

PROVIDER IT. | Caminhe por novos futuros

Política de Inteligência Artificial

ÍNDICE

1 Objetivo 02

2 Escopo 02

3 Exclusões 03

4 Princípios éticos e conformidade legal 04

5 Governança e Responsabilidades 08

6 Privacidade e Segurança de Dados 10

7 Transparência e Explicabilidade 15

8 Diretrizes para o uso responsável de IA na geração de conteúdo sintético 18

9 Treinamento e Capacitação 21

10 Monitoramento e Avaliação Contínua 23

11 Gestão de Riscos e Mitigação 27

12 Incidentes Éticos de IA 30

13 Relatório de Impacto à Proteção de Dados Pessoais (RIPD) 34

14 Direitos dos Usuários 37

15 Atualização e Revisão da Política 40

01 OBJETIVO

Esta política tem como objetivo garantir o uso responsável, eficiente e ético dos portais de Inteligência Artificial baseados em Modelos de Linguagem (LLM e SLM) na empresa. Pretendemos orientar todos os colaboradores sobre como utilizar essas ferramentas para melhorar a produtividade, a qualidade do trabalho e a tomada de decisões, sempre respeitando as leis, os valores da empresa e os direitos de terceiros.

Além disso, buscamos minimizar riscos associados ao uso inadequado ou não autorizado dessas tecnologias, protegendo dados sensíveis e assegurando que as aplicações estejam alinhadas aos objetivos estratégicos da organização.

02 ESCOPO

Esta política se aplica a todos os colaboradores, departamentos, que utilizam, direta ou indiretamente, portais de IA baseados em Modelos de Linguagem no desempenho de suas atividades relacionadas à empresa.

Tendo sempre que a IA no estágio atual é um copiloto fazendo a comparação com aviação e o responsável do trabalho ou da área tem que ser o piloto e criar processos de verificação e de controle de qualidade para garantir o máximo de qualidade para o cliente sempre.

Estão incluídas as seguintes áreas de uso:
1. Criação de Conteúdo: Redação de textos, resumos, e-mails, relatórios ou outros documentos corporativos.

2. Apoio à Decisão: Análise de dados e informações para fundamentar decisões estratégicas e operacionais.

3. Automação de Processos: Uso de IA para agilizar tarefas repetitivas ou melhorar fluxos de trabalho.

4. Atendimento ao Cliente e Comunicação: Geração de respostas automatizadas ou assistidas em canais de comunicação com clientes e parceiros.

5. Aprendizado e Desenvolvimento: Treinamento e capacitação dos colaboradores no uso das ferramentas de LLM e SLM.

03 EXCLUSÕES

Esta política não cobre o uso de tecnologias de IA fora do ambiente corporativo ou para fins pessoais. Para esses casos,

orienta-se que os colaboradores sigam as diretrizes gerais de ética e responsabilidade digital.

Com esta política, buscamos proporcionar um ambiente de trabalho mais produtivo e inovador, mantendo o compromisso com a transparência, a segurança e o respeito aos nossos valores institucionais.

04 PRINCÍPIOS ÉTICOS E CONFORMIDADE LEGAL

O uso de portais de IA baseados em Modelos de Linguagem (LLM) na empresa deve seguir princípios éticos claros e estar em conformidade com todas as leis e regulamentações aplicáveis. Este capítulo apresenta os fundamentos que todos os colaboradores devem seguir para garantir um uso responsável e respeitoso dessa tecnologia.

Na Provider IT, prezamos e pregamos a utilização responsável da Inteligência Artificial como ferramenta de transformação digital que potencializa capacidades humanas sem substituir o julgamento crítico e a responsabilidade das pessoas.

Nos comprometemos a utilizar a IA de forma que:

- **Respeite a dignidade humana** em todas as suas dimensões,

- **Promova a transparência e explicabilidade** nas decisões automatizadas,
- Garanta a **equidade e não-discriminação**,
- **Proteja a privacidade** e os dados pessoais,
- Mantenha a **supervisão humana** como elemento central.

