CORSO IA CON CLAUDE · DISPENSA PER L'ALLIEVO

Applicazione desktop, MCP e IA agentica

Quando l'assistente esce dal browser e comincia ad agire

ORA	DURATA	MODULO
11 di 12	60 minuti	6 — Integrazioni

Gianluca Bonomo · www.gianlu.it · info@gianlu.it

Indice

Indice 2

Come usare questa dispensa 3

1. Fuori dal browser 4

1.1 Che cosa vuol dire, in pratica 4

1.2 Le tre forme del collegamento 4

2. Il Model Context Protocol 5

2.1 Perché serviva uno standard 6

2.2 Che cosa chiedere a un fornitore, prima di collegare qualcosa 7

2.3 Tre integrazioni che si vedono spesso 8

2.4 Chi risponde di che cosa, una volta collegato 8

3. Dall'assistente all'agente 9

3.1 Le regole di sicurezza, prima di provarci 9

3.2 Quando un agente conviene e quando no 10

3.3 Un flusso agentico, passo per passo 11

4. Esercitazione pratica dell'ora 11

4.1 L'integrazione 11

4.2 Il flusso agentico 12

4.3 Che cosa provare senza correre rischi 12

Le domande che arrivano in aula 13

Glossario 14

Per approfondire 15

Come usare questa dispensa

Questa dispensa raccoglie, in forma scritta e ordinata, tutto quello che vediamo insieme durante l'ora di lezione. Non devi studiarla a memoria: serve a farti ritrovare le cose con calma, dopo, quando l'aula è finita e ti resta una domanda in sospeso.

È pensata per chi parte da zero. Ogni termine tecnico viene spiegato la prima volta che compare, e a fine dispensa trovi un glossario con tutte le parole nuove. Se una pagina ti sembra difficile, saltala e torna indietro dopo: nessun concetto di questa dispensa richiede conoscenze informatiche precedenti.

> **COME SONO FATTI I RIQUADRI**
>
> **In parole semplici** (azzurro): la spiegazione senza tecnicismi, quella da portarsi a casa se si ricorda una cosa sola.
>
> **Attenzione** (oro): un errore frequente, un rischio, una cosa da non fare.
>
> **Esempio** (grigio): un caso concreto, preso dalla vita di tutti i giorni o dal lavoro in azienda.

Obiettivo dell'ora

Capire che cosa cambia portando Claude sul computer, che cos'è il protocollo aperto con cui si collega ai dati aziendali, e dove va messo il freno quando un sistema comincia ad agire da solo.

Che cosa saprai fare alla fine

- Spiegare che cos'è MCP e perché essere un protocollo aperto conta.
- Riconoscere le quattro fasi del ciclo di un agente.
- Definire il perimetro di accesso di un'integrazione.
- Individuare le azioni che devono sempre passare da una conferma umana.

1. Fuori dal browser

Finché l'assistente vive in una scheda del browser, i vostri dati restano dall'altra parte del vetro: bisogna passarglieli a mano.

L'applicazione **desktop** per Windows e Mac porta Claude accanto agli altri programmi. Il vantaggio non è estetico: è che da lì diventa possibile collegarlo a quello che sta sul computer e nei sistemi aziendali.

Fino a oggi, nel corso, il flusso è sempre stato lo stesso: apri il file, copi, incolli nella chat. Funziona, ma ogni passaggio è manuale e ogni passaggio manuale è un punto in cui si sbaglia.

1.1 Che cosa vuol dire, in pratica

Finora abbiamo lavorato sempre allo stesso modo: si apre una pagina, si scrive, si incolla il materiale. Funziona, ma ha un limite evidente: **tutto quello che serve dovete portarglielo voi**, a mano, ogni volta.

Il passo successivo è dare all'assistente un accesso diretto ai posti in cui le informazioni vivono già.

