

Creare agenti in Copilot

1. Creare agenti in Copilot

Benvenuti in questo nuovo mini percorso dedicato alla costruzione di **agenti con Copilot**. Sebbene siano già stati esplorati la potenza degli strumenti di intelligenza artificiale, ora si affronta la parte relativa agli agenti.

È importante ricordare che il concetto di agente non è nuovo. Agenti come il *prompt coach*, l'*idea coach* e il *writing coach* sono già stati messi a disposizione da Microsoft all'interno di Copilot per fornire funzioni aggiuntive. Analogamente, con ChatGPT si è parlato di Dall-E come esempio di agente dedicato.

L'obiettivo di questa serie di lezioni è esplorare la possibilità di **creare autonomamente i propri agenti** all'interno di Copilot di Microsoft, in aggiunta a quelli già sviluppati da Microsoft. La creazione di questi agenti è possibile senza la minima conoscenza di programmazione, utilizzando semplicemente i prompt.

Cosa sono gli agenti

È fondamentale avere chiaro cosa siano gli agenti, soprattutto all'interno del mondo Microsoft. Gli agenti sono dei **Copilot verticali** o dei **ChatGPT specializzati in un compito singolo**. Più il compito è specifico e specializzato, più facile è creare agenti che facciano esattamente ciò che serve.

Il punto chiave di questo percorso è la trasformazione: passare dal semplice scrivere un prompt e ottenere risposte al **creare un agente**. L'agente funge da prompt che agisce in modo costante e coerente.

Un buon indicatore per identificare un contenuto che può diventare un agente è un prompt che si utilizza molte volte ogni mese. L'intelligenza artificiale, che prima era vista come uno strumento passivo, diventa ora un **collaboratore attivo** e una vera e propria estensione del nostro team. Attivare gli agenti permette di migliorare significativamente la performance.

La prima creazione: Autocomposizione

Per iniziare a creare un agente si utilizza l'interfaccia classica di Copilot, cliccando sul pulsante **"crea agente"**. Esistono tre modi per creare un agente, e il primo e più semplice è utilizzare la nuova funzionalità di Copilot, che è una sorta di *wizard* o *autocomposizione*.

In questa fase, si può descrivere cosa fa l'agente. L'assistente propone anche esempi preimpostati, come l'assistente alle domande per il colloquio o l'assistente alle riunioni.

Per un esempio pratico, si procede alla creazione di un agente che scriva post su LinkedIn. (È bene ricordare che nessuno di questi agenti può prendere il controllo del computer e pubblicare direttamente su LinkedIn). L'agente viene configurato per creare **post professionali originali su LinkedIn**, adattando tono e stile e fornendo suggerimenti per titoli, call to action e ottimizzazione della visibilità. Viene suggerito il nome "creatore post LinkedIn".

Nella configurazione, si può definire che i post siano, ad esempio, informali, lunghi ma con punti elenco, e che includano hashtag e menzioni. La personalizzazione è cruciale: più l'agente è personalizzato, meglio è, sebbene si possa anche creare un agente aziendale che rispetti il *tone of voice* dell'azienda. Creare agenti è paragonabile ad avere un team di assistenti personali, ognuno specializzato in una singola mansione. Si possono anche aggiungere fonti di conoscenza pubbliche, indicando una URL specifica (non un intero sito web).

Anatomia dell'Agente

Dopo la creazione, è essenziale esaminare la sua anatomia, accedendo alla sezione di modifica. La struttura del prompt si compone di:

1. **Nome.**
2. **Descrizione:** Questa serve solo all'utente per sapere cosa fa l'agente e non è funzionale all'intelligenza artificiale.
3. **Istruzioni:** Definiscono il comportamento, come "Genera post originali professionali per LinkedIn...".
4. **Regole di sicurezza:** Per esempio, "Non generare contenuti offensivi. Discriminatorio che violino non li guida LinkedIn. Rispondi sempre in italiano".
5. **Interattività:** La frase che rende l'agente interattivo è: "**Chiedi all'utente il tema, l'obiettivo al pubblico di riferimento prima di il post**". Senza questa frase, l'agente genererebbe subito una risposta.
6. **Knowledge Base:** Informazioni sull'utente possono essere inserite qui.
7. **Richieste Suggeste:** Sono strutturate con un titolo in grassetto e il prompt passato.

Quando l'agente viene testato, ad esempio, con una richiesta per un post, risponde con domande veloci (pubblico, stato del progetto, tono) per centrare l'obiettivo, comportandosi come gli agenti predefiniti di Microsoft.

2. Creare i propri agenti

Per creare agenti in modo più controllato, si segue uno schema per un **System Prompt** efficace, organizzato su **quattro livelli**:

1. **Identità e Ruolo:** Chi sei e cosa fai. Include personalità, *tono of voice*, specializzazioni e competenze.
2. **Obiettivi e Comportamenti:** I gol primari da perseguire, come interagisce con gli utenti e come gestisce situazioni diverse.
3. **Task/Flusso di Lavoro:** Come procede passo dopo passo, se usa framework decisionali e come valuta la qualità delle risposte.

4. **Vincoli/Protocolli:** Cosa non deve fare mai, quando chiedere supporto umano ed eventuali protocolli di sicurezza.

Creazione tramite "Configura"

Invece di affidarsi all'autocomposizione, si parte da "nuovo agente" e si va direttamente in **Configura**. Si dà subito un nome (ad esempio, "copywriter personale").

Nelle **Istruzioni** (che indicano il comportamento), si definisce l'identità e il ruolo utilizzando il *roll prompting*: "Agisci come un copywriter senior specializzato in testi per il web, sia social, blog post e newsletter".

Si definiscono poi gli altri elementi dello schema:

- **Personalità:** "Sei molto disponibile, propositivo".
- **Specializzazioni:** "in testi per il web sia social, blog post e newsletter".
- **Obiettivi:** "Genera risposte coerenti con il con il contenuto che ti chiedo usando al meglio la tua grande esperienza".
- **Comportamento:** "Se nelle mie domande mancano delle informazioni per svolgere al meglio il tuo compito non andare avanti a eseguirle, ma chiedimi direttamente cosa ti serve".

Questo approccio offre molto più controllo sulle singole parole che si possono utilizzare.

Test dell'Agente Copywriter

Testando l'agente copywriter con la richiesta di scrivere un articolo sulle "allucinazioni AI", l'agente risponde immediatamente chiedendo dettagli per un contenuto efficace: pubblico di riferimento, tono, titolo, lunghezza e inclusione di esempi pratici. Questo comportamento è direttamente collegato all'istruzione di chiedere le informazioni mancanti.

Si può tentare un *azzardo*, fornendo l'URL del proprio blog e chiedendo all'agente di dedurre il pubblico di riferimento. L'agente è in grado di leggere il sito e di dedurre che è rivolto a professionisti, formatori, e operatori del mondo della cultura e della formazione.

Dopo aver fornito i dettagli richiesti (tono divulgativo, cinque proposte di titolo, lunghezza di 1500 caratteri, inclusione di casi reali), l'agente genera l'articolo. L'agente copywriter può essere utilizzato per compiti successivi nella stessa chat, come creare uno slogan di massimo 120 caratteri per TikTok e Twitter per promuovere l'articolo, o generare il testo della newsletter (in tal caso, chiederà ancora chi è il destinatario).

3. Creazione agenti avanzata

Per una creazione avanzata si utilizza il **meta prompting**: l'intelligenza artificiale viene usata per aiutare a creare un'altra entità di intelligenza artificiale (l'agente).

Esempio: Agente SEO

Si chiede all'IA di aiutare a creare le istruzioni per un agente specializzato nell'ottimizzazione SEO dei siti web. L'IA pone una serie di domande essenziali:

1. **Priorità dell'agente:** Aumento traffico organico, posizionamento per keyword, ottimizzazione *on page* e *home page*.
2. **Ambito operativo:** Blog aziendali, siti istituzionali, e-commerce, con lingua solo italiana e keyword variabili.
3. **Integrazione strumenti:** Deve leggere e interpretare report da Google Search Console, Google Analytics e Ahrefs, generando report comprensibili.
4. **Linee guida contenuti:** Tono chiaro, diretto, esplicativo. Tono dei report chiaro. Tono dei contenuti in base al sito. Deve ottimizzare contenuti esistenti e crearne di nuovi, gestendo metatitle, metadescription, alt text e slug delle immagini.
5. **Output:** L'agente deve mostrare a video le modifiche da applicare. Si nota che gli agenti Copilot non possono prendere il controllo o modificare strumenti esterni.

L'IA procede quindi a strutturare una bozza delle istruzioni (funzionalità principali, tono di voce, workflow operativo, regole chiave) e, su richiesta, genera il system prompt completo da inserire nell'agente.

L'agente viene creato (chiamato "SEO") e configurato con il prompt generato.

Gestione dei Contenuti Web e Abilitazione Funzionalità

Durante il test, incollando un articolo web e chiedendo di ottimizzarlo, l'agente fornisce un'analisi preliminare SEO (titolo, meta description, suggerimenti per la struttura H2/H3 e keyword). Tuttavia, se si prova a riscrivere il testo completo, l'agente può fallire, in quanto chiarisce: **"non ho accesso ai contenuti web esterni"**. L'utente dovrebbe quindi copiare e incollare il testo completo.

Per risolvere il problema dell'accesso web, bisogna abilitare l'**interprete di codice** nel *flag* dell'agente. Questa funzionalità è cruciale per permettere al tool di muoversi online ed è da abilitare solo negli agenti, poiché Copilot la possiede nativamente.

Un metodo alternativo e molto affidabile per ottimizzare il contenuto di una pagina web specifica è usare Copilot attivo sul browser. Gli agenti personali si attivano con la chiocciola (@). Ad esempio, attivando l'agente "esperto SEO" e chiedendo di ottimizzare il contenuto della pagina che si sta visualizzando, l'agente lavora in collaborazione con il browser web, leggendo il contenuto direttamente dalla fonte. Questo approccio permette di avere un "super agente".

4. Creazione avanzata di agenti parte 2

Continuando con la creazione avanzata, si esplorano altre tipologie di agenti e si affinano i prompt.

Esempio: LinkedIn Content Creator

Si crea un agente chiamato **LinkedIn Content Creator**. Nella configurazione, si imposta un prompt dettagliato:

- **Identità e Esperienza:** Content strategist LinkedIn specializzato in B2B con 10 anni di esperienza.
- **Personalità:** Strategico ma pratico, data-driven, creativo nei messaggi, sempre aggiornato sui trend.
- **Specializzazioni:** Esperto di *community building* e *personal branding* per C-level.
- **Processo:** Si definisce il processo di creazione e l'output.

Testando l'agente con una richiesta per un post sull'AI nel marketing per generare lead, l'agente pone domande preliminari (tipo di post, target, obiettivo) prima di fornire una proposta di titolo e la struttura principale del post.

Modifica e Perfezionamento

È possibile modificare l'agente per affinare i risultati. Per esempio:

- Ridurre il corpo del post a 2000 caratteri.
- Specificare di non volere hashtag nei post di LinkedIn.
- Abilitare l'**Interprete codice** per consentire all'agente di trasformare il contenuto in file come Word, Excel o PowerPoint.
- Aggiungere una regola chiave per lo sviluppo dei contenuti: **"fondamentale non usare strutture tipiche della AI nella generazione dell'output. Deve sembrare un contenuto scritto da un utente"**.

Dopo l'aggiornamento, l'agente genera contenuti che riflettono meglio queste istruzioni.

Esempio: Micro Copy (Agente Essenziale)

Non tutti gli agenti richiedono istruzioni complessissime. Si crea un agente focalizzato sull'essenzialità, chiamato **Micro copy**.

- **Istruzioni:** "Sei un super esperto di microcopie. Qualsiasi testo lungo... lo trasformi in una riga di testo essenziale e conciso che cattura l'attenzione".

Testando l'agente con un testo lungo, questo lo trasforma immediatamente in cinque varianti di microcopie concise.

Pubblicazione e Condivisione

Dopo aver creato e testato l'agente, si procede alla creazione definitiva. A questo punto, si può decidere chi può utilizzare l'agente:

1. Solo tu.
2. Utenti specifici nella tua organizzazione.
3. **Chiunque nella tua organizzazione.**

Questa funzionalità permette di condividere agenti specializzati, come il micro copy, con i colleghi.

5. Creare agenti esperti di dati

Per creare agenti super esperti di analisi dati si usa nuovamente il **metaprompting**, ma con un approccio mirato ai dati.

Processo:

1. Si inizia da una chat normale, attivando GPT-5 per una maggiore qualità di pensiero.
2. Si allega un file (ad esempio, un report di vendite e-commerce in formato XLS).
3. Si chiede all'IA di generare le istruzioni (il *system prompt*) per un agente di analisi dati che gestisca solo file del tipo allegato (report di vendite e-commerce).

L'IA crea un prompt che include elementi cruciali per l'analisi dei dati: schema di dati atteso, regole di pulizia e coerenza, metriche KPI da produrre, filtri per segmentazione, privacy ed *error handling*. Dopo aver perfezionato il prompt con la parte di *roll prompting*, si ottiene la configurazione finale.

Si crea l'agente, lo si chiama "XLS e-commerce", si incolla il system prompt e si abilita l'**interprete di codice**.

Test: Allegando il file degli ordini anonimizzati, l'agente analizza automaticamente il documento, fornendo una serie di risultati dettagliati: numero degli ordini, prezzi venduti, incassi totale, i 10 titoli per incassi, le collane più vendute, il mix per tipo prodotto, quote per metodo di pagamento e trend incasso.

Nel prompt si può specificare che i risultati desiderati siano in formato Excel, CSV, grafici o diagrammi.

6. Conclusioni

Siamo giunti alla fine del percorso sulla creazione di agenti con Copilot. La considerazione finale è che l'utente deve pensare a quali agenti gli servono nel proprio quotidiano e cosa può delegare.

Esempi di agenti delegabili: È possibile creare agenti per:

- La SEO (o solo per la Search Console o Google Analytics).
- Analizzare dati di vendite.
- Analizzare le fatture o i mastrini contabili.

Qualsiasi struttura dati può essere analizzata, creando agenti che producono in automatico un *output* specifico.

Nomi degli Agenti

Esistono diversi approcci per generare i nomi degli agenti:

1. **Per Funzione:** Come visto in questo percorso (es. SEO, Micro copy).
2. **Con Nomi Propri:** Assegnare nomi propri (es. Mario è l'esperto SEO, Giovanni è l'esperto di microcopy, Sara è l'esperta di analitica X).

L'uso di nomi propri può essere un approccio molto interessante, specialmente in contesti di riunione, dove si può chiedere attivamente il parere dell'agente nominato: "Aspetta, Mario cosa ne pensa? Sara cosa dice?". La scelta del naming (funzione o nome proprio) spetta all'utente.

La sfida finale è quella di aver implementato almeno due agenti personali entro una settimana.