PILARES ÉTICOS:

Conformidade Regulatória e Engajamento Proativo:

- **Cumprimento rigoroso das normas:** Adotamos integralmente a LGPD e demais regulamentações locais e internacionais, estabelecendo processos internos que excedem os requisitos mínimos legais.
- **Participação ativa no desenvolvimento normativo**: Engajamo-nos proativamente com reguladores, comitês técnicos e grupos de trabalho para contribuir na construção de frameworks regulatórios equilibrados e eficazes.
- **Ambiente controlado (Regulatory Sandbox)**: Implementamos práticas de "sandbox regulatório" interno, testando soluções de IA em ambientes controlados antes da implementação plena, garantindo conformidade e identificação prévia de riscos.
- **Monitoramento contínuo:** Mantemos sistemas de acompanhamento regulatório em tempo real, adaptando nossos processos conforme evolução das normas nacionais e internacionais.

VIÉS E JUSTIÇAS:

- **Diversidade nos dados:** Temos representatividade adequada em datasets, evitando amostras enviesadas que possam perpetuar discriminação contra grupos específicos ou comunidades vulneráveis.
- **Equipes diversificadas:** Promovemos diversidade em nossas equipes de desenvolvimento, reconhecendo que perspectivas variadas são essenciais para identificar e mitigar vieses sistêmicos.
- **Inclusão por design:** Incorporamos princípios de inclusão desde a concepção dos projetos, garantindo que soluções de IA sejam acessíveis e benéficas para todos os usuários.

PRIVACIDADE DOS DADOS:

- **Proteção integral de dados pessoais:** Implementamos controles rigorosos de acesso, e técnicas de anonimização/pseudonimização, seguindo os mais altos padrões da LGPD e GDPR.
- **Minimização de dados:** Coletamos e processamos apenas os dados estritamente necessários para a finalidade específica, aplicando o princípio da necessidade em todas as operações.
- **Dados sintéticos:** Utilizamos técnicas de geração de 08 dados sintéticos para preservar privacidade em pesquisas e desenvolvimento, reduzindo riscos de reidentificação.

RESPONSABILIDADE:

- **Responsabilidade humana:** Mantemos supervisão humana em todas as decisões críticas, implementando mecanismos que garantam controle humano sobre sistemas automatizados.
- **Accountability organizacional:** Estabelecemos estruturas claras de responsabilidade, com papéis e responsabilidades definidos para todas as etapas do ciclo de vida da IA.
- **Gestão de riscos:** Implementamos frameworks de avaliação e mitigação de riscos, incluindo planos de contingência.
- **Monitoramento contínuo:** Mantemos vigilância constante sobre o desempenho e impacto de nossos sistemas, com indicadores de qualidade e mecanismos de alerta para desvios.
- **Reparação de danos:** Estabelecemos processos claros para identificação, investigação e reparação de danos, incluindo mecanismos de compensação adequada.

CRIATIVIDADE E PROPRIEDADE:

- **Inovação responsável:** Promovemos o desenvolvimento de soluções criativas que agreguem valor real à sociedade, equilibrando inovação tecnológica com responsabilidade social e ética.
- **Estímulo à criatividade humana:** Utilizamos IA como ferramenta de potencialização da criatividade humana, não substituição, garantindo que profissionais mantenham papel central no processo criativo.

- **Respeito a direitos autorais:** Realizamos investigação constante para verificar e respeitar direitos de propriedade intelectual em treinamento de modelos e geração de conteúdos.
- **Transparência na colaboração IA-Humano:** Como empresa AI-first, comunicamos publicamente nossa adoção estratégica de inteligência artificial em todos os nossos processos e produtos. Esta transparência posicional atende aos requisitos éticos de comunicação com o mercado, informando claramente que a IA é parte integral de nossa proposta de valor.

Estes pilares são revisados regularmente pelo nosso Comitê de Ética em IA, garantindo evolução contínua alinhada às melhores práticas globais e às necessidades de nossos stakeholders.

Lembre-se: A IA é uma poderosa aliada para melhorar processos e facilitar o trabalho, mas sua utilização exige cuidado, bom senso e respeito às normas. Todos somos responsáveis por garantir que o uso dessas ferramentas esteja alinhado aos princípios éticos e legais da empresa.

