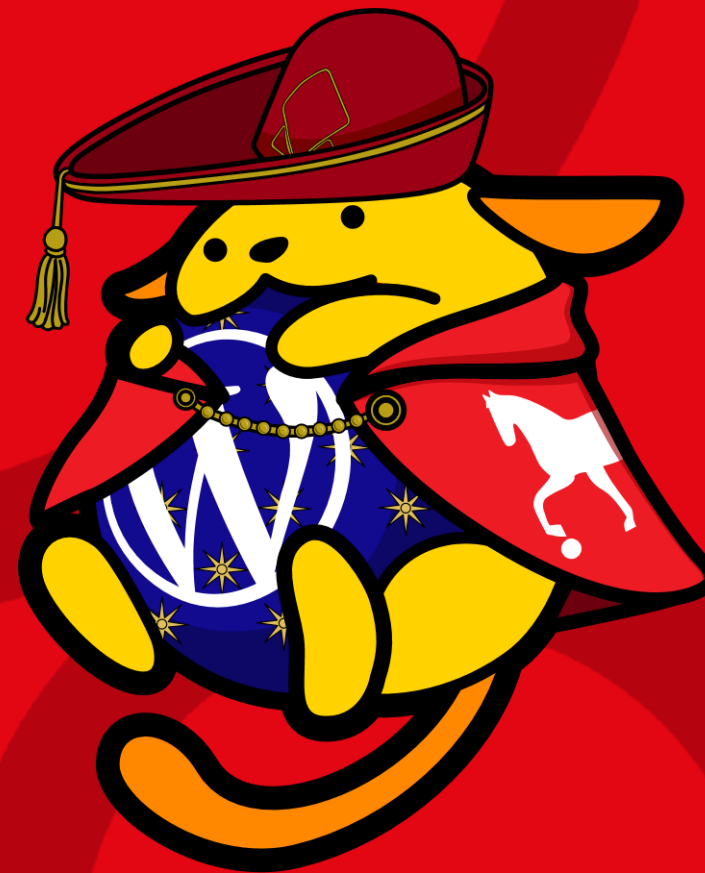


Padova

WordPress

Meetup



Padova
WordPress
Meetup

Sponsor:



NOVAMIRA

WORDPRESS 7.x · CINQUE MESI DOPO



I pericoli del nuovo Client AI di WordPress

*«Da grandi poteri derivano grandi responsabilità»
(ma non tutti sembrano rendersene conto...)»*

22 ottobre 2026 · WordPress Meetup Padova
Maurizio Pelizzone · Mavida S.n.c.



Padova
WordPress
Meetup

Sponsor:



NOVAMIRA



CHI SONO

Maurizio Pelizzone

Dev Ninja, Vibe Coder, Prompt Engineer, WordPress expert & Speaker

<https://www.linkedin.com/in/mauriziopelizzone/>
maurizio@mavida.com

- WordPress dal 2004, Mavida dal 2001
- Plugin su misura e integrazioni con CRM e gestionali
- WordPress Meetup Torino, dal 2015
- L'AI nel lavoro di ogni giorno, dal 2023

Oggi aiuto le aziende a far dialogare WordPress con il resto del mondo digitale: lavoro più fluido, intelligente e scalabile.



METTIAMOCI D'ACCORDO

Non è un talk contro l'AI



In Mavida la usiamo ogni giorno

- Generiamo codice, velocizziamo lo sviluppo, costruiamo automazioni.
- L'AI è una leva straordinaria... quando la usiamo per costruire meglio.
- Il problema non è l'AI: è infilarla ovunque, a prescindere dal contesto.

CAMBIAMO PROSPETTIVA

da «cosa possiamo costruire»

a

«cosa può andare storto»

(tanto a me non succede mai nulla...)



Cosa è successo da giugno

Cinque mesi dopo: poche novità nel core, molte nel plugin AI e una nuova superficie d'attacco, MCP.

1

7.0.x · luglio e agosto

Quattro release senza novità AI: correzioni e sicurezza, anche RCE. Aggiornare sempre.

2

7.1 «Mary Lou» · 19 agosto

Abilities con filtri e audit, connettori con application password. Tetto di spesa: ancora no.

3

Plugin AI 1.4 e MCP Adapter

Log, approvazioni e cifratura opt-in nel plugin. L'adapter MCP arriva su wordpress.org il 7/10.

