GUIA PRÁTICO

Mapeando IA generativa na operação

Quatro passos para descobrir onde a IA já entrou na sua empresa, classificar o risco de cada uso e governar sem travar a adoção.

SÉRIE	EDIÇÃO	PÁGINAS	PÚBLICO
Guias de execução	Junho 2026	6	CISOs, DPOs, TI e líderes de área

SUMÁRIO EXECUTIVO

A IA generativa já está na sua operação. A única dúvida é se ela entrou pela porta da frente, com inventário e controle, ou pela conta pessoal de um funcionário.

Bloquear não funcionou. Empresas que proibiram assistentes de IA descobriram o uso migrando para o celular pessoal, fora de qualquer visibilidade, levando junto dados de clientes, código-fonte e minutas contratuais. Ignorar também não funciona: cada uso não mapeado é tratamento de dados sem base legal documentada, propriedade intelectual saindo do perímetro e decisão automatizada sem revisão humana. O caminho que funciona é o do meio: mapear, classificar, controlar por nível de risco e governar continuamente. Este guia entrega os quatro passos com ferramentas de aplicação imediata: as quatro superfícies de inventário, a matriz de classificação, a escada de controles e o plano de 30 dias.

4 superfícies
de uso de IA precisam entrar no inventário: assistentes, copilots, APIs e agentes
método de inventário · §1

9 células
na matriz que cruza sensibilidade do dado com autonomia do uso e define o controle exigido
classificação de risco · §2

30 dias
é o prazo realista para sair do zero e chegar a inventário, política e bloqueios essenciais
plano de arranque · §4

1 Passo 1 · Inventarie as quatro superfícies

O erro clássico do inventário é procurar só "ferramentas de IA" compradas pela TI. A maior parte do uso real não passou por compra nenhuma. O mapeamento precisa cobrir quatro superfícies distintas, porque cada uma tem um método de descoberta diferente.

Figura 1 · As quatro superfícies. Cada quadrante exige um método de descoberta próprio; nenhum método cobre os quatro.

SUPERFÍCIE	COMO DESCOBRIR	O QUE REGISTRAR
Assistentes públicos	Logs de proxy/DNS e firewall (domínios de IA), pesquisa anônima com as equipes, análise de extensões de navegador.	Quem usa, para quê, com que tipo de dado, em conta pessoal ou corporativa.
Copilots embarcados	Inventário de SaaS contratado: revisar quais fornecedores ativaram recursos de IA por padrão nos últimos 18 meses.	Recurso ativado, dados acessados, opção de opt-out, cláusula de uso de dados para treinamento.
APIs e integrações	Varredura de código e pipelines: chaves de API de provedores de IA, SDKs, chamadas em automações (n8n, RPA, scripts).	Sistema chamador, modelo usado, dados enviados, logs mantidos, dono técnico.
Agentes e automações	Revisão de fluxos com permissões de escrita: o que executa ações em sistemas sem aprovação humana a cada passo.	Escopo de permissões, gatilhos, ações possíveis, mecanismo de interrupção, trilha de auditoria.

ARMADILHA COMUM

Sobre a pesquisa com equipes: ela só funciona com anistia explícita. Comunique antes que o objetivo é mapear, não punir. Inventário construído sob medo retrata o uso declarado, não o uso real, e governa um cenário que não existe.

2 Passo 2 · Classifique cada uso na matriz

Com o inventário em mãos, cada caso de uso recebe uma posição na matriz que cruza duas perguntas: que dado o uso processa e quanta autonomia ele tem. A posição na matriz define o tratamento, e isso evita as duas distorções comuns: burocratizar um resumo de texto público com o mesmo rigor de um chatbot de clientes, ou liberar um

agente autônomo com a mesma leveza de um corretor gramatical.

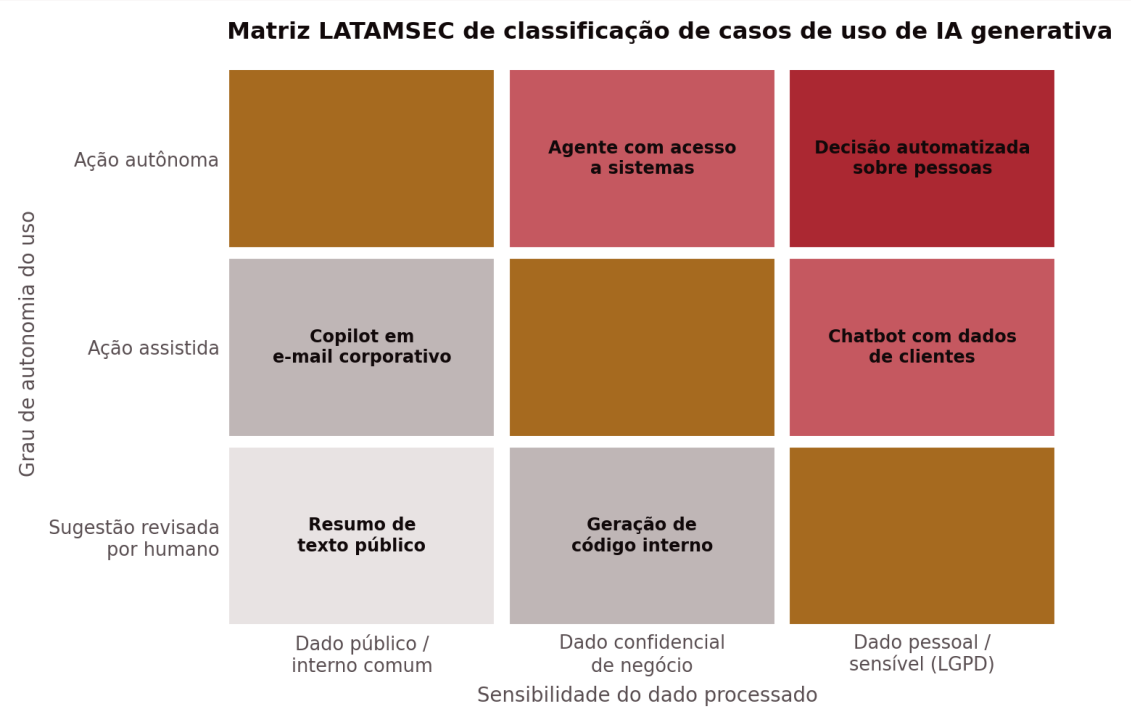

Figura 2 · Matriz de classificação. Casos no canto superior direito exigem avaliação formal de impacto (a LGPD chama de RIPD quando há dado pessoal) antes de entrar em produção.

Uma regra de decisão simples para a zona vermelha: uso que combina dado pessoal ou sensível com ação autônoma não entra em produção sem três coisas por escrito: avaliação de impacto, mecanismo de revisão humana para casos limítrofes e plano de reversão. Se uma das três não existe, o caso de uso espera. Essa regra cabe em um parágrafo de política e elimina 80% das discussões caso a caso.

3 Passo 3 · Aplique a escada de controles

Controles de IA não nascem todos no mesmo dia. A sequência importa: política e inventário primeiro, porque são baratos e destravam o resto; prevenção técnica de vazamento em seguida; trilha de auditoria e gestão de fornecedores na maturidade plena. A escada abaixo organiza a implantação em três níveis com prazos realistas.

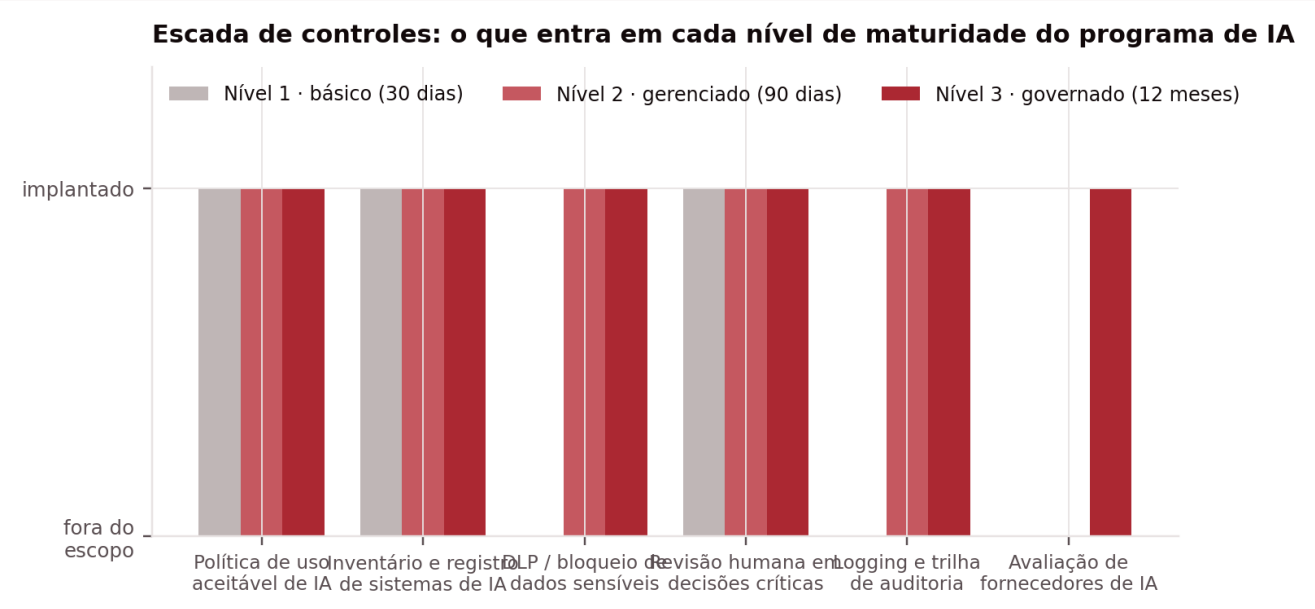

Figura 3 · Escada de implantação. O nível 1 é alcançável em 30 dias por qualquer empresa; o nível 3 alinha o programa a referências como ISO/IEC 42001 e NIST AI RMF.

CONTROLE	O QUE SIGNIFICA NA PRÁTICA
Política de uso aceitável	Uma página, linguagem direta: o que pode, o que não pode, o que exige aprovação. Proibições absolutas só para o que for de fato inegociável (ex.: dado de cliente em conta pessoal).
Registro de sistemas de IA	Tabela viva com dono, finalidade, dados, classificação na matriz e data de revisão. É o equivalente, para IA, do registro de operações de tratamento da LGPD.
DLP e bloqueio seletivo	Prevenção de envio de padrões sensíveis (CPF, cartão, segredos de código) para domínios de IA, mantendo o uso de baixo risco liberado. Bloqueio cirúrgico, não muro.
Revisão humana obrigatória	Para decisões sobre pessoas (crédito, contratação, atendimento crítico): humano aprova, IA sugere. Documentar quem revisou é tão importante quanto revisar.
Logging e auditoria	Prompts e respostas de sistemas críticos retidos por prazo definido. Sem trilha, não há como investigar incidente nem demonstrar conformidade.
Avaliação de fornecedores	Perguntas específicas de IA no questionário de terceiros: uso de dados para treinamento, residência de dados, subcontratação de modelos, certificações.

4 Passo 4 · O plano dos primeiros 30 dias

SEMANA	ENTREGAS
Semana 1	Comunicado de anistia e propósito. Levantamento de logs de rede e inventário de SaaS. Designação do dono do programa (segurança e privacidade juntos).
Semana 2	Pesquisa com as equipes. Varredura de chaves de API e automações. Primeira versão do registro de sistemas de IA com os 10 usos mais relevantes.
Semana 3	Classificação dos usos na matriz. Decisão sobre os casos da zona vermelha: adequar, suspender ou aceitar formalmente o risco. Rascunho da política de uma página.
Semana 4	Publicação da política com sessão de perguntas abertas. Ativação dos bloqueios DLP essenciais. Relatório executivo: o que existe, o que foi tratado, o que vem no trimestre.

POR QUE FUNCIONA

O entregável da semana 4 importa mais do que parece: é a primeira vez que a diretoria verá o uso real de IA da empresa em uma página. Esse relatório costuma destravar orçamento para os níveis 2 e 3 com mais eficácia do que qualquer apresentação sobre riscos teóricos.

5 Modelo de registro de sistemas de IA

O registro abaixo é o artefato central da governança contínua. Uma linha por caso de uso, revisão trimestral, e a regra de que nada novo entra em produção sem linha correspondente.

CAMPO	EXEMPLO PREENCHIDO
Caso de uso	Assistente de rascunho de propostas comerciais
Superfície	Copilot embarcado (CRM corporativo)

CAMPO	EXEMPLO PREENCHIDO
Dono de negócio / dono técnico	Diretora comercial / Coordenador de plataformas
Dados processados	Dados cadastrais de clientes PJ, histórico de negociação
Célula na matriz	Dado confidencial × ação assistida → risco médio
Controles aplicados	Opt-out de treinamento ativado; DLP; cláusula contratual de confidencialidade
Base legal (se dado pessoal)	Legítimo interesse, com teste documentado
Próxima revisão	Setembro 2026

Na LATAMSEC Governance Cloud, esse registro deixa de ser planilha: cada sistema de IA vira um ativo com controles mapeados, evidências anexadas e validade monitorada, entrando no mesmo score de maturidade e nos mesmos relatórios executivos que o restante do programa de segurança. IA generativa passa a ser mais um domínio governado da arquitetura, não uma exceção administrada no improviso.