05 GOVERNANÇA E RESPONSABILIDADES

O uso de portais de IA baseados em Modelos de Linguagem (LLM) exige uma estrutura de governança clara e bem

definida. Essa estrutura garante que as ferramentas sejam utilizadas de forma responsável, alinhadas às diretrizes da empresa e às exigências legais.

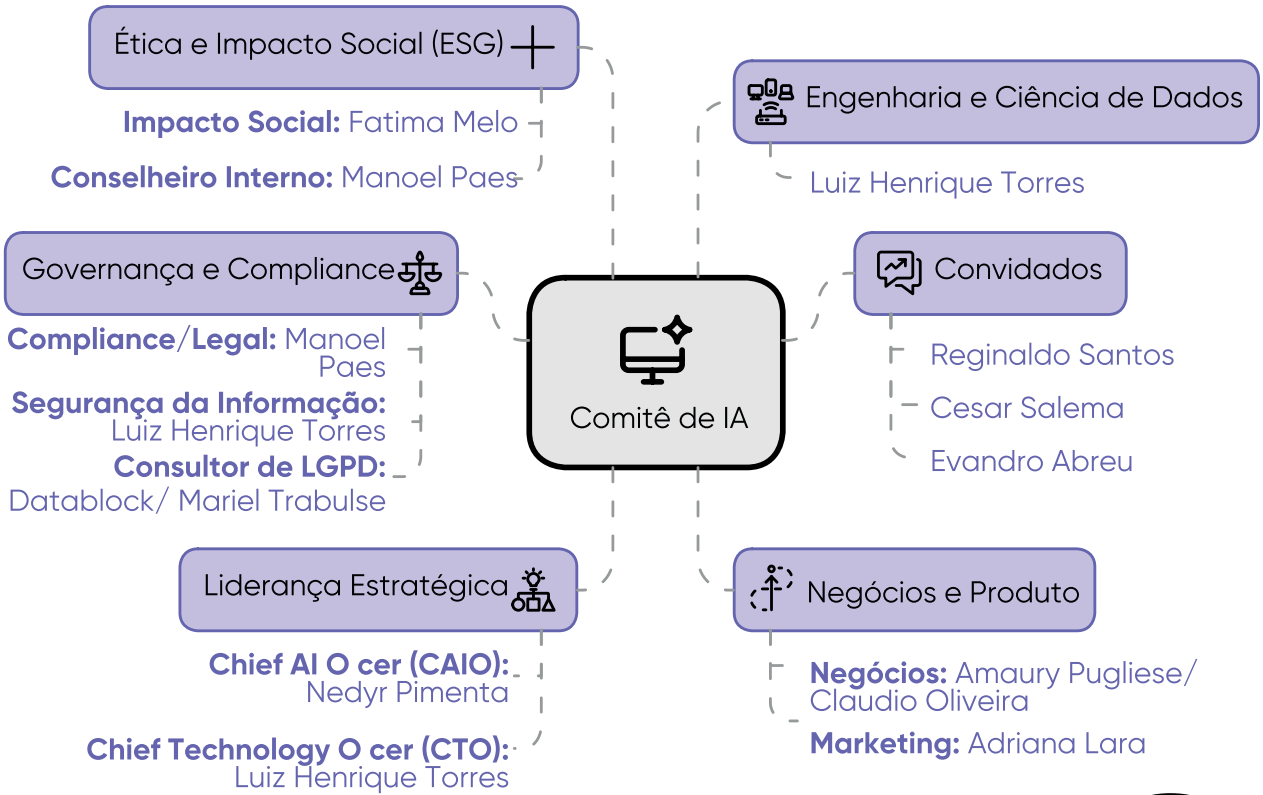
OBJETIVO:

Estabelecer diretrizes estratégicas, éticas, jurídicas e operacionais para o uso da IA na Provider IT, garantindo segurança, transparência, compliance e alinhamento com os interesses dos clientes e da sociedade.
Supervisionar riscos regulatórios, técnicos e reputacionais relacionados ao uso da IA.