4

7.2 · Beta 1 il 20 ottobre

Secrets API sì, ma chiavi ancora in chiaro; nel core embeddings e tre nuove abilities.



DA 7.0 A 7.1 • 19 AGOSTO 2026

Le fondamenta: WordPress 7.0 e 7.1

L'AI è nel core come infrastruttura, una base unica a cui i plugin si agganciano. La 7.1 l'ha rifinita.



AI Client

Interfaccia unica nel core: i plugin chiedono «genera questo testo», WordPress smista al modello configurato. In 7.1 solo ritocchi.



Connettori

Connettori per OpenAI, Anthropic e Google (servono i plugin provider). Dalla 7.1 anche username e application password.



Abilities API

Registro di «azioni» che l'AI può eseguire sul sito. La 7.1 aggiunge filtri sull'esecuzione e `wp_ability_invoked` per l'audit.



Ma erano queste le priorità?

Il client AI è bellissimo. Per chi ci lavora ogni giorno, però, le cose da sistemare erano altre.

Buchi ancora aperti a ottobre 2026

- Localizzazione multilingua nativa: nessun progresso da giugno, si va di plugin.
- SEO di base (meta, schema, sitemap): delegata a Yoast & co.
- Form contatti: ancora nessuno integrato.
- Modello dati da blog del 2003 che scala male.



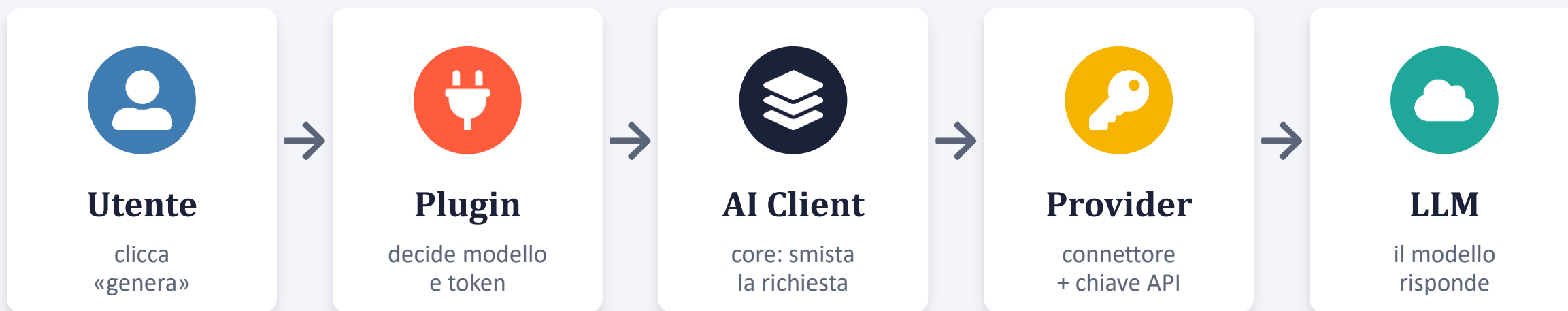
E intanto...

la real-time collaboration (la feature centrale della Fase 3, in sviluppo dal 2021) è stata **rimossa** dalla 7.0: non è arrivata nella 7.1 e non è prevista nemmeno per la 7.2.



IL FLUSSO DI UNA RICHIESTA

Come funziona, in pratica



Nota chiave: chi decide quale modello usare e quanti token spendere è **il plugin**, non tu.



Prima di tutto: serve un provider

«Nativo» non vuol dire «pronto all'uso»: senza provider il client AI non fa nulla. E per un utente base procurarsi una chiave è un ostacolo enorme.

1

Scegli un provider

OpenAI, Anthropic o Google tramite i plugin provider ufficiali (o un connettore di terze parti).

2

Crea un account

Sul sito del provider, con carta di credito e fatturazione attiva.

3

Genera una chiave API

Una stringa segreta che autorizza la spesa sul tuo account.

4

Incolla la chiave in WordPress

Nella schermata Connettori. E qui iniziano i problemi.



IL NODO ARCHITETTURALE

Chi decide cosa (e chi paga)

L'utente controlla...

- quali provider sono disponibili sul sito
- la chiave API inserita

Nessun tetto di spesa globale, nemmeno in 7.1.

Il plugin decide...

