Taller de Digitalización

PRACTICAL GUIDE

How to automate a process with AI

The three-phase method we use ourselves: document, run with supervision, and decide how to harden it.

PHASE 1
Document

PHASE 2
Run

PHASE 3
Harden

Pablo Leone · Taller de Digitalización
tallerdedigitalizacion.com · info@tallerdedigitalizacion.com

Before you start

Automating a process with AI does not start with the tool. It starts with knowing which process it is, who does it and what can go wrong. This guide sums up the method we follow ourselves and that any operating company can follow. It is no secret: the hard part is in the details of each case, and that is where experience shows.

PHASE 1

Document

Write the process down as it is done today and place it in one domain of your company.

PHASE 2

Run

Give that process and the tools to an AI. It works under supervision and learns from every run.

PHASE 3

Harden

With what you learned, decide how to make it safe, auditable and stable. It may end up as software.

Two rules for the whole journey

1. Human supervision. A person reviews what the AI does, especially at the start and at any step that cannot be undone.

2. One process at a time. Pick one that repeats, costs time and has clear data. Finish all three phases with it before moving on to the next.

Which process to start with

- It repeats often (daily or weekly).
- It takes time you can feel and causes mistakes through tiredness or copying data by hand.
- Its inputs and outputs are data or documents, not decisions that depend only on someone’s gut feeling.
- If it fails, the damage is small and can be corrected. Leave critical or irreversible work for later.

How do I know if this is for me?

If you have read this far, something here probably sounds familiar:

- Invoices and payments that someone types, checks or chases by hand.
- The same customer questions answered again and again.
- Data copied from one program to another.
- Reports put together by hand every week or every month.
- Orders or appointments handled across email, WhatsApp and a spreadsheet.
- Tasks that only one person knows how to do: if they are away, everything stops.

If any of these sounds familiar, then yes: this is for you. If none does, you probably do not need to automate anything right now, and that is good news.

What the questionnaire asks, and why

The questions are not random: each one matches something the method needs before moving to the next step.

Question	Why it matters
1 · Are your processes documented and formalised?	What is not written down cannot be automated, by a person or by an AI. **Phase 1.**
2 · Do you use any automation today (rules, scripts, integrations)?	AI makes automation easier; it does not replace it. If you have never automated anything, the first obstacle is not technical: it is understanding what automating means. **Phases 1 and 2.**
3 · What technical infrastructure do you have?	With only closed software and nobody technical, there are few places to connect an AI and nobody to supervise it. **Phases 2 and 3.**
4 · What happens if the person who does the process is away for a week?	If it all lives in one head, it has to come out of there first. **Phase 1.**
5 · Could you reconstruct who did what, and when?	It is the basis of traceability and of auditing whatever an AI does. **Phase 3.**

Your starting point

No documented processes: start with phase 1. It is the most worthwhile thing you can do, with or without AI.
Documented processes, but never automated anything: finish phase 1 and try phase 2 with one small, supervised process.
No technical infrastructure, or expecting the AI to do everything on its own: stay in phase 1 until you have something to connect the AI to and someone to supervise it. AI is not a magic wand: it works on what is already in order.

PHASE 1

Document the process

As it is done today, not as it should be done.

1 Describe the real process

Write down, step by step, what happens from the moment the work arrives until it is finished: who does it, when, with which programs, what goes in and what comes out, which decisions are made and what the usual exceptions are. If two people do it differently, note both.

2 Assign it to a domain

A domain is an area of the company with its own data, people and permissions. Every process belongs to one. Examples:

Invoicing and payments	**Administration**	**Employee management**	**Sales and customers**
Purchasing and suppliers	**Customer support**	**Operations**	**IT and systems**

Recommendation: keep automations inside their domain

This is a good practice, not a rule. An automation that only touches invoicing needs invoicing permissions only; if it goes wrong, the error stays contained and is easier to audit. When a process needs data from another domain, it is better for another automation or a person to hand it over than for it to go looking by itself.

3 Store it in a document an AI can read

The document is the asset of this phase. It should be plain text (for example Markdown), versioned, and in a folder an AI can be connected to. A Word file lost in someone's inbox will not do. Suggested structure:

Name and domain · **Goal** · **Who does it today** · **When it starts** · **Tools and access** · **Numbered steps** · **Exceptions and what to do** · **What must NEVER be done** · **How you know it went well**

Result of the phase: one document per process, assigned to a domain, that another person (or an AI) could follow without asking you anything.

