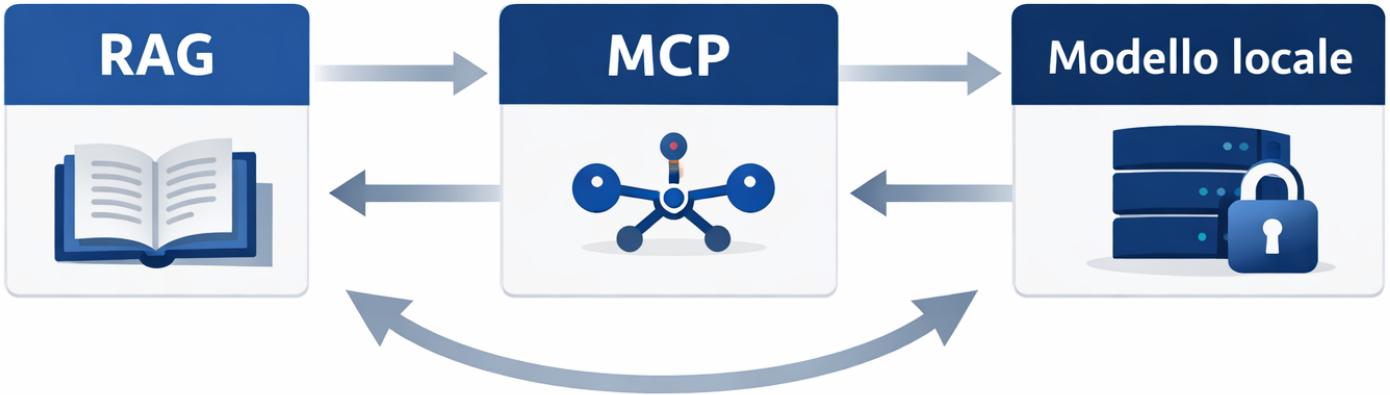
Due livelli del problema

1 Qualità delle risposte
L'IA può usare fonti non validate con il rischio di errori o informazioni superate

2 Governo dei dati
I dati dell'ente possono essere trattati fuori da un perimetro controllato

Riferimenti: AI Act, GDPR, CAD.

Tre approcci, un principio



Tre approcci, un principio

L'affidabilità di un sistema di IA dipende da quali fonti consulta e dove opera.

01
RAG

Base documentale controllata

Il sistema consulta solo documenti caricati, selezionati e aggiornati dall'amministrazione.
Se ben progettato dovrebbe segnalare quando le fonti disponibili non consentono una risposta affidabile.

02
MCP

Accesso standardizzato a fonti esterne

MCP è un protocollo aperto che consente di collegare l'IA a banche dati e servizi esterni in modo standardizzato.
La qualità della risposta dipende comunque dall'affidabilità della fonte collegata

03
Modello locale

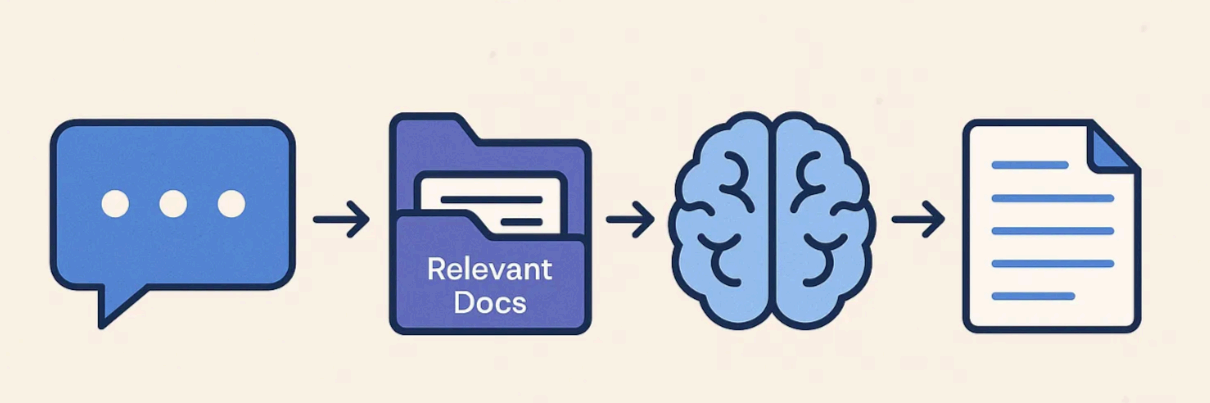
Elaborazione dentro il perimetro dell'ente

Il modello può essere eseguito su infrastrutture controllate dall'amministrazione, riducendo l'esposizione dei dati verso servizi esterni.