Prima	Dopo
Esporto il report dal gestionale, lo salvo, lo carico, chiedo l'analisi	Chiedo l'analisi, e i dati vengono letti dal gestionale
Cerco tre documenti nell'archivio, li apro, ne copio le parti utili	Chiedo la risposta, e i documenti vengono trovati e letti
Rileggo dieci mail per ricostruire una vicenda	Chiedo la ricostruzione, con il riferimento a ciascuna mail

È un salto di comodità notevole, ed è anche il punto in cui le domande sulla sicurezza e sui permessi smettono di essere teoriche: da qui in poi lo strumento non aspetta più che gli diate i dati, **li va a prendere**.

1.2 Le tre forme del collegamento

«Collegare l'assistente ai nostri sistemi» copre tre cose molto diverse per impegno, costo e rischio. Distinguerle evita discussioni confuse in azienda.

La forma	Che cos'è	Che impegno richiede
Il connettore già pronto	Un collegamento verso un servizio diffuso, che si attiva dalle impostazioni concedendo i permessi	Minimo: è una configurazione, non uno sviluppo
Il collegamento a un sistema interno	Un componente che espone i dati del vostro gestionale o archivio nel modo standard	Medio: serve qualcuno che lo installi e ne definisca i permessi
L'integrazione dentro un vostro programma	L'assistente richiamato dall'interno di un'applicazione aziendale, tramite interfaccia di programmazione	Alto: è sviluppo software a tutti gli effetti

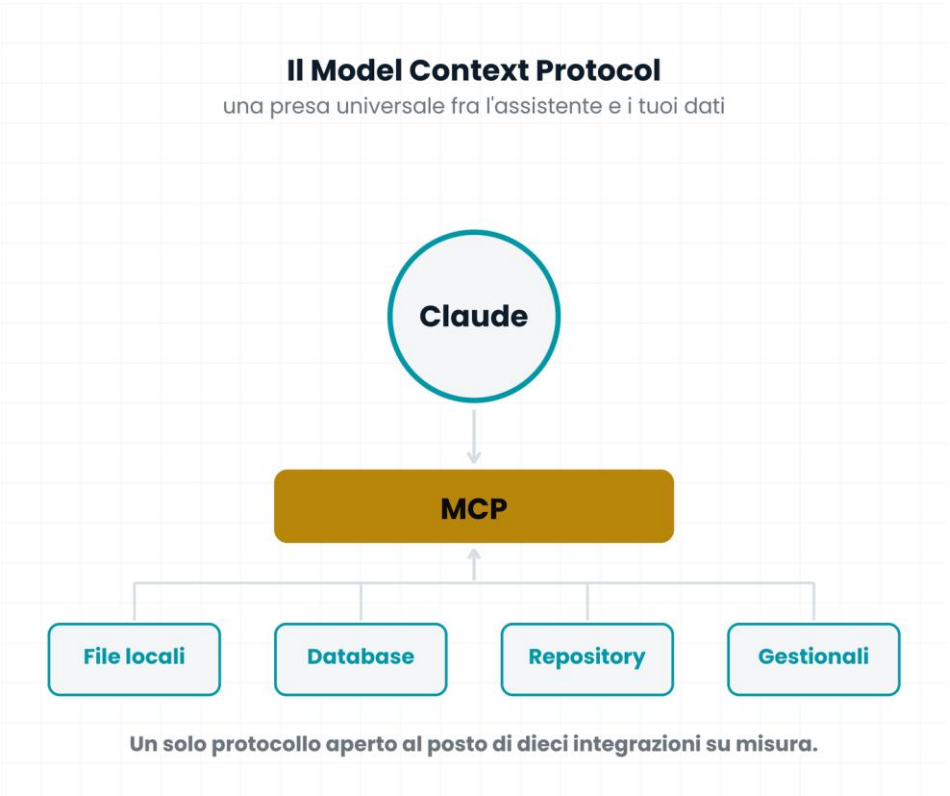
Per quasi tutte le aziende piccole e medie il percorso sensato è esattamente questo ordine: si comincia dalla prima riga, e si passa alla seconda solo quando la prima ha dimostrato di servire.