- quale modello usare (anche il più costoso)
- quanti token consumare per richiesta
- se mettere un limite... oppure no

Cinque mesi dopo, nessun freno nel core: restano il blocco di un singolo prompt e il limite di token per richiesta. Più plugin con la stessa chiave spendono dallo stesso conto.



RISCHIO N.1

Il plugin può bruciare i tuoi euro

...e te ne accorgi solo leggendo la fattura.



USD PER MILIONE DI TOKEN • OTTOBRE 2026

Quanto costano i modelli

Provider	Modello economico	input / output	Modello potente	input / output
Anthropic	Haiku 5.5	\$0,10 / \$0,50	Fable 5.1	\$10 / \$50
OpenAI	GPT-6 Luna	\$0,10 / \$0,50	GPT-6 Astra	\$10 / \$50
Google	Gemini 3.5 Flash-Lite	\$0,30 / \$2,50	Gemini 4 Argon	\$2 / \$10



Tra il modello più economico e il più potente ci sono fino a ~100x, sia sull'input sia sull'output. **Stesso lavoro, conto diverso: e a deciderlo non sei tu.**



Scenari (da “best effort” a “worst case”)

Stesso identico lavoro mensile (circa 20 milioni di token in input e 5 in output), due plugin che scelgono modelli diversi:

Plugin «accorto»

modello economico (Haiku 5.5)

~ \$4,50

al mese

Plugin «ingordo»

modello premium (Fable 5.1)

~ \$450

...la stessa attività, 100 volte più cara



Tra il modello più economico e il più potente c'è ora un fattore ~100x, sia sull'input sia sull'output.
Stesso lavoro, conto diverso: e a deciderlo non sei tu.



RISCHIO SICUREZZA

La tua chiave vale oro

L'allarme di Patchstack

«WordPress 7.0 + vulnerabilità dei plugin = token AI gratis. Ci sarà una corsa a rubare le chiavi API»

— Oliver Sild, fondatore di Patchstack (22 maggio 2026)

Una chiave rubata = soldi, non solo dati

- LLMjacking: stime di danno oltre \$100.000 al giorno (Sysdig)
- alimenta reti di bot per truffe e phishing
- già successo: AI Engine mostrava le chiavi agli Editor (CVE-2026-16954, agosto)
- te ne accorgi a fattura emessa



RISCHIO SICUREZZA

La chiave è nel database, in chiaro

Il dev note del core: le chiavi nel database «are not encrypted but are masked in the user interface». Se qualcuno esegue PHP sul tuo sito:

```
<?php
$key = get_option( 'connectors_ai_anthropic_api_key' );
// e la chiave è tua. Una riga.
```

Cosa si muove: la Secrets API (cifatura libsodium) è nella Beta 1 della 7.2, ma le chiavi dei Connettori non la usano ancora (verificato nel codice). Intanto: chiave in una costante o in una variabile d'ambiente, fuori dal database.

Il punto vero

Cifrata o no, nel DB o nel filesystem: se l'attaccante prende il controllo del sito, la chiave esce. Scenario peggiore: un plugin popolare compromesso la raccoglie da ogni sito.



LE CONTROMISURE

Come tenerlo sotto controllo



Una chiave solo per WordPress

Dedicata e revocabile, in una costante o variabile d'ambiente: meglio che nel database.



Imposta un limite di spesa

Sul provider: tetto mensile per progetto o workspace e alert di consumo.



Ruota la chiave

Con una cadenza fissa e subito dopo ogni sospetto o cambio di fornitore.



Verifica i plugin AI

Quale modello usano, se mettono limiti, se «telefonano a casa». Attiva il log delle richieste del plugin AI.



IN PRATICA • WP-CONFIG.PHP

La chiave fuori dal database

WordPress cerca la chiave in quest'ordine: variabile d'ambiente, costante, database. Il nome è l'ID del provider in maiuscolo più `_API_KEY`.

```
// wp-config.php, prima di «That's all, stop editing!»  
define( 'ANTHROPIC_API_KEY', 'sk-ant-api03-...' );  
define( 'OPENAI_API_KEY', 'sk-proj-...' );  
define( 'GOOGLE_API_KEY', 'AIza...' );  
  
// Meglio ancora, fuori dai file del sito (PHP-FPM, pool.d/www.conf):  
env[ANTHROPIC_API_KEY] = sk-ant-api03-...
```

Pulisci e ruota: toglì la chiave dalla schermata Connettori e generane una nuova: la vecchia è già nei backup.

