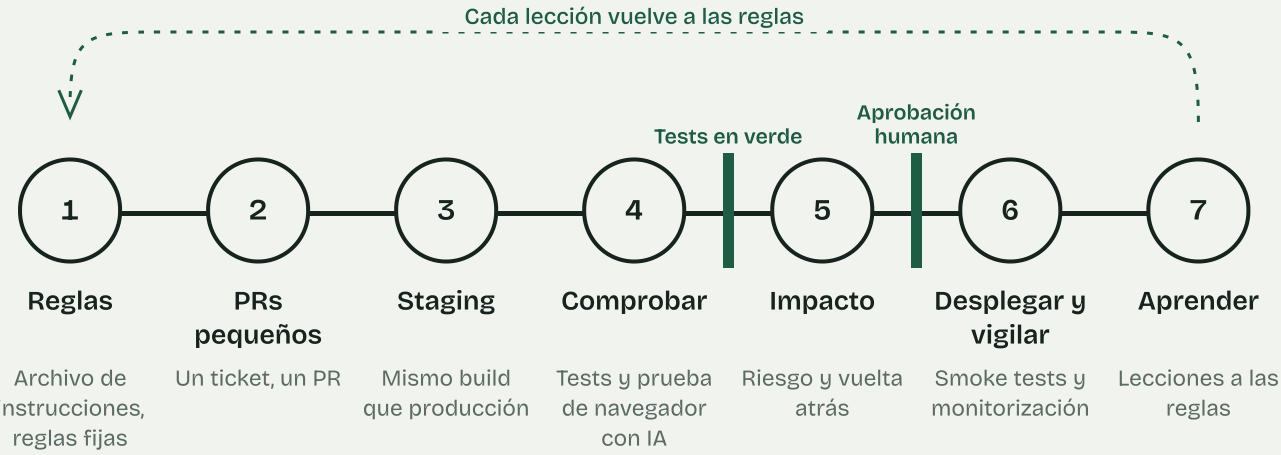


Dominik Heinrich, arquitecto de soluciones DevOps multicloud e IA

Desarrolla con agentes de IA, de forma segura

Un marco de adopción para un ciclo de desarrollo de software asistido por IA (AI-SDLC). Es el proceso detrás de más de 5.000 pull requests fusionados en dos plataformas en producción.



Siete etapas, dos puertas obligatorias. Los agentes escriben el código; las personas aprueban lo que llega a producción.

Un SaaS en producción construido con este proceso, anonimizado

3.025	1.048	160	3
pull requests fusionados en diez meses	archivos de tests automatizados	funciones serverless	apps: web, iOS y Android

Las siete etapas

Configúralas una vez por equipo y repositorio. Márcalas cuando estén en marcha.

01 Escribe primero las reglas

- [ ] Un archivo corto de instrucciones por repositorio: arquitectura, convenciones, qué puede hacer el agente y qué no.
- [ ] **Reglas fijas:** login, pagos, borrado de datos y secretos siempre requieren la aprobación de una persona.
- [ ] Los agentes nunca trabajan con datos de producción ni cuentas reales de clientes, solo con cuentas de prueba.

02 Cada cambio, pequeño y reversible

- [ ] Un ticket, un pull request. Ramas protegidas y trabajo solo con PRs, sin pushes directos.
- [ ] Migraciones de base de datos idempotentes y con dry-run contra la base de datos de destino antes del merge.

03 Siempre staging primero

- [ ] Cada cambio pasa por un entorno de staging antes de producción, con el mismo build y la misma configuración.
- [ ] Solo se despliegan las funciones o servicios que han cambiado, para que cada release sea pequeño.

04 Comprobar como un usuario

- [ ] Tests unitarios y end-to-end, más líneas base de typecheck y lint que solo pueden mejorar.
- [ ] Un test de navegador con IA en un Chrome real: el flujo descrito en lenguaje natural, con resultado, errores y propuesta de corrección.

05 Analizar el impacto antes de producción

- [ ] **Una tabla corta por release:** qué cambia, a quién afecta, el riesgo y cómo volver atrás.
- [ ] Una persona aprueba el merge a producción.

06 Desplegar y vigilar

- [ ] Smoke tests en las rutas vitales tras cada despliegue, y el despliegue se marca en rojo si una falla.
- [ ] Monitorización de resultados y una issue abierta automáticamente por fallo, que se cierra al recuperarse.

07 Cerrar el ciclo

- [ ] El agente redacta las respuestas a clientes y una persona las envía.
- [ ] Cada aprendizaje vuelve a los archivos de instrucciones, así el proceso se mejora solo.

Implantación según el tamaño de la empresa

Startup: reglas, staging y pruebas de navegador en una o dos semanas. La velocidad sale del ciclo, no de saltárselo.

Pyme: un equipo piloto durante cuatro a seis semanas, una revisión de seguridad y después el despliegue al resto de equipos.

Gran empresa: primero la gobernanza: una lista aprobada de modelos y proveedores, clasificación de datos, modelos locales para código sensible, trazabilidad y un equipo de plataforma que capacita a los demás.

Qué medir

Tiempo del ticket a producción, tasa de cambios fallidos, pull requests fusionados por semana y errores encontrados por los usuarios.

Los errores que más veo

- Agentes que hacen push directo a la rama principal o que tienen credenciales de producción.
- Pull requests de miles de líneas que nadie puede revisar de verdad.
- Saltarse staging porque los tests están en verde.
- Sin archivo de instrucciones: cada sesión empieza de cero y repite errores antiguos.
- Medir líneas de código en vez del tiempo de entrega y la tasa de fallos de los cambios.

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.



¿Lo quieres en tu equipo?

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.