PHASE 2

Run it with AI, under supervision

The AI does the work; you check it does it well.

1 Give the AI the process and what it needs to run it

The phase 1 document is its script. It also needs access to what a person would use: **APIs**, **MCP servers** (standard connectors that let an AI use your programs), **files and documentation** and, if there is no other way, the **browser**. The more structured the access, the more reliable the result.

2 Set it up as an AI project, not a loose conversation

A recommended set-up brings together, in one project:

- **Instructions** for the project: role, rules and limits.
- **Scheduled tasks** so it runs without you asking every time.
- **Browser access** only if needed.
- **A context folder** with the documented processes.
- **MCP connectors and APIs** to the programs of the domain.
- **Human approval points** before anything irreversible.

3 Ask the AI to document itself while it works

Add a **self-learning** section to its instructions: after every run it must note what it did, which path was fastest and most reliable, what failed, which exceptions it met and how long it took. Those notes are the recipe from which, later on, the process is automated in a stable way.

When to move to phase 3?

A reasonable reference: **after about three complete, reviewed runs**. With fewer you have anecdotes; with three you can usually see what repeats, what changes and where the risks are. It is a starting rule, not a law: if the process is very variable, you will need more runs.

Result of the phase: a process that works under supervision, a recipe written by the run itself and a list of the problems found.

PHASE 3

Decide how to harden it

With what you learned, make the process safe, auditable and stable.

Check whether the process, as it works now, has any of these problems. If it has none and the volume is low, it can stay as it is in phase 2.

Criterion	The question you must be able to answer
Security	Can the AI, through a mistake or a malicious instruction, do something irreversible (delete, pay, send)?
Auditability	Do we know whether a step was done by a person or by the AI, and with which permissions?
Observability	Can we see, at any moment, which step is running?
Traceability	Is it recorded what was done, when and with which data (when it matters)?
Access control	Who can start the process? Could someone unauthorised do it?
Resistance to attacks	Does it withstand instructions hidden in an email, a PDF or a web page the AI reads (prompt injection)?
Repeatability	Does it give the same result for the same case, or does it vary without explanation?

If any of them fails, these are the usual measures, from lighter to heavier:

When…	Do this
You want to repeat it in an orderly way	Turn it into a **skill** (or several) and orchestrate them with scheduled tasks.
There is an old system with no API (old website, old CRM)	Extract the information and build an **intermediate database**. The AI works on it, not on the screen.
A step is sensitive	Write a **deterministic script** that performs it: the AI calls it, but cannot step outside what the script allows. It is a guardrail.
You must operate on a platform	Give it **only the permissions it needs**, so any possible mistake is small and reversible.
There is external risk	Limit who can start it, treat everything it reads as data (not as instructions) and log the access.

The usual destination: an unattended process

If the process is routine, always the same and can be left unattended —you only need to see the result—, the most solid option is usually to take it out of conversational AI and turn it into **a software project**:

- AI is used to **write the code** of the process, now that it is documented and tested in phase 2.
- It runs **in the cloud, unattended**, without depending on one particular computer.
- If it still needs AI in some step, it calls it **through an API**, not through a chat application.
- It stays **auditable, observable and traceable**: nobody watching does not mean you cannot know what happened.

This only pays off when conditions allow it. A process that changes often or needs human judgement is better left in phase 2.

Summary

Phase	What you do	What you get
1 · Document	You describe the real process and assign it to a domain.	A document an AI can read.
2 · Run	The AI runs it with tools, supervised, and documents itself.	A recipe and a list of problems, after about three runs.
3 · Harden	You apply skills, scripts and minimum permissions; if it fits, you turn it into software.	A safe, traceable, stable process.

HOW WE CAN HELP

This is the method. If you would rather not walk it alone, we walk it with you.

We help you document the process, set up the AI run and decide how to harden it, or we implement it for you. The first call is free and lasts 30 minutes: you tell us which process you want to automate and we tell you where we would start.

Book the call: tallerdedigitalizacion.com/ai-process-automation/
Write to us: info@tallerdedigitalizacion.com