PERIODICIDADE:

Semanal

COMPOSIÇÃO:



ASSUNTOS PERTINENTES:

- Lançamento de novos modelos e ferramentas com alto impacto.
- Incidentes envolvendo decisões automatizadas ou vazamento de dados.
- Alterações regulatórias relevantes.
- Avaliações de maturidade da governança de IA.
- Criação e Revisão de KPIs de IA responsável (ex: métricas de fairness, drift, explicabilidade, etc).
- Promoção de cultura de IA responsável e treinamentos internos.
- Garantia de mecanismos de auditabilidade, explicabilidade e revisão humana.

06 PRIVACIDADE E SEGURANÇA DE DADOS

O uso de portais de Inteligência Artificial (IA) baseados em Modelos de Linguagem (LLM) na empresa deve garantir que todas as informações coletadas, processadas e armazenadas sejam tratadas com o mais alto nível de cuidado, em conformidade com a Lei Geral de Proteção de Dados (LGPD) e as melhores práticas de segurança. Este capítulo apresenta os protocolos que devem ser seguidos para proteger dados pessoais e sensíveis contra acessos não autorizados e usos indevidos.

Procedimento de Aprovação para Projetos de IA:

Todo projeto de IA proposto deve passar pela **Classificação de Risco**, que realizará:

- Análise automática de dados sensíveis (score baseado em algoritmo),
- Verificação de compliance LGPD/regulatórios,
- Comparação com casos similares na base de conhecimento (quando disponível),
- Geração de relatório preliminar de risco.

Sistema de Classificação de Risco:

RISCO BAIXO:

Avaliação:

- Gerar checklist personalizado de conformidade,
- Pré-aprovação automática com validação humana obrigatória,
- Documentação simplificada.

RISCO MÉDIO:

Avaliação:

- Preparar dossiê completo com análise de impacto,
- Sugerir mitigações específicas baseadas em melhores práticas,
- Facilitar submissão estruturada ao Comitê de IA.

RISCO ALTO/CRÍTICO:

Avaliação:

- Analisar detalhadamente,
- Agendar reunião com o Comitê de IA,

- Preparar documentação completa incluindo DPIA,
- Aprovação do Comitê é obrigatória antes de qualquer implementação.

Procedimentos Específicos para Dados Sensíveis:

Objetivo Claro: Antes de coletar dados, identifique e documente o motivo pelo qual eles são necessários. Só colete dados essenciais para a atividade em questão.
Consentimento: Sempre que for necessário coletar dados de indivíduos (clientes, colaboradores ou parceiros), obtenha consentimento explícito e informe de forma clara como as informações serão utilizadas.

Dados Sensíveis:

- É vedado inserir, carregar, transmitir ou disponibilizar em ferramentas de IA públicas (ChatGPT, Gemini, etc.), abertas ou não aprovadas pela Provider IT informações não públicas da empresa, de clientes, fornecedores, parceiros, colaboradores ou terceiros. A vedação inclui, sem se limitar a, contratos e anexos, e-mails e documentos internos, dados pessoais, informações financeiras, comerciais ou estratégicas, códigos-fonte, especificações técnicas, arquiteturas de sistemas, credenciais, senhas, chaves, tokens e informações protegidas por obrigação de confidencialidade.
- Proibição de upload de dados de saúde, origem racial, convicções políticas/religiosas em plataformas externas,
- Restrições específicas para dados estratégicos da Provider IT.

Tratamento de Dados

- **Minimização de Dados:** Trabalhe apenas com os dados estritamente necessários para a atividade. Evite armazenar informações que não serão utilizadas.
- **Anonimização e Pseudonimização:** Sempre que possível, substitua dados pessoais por identificadores genéricos ou torne-os anônimos antes de processá-los nos portais de IA.
- **Validação de Dados:** Revise e valide os dados antes de inseri-los nos portais de IA para evitar o uso de informações imprecisas ou inadequadas.

Compartilhamento de Dados

- **Consentimento Prévio:** Dados pessoais só podem ser compartilhados com terceiros com consentimento explícito do titular ou em conformidade com a legislação.
- **Acordos com Terceiros:** Sempre que dados forem compartilhados com fornecedores ou parceiros, celebre contratos que assegurem a proteção das informações e a conformidade com a LGPD.