2. Il Model Context Protocol

Il pezzo tecnico dell'ora. Si spiega bene con un'immagine sola.

Ogni sistema aziendale parla una lingua diversa: il gestionale, l'archivio documentale, la banca dati, il repository del codice. Costruire un'integrazione su misura per ciascuno costa, e invecchia.

Il **Model Context Protocol** (MCP) è un protocollo **aperto**, pubblicato da Anthropic, che definisce un modo standard per esporre dati e strumenti a un assistente. È come una presa elettrica: dietro il muro ci può essere qualsiasi impianto, ma la spina è sempre quella.



Un solo protocollo al posto di dieci integrazioni su misura.

PERCHÉ CONTA CHE SIA APERTO

Un protocollo aperto significa che chiunque può scrivere un connettore, e che il lavoro fatto per collegare un sistema non è legato a un solo fornitore di IA.

Per un'azienda è una garanzia contro il vincolo tecnologico: se domani cambiate assistente, i connettori restano.

Senza MCP	Con MCP
Apri il file, copi, incolli nella chat	Chiedi, e Claude legge dove gli hai dato accesso
Ripeti per ogni documento	Il perimetro lo decidi tu, una volta sola
I dati passano dalle tue mani ogni volta	Meno passaggi manuali, meno errori di copia
Ogni integrazione va costruita da zero	Un modo standard per tutte le sorgenti

2.1 Perché serviva uno standard

Fino a poco tempo fa, ogni collegamento fra un assistente e un programma aziendale andava costruito su misura: un lavoro dedicato per ogni combinazione di strumento e sistema. Con cinque assistenti e dieci gestionali, i collegamenti possibili diventano cinquanta, e nessuno li costruisce.

Uno standard rovescia il conto: ogni sistema espone i propri dati **una volta sola**, in un modo che qualsiasi assistente sa leggere. Da cinquanta lavori su misura si passa a quindici, e soprattutto riutilizzabili.

> **L'ANALOGIA CHE FUNZIONA IN AULA**
>
> È successa la stessa cosa con le prese elettriche, con i formati dei file e con le porte USB: finché ogni produttore aveva la sua, servivano gli adattatori.
>
> Uno standard non è una tecnologia più potente: è una convenzione condivisa. E quasi sempre vale molto di più.

Per voi, in pratica, significa due cose: che il collegamento al vostro gestionale ha buone probabilità di esistere già, e che se cambiate assistente non buttate via il lavoro fatto.

2.2 Che cosa chiedere a un fornitore, prima di collegare qualcosa

Collegare un assistente al gestionale o all'archivio documentale non è una decisione tecnica: è una decisione sui dati. Sono cinque domande, e vanno fatte prima della firma, non dopo.

1. **A quali dati accede, esattamente?** Non «all'archivio», ma quali cartelle, quali tabelle, quali campi.
2. **In lettura o anche in scrittura?** Un collegamento che può solo leggere è un rischio; uno che può anche modificare o cancellare è un rischio di un altro ordine di grandezza.
3. **Chi vede che cosa?** Il collegamento rispetta i permessi che ogni persona ha già nel sistema, o li scavalca dando a tutti la stessa visibilità?
4. **Che cosa resta scritto?** Esiste un registro di chi ha chiesto che cosa e quando? Senza registro, in caso di contestazione non avete niente in mano.
5. **Come si stacca?** Deve esserci un modo immediato di revocare l'accesso, e qualcuno che sappia usarlo.

> **IL PRINCIPIO DEL MINIMO INDISPENSABILE**
>
> Si parte dal **meno** possibile: sola lettura, su una cartella sola, per poche persone. Si allarga dopo, se serve.
>
> Il percorso inverso — dare tutto e restringere dopo un incidente — è quello che riempie i comunicati stampa.