Proteggi il file: permessi 400 o 440, wp-config.php mai in Git né in backup condivisi.

Controlla la fonte: la schermata Connettori mostra se la chiave arriva da ambiente, costante o database.



COSTANTE E SECRETS API

Cosa protegge e cosa no

Chiave nel database

- **Dump o backup del DB:** la chiave esce
- **SQL injection:** la chiave esce
- **Plugin compromesso:** `get_option()`, una riga

È il default dei Connettori.

Costante o ambiente

- **Dump o backup del DB:** non esce
- **Backup dei file:** esce, se è in `wp-config.php`
- **Plugin compromesso:** `constant()`, una riga

Si può fare oggi.

Secrets API (7.2)

- **Dump o backup del DB:** solo il cifrato
- **Backup completo:** si decifra, la chiave è nei file
- **Plugin compromesso:** `wp_get_secret()->reveal()`

I Connettori non la usano ancora.

In sintesi: costante e Secrets API proteggono i dati a riposo, non il sito in esecuzione. Contro un plugin malevolo servono plugin verificati e un limite di spesa.



PLUGIN · AI-PROVIDER-FOR-OPENROUTER

Un'alternativa: OpenRouter

Un solo gateway davanti a centinaia di modelli, con il controllo della spesa dalla tua parte (fee 5,5% sull'acquisto dei crediti).



Una chiave sola

Accesso a OpenAI, Anthropic, Google, Meta e tanti altri da un'unica API.



Credito prepagato

Paghi in anticipo: una chiave rubata o un plugin ingordo svuotano al massimo il credito che hai messo tu.



Limiti per chiave

Imposti un tetto di spesa sulla singola chiave: niente fattura a sorpresa.



Il prezzo non è più il motivo

Haiku 5.5 e GPT-6 Luna fanno 100 articoli a meno di 10 centesimi: qui si sceglie il controllo, non il risparmio.



RISCHIO N.2

Hai dato le chiavi di casa a un agente

...e un agente non chiede solo testi: esegue azioni sul tuo sito.



MCP • MODEL CONTEXT PROTOCOL

Che cos'è un MCP e come funziona

Una presa standard tra un'app AI e un servizio. Il client legge la lista dei tool esposti dal server, con nome, descrizione e parametri, e il modello sceglie quale chiamare.



In sintesi: MCP è fatto per i modelli, non per il codice. Quale tool chiamare, e quando, non lo decide un programma: lo decide il modello.



MCP • PRO E CONTRO

Cosa ci guadagni, cosa ci rimetti

I vantaggi...

- uno standard: lo stesso server va con Claude, ChatGPT, Cursor e VS Code
- l'agente scopre da solo cosa può fare
- superficie curata: poche abilities, non centinaia di endpoint
- il client chiede conferma prima di agire

Caso giusto: chiedere a Claude.ai di lavorare sul blog.

...e i costi

- gli schemi di tutti i tool occupano contesto a ogni turno
- ogni risultato passa dal modello: più token e più lentezza
- un livello in più: sessione, JSON-RPC, adapter
- a scegliere è il modello: prompt injection

Caso sbagliato: un plugin che usa MCP.

Un plugin non dovrebbe usare MCP: sa già cosa chiamare, quindi usa le REST API o l'AI Client del core. Esporre abilities con l'MCP Adapter, per lavorare con Claude, è un'altra storia.



REST, ABILITIES E MCP

Chi decide cosa chiamare?

REST API

- **Chi chiama:** il tuo codice
- **Cosa vede:** tutti gli endpoint, con i privilegi dell'utente
- **Token:** zero, chiama un programma

Esempi: plugin, n8n, script.

Abilities

- **Chi chiama:** codice o agente, via REST o MCP
- **Cosa vede:** solo le azioni che registri
- **Freno:** il permission_callback

Qui sta la sicurezza vera.

MCP

- **Chi chiama:** il modello, che sceglie il tool
- **Cosa vede:** le abilities pubbliche
- **Token:** schemi e risultati a ogni turno

Esempio: Claude sul blog.

Regola pratica: se sai già cosa chiamare usa le REST API; MCP serve quando a scegliere è un agente.



MCP ADAPTER • PLUGIN UFFICIALE

Come entra un agente in WordPress



Nota chiave: l'agente ha i permessi dell'utente con cui si collega. L'unico freno vero è il permission_callback di ogni ability.



MCP • I PUNTI DEBOLI

Cosa può andare storto

Il default è generoso...

