GUIA EXECUTIVO

# 12 riscos que sua empresa corre ao usar IA sem política interna

Governança de IA • Reputação Digital • Compliance Regulatório

**Maschietto Advisory**

Eduardo Maschietto — AI Governance & Digital Risk

2026 | maschiettoadvisory.com

CONTEXTO

# Por que este guia existe

Sua empresa já está usando inteligência artificial. Mesmo que não exista nenhuma política formal, nenhum projeto aprovado e nenhum sistema contratado. Seus funcionários estão usando ferramentas de IA publicamente disponíveis para redigir e-mails, resumir documentos, responder clientes, analisar planilhas e automatizar decisões. Isso acontece agora, todos os dias, sem controle e sem rastro.

O problema não é a tecnologia. O problema é a ausência de governança. Sem política interna, sem treinamento e sem mapeamento de riscos, cada uso de IA representa um vetor potencial de exposição jurídica, reputacional ou regulatória. A LGPD, o GDPR, a NIS2 e o AI Act europeu já preveem obrigações específicas que as empresas precisam cumprir, independentemente de terem ou não adotado IA formalmente.

Este guia apresenta os doze riscos mais comuns que empresas de pequeno e médio porte enfrentam ao usar IA sem estrutura de governança. Cada risco é descrito de forma direta, com o sinal de alerta que indica sua presença e o enquadramento regulatório aplicável. O objetivo não é gerar medo, mas oferecer clareza suficiente para que uma decisão de diagnóstico possa ser tomada antes que um incidente aconteça.

> ***A maioria dos incidentes com IA não começa por um ataque externo.*** *Começa por um funcionário bem-intencionado que colou o documento errado no lugar errado.*

CONTEÚDO DESTE GUIA

## 01 Funcionários inserindo dados sensíveis em IA pública

**Enquadramento:** LGPD art. 46, GDPR art. 32, NIS2 Seção 21

Dados contratuais, fiscais, de clientes e estratégicos são colados diariamente em ferramentas como ChatGPT, Gemini e Copilot. Essas plataformas processam e retêm o conteúdo em servidores externos. Não há controle sobre o que sai da empresa.

> **Sinal de alerta:** Nenhum registro de quais dados foram enviados para fora.

## 02 IA gerando comunicações sem revisão humana

**Enquadramento:** Responsabilidade civil contratual, risco reputacional

E-mails, propostas e contratos gerados por IA e enviados sem revisão crítica. O modelo pode inventar cláusulas, distorcer fatos ou adotar tom incompatível com a posição da empresa. A responsabilidade legal é inteiramente do emissor humano.

> **Sinal de alerta:** Respostas automáticas a clientes sem aprovação.

## 03 Atendimento automatizado criando responsabilidade

**Enquadramento:** CDC, PROCON, reclamações regulatórias setoriais

Chatbots e agentes de IA que tomam compromissos, fornecem informações técnicas ou orientam clientes sem supervisão geram obrigações juridicamente vinculantes. Um erro de IA pode equivaler a uma promessa da empresa.

> **Sinal de alerta:** Bot confirma prazo, desconto ou condição não autorizada.

## 04 Vazamento de prompts e documentos internos

**Enquadramento:** Segredo industrial, PI, cláusulas de confidencialidade

Prompts elaborados internamente, documentos estratégicos e manuais operacionais enviados para IA pública podem ser incorporados a modelos futuros ou acessados por terceiros em cenários de falha de segurança.

> **Sinal de alerta:** Propriedade intelectual enviada para APIs sem contrato NDA.

---

## 05 Decisões automatizadas sem critério documentado

**Enquadramento:** LGPD art. 20, AI Act art. 14, risco de autuação

Quando IA apoia decisões de crédito, contratação, precificação ou retenção sem trilha auditável, a empresa não consegue justificar a decisão perante reguladores ou clientes. Ausência de explicabilidade é infração direta à LGPD.

> **Sinal de alerta:** Decisão que afeta titular sem revisão humana registrada.

---

## 06 Uso de dados pessoais sem base legal adequada

**Enquadramento:** LGPD art. 7, GDPR art. 6, ANPD, multa de até 2% da receita

Alimentar sistemas de IA com listas de clientes, histórico de atendimento ou dados biométricos sem base legal explícita é violação direta da LGPD e do GDPR. A base 'interesse legítimo' não cobre usos de treinamento de modelos.