2.3 Tre integrazioni che si vedono spesso

Al di là del principio, queste sono le tre che compaiono più di frequente nelle aziende piccole e medie, e che danno il risultato più immediato.

1. **L'archivio documentale.** Sola lettura su alcune cartelle. Serve a rispondere a domande su procedure, contratti e capitolati senza andarli a cercare. È l'integrazione con il miglior rapporto fra utilità e rischio.
2. **Il sistema di ticket o assistenza.** Lettura delle segnalazioni per ricavarne classificazioni, riassunti e ricorrenze. La scrittura — chiudere un ticket, rispondere al cliente — si tiene fuori, almeno all'inizio.
3. **Il repository del codice**, per chi sviluppa. È il caso in cui il guadagno si misura meglio, perché il contesto tecnico è tutto lì dentro.

> **IL CRITERIO PER LA PRIMA INTEGRAZIONE**
>
> Scegliete quella in cui **le informazioni sono già viste da tutti quelli che useranno l'assistente**.
>
> Così il problema dei permessi non si pone, e potete concentrarvi sull'imparare come funziona.

2.4 Chi risponde di che cosa, una volta collegato

Con un collegamento attivo, le responsabilità non cambiano ma diventano più difficili da vedere. Vale la pena fissarle prima, perché dopo un problema è tardi.

Che cosa succede	Di chi è la responsabilità
Il collegamento espone più dati di quelli che servivano	Di chi ha configurato i permessi: è una scelta aziendale, non del fornitore
Una risposta riporta un'informazione riservata a chi non doveva vederla	Di chi ha deciso quali documenti rendere leggibili al collegamento
Un contenuto generato e inviato risulta sbagliato	Di chi lo ha inviato. Vale esattamente come nella seconda ora: lo strumento non firma
Il fornitore subisce un incidente di sicurezza	Del fornitore per l'incidente; dell'azienda per aver valutato il fornitore e gli accessi concessi

È il motivo per cui, in questa materia, la configurazione dei permessi non è un dettaglio tecnico da delegare: è una decisione che ha conseguenze giuridiche, e va presa da chi può assumersele.

3. Dall'assistente all'agente

L'ultimo passo del percorso: un sistema che non risponde soltanto, ma fa.

Nel libro, il capitolo 7 chiama **agente** un sistema che percepisce l'ambiente, ragiona su un obiettivo, decide quali azioni compiere e osserva i risultati per correggersi. La differenza con l'assistente che abbiamo usato finora non è di potenza: è di **autonomia**.



Quattro fasi in cerchio, e un punto in cui l'uomo deve restare.

- **Osserva**: legge lo schermo, i file, i dati a cui ha accesso.
- **Decide**: sceglie l'azione successiva verso l'obiettivo.
- **Agisce**: clicca, scrive, chiama uno strumento, modifica un file.
- **Verifica**: guarda il risultato e, se serve, cambia strada.

3.1 Le regole di sicurezza, prima di provarci

Regola	In concreto
Accesso minimo	Dai accesso a una cartella, non al disco. A una tabella, non al database.
Separa lettura e scrittura	Far leggere è molto meno rischioso che far modificare. Comincia dalla sola lettura.
Conferma sulle azioni	Cancellare, inviare, pagare, firmare, pubblicare: mai in automatico.

Regola	In concreto
irreversibili	
Tieni un registro	Che cosa ha fatto l'agente, quando, su quali dati. Serve quando qualcosa va storto.
Parti da un ambiente di prova	Mai dai dati veri. Un agente che sbaglia su dati di prova è una lezione; sui dati veri è un incidente.

IL LIMITE VERO DEGLI AGENTI

Un agente non sa quando sta sbagliando, e soprattutto **non conosce il costo aziendale** di un errore. Per lui cancellare una cartella e rinominarla sono due azioni equivalenti.

