

Roadmap Agent — AutoProduct AI

Objetivo: convertir el Agent en un ejecutor WooCommerce completo, determinista y auditable, capaz de soportar un gestor de tienda 100% por chat (Brain F7).

Principios del Agent

- 1 Determinista: no interpreta lenguaje natural.
- 2 Validaciones estrictas y whitelists por acción.
- 3 Idempotencia y NOOP cuando aplica.
- 4 Seguridad: permisos WordPress y protección REST.
- 5 Observabilidad y trazabilidad completa.

A0 — Fundaciones

- 1 ActionRegistry y catálogo oficial de acciones.
- 2 SchemaValidator por acción. FieldWhitelist
- 3 por entidad. ResultEnvelope estándar.
- 4 Endpoint /capabilities.
- 5

A1 — Productos CRUD (completo)

- 1 Crear producto simple (draft por defecto).
- 2 Actualizar producto (nombre, descripciones, status, precios, stock, SKU).
- 3 Duplicar producto.
- 4 Eliminar producto (trash / force).
- 5 Leer y buscar productos.

A2 — Taxonomías y Media

- 1 Asignar y remover categorías y tags.
- 2 Imagen destacada y galería.

A3 — Productos variables y variaciones

- 1 Crear producto variable.
- 2 Agregar, actualizar y eliminar variaciones.
- 3 Gestión de atributos.

A4 — Operaciones masivas (Bulk)

- 1 Bulk update con límites.
- 2 Bulk change status.
- 3 Bulk delete con confirmaciones.

A5 — Pedidos

- 1 Buscar y leer pedidos.
- 2 Actualizar estado.
- 3 Notas y reembolsos.

A6 — Cupones

- 1 Crear, actualizar y eliminar cupones.
- 2 Buscar y leer cupones.

A7 — Clientes

- 1 Buscar clientes.
- 2 Leer cliente.

A8 — Observabilidad y QA

- 1 Telemetry por acción.
- 2 QA y regression del Agent.
- 3 Matriz de errores estandarizada.

Extensiones Preventivas Agregadas • Dry-run / Preview Mode: Todas las acciones aceptan `dry_run=true` y devuelven `diff`, `warnings` e impacto sin ejecutar cambios. • Errores tipados y normalizados: Contrato estándar de errores con `error_code`, `severity` y `hint`. • Resolve References (lookup read-only): Acción dedicada para resolver productos, categorías o variaciones sin ejecutar. • Versionado explícito de acciones: Cada acción incluye `action_version` para compatibilidad y deprecación controlada.