

Assunto: Política Corporativa para Uso Ético de Inteligência Artificial	
Identificação: Versão 2.0	Uso: Público
Responsável: Gustavo Henrique, Especialista em Governança de IA	Emissão em: janeiro de 2026

1. Natureza e Condição de Uso (Modelo)

Este documento é um modelo autoral elaborado por Gustavo Henrique, para orientar a elaboração de uma **Política Corporativa de Uso Ético de IA**. Este documento não representa, por si só, uma política vigente de qualquer organização, salvo quando formalmente adotado, adaptado e aprovado pela organização interessada.

Ao institucionalizar este modelo, a organização adotante deverá: (I) identificar o proprietário interno do documento; (II) definir a estrutura de governança aplicável, por exemplo um Comitê de IA ou instância equivalente; e (III) publicar versão oficial em seu repositório normativo.

2. Objetivo

Este documento estabelece diretrizes, responsabilidades e controles fundamentais para garantir o uso responsável de sistemas de Inteligência Artificial (IA) no ambiente corporativo, tendo como foco assegurar:

- 2.1.** Adoção ética, responsável e transparente da IA;
- 2.2.** Conformidade com as normas legais e regulatórias;
- 2.3.** Proteção de dados pessoais e informações sensíveis;
- 2.4.** Minimização de riscos operacionais, reputacionais e regulatórios;
- 2.5.** Supervisão humana nas decisões automatizadas.

3. Aplicação

Esta política se aplica a todos os colaboradores, gerentes, estagiários, prestadores de serviços, parceiros e terceiros que:

- 3.1.** Utilizem sistemas de IA em nome da organização adotante;
- 3.2.** Desenvolvam, implementem ou adquiram soluções de IA;
- 3.3.** Tomem decisões baseadas em IA no contexto corporativo.

Inclui-se ao projeto de aplicação de IA:

- 3.4.** Sistemas de IA generativa;
- 3.5.** Ferramentas de automação decisória;
- 3.6.** Plataformas corporativas integradas com IA;
- 3.7.** Modelos de aprendizado de máquina, visão computacional e Processamento de Linguagem Natural (PLN).

4. Referências Legais e Normativas

Este modelo de política foi elaborado com referência às seguintes normas e legislações relevantes, devendo a organização adotante avaliar e assegurar sua conformidade aplicável:

- 4.1.** Lei nº 13.709/2018: Lei Geral de Proteção de Dados (LGPD);
- 4.2.** Projeto de Lei nº 2338/2023: Marco Legal da IA no Brasil, a qual está em tramitação. A organização adotante deverá monitorar sua evolução e adequar esta política quando aplicável;
- 4.3.** ISO/IEC 42001:2023: Sistema de Gestão de Inteligência Artificial;
- 4.4.** ISO/IEC 27001: Segurança da Informação;
- 4.5.** Recomendações da OCDE para Inteligência Artificial Confiável (2019).

A adoção das normas ISO mencionadas neste documento se referem ao alinhamento conceitual e estrutural às boas práticas internacionais, não implicando, necessariamente, certificação formal, salvo quando explicitamente declarado pela organização.

5. Definições

Para a aplicação desta política, consideram-se as seguintes definições:

- 5.1.** Sistema de IA: sistema técnico que utiliza algoritmos computacionais para gerar inferências, previsões ou tomar decisões automatizadas;
- 5.2.** IA Gerativa: tecnologia que cria conteúdo a partir de diretrizes fornecidas por humanos;
- 5.3.** Shadow AI: uso de sistemas de IA sem a devida autorização ou supervisão institucional;
- 5.4.** Dados Sensíveis: dados pessoais considerados sensíveis pela legislação vigente;
- 5.5.** Viés Algorítmico: distorções sistemáticas nos resultados gerados por sistemas de IA;
- 5.6.** Explicabilidade: capacidade de compreender e interpretar decisões e resultados gerados por sistemas de IA;
- 5.7.** Organização Adotante (ou “Organização”): entidade que adotar e aprovar esta política, tornando-a documento corporativo vigente.

6. Princípios de Utilização da IA

O uso de IA dentro da organização adotante deve seguir, rigorosamente, os seguintes princípios:

- 6.1.** Transparência e explicabilidade;
- 6.2.** Justiça e não discriminação;
- 6.3.** Segurança, robustez e resiliência;
- 6.4.** Privacidade e proteção de dados;
- 6.5.** Responsabilidade humana;
- 6.6.** Supervisão humana contínua.

7. Diretrizes de Uso Aceitável (em complemento aos princípios éticos desta política)

7.1. Autorização e Controle:

- Toda ferramenta ou sistema de IA deve receber aprovação prévia da instância de governança designada pela organização adotante (como por exemplo Governança de TI, Comitê de IA, Segurança da Informação, Privacidade ou equivalente), conforme matriz interna de responsabilidades;
- O uso de soluções de IA não registradas é estritamente proibido.

7.2. Uso de Dados:

- A inserção de dados pessoais, sensíveis ou confidenciais em sistemas não autorizados é proibida;
- O tratamento de dados deve estar em conformidade com os princípios da LGPD.