I tre approcci non si escludono: possono essere combinati per aumentare controllo delle fonti, tracciabilità delle risposte e governo dei dati.

1 - Come funziona RAG

RAG (Retrieval-Augmented Generation) significa “**generazione arricchita dal recupero di documenti**”.
In pratica, prima di rispondere, l’IA cerca **nei documenti dell’ente** le informazioni pertinenti e usa quei contenuti per costruire la risposta.



È come avere un assistente che **non inventa**, ma **consulta gli archivi ufficiali** prima di parlare

REQUISITI TECNICI
(coordinarsi con il settore IT)

Archivio indicizzato
Un archivio dove i documenti sono organizzati in modo che l’IA li trovi velocemente.

Rappresentazione semantica dei testi
I testi vengono trasformati in “significato” numerico, così il sistema capisce di cosa parlano.

Ricerca semantica
L’IA non cerca parole identiche, ma contenuti che hanno lo stesso senso.

Base documentale (KB)
L’insieme dei documenti ufficiali che l’ente decide di rendere consultabili.

Modello linguistico con contesto documentale
L’IA genera la risposta usando solo i documenti trovati, non conoscenze generiche.

Come funziona RAG

1 L’utente fa una domanda

2 Il sistema cerca i documenti più rilevanti

3 I passaggi trovati diventano il “contesto” della risposta

4 L’IA risponde citando le fonti o segnala se non ha dati sufficienti

Cosa significa base documentale controllata (KB chiusa)

- Contiene solo documenti approvati (circolari, regolamenti, FAQ, modulistica).
- Si aggiorna con procedure definite, evitando testi superati.
- Limita le risposte alle fonti disponibili, senza ricorrere a conoscenze generiche o non verificate.

Casi d'uso concreti per la PA

Chatbot di sportello

Risponde a cittadini e imprese su procedure, modulistica e scadenze usando solo documenti validati dall’ente. Se l’informazione non è presente o non è aggiornata, il sistema deve segnalarlo

Assistente interno PA

Aiuta il personale a ritrovare istruzioni operative, circolari e manuali interni, riducendo tempi di ricerca e quesiti ripetitivi

Supporto ai bandi

Recupera criteri, scadenze e requisiti a partire dal testo ufficiale del bando, distinguendo tra versioni e allegati quando la base documentale è aggiornata e ben gestita

Ricerca normativa interna

Individua rapidamente articoli, passaggi e riferimenti presenti in regolamenti, delibere e determine, restituendo il punto esatto del documento

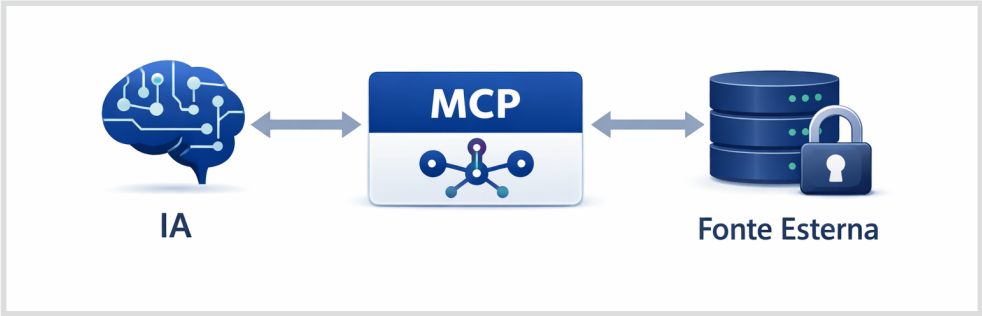
2 - MCP: un protocollo aperto per collegare l'IA a dati e strumenti

MCP (Model Context Protocol) è un **protocollo aperto** che permette a un sistema di intelligenza artificiale di collegarsi **in modo sicuro e standardizzato** a fonti esterne come **banche dati, servizi online o archivi digitali**.

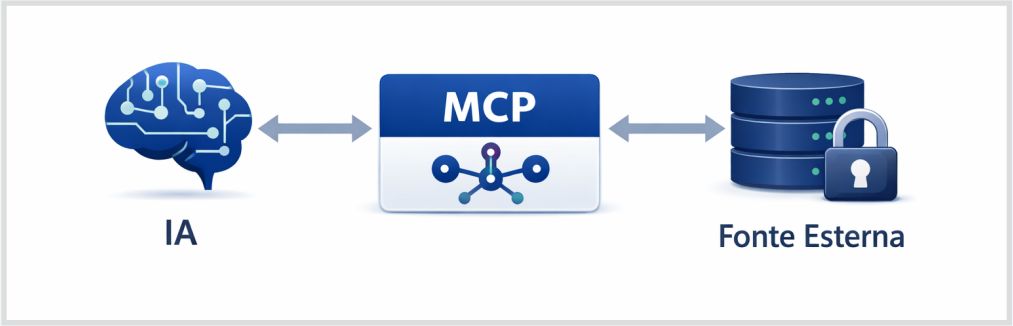
"Se RAG è la biblioteca interna dell'ente, MCP è il collegamento alle biblioteche pubbliche nazionali, collegate a fonti ufficiali e aggiornabili in tempo reale."

Come funziona (in parole semplici):

- L'IA chiede informazioni
- MCP traduce la richiesta in un formato standard
- Il sistema esterno risponde con dati verificabili
- L'IA usa quei dati per generare la risposta, mantenendo il collegamento alla fonte



MCP: un protocollo aperto per collegare l'IA a dati e strumenti



Perché serve

- Evita soluzioni "su misura" per ogni fonte esterna
- Garantisce **tracciabilità** e **controllo** su ciò che l'IA consulta
- Permette di **limitare l'accesso** solo a fonti affidabili e autorizzate
- Favorisce **interoperabilità** tra enti e piattaforme

STORIA E ADOZIONE

Nato come iniziativa open source annunciata da Anthropic, oggi è un progetto aperto ospitato dalla Linux Foundation e supportato da un ecosistema di specifiche, ambienti di sviluppo e server.

In pratica, è come un **adattatore universale** che consente all'IA di dialogare con sistemi terzi, senza doverli integrare manualmente

onData una sperimentazione che ha anticipato il tema

L'attivismo civico italiano, con **onData**, ha anticipato l'uso dell'IA sui dati pubblici creando strumenti aperti per interrogarli in linguaggio naturale.

CKAN MCP Server

Consente di collegare agenti di IA a portali basati su CKAN, compreso Dati.gov.it. È una soluzione aperta, riusabile e già applicabile a cataloghi pubblici esistenti.

ISTAT MCP Server

Permette di interrogare dati statistici ufficiali tramite linguaggio naturale. Mostra il potenziale di interazione con basi informative autorevoli senza passare da query tecniche tradizionali.

> Il valore di queste esperienze non è solo tecnico: hanno anticipato un'esigenza che oggi comincia a trovare anche un riscontro istituzionale

Dall’ecosistema civico agli strumenti istituzionali

AGID ha presentato due nuovi strumenti per rendere i dati pubblici più accessibili, di qualità e più facili da consultare anche con il supporto dell’IA

Cruscotto Italia

Piattaforma di analisi e visualizzazione che raccoglie in un unico spazio i principali dati pubblici disponibili su tutti i Comuni italiani, acquisiti da fonti istituzionali ufficiali. Integra anche un protocollo aperto MCP, che consente ad agenti di IA e chatbot di interrogare dati affidabili e aggiornati in linguaggio naturale, con collegamento alla fonte istituzionale dichiarata

SIMBA

Suite operativa per ricerca dei metadati, bonifica e arricchimento semantico dei dataset pubblici. Non si limita alla correttezza formale dei metadati, ma interviene anche sulla qualità effettiva dei dati, segnalando problemi come campi vuoti, formati incoerenti e codifiche miste

Cruscotto Italia rende il dato interrogabile; SIMBA lo rende più governabile.

