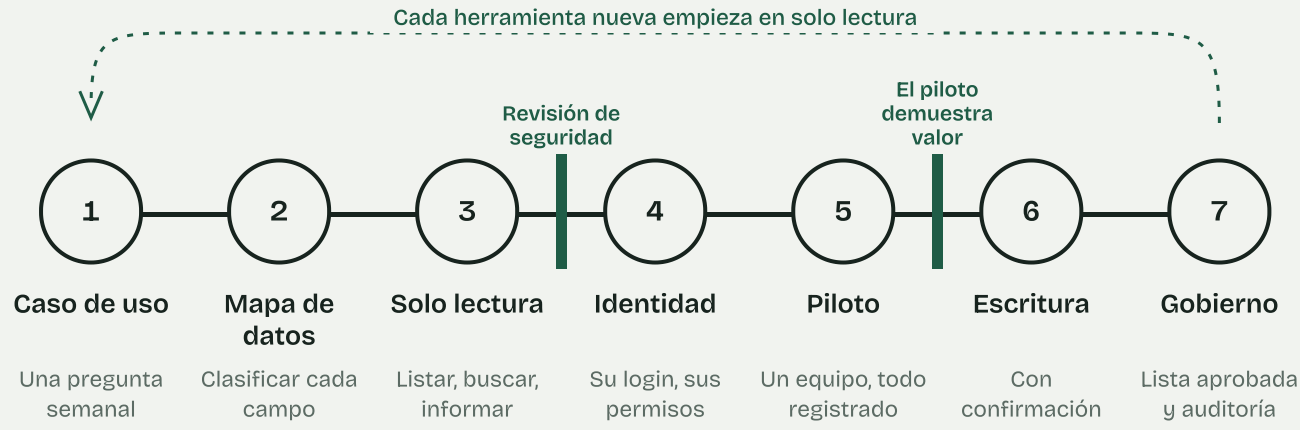


Dominik Heinrich, arquitecto de soluciones DevOps multicloud e IA

Conecta tu empresa a la IA con MCP

Cómo conecto herramientas y datos a Claude, ChatGPT y agentes de código con el Model Context Protocol, de forma segura. Siete pasos desde el primer servidor de solo lectura hasta el uso en toda la empresa.



Siete pasos, dos controles. La IA solo actúa con los permisos de la persona que la usa.

De dos plataformas en producción que he construido, anonimizado

100 % de la interfaz de la app también usable por agentes de IA vía MCP	**0** datos personales en la API de solo lectura y el servidor MCP de un cliente	**Semanal** planificación que un cliente automatiza con MCP	**2** plataformas en producción con su propio servidor MCP

Los siete pasos

De un servidor de solo lectura al uso en toda la empresa. Márcalos cuando estén en marcha.

01 Empieza por una pregunta que se repite cada semana

- [ ] Elige un caso de uso con un responsable claro: planificación semanal, un informe de ventas, clasificación de tickets, preguntas de costes.
- [ ] Apunta qué datos necesita la respuesta y quién puede verlos.
- [ ] Mide cuánto tarda hoy, para poder enseñar la diferencia después.

02 Conoce tus datos antes de abrirlos

- [ ] **Clasifica cada campo:** público, interno, personal, secreto.
- [ ] Los datos personales y secretos se quedan fuera de la primera versión. Los agregados suelen bastar.
- [ ] Datos que nunca pueden salir de tu red: sírvelos a un modelo local detrás del mismo servidor MCP.

03 Primero, solo lectura

- [ ] **El primer servidor solo lee:** listar, buscar, informar. Nada de crear, modificar ni borrar.
- [ ] Una herramienta, una tarea, con un nombre claro y una descripción que el modelo entienda.
- [ ] Respuestas pequeñas y estructuradas en vez de tablas enteras: más rápido, más barato y menos fugas.