- l'application password ha tutti i privilegi dell'utente e non scade
- il trasporto chiede solo di essere loggati

readonly e destructive? Solo suggerimenti.

...il resto lo decide il codice

- ogni plugin decide cosa esporre (WooCommerce: anche product-delete)
- il testo che l'agente legge può contenere istruzioni: prompt injection
- plugin MCP di terze parti: CVE 9,8, già sfruttata

Ufficiale ma sperimentale: l'adapter è alla 0.7.1 e due issue di sicurezza (#323, #297) sono ancora aperte al 22 ottobre.



MCP CON LA TESTA

Un'ability minima, fatta bene

Sola lettura, permesso reale, solo MCP. Estratto: servono anche label, description e categoria.

```
wp_register_ability( 'demo/count-drafts', array(  
    'execute_callback' => fn() => (int) wp_count_posts()->draft,  
    'permission_callback' => fn() => current_user_can( 'edit_posts' ),  
    'meta' => array(  
        'annotations' => array( 'readonly' => true ),  
        'mcp' => array( 'public' => true ) ),  
) ); // + label, description, category
```

Utente dedicato: ruolo minimo, mai un amministratore, una application password per agente.

Sola lettura su internet: le azioni distruttive restano in locale o dietro approvazione.

Audit e freni: wp_ability_invoked per tracciare, wp_pre_execute_ability per limitare.



La sfera di cristallo, cinque mesi dopo

«Graceful degradation» rovesciata: previsione in parte avverata

Chi sviluppa plugin AI si assume una responsabilità economica e molti aggirano il sistema integrato. AI Engine mostrava le chiavi agli Editor, e SiteGround offre già un provider proprio, senza chiave. Da verificare: quanti plugin ignorano il client del core.



La morale: pensateci dieci volte prima di affidare la vostra chiave di Anthropic o Gemini a un plugin scritto «dalla mamma di Goldrake».



LO SFONDO

Non è solo WordPress: «AI feature creep»

L'accumulo graduale di componenti AI che diluiscono il valore core di un prodotto.

● Postman

Da tool API leggero a piattaforma cloud con funzioni AI. Dal 1° marzo il piano Free è a un solo utente: molti migrano verso Bruno, locale e senza cloud.

● Notion

Il piano Business è a €19,50 a membro con Notion Agent incluso, e i Custom Agents consumano crediti a pagamento.

● Microsoft e Meta

A maggio, dopo il caso «Microslop»: «togliamo Copilot da dove non serve». A luglio Meta ritira una funzione AI di Instagram dopo le proteste.

La domanda da farsi prima di ogni integrazione AI:

questa feature aumenta il valore per l'utente, o lo seppellisce sotto un livello di complessità in più?



IN SINTESI

Il dito e la luna

Guardare il dito invece della luna

Non si vince con le feature di tendenza, si vince con le basi solide. L'AI nel core è marketing-ready, ma chi installa WordPress non ne aveva bisogno. Cinque mesi dopo, la 7.2 porta nel core embeddings e nuove abilities, ma ancora nessun freno alla spesa.



Ma WordPress non è morto

- Resta la risposta giusta per moltissimi contesti.
- Per certi progetti (vetrina, landing, blog statico) oggi ci sono alternative valide.
- «Tanto l'AI scrive il codice» non è una strategia: è creare scatole nere.



DA PORTARE A CASA

Usate l'AI per costruire meglio, non affidatele le chiavi a scatola chiusa.

- ✓ Chiave dedicata
- ✓ Limite di spesa
- ✓ Rotazione + audit dei plugin
- ✓ Agenti MCP: utente dedicato, minimi privilegi

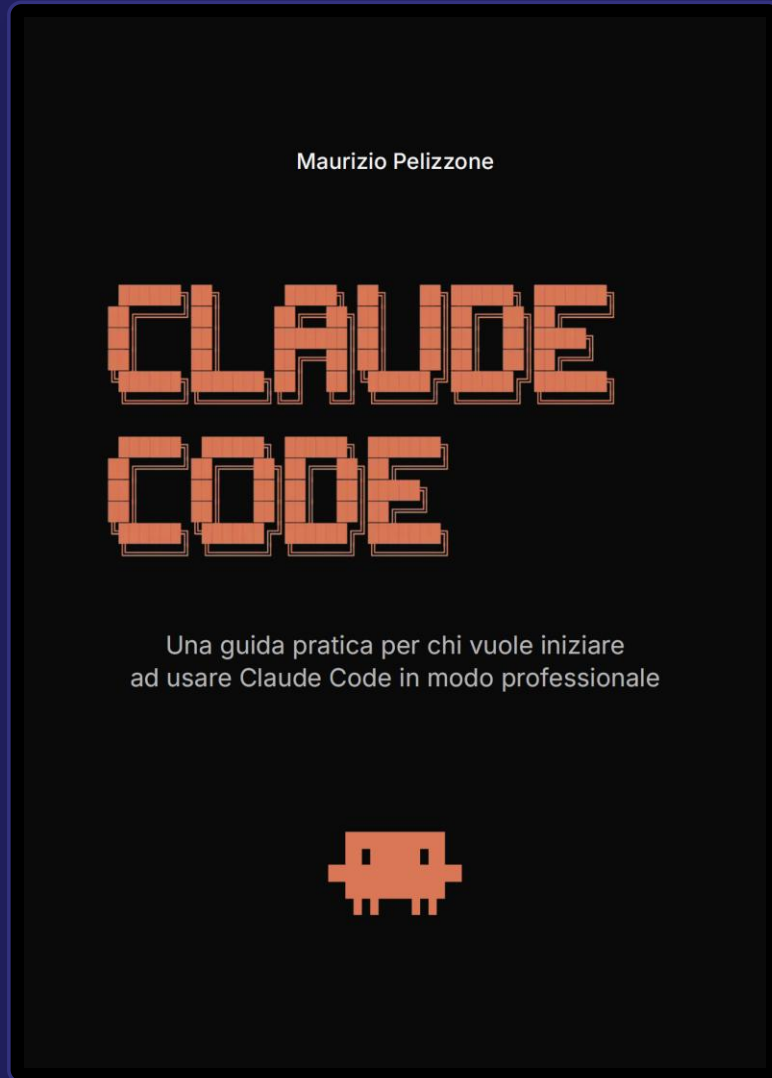


GUIDA GRATUITA · VERSIONE 6.1 · CC BY-SA 4.0

Claude Code: una guida pratica

Oltre 300 pagine, allineate a Claude Code v2.1.286 e riviste sulla documentazione ufficiale Anthropic. Novità della 6.1: modello e harness, confronto con Codex, OpenCode e Gemini CLI, sandbox, subagent annidati, Remote Control e sessioni cloud. Esempi su PHP, JavaScript e WordPress. Niente hype.

github.com/miziomon/claude-code-guide
maurizio.mavida.com/guida-claude-code
leanpub.com/claude-code-guide





- Wandy articoli
- Slide-orama caroselli
- Social Planner calendario
- WooSync negozio
- VoiceNote note vocali
- **Fleet siti dei clienti**

FLEET · DALL'ECOSISTEMA MAVIDA

I siti dei clienti in un cruscotto

Per agenzie e freelance che fanno manutenzione WordPress: stato di ogni sito, aggiornamenti in blocco, avvisi su vulnerabilità note e scadenze, report PDF con il tuo logo.

Il racconto completo è sul blog, e nella prossima slide c'è un regalo per chi è in sala.

Inquadra il QR e leggi l'articolo sul blog: come Fleet semplifica la manutenzione dei siti WordPress.

Fleet è una delle sei app Mavida · <https://fleet.mavida.com>



Fleet

Monitoraggio flotta WordPress

Crea il tuo account

Nome utente

Mario Rossi

Email

nome@esempio.com

Coupon

PADOVA2026

☐ Ho letto e accetto l'[informativa sulla privacy](#)

[Visualizza il testo completo dell'informativa](#)

Registrati

[Hai già un account? Accedi](#)

FLEET · UN REGALO PER IL MEETUP DI PADOVA

Provalo 30 giorni, non 7

COUPON **PADOVA2026**

- Prova gratuita di **30 giorni** invece di 7
- Prezzi di lancio **bloccati fino alla fine dell'anno**

Inquadra il QR: si apre la registrazione con il coupon già inserito. Nome, email, Registrati.

<https://fleet.mavida.com/?coupon=PADOVA2026>





Domande?

*Grazie per l'attenzione.
Parliamone.*

Grazie!



NOVAMIRA



LinkedIn



Meetup



Facebook



Padova
WordPress
Meetup

Sponsor:



NOVAMIRA