Proteção Contra Acessos Não Autorizados

- **Criptografia:** Utilize criptografia para proteger informações durante o armazenamento e o envio, especialmente dados sensíveis.
- **Segurança de Senhas:** Adote políticas rigorosas de gestão de senhas, exigindo complexidade e troca periódica.
- **Monitoramento Contínuo:** Implante sistemas de monitoramento para detectar e responder rapidamente a possíveis ameaças ou violações.

Capacitação e Conscientização

- **Treinamento Regular:** Todos os colaboradores que lidam com dados devem ser treinados regularmente sobre boas práticas de privacidade e segurança.
- **Conscientização:** Promova campanhas internas para reforçar a importância da proteção de dados em todas as atividades realizadas na empresa.

Conformidade com a LGPD

A utilização de IA na Provider IT está alinhado com a LGPD já implementado na empresa e os pontos a serem destacados são:

- **Direitos dos Titulares de Dados:** Garanta que indivíduos possam solicitar acesso, correção ou exclusão de seus dados pessoais, conforme previsto na LGPD.
- **Análise de Impacto à Proteção de Dados (DPIA):** Realize análises de impacto sempre que o uso de IA puder afetar os direitos dos titulares de dados.
- **Relatório de Incidentes:** Qualquer incidente de segurança envolvendo dados deve ser reportado imediatamente ao Encarregado de Proteção de Dados (DPO) e tratado conforme o protocolo estabelecido.

Auditorias e Revisões

- Realizamos **auditorias regulares** para verificar a conformidade com esta política e identificar possíveis melhorias nos processos de privacidade e segurança.
- **Atualizamos os protocolos** sempre que houver mudanças nas leis ou avanços nas melhores práticas de mercado.

Plataforma de IA Corporativa

A Provider IT adotou para um grupo de colaboradores uma plataforma padrão como ferramenta corporativa aprovada para projetos de Inteligência Artificial, considerando seus rigorosos padrões de segurança e conformidade. A escolha baseia-se em critérios técnicos e éticos específicos:

- **Conformidade Regulatória:** A plataforma possui certificação SOC II Tipo 1 e conformidade total com a LGPD, alinhando-se aos requisitos normativos da Provider IT.
- **Política de Não-Treinamento:** Garantia contratual de que nenhum dado de cliente é utilizado para treinar modelos de IA, com testes trimestrais independentes de exfiltração de dados para validar esta política.
- **Controle de Residência de Dados:** Para projetos enterprise, a plataforma oferece opções de processamento e armazenamento exclusivamente no Brasil, Estados Unidos ou Europa, com possibilidade de implantação on-premise.
- **Criptografia Avançada:** Todos os dados são criptografados em repouso com criptografia em nível de campo para informações sensíveis, incluindo opção de chaves gerenciadas pelo cliente.

Os colaboradores selecionados para utilizar a plataforma não podem utilizar qualquer portal de acesso de IA do mercado para realizar qualquer trabalho da Provider IT.

07 TRANSPARÊNCIA E EXPLICABILIDADE

A transparência no uso de sistemas de Inteligência Artificial (IA) é essencial para construir confiança e garantir que colaboradores, clientes e parceiros compreendam como esses sistemas operam e como impactam suas decisões e interações. Este capítulo estabelece diretrizes para informar, de forma clara e acessível, o uso de portais de IA baseados em Modelos de Linguagem (LLM) e garantir que decisões automatizadas sejam explicadas de maneira compreensível.

Comunicação Aberta sobre o Uso de IA

Informação aos Colaboradores: Todos os colaboradores do processo devem ser informados sobre quando e como os sistemas de IA estão sendo utilizados em processos internos ou em suas funções diárias.

Aviso aos Clientes e Parceiros: Sempre que a IA for utilizada em comunicações, processos ou decisões que impactem diretamente clientes ou parceiros, essa informação deve ser claramente comunicada, como por meio de notificações, disclaimers ou avisos.

Explicabilidade das Decisões Automatizadas

Clareza na Comunicação:

- Sempre que uma decisão for tomada, total ou parcialmente, com base em sistemas de IA, deve ser possível explicar, em linguagem simples, como essa decisão foi alcançada.
- Os dados usados para a análise (respeitando a privacidade);

- A lógica geral que orienta o sistema (sem expor segredos comerciais);
- O impacto esperado da decisão sobre o indivíduo ou o processo.