04 Identidad y claves

- [ ] Cada persona se conecta con su propia identidad (OAuth u OIDC), así el agente actúa con sus permisos, nunca con más.
- [ ] Claves de API guardadas con hash, limitadas por herramienta, con caducidad y forma de revocarlas.
- [ ] Nunca un token de administrador compartido.

05 Piloto con un equipo

- [ ] De cinco a diez personas, dos semanas, un canal para comentarios.
- [ ] **Registra cada llamada:** quién, qué herramienta, qué parámetros, cuánto tardó y qué devolvió.
- [ ] Límites de uso y un tope de coste por persona desde el primer día.

06 Escritura con un paso de confirmación

- [ ] Escribir solo donde el piloto demostró valor, y cada acción la confirma la persona antes de ejecutarse.
- [ ] Las acciones destructivas (borrar, pagos, permisos) van al final, con confirmación explícita y los mismos permisos que en la interfaz.
- [ ] Cada escritura se puede deshacer o, como mínimo, queda registrada con el estado anterior y posterior.

07 Escala y gobierna

- [ ] Una lista aprobada de servidores MCP y clientes de IA para la empresa; todo lo demás, bloqueado por política.
- [ ] Las herramientas nuevas se revisan como código: pull request, revisión de seguridad y un responsable.
- [ ] Un informe mensual de uso, errores y horas ahorradas.

Cómo implantarlo según el tamaño de la empresa

Startup: un servidor para tu propio producto, para que clientes y equipo trabajen en él desde su asistente de IA.

Empresa mediana: un servidor por sistema principal (ERP, CRM, tickets) detrás del inicio de sesión único.

Gran empresa: un gateway central con lista de permitidos, registros de auditoría y clasificación de datos, más modelos locales para datos confidenciales.

Los errores que más veo

- Empezar con permisos de escritura porque la demo queda mejor.
- Una clave de administrador compartida, y en la auditoría no aparece nadie.
- Devolver tablas enteras de la base de datos y luego sorprenderse por el coste y las fugas.
- Conectar datos personales antes de consultar al delegado de protección de datos.
- Servidores MCP de la comunidad sin revisar en portátiles con datos de la empresa.

Cómo podemos trabajar juntos

La misma calidad para una startup de diez personas y para un grupo global. El formato se adapta a ti.

Startups

Responsable de DevOps e IA a tiempo parcial

Unos días al mes: arquitectura, pipeline de releases y funciones de IA, para que los fundadores se centren en los clientes. Del prototipo a producción sin reescribir.

Pymes

Un proyecto con un resultado claro

Un objetivo definido, como una factura cloud más baja, una migración o los primeros agentes de IA en producción, con alcance cerrado, avances semanales y una entrega que tu equipo pueda operar.

Grandes empresas

Un arquitecto dentro de tus equipos

Integrado con tus equipos de plataforma, seguridad y producto: decisiones de arquitectura, gobernanza de la IA y entornos regulados. Para alcances mayores traigo un equipo senior de confianza.

Cómo trabajo

Decisiones por escrito: registros de decisiones de arquitectura con sus pros y contras, para que tu equipo sepa el porqué, no solo el qué.

Operado, no solo entregado: SLOs, alertas sobre resultados de negocio y una rutina de incidencias.

El conocimiento se queda contigo: runbooks, documentación y talleres para tu equipo.

Seguro por defecto: OIDC e identidades gestionadas, mínimo privilegio, secretos en un almacén seguro y trazabilidad.

Medido: coste, tiempo de entrega, disponibilidad y horas ahorradas, con un informe semanal.

Un único interlocutor que habla con ingeniería y con dirección, en alemán, inglés y español.



¿Quieres que tus sistemas hablen con la IA de forma segura?

Reservar una llamada de 30 minutos

E-mail mail@dominikheinrich.ch
Web dominikheinrich.ch

Disponible en todo el mundo en remoto. Presencial bajo petición, según el país.