Maturità dei dati per agenti IA

- **I dati aperti non sono automaticamente pronti per gli agenti IA**
- **Serve maturità: qualità, aggiornamento, metadati, standard e vocabolari condivisi**
- **Strumenti come SIMBA abilitano dati davvero interrogabili**

Sintesi: l'IA funziona bene solo con dati pubblici affidabili e standardizzati.

3 L’IA che resta nel perimetro dell’ente

Modelli in Cloud

- Dati fuori controllo
- Rischi sulla privacy

VS

Modelli Locali

Ollama · LM Studio · Google AI Edge Gallery

- Massima sicurezza
- Presidio interno

Più controllo, meno esposizione dei dati

Eseguire i modelli su infrastrutture interne e controllate consente di preservare il controllo sui dati sensibili e ridurre l'esposizione verso servizi esterni.

Ollama

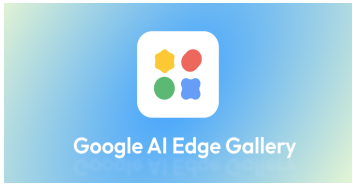
Esegue modelli in locale e offre un'API utilizzabile da applicazioni interne

→ ollama.com

LM Studio

Ambiente grafico per usare modelli locali in modo semplice sul proprio computer.

→ lmstudio.ai



Mostra casi d'uso e modelli eseguiti direttamente sul dispositivo

→ github.com/google-ai-edge/gallery

*I modelli locali offrono **più controllo sui dati**, con prestazioni inferiori ai modelli cloud ma **adeguate per attività interne** della PA (consultazione, FAQ, classificazione, supporto).*

DUE INFOGRAFICHE GENERATE DALL'AI PER RIASSUMERE IL MODELLO

ARCHITETTURA INTEGRATA PER SERVIZI DIGITALI SICURI
RAG + MCP + LLM LOCALE INSIEME

FRONTEND
Interfaccia Utente

- Sportello digitale
- Assistente interno
- Modulo di richiesta
- Cruscotto di consultazione

INTELLIGENZA APPLICATA - Il Cuore del Sistema

RECUPERO DOCUMENTALE (RAG)
Ricerca su Fonti Interne Validate

MODELLO LINGUISTICO (LLM LOCALE)
Elaborazione e Risposte Sicure (perimetro controllato)

CONNETTORE FONTI ESTERNE (MCP)
Collegamento a Fonti & Servizi Selezionati

INFRASTRUTTURA CONTROLLATA DALL'ENTE
(Locale o Cloud Sicuro)

Il modello è eseguito localmente per massimo controllo e sicurezza dei dati.

FONTI DATI E SERVIZI

INTERNO - Fonti Validate

- Documenti dell'ente [per RAG]
- Basi informative e gestionali interni [per MCP]

ESTERNO UFFICIALE Fonti Selezionate

- Cataloghi pubblici e dati aperti
- Servizi statistici e altre fonti ufficiali

NOTA CHIAVE: RAG presidia le fonti **documentali, MCP** i collegamenti ai dati, l'**LLM locale il perimetro dell'elaborazione**. Lavorano insieme per scopi diversi.

RAG + MCP + LLM

Insieme per servizi digitali intelligenti e sicuri

LIVELLO 1
FRONTEND

- Sportello digitale
- Assistente interno
- Modulo di richiesta
- Cruscotto di consultazione

LIVELLO 2
INTELLIGENZA APPLICATA

- **Modello linguistico (LLM)**
  Elaborazione e ragionamento sicuro sui dati
- **Recupero documentale (RAG)**
  Recupero di informazioni da documenti interni validati
- **Collegamento a fonti e servizi esterni (MCP)**
  Connessione controllata a dati e servizi esterni selezionati

LIVELLO 3A
INTERNO

- Documenti validati dell'ente (RAG)
- Basi informative e gestionali interni (MCP)

LIVELLO 3B
ESTERNO UFFICIALE

- Cataloghi pubblici e dati aperti
- Servizi statistici e altre fonti ufficiali

RAG, MCP e modello locale non risolvono lo stesso problema:
il primo presidia le **fonti documentali,** il secondo i **collegamenti ai dati,** il terzo il **perimetro dell'elaborazione.**

LIVELLO 4
INFRASTRUTTURA

- Servizi esterni (Cloud)
- Infrastrutture controllate dall'ente (On-premise)

Il modello può essere eseguito su servizi esterni oppure su infrastrutture controllate dall'ente, a seconda del profilo di rischio e dei dati trattati.