Ferramentas de Feedback

Acesso a Informações: Clientes e colaboradores devem ter acesso a canais para solicitar informações adicionais sobre como a IA foi usada em determinado contexto.

Direito de Revisão: Sempre que aplicável, ofereça a possibilidade de revisão manual de decisões tomadas pela IA, especialmente em situações que impactem diretamente direitos ou interesses das pessoas envolvidas.

Comunicação Proativa

Política de Transparência: Divulgue de forma clara a política da empresa sobre o uso de IA, incluindo objetivos, limites e como ela beneficia os envolvidos.

Atualizações Regulares: Notifique os stakeholders sempre que houver mudanças relevantes no uso de sistemas de IA, como a introdução de novas ferramentas ou métodos de processamento.

Monitoramento da Transparência

Avaliação Regular: Realize auditorias periódicas para garantir que os princípios de transparência estão sendo seguidos e que as explicações fornecidas são compreensíveis e adequadas.

Correção de Falhas: Caso sejam identificadas falhas na explicação ou na comunicação do uso de IA, corrija imediatamente e melhore os processos.

08 DIRETRIZES PARA O USO RESPONSÁVEL DE IA NA GERAÇÃO DE CONTEÚDO SINTÉTICO

Princípios Gerais:

- O uso de IA para gerar ou modificar conteúdos visuais, textuais e auditivos deve ser transparente, ético e alinhado com as diretrizes da empresa e as regulamentações aplicáveis.
- Sempre que um conteúdo gerado por IA puder ser confundido com um conteúdo real produzido por humanos, deve haver uma indicação clara e visível de que se trata de um material sintético.
- O uso dessas tecnologias deve respeitar direitos autorais, privacidade, conformidade legal e evitar disseminação de desinformação.

Proibições:

É estritamente proibido o uso de IA para:

- **Criar deepfakes para fins enganosos:** Produzir vídeos, áudios ou imagens manipuladas que possam induzir terceiros a erro, prejudicar indivíduos ou a reputação da empresa.
- **Gerar conteúdo falso para comunicação oficial:** O uso de IA para criar ou alterar falas, entrevistas, depoimentos ou imagens em nome da empresa, sem autorização prévia e sem um aviso claro de que se trata de conteúdo gerado por IA.

- **Modificar a identidade de indivíduos sem consentimento:** Alterar rostos, vozes ou comportamentos de pessoas em vídeos, áudios ou fotos sem sua permissão explícita.
- **Criar ou divulgar notícias falsas (fake news):** Utilizar IA para produzir ou amplificar desinformação, incluindo textos, vídeos ou imagens que possam enganar o público sobre fatos relevantes.
- **Simular comunicações humanas sem identificação:** Chatbots, assistentes virtuais e qualquer outro sistema de IA que interaja diretamente com clientes ou colaboradores devem informar claramente que são sistemas automatizados.

Uso Permitido sob Regras Específicas

A IA pode ser utilizada para a criação de conteúdos audiovisuais e sintéticos nas seguintes condições:

- **Treinamento e Simulação:** Deepfakes e avatares sintéticos podem ser utilizados para simulações de treinamento interno, desde que seja indicado que o conteúdo é gerado por IA e não distorça a realidade.
- **Efeitos Visuais e Criativos:** O uso de IA para edição de imagens e vídeos é permitido para efeitos artísticos, design e publicidade, desde que respeite os direitos de imagem de terceiros e esteja de acordo com a política de comunicação da empresa.
- **Reconstrução de Vozes para Fins Específicos:** A clonagem de voz por IA só pode ser usada mediante consentimento explícito da pessoa envolvida e com uma indicação clara ao público de que se trata de um áudio gerado artificialmente.

- **Assistência na Produção de Conteúdo:** Ferramentas de IA podem auxiliar na criação de roteiros, textos e conteúdos audiovisuais, desde que a responsabilidade final pelo material seja de um profissional humano.