La regola operativa è semplice: autonomia sulle azioni reversibili, conferma umana su tutto il resto. Il perimetro si allarga solo dopo che qualcosa ha funzionato a lungo.

3.2 Quando un agente conviene e quando no

Conviene	Non conviene
Il compito ha molti passaggi meccanici e un risultato verificabile alla fine	Il compito richiede una decisione discrezionale che qualcuno dovrà comunque firmare
Un errore si accorge subito e si corregge senza danni	Un errore produce effetti verso l'esterno prima che qualcuno se ne accorga
Il lavoro si ripete spesso abbastanza da ripagare l'impostazione	È un caso isolato: impostare l'agente costa più che farlo a mano
I dati coinvolti sono interni e non particolarmente delicati	Ci sono dati personali di terzi, o dati coperti da segreto

LA REGOLA DI PARTENZA

Il primo agente che mettete in piedi dovrebbe fare qualcosa che, se sbagliasse completamente, **non farebbe alcun danno**.

Serve a imparare come si comporta, non a risparmiare tempo. Il risparmio arriva dal secondo in poi.

3.3 Un flusso agentico, passo per passo

Per capire che cosa cambia davvero, seguiamo un compito completo: preparare la rassegna settimanale delle segnalazioni per la riunione del lunedì. È un lavoro reale, che in molte aziende occupa un'ora a settimana.

Passo	Che cosa succede	Chi decide
1	Legge le segnalazioni arrivate negli ultimi sette giorni dal sistema di assistenza	L'agente, in sola lettura
2	Le classifica per tipo e per urgenza, seguendo gli esempi che gli avete dato	L'agente
3	Si accorge che una categoria è cresciuta molto e va a cercare le segnalazioni simili dei mesi precedenti	L'agente: è il passo che un programma tradizionale non farebbe
4	Prepara la bozza della rassegna, con i numeri e i riferimenti alle segnalazioni citate	L'agente
5	Si ferma e ve la mostra	**Voi**: la rilettura e l'invio restano una decisione umana

Il terzo passo è quello che distingue un agente da un'automazione: nessuno gli aveva detto di andare a guardare i mesi precedenti. Lo ha fatto perché serviva a rispondere bene alla richiesta.

> **ED È ANCHE IL PASSO DA SORVEGLIARE**
>
> La stessa capacità che rende utile un agente lo rende imprevedibile: può decidere di fare qualcosa che non avevate previsto.
>
> Per questo il quinto passo non si toglie mai. Un agente propone; la responsabilità di quello che esce resta di una persona.

4. Esercitazione pratica dell'ora

Due progettazioni sulla carta. Non serve configurare nulla: serve pensarci prima.

4.1 L'integrazione

Domanda	La vostra risposta
Quale archivio o cartella volete collegare?	.....

Domanda	La vostra risposta
Quali dati servono davvero? Quali no?	.....
Solo lettura, o anche scrittura?	.....
Chi autorizza l'accesso, e chi lo revoca?	.....

4.2 Il flusso agentico

Prendete un compito ripetitivo del vostro ufficio e scomponetelo nelle quattro fasi: che cosa osserva, che cosa decide, che cosa fa, come verifica. Poi segnate con una croce **il punto preciso** in cui una persona deve dire sì prima di proseguire.

> **SE NON TROVATE QUEL PUNTO**
>
> Vuol dire che il compito non è adatto a essere automatizzato, oppure che non lo avete ancora capito abbastanza bene.
>
> In entrambi i casi, meglio scoprirlo su un foglio che in produzione.

4.3 Che cosa provare senza correre rischi

Per farsi un'idea concreta non serve toccare i sistemi aziendali. Queste tre prove si fanno subito, non richiedono autorizzazioni e insegnano quasi tutto quello che serve sapere.