> **Sinal de alerta:** Dataset de clientes usado para fine-tuning sem consentimento.

---

## 07 Ausência de política interna de uso de IA

**Enquadramento:** Agravante regulatório, responsabilidade objetiva ampliada

Sem política formal, a empresa não tem como provar que adotou medidas razoáveis. Em caso de incidente, autuação ou ação judicial, a ausência de política agrava a responsabilidade e elimina qualquer defesa baseada em boa-fé.

> **Sinal de alerta:** Uso irrestrito de IA sem norma, treinamento ou registro.

---

## 08 Falta de treinamento da equipe

**Enquadramento:** Responsabilidade patronal, violação de dever de diligência

Funcionários sem formação específica não reconhecem o que pode ou não ser compartilhado com ferramentas de IA. A ingenuidade técnica não é excludente de responsabilidade. O dano causado por um colaborador recai sobre a empresa.

> **Sinal de alerta:** Nenhum treinamento documentado sobre uso seguro de IA.

---

## 09 Risco reputacional por resposta artificial mal calibrada

**Enquadramento:** Crise de mídia, cancel, perda de contratos e parcerias

Uma IA que responde de forma agressiva, discriminatória ou politicamente inadequada em nome da empresa pode causar crise de imagem em minutos. O dano reputacional excede em muito qualquer eventual ganho de produtividade.

> **Sinal de alerta:** Respostas públicas geradas por IA sem revisão editorial.

---

## 10 Confusão entre produtividade e exposição

**Enquadramento:** Risco sistêmico não mapeado, decisões sem lastro

A narrativa de eficiência oculta os riscos reais. Cada ganho de velocidade via IA pode corresponder a um novo vetor de exposição jurídica, reputacional ou regulatória. A relação custo-benefício precisa ser avaliada formalmente.

> **Sinal de alerta:** IA adotada sem análise de risco documentada.

---

## 11 Uso de IA por terceiros e fornecedores

**Enquadramento:** LGPD art. 39, NIS2 art. 21, GDPR art. 28

Fornecedores, prestadores e parceiros que utilizam IA no processamento de dados da empresa geram responsabilidade solidária. A cadeia de fornecimento digital precisa ser contratualmente regulada e auditada.

> **Sinal de alerta:** Contratos com fornecedores sem cláusula de uso de IA.

---

## 12 Ausência de plano de resposta a incidentes

**Enquadramento:** LGPD art. 48, GDPR art. 33, NIS2 art. 23

Quando um incidente envolvendo IA ocorre, a empresa tem janelas estreitas para notificar reguladores e titulares. Sem plano documentado, o tempo de resposta aumenta, o dano se amplifica e as sanções se tornam inevitáveis.

> **Sinal de alerta:** Nenhum playbook de incidente que inclua vetores de IA.

---

DIAGNÓSTICO DE EXPOSIÇÃO AO USO DE IA

# Maschietto Advisory

A maioria das empresas não sabe exatamente como a IA está sendo usada internamente. Funcionários adotam ferramentas por conta própria, sem política, sem registro e sem controle de riscos. O resultado é uma exposição crescente que permanece invisível até que um incidente aconteça.

O diagnóstico da Maschietto Advisory mapeia em até 72 horas:

- Quais ferramentas de IA estão em uso na empresa, declaradas ou não
- Que tipo de dados estão sendo compartilhados com plataformas externas
- Quais obrigações regulatórias se aplicam ao perfil da empresa
- Quais os vetores de maior risco jurídico, reputacional e operacional
- O que precisa ser feito para mitigar os riscos prioritários

**Maschietto Advisory realiza diagnóstico de exposição ao uso de IA, reputação e governança interna.**

Solicite uma conversa inicial: **maschiettoadvisory.com**

| AI Exposure Audit | Política Interna de IA | Treinamento de Equipes | Compliance LGPD / GDPR |
|---|---|---|---|
| Mapeamento de uso e risco de IA | Norma aplicável e exigível | Uso seguro e responsável de IA | Adequação regulatória documentada |