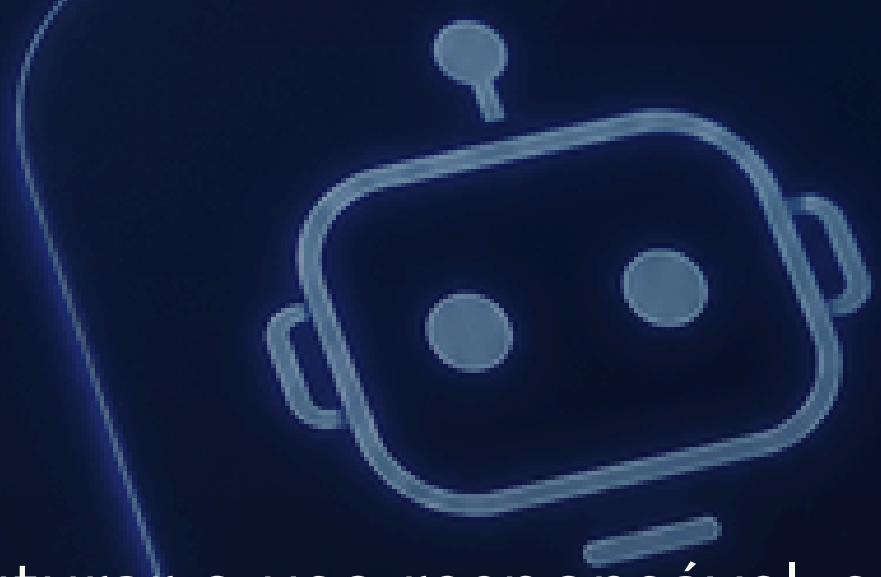
Assis e Mendes
DIREITO DIGITAL, TECNOLOGIA E EMPRESARIAL

GUIA PRÁTICO

# Governança de Inteligência Artificial



Como estruturar o uso responsável, seguro e estratégico da IA nas organizações

@assisemendes.adv

# Índice

# Apresentação

Este material foi elaborado para apoiar empresas que desejam iniciar ou amadurecer a governança de inteligência artificial. Ele reúne conceitos essenciais, riscos que merecem atenção e um roteiro de implantação que pode ser adaptado ao porte, à atividade e à maturidade de cada organização.

***Objetivo***

Permitir que a empresa aproveite os benefícios da IA sem perder o controle sobre dados, informações estratégicas, decisões, contratos e responsabilidades.

Este material foi desenvolvido pelo Assis e Mendes Advogados, escritório especializado em Direito Digital, Proteção de Dados (LGPD), Direito Empresarial, Governança e Compliance. Atuamos ao lado de empresas de tecnologia e organizações que utilizam soluções digitais e inteligência artificial, oferecendo orientação jurídica para estruturar operações, estabelecer responsabilidades e apoiar a adoção segura e estratégica de novas tecnologias.

Acreditamos que a governança jurídica deve acompanhar a inovação desde o início, contribuindo para que a inteligência artificial seja incorporada às operações com clareza, previsibilidade e segurança jurídica. É essa visão que orienta nosso trabalho e que buscamos compartilhar nas próximas páginas.

# 1. Introdução

***Por que a governança de IA se tornou necessária?***

A inteligência artificial deixou de ser um tema restrito à tecnologia. Ela já é utilizada para criar conteúdos, revisar documentos, desenvolver códigos, analisar dados, apoiar decisões, atender clientes e automatizar processos. Em muitos casos, esse uso começa antes de a organização definir critérios sobre ferramentas permitidas, dados que podem ser inseridos, revisão humana e responsabilidade pelos resultados.

A adoção pode ocorrer por meio de uma ferramenta contratada, de uma nova funcionalidade incorporada a um sistema já utilizado, de uma extensão instalada pelo colaborador ou de uma solução pública acessada diretamente por uma área de negócio. Por isso, uma empresa pode utilizar IA mesmo quando acredita que ainda não iniciou um projeto formal sobre o tema.

# 2. Conceitos essenciais

## 2.1 Governança de IA

Governança de IA é o conjunto de princípios, responsabilidades, processos e controles utilizados para orientar o desenvolvimento, a contratação e o uso de sistemas de inteligência artificial. Seu objetivo é garantir que a tecnologia seja utilizada de forma alinhada à estratégia da organização, proporcional aos riscos e compatível com obrigações jurídicas, contratuais, éticas e de segurança.

Na prática, governar IA significa saber quais ferramentas existem, quem pode utilizá-las, quais usos são aceitáveis, como os riscos são avaliados, quando a revisão humana é necessária, quem aprova novas soluções e como os problemas devem ser comunicados e tratados.