1. **Un collegamento in sola lettura a una cartella di documenti pubblici** o non riservati: manuali, normative, procedure già diffuse. Serve a vedere come cambia il modo di fare le domande.
2. **Un flusso a più passi su materiale finto.** Costruite un piccolo archivio di dati inventati e chiedete un'analisi che richieda di incrociarli. Osservate che cosa decide di fare senza che glielo abbiate detto.
3. **Una prova di limite.** Chiedetegli di fare qualcosa che avete esplicitamente vietato nelle istruzioni, e verificate che si fermi. È la prova che nessuno fa e che dice di più sulla sicurezza di qualsiasi documentazione.

> **CHE COSA AVRETE IMPARATO**
>
> Che il collegamento cambia il modo di lavorare più di quanto cambi lo strumento: si smette di preparare il materiale e si comincia a fare domande.
>
> E che i confini vanno scritti, perché quello che non è scritto prima o poi viene tentato.

Le domande che arrivano in aula

Sono le stesse in ogni corso. Vale la pena avere pronta una risposta breve e onesta, anche per quando le farà un collega.

«Serve un informatico per attivare questi collegamenti?»

Per la configurazione iniziale sì, quasi sempre: si tratta di permessi, credenziali e accessi a sistemi aziendali.

Per l'uso quotidiano no: una volta collegato, si chiede a parole come sempre.

«È rischioso dare accesso ai nostri sistemi?»

Dipende interamente da come si imposta. Sola lettura su una cartella definita, con un registro degli accessi, è un rischio governabile.

Accesso completo in scrittura a tutto l'archivio, senza registro, non lo è. La tecnologia è la stessa: cambia la configurazione.

«Un agente può sbagliare e fare danni?»

Sì, ed è il motivo per cui si definiscono in anticipo i confini: che cosa può toccare, che cosa deve solo proporre, dove si ferma per chiedere conferma.

Le azioni irreversibili — inviare, pubblicare, cancellare, pagare — restano a una persona. Sempre.

«È già maturo, o conviene aspettare?»

Per i collegamenti in sola lettura, è maturo: funziona e si governa.

Per gli agenti che agiscono da soli su processi aziendali, siamo nella fase in cui conviene sperimentare su qualcosa di innocuo e imparare, non nella fase in cui ci si appoggia per le attività critiche.

Glossario

Le parole che incontri in questa dispensa, spiegate in una riga. Tienilo a portata di mano: torneranno in tutte le ore successive del corso.

Termine	Che cosa significa
Agente	Sistema che percepisce, decide, agisce e verifica in autonomia verso un obiettivo.
Computer use	Capacità di osservare lo schermo e usare le applicazioni come farebbe una persona.
Connettore	Componente che espone una sorgente dati secondo il protocollo, rendendola utilizzabile.
Human-in-the-loop	L'uomo nel processo: la persona che conferma o blocca le azioni delicate.
MCP	*Model Context Protocol*: protocollo aperto per collegare un assistente a dati e strumenti.
Protocollo aperto	Specifica pubblica che chiunque può implementare, senza dipendere da un unico fornitore.

Per approfondire

Le fonti usate per costruire questa dispensa. Sono tutte pubbliche e consultabili: se un dato ti interessa, vai alla fonte e verificalo. È esattamente quello che chiediamo di fare anche all'intelligenza artificiale.

La specifica del protocollo

Il Model Context Protocol è pubblicato come progetto aperto: specifica, connettori e documentazione sono consultabili liberamente.

L'IA agentica nel libro

Niente paura, è solo IA, capitolo 7, dedicato agli agenti: che cosa sono, esempi reali, rischi e limiti.

Il libro di riferimento del corso

Gianluca Bonomo, *Niente paura, è solo IA. La guida completa per capirla, usarla e restare umani*.

UNA NOTA SULLE DATE

Le norme sull'intelligenza artificiale cambiano in fretta. I dati normativi di questa dispensa sono verificati a **settembre 2026**. Prima di usarli in una decisione aziendale, controlla sempre la fonte ufficiale: il calendario dell'AI Act è già stato modificato una volta.