E quando arriva un agente IA?

Un agente non sostituisce queste componenti

UN AGENTE AI E' UN SISTEMA CHE:

- Interpreta un obiettivo
- Consulta documenti e dati
- Utilizza strumenti esterni
- Compone più azioni in sequenza

PER FUNZIONARE BENE, HA BISOGNO DI:

- **Fonti documentali controllate** (RAG)
- **Accesso governato** a dati e servizi (MCP)
- **Regole di sicurezza** e supervisione
- **Tracciabilità** delle operazioni svolte

Senza queste basi l'agente diventa soltanto più autonomo nel commettere errori.

Da dove cominciare

STEP 1

Mappatura conoscenza

Individuare documenti, regolamenti, FAQ, circolari e modulistica già digitali e aggiornati.
Sono i **candidati naturali** per una base documentale controllata

STEP 2

Censire i dati pubblici utili

Verificare quali dataset, cataloghi o servizi esterni sono davvero **rilevanti** per i procedimenti e per i servizi dell'ente. La disponibilità del dato non basta: servono qualità, metadati e riusabilità.

Da dove cominciare

STEP 3

Analisi del rischio

Distinguere tra dati **pubblici, interni e sensibili** per definire **architettura, controlli e fonti ammissibili** del modello.

STEP 4

Sperimentazione mirata

Partire da un servizio **delimitato**, con responsabilità chiare e verifica periodica dei risultati prima di **estendere** il sistema

TAKEAWAY

Oggi si parla molto di IA agentica. Ma prima di chiedersi cosa un agente possa fare per una pubblica amministrazione, è utile chiedersi quali dati, quali fonti e quali regole gli consentano di operare in modo affidabile.

https://gigicogo.substack.com

Linkografia

Fonti istituzionali

📊 **Dati.gov.it**

Catalogo nazionale dei dati aperti delle pubbliche amministrazioni

🏛️ **AgID / Open Data**

Quadro nazionale di riferimento su dati aperti, qualità e valorizzazione del patrimonio informativo pubblico

📜 **AI Act su EUR-Lex**

Testo ufficiale del Regolamento UE 2024/1689

Riferimenti tecnici

🔧 **Model Context Protocol**

Specifica tecnica del protocollo aperto per collegare applicazioni di IA a dati e strumenti esterni

🤖 **Ollama.com**

Esempio di ambiente per eseguire modelli in locale

🖥️ **lMstudio.ai**

Esempio di interfaccia grafica per l’uso di modelli locali

Società civile

🔬 **Ondata**

Comunità civica e casi d’uso sul riuso dei dati pubblici

Sintesi del quadro normativo

Reg. UE 2024/1689

Alcuni usi dell'IA nella PA possono rientrare tra i casi ad alto rischio previsti dall'Allegato III, in particolare quando incidono su diritti, accesso a servizi essenziali o decisioni rilevanti per le persone. In questi casi diventano centrali qualità dei dati, documentazione, tracciabilità, supervisione umana, robustezza e sicurezza.

Reg. UE 2016/679

Se il sistema tratta dati personali, l'ente deve valutare basi giuridiche, ruoli, misure di sicurezza, minimizzazione e, quando rilevante, i trasferimenti verso soggetti o infrastrutture esterne. L'esecuzione su infrastruttura controllata dall'ente può ridurre alcuni rischi, ma non sostituisce gli adempimenti privacy

D.Lgs. 82/2005

Il CAD resta il riferimento per disponibilità, interoperabilità, uso corretto dei dati pubblici e qualità dei servizi digitali della PA. Un sistema che usa fonti documentate e dati governati è più coerente con questa logica di uno che risponde su basi opache

Open data e qualità del dato

Nel contesto della PA, apertura e riuso dei dati vanno accompagnati da validazione, qualità e misurazione dell'affidabilità.
È un punto spesso richiamato anche nei percorsi formativi Formez, dedicati proprio a qualità e validazione dei dati aperti.