7.3. Decisões Automatizadas:

- Decisões com impacto significativo devem ser revisadas por profissionais responsáveis;
- As partes afetadas devem ser informadas sempre que a IA influenciar decisões;
- Para fins desta política, distinguem-se decisões totalmente automatizadas, sem intervenção humana, de decisões assistidas por IA, nas quais a tecnologia atua como suporte à decisão humana;
- Decisões totalmente automatizadas que afetem os interesses dos titulares de dados observarão, obrigatoriamente, os direitos previstos na legislação de proteção de dados.

7.4. Uso Indevido:

- É proibido aproveitar IA para fins ilegais, discriminatórios, enganosos ou manipulativos;
- O uso deve estar de acordo com os contratos, as licenças e os termos relevantes.

8. Estrutura de Governança da IA

A organização adotante deverá estabelecer uma estrutura de governança para IA, podendo fazê-lo por meio de um Comitê de Governança de IA ou por instância equivalente formalmente designada.

Quando instituída, a instância de governança (Comitê de Governança de IA ou equivalente) deve ser composta, no mínimo, por representantes das áreas de Tecnologia da Informação, Jurídico, Privacidade e Segurança da Informação (ou áreas equivalentes), conforme a estrutura organizacional aplicável.

8.1. Competências da instância de governança de IA (Comitê ou equivalente):

- Avaliar e classificar riscos associados a sistemas de IA;
- Aprovar ferramentas e aplicações;
- Conduzir avaliações de impacto algorítmico em sistemas de IA classificados como de risco elevado, especialmente quando envolverem dados pessoais sensíveis, decisões críticas ou impactos relevantes sobre indivíduos ou a organização;
- Monitorar conformidade, viés e incidentes;
- Atualizar as políticas e os controles conforme necessário.

A instância de governança de IA (Comitê ou equivalente) deverá se reunir periodicamente, com registros formais das deliberações, definição de responsáveis e prazos para execução das decisões. Casos de alto risco ou de divergência relevante deverão ser escalonados à alta administração.

9. Segurança da Informação e Privacidade

- 9.1.** Os dados utilizados em sistemas de IA devem ser anonimizados ou tratados com base legal válida;
- 9.2.** Os sistemas devem garantir a possibilidade de exclusão e correção de dados;
- 9.3.** Transferências internacionais requerem respaldo jurídico;
- 9.4.** A manutenção de logs de uso para fins de auditoria é obrigatória.

10. Prevenção e Mitigação de Shadow AI

10.1. Todas as soluções de IA devem constar no inventário oficial da organização adotante;

10.2. O uso não autorizado será monitorado e investigado;

10.3. Violações podem resultar em medidas disciplinares, conforme o regime interno da organização adotante, e, quando aplicável, na notificação às autoridades competentes.

11. Responsabilidades

11.1. Constitui responsabilidade dos usuários:

- Utilizar IA de maneira ética, legal e transparente;
- Registrar utilizações e intervenções humanas;
- Reportar desvios ou incidentes.

11.2. Constitui responsabilidade da área de TI e Governança:

- Manter o inventário atualizado de ferramentas de IA;
- Monitorar riscos e conformidade;
- Restringir acessos não autorizados.

12. Monitoramento, Auditoria e Controle

12.1. Auditorias periódicas deverão avaliar riscos, viés e segurança;

12.2. Evidências devem ser armazenadas conforme políticas internas da organização adotante;

12.3. As não conformidades devem resultar em planos de ação corretivos.

13. Sanções e Medidas Disciplinares

As medidas abaixo são referenciais e devem ser adequadas ao código de conduta, ao regime disciplinar e às políticas internas da organização adotante, após aprovação formal. O descumprimento desta política poderá levar a:

- Advertências formais;
- Suspensão de acessos;
- Medidas disciplinares, incluindo desligamento;
- Comunicação à Autoridade Nacional de Proteção de Dados (ANPD), quando o incidente envolver dados pessoais e atender aos critérios legais de notificação obrigatória.

14. Disposições Finais

Esta política foi elaborada por Gustavo Henrique como modelo autoral e poderá ser adotada por outras organizações, total ou parcialmente, desde que adaptada ao contexto interno, validada pelas áreas competentes e aprovada formalmente pelos órgãos responsáveis.

Quando institucionalizada, a organização adotante deverá identificar: (I) o proprietário interno do documento; (II) a estrutura de governança de IA aplicável; e (III) o ciclo de revisão periódica, de modo a incorporar mudanças regulatórias, tecnológicas e organizacionais.

Anexo I - Registro de Verificação de Conformidade

Esta lista de controle deverá ser preenchida pelo responsável pela solução de IA e validado pela instância de governança definida pela organização adotante (ex.: Governança de TI, Comitê de IA ou equivalente), mantendo-se como evidência para auditorias internas e externas.

- () Ferramenta aprovada pela instância de governança designada (ex.: Comitê de IA ou equivalente);
- () Inventário corporativo da organização adotante;
- () Avaliação de riscos documentada;
- () Revisão humana realizada;
- () Comunicação às partes afetadas;
- () Registro para auditoria.

Responsável pela Solução de IA

Nome:

Cargo:

Área:

Data:

Instância de Governança / Comitê de IA

Nome do representante:

Cargo:

Data: