AutoProduct AI — Arquitectura, Contexto y Roadmap Técnico (v2)

Visión General

AutoProduct AI es un sistema profesional para administrar WooCommerce mediante lenguaje natural. El usuario conversa con su tienda como con un gerente humano.

Arquitectura Obligatoria

Core: infraestructura y configuración.
Brain: interpretación, decisión y generación de acciones.
Agent: ejecución determinista en WooCommerce.
Contexto/Memoria: persistente, server-side y fuente de verdad.

Contexto Lite vs Full

Lite: ultra chico, estable y único contexto enviado al modelo.
Full: solo para debug y auditoría humana, nunca enviado al modelo.

Estado Actual

Agent v7.6.x con Lite definitivo cerrado, limpio y consistente.
Separación completa Lite / Full implementada.

Implementación de Próximos Pasos (Plus)

Modo Consulta vs Modo Ejecución.
Verificación post-ejecución.
Seguridad, validación y confirmaciones obligatorias.
Optimización permanente del contexto.
Medición de resultados operativos.
Aprendizaje local por tienda.

Objetivo Final

Convertir AutoProduct AI en el primer plugin del mundo que permita administrar WooCommerce conversando como humano, con contexto real, memoria operativa y ejecución segura.

1. Errores esperables (no bugs)– El sistema puede pedir aclaraciones aunque el usuario crea haber sido claro.– El sistema puede responder con una pregunta en lugar de ejecutar una acción.– El sistema puede negarse a ejecutar una acción sin confirmación explícita.– El sistema no recuerda información fuera del alcance de la memoria operativa definida.– El sistema prioriza seguridad y consistencia por sobre "adivinar" la intención del usuario.

2. Límites actuales del sistema– No predice intenciones futuras del usuario.– No aprende globalmente de todas las tiendas.– No mantiene memoria infinita de conversaciones pasadas.– No ejecuta acciones implícitas sin confirmación explícita.– No reemplaza la validación humana en acciones críticas.

3. Flujo operativo del sistema (diagrama mental) Usuario → Normalización del lenguaje → Detección de modo (Consulta / Ejecución) → Brain → Contexto Lite → Propuesta → Confirmación → Agent → WooCommerce → Verificación post-ejecución → Memoria