# 2. Conceitos essenciais

## 2.2 Shadow AI

Shadow AI é o uso de ferramentas ou funcionalidades de inteligência artificial sem conhecimento, avaliação ou aprovação da organização. O fenômeno pode envolver soluções gratuitas, contas pessoais, extensões, assistentes incorporados a sistemas e até ferramentas contratadas diretamente por uma área sem participação das equipes responsáveis.

## 2.3 Revisão humana

Revisão humana é a análise crítica realizada por uma pessoa antes que o resultado da IA seja utilizado, enviado ou produza efeitos. Ela deve ser efetiva: o responsável precisa ter conhecimento, autonomia e informações suficientes para questionar, corrigir ou rejeitar o resultado.

## 3. Quais riscos precisam ser considerados?

| Frente | Exemplos de exposição |
|---|---|
| Proteção de dados | Inserção de dados pessoais ou sensíveis sem avaliação de finalidade, base legal, transparência, segurança, retenção ou transferência internacional. |
| Confidencialidade | Compartilhamento de contratos, propostas, estratégias, bases de dados ou informações internas com ferramentas não autorizadas. |
| Contratos | Descumprimento de deveres de sigilo, segurança, subcontratação, dentre outros. |
| Propriedade intelectual | Uso de códigos, obras, marcas, documentos ou conteúdos protegidos sem autorização. |
| Decisões e pessoas | Erros, vieses ou discriminação em processos que afetam candidatos, empregados, clientes ou terceiros. |
| Segurança da informação | Perda de controle sobre dados, credenciais, integrações, registros e acessos. |
| Reputação e responsabilidade | Comunicações incorretas, decisões inadequadas ou falhas que podem gerar danos financeiros, regulatórios e reputacionais. |

## 4. Passo a passo para implantar a governança

1

### Defina responsáveis e escopo inicial

- Escolha um ponto focal;
- Forme um grupo com as áreas de negócio, tecnologia, segurança, jurídico, privacidade, compliance e recursos humanos, conforme a realidade da empresa.
- Defina quais unidades, áreas ou usos serão priorizados.
- Estabeleça quem poderá aprovar ferramentas e aceitar riscos.

2

### Mapeie ferramentas e casos de uso

- Identifique ferramentas contratadas, gratuitas, testes, extensões e funcionalidades incorporadas a sistemas internos.
- Registre as finalidade, usuários, dados inseridos, integrações, resultados e pessoas afetadas.

3

## Avalie e classifique os riscos

- Analise o tipo de dado e de informação utilizada.
- Considere o impacto sobre pessoas, clientes e operações.
- Verifique autonomia, possibilidade de discriminação, exposição contratual e necessidade de revisão humana.
- Classifique o caso de uso por nível de risco e documente a justificativa.

4

## Avalie a ferramenta e o fornecedor

- Analise termos de uso, política de privacidade, segurança, retenção e uso dos dados para treinamento.
- Identifique locais de processamento e transferências internacionais.
- Verifique controles administrativos, gestão de acessos, registros, exclusão e suporte a incidentes.
- Formalize obrigações contratuais compatíveis com o risco.

5

**Identifique gaps e defina controles**

- Compare o cenário atual com os controles necessários.
- Decida se o uso será permitido, condicionado, ajustado, suspenso ou proibido.
- Atribua responsabilidades e prazos para cada ação.

6

**Formalize regras e fluxos**

- Crie uma política de uso adequado com linguagem acessível.
- Crie um canal simples para declarar novos casos de uso.
- Defina ferramentas permitidas, dados proibidos, usos que exigem aprovação e situações de revisão humana.
- Estruture fluxo para homologação de novas soluções e comunicação de incidentes.

7

## Treine e comunique

- Explique riscos com exemplos próximos da rotina.
- Mostre quais ferramentas podem ser utilizadas e onde pedir ajuda.
- Treine gestores e áreas de maior risco de forma específica.
- Reforce que a revisão humana inclui verificar fatos, contexto, linguagem e impacto.

8

## Monitore e melhore

- Revise periodicamente o inventário e os casos de uso.
- Atualize classificações, controles e documentos.

# Conclusão

Governança de IA não significa bloquear a inovação. Significa criar condições para que a tecnologia gere valor sem expor a organização a riscos desproporcionais. A empresa não precisa resolver tudo ao mesmo tempo: o ponto de partida é obter visibilidade, priorizar os usos mais críticos e estabelecer um processo contínuo de avaliação, decisão e melhoria.

***Lembre-se!***

*Frameworks e boas práticas oferecem direção, mas a governança precisa refletir os usos reais, os dados, os contratos, os clientes, a cultura e o nível de maturidade de cada negócio.*

# Assis e Mendes

DIREITO DIGITAL, TECNOLOGIA E EMPRESARIAL




(11) 3141-9009

contato@assisemendes.com.br

@assisemendes.adv