Transparência e Identificação

- **Rotulagem:** Sempre que necessário, conteúdos gerados ou modificados por IA, devem conter um rótulo, como: "Imagem gerada por IA" ; "Vídeo criado com inteligência artificial" ; "Este áudio foi sintetizado por IA".
- **Aviso aos Usuários:** Clientes, colaboradores e parceiros devem ser informados sobre o uso de IA na geração de conteúdos interativos ou automatizados, especialmente em interfaces conversacionais.
- **Validação por Humanos:** Antes da publicação de conteúdos gerados por IA que possam impactar a percepção pública da empresa, deve haver uma revisão e 22 validação por uma equipe responsável.

Penalidades pelo Uso Indevido

O descumprimento dessas diretrizes pode resultar em **sanções disciplinares**, incluindo:

- Advertências formais;
- Restrição ou suspensão do acesso a ferramentas de IA;
- Ações legais, caso o uso indevido viole leis ou regulamentos.

09 TREINAMENTO E CAPACITAÇÃO

O uso responsável e eficaz de ferramentas de Inteligência Artificial (IA), como os portais baseados em Modelos de Linguagem (LLM), exige que todos os colaboradores estejam preparados para lidar com a tecnologia de forma segura, ética e alinhada às necessidades da empresa. Este capítulo descreve as ações necessárias para capacitar os funcionários no uso correto dessas ferramentas e conscientizá-los sobre os princípios éticos e legais envolvidos.

Objetivo do Treinamento:

- **Capacitação Técnica:** Garantir que os colaboradores saibam utilizar as ferramentas de IA corretamente, compreendendo suas funcionalidades e limitações.
- **Consciência Ética e Legal:** Sensibilizar os funcionários sobre os princípios éticos no uso de IA e as leis aplicáveis, como a Lei Geral de Proteção de Dados (LGPD).
- **Prevenção de Riscos:** Ensinar boas práticas para evitar o uso indevido da tecnologia e identificar potenciais problemas, como vieses ou falhas no sistema.

Módulo Básico:

- Princípios éticos,
- Transparência,
- Autoria humana.

Módulo Especializado:

- Serão oferecidos treinamentos regulares para atualizar os colaboradores sobre novas funcionalidades, regulamentações ou mudanças nas ferramentas de IA. Esses treinamentos podem incluir:
- Workshops presenciais ou online;
- Tutoriais interativos e estudos de caso;
- Sessões de perguntas e respostas com especialistas internos ou externos.

Treinamento Específico por Área:

- Capacitações personalizadas para cada setor, com foco nas ferramentas e aplicações mais relevantes para suas atividades.

Recursos Disponíveis

- **Portal de Aprendizado:** A empresa disponibilizará um portal interno com materiais educativos, como manuais, vídeos e guias rápidos sobre o uso das ferramentas de IA.
- **Equipe de Apoio:** Uma equipe de especialistas estará disponível para oferecer suporte técnico e tirar dúvidas sobre o uso de IA.

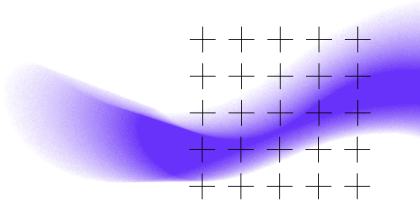
Avaliação e Certificação

- **Testes de Conhecimento:** Após os treinamentos, poderão ser aplicados testes para garantir que os colaboradores compreenderam os conteúdos.
- **Certificados Internos:** Os participantes que concluírem os treinamentos receberão certificados de capacitação no uso responsável de IA.

Revisão e Atualização dos Programas

- **Atualizações Regulares:** Os programas de treinamento serão revisados periodicamente para refletir mudanças nas ferramentas, regulamentações ou demandas da empresa.
- **Feedback dos Colaboradores:** Os colaboradores serão incentivados a dar sugestões para melhorar os treinamentos, garantindo que sejam relevantes e eficazes.

10 MONITORAMENTO E AVALIAÇÃO CONTÍNUA



Para garantir que os portais de Inteligência Artificial (IA) baseados em Modelos de Linguagem (LLM) sejam usados de forma segura, eficaz e alinhada aos objetivos da empresa, é essencial estabelecer procedimentos regulares de monitoramento e avaliação. Este capítulo apresenta as práticas para revisar continuamente os sistemas de IA, identificar e corrigir falhas ou vieses, e promover melhorias constantes.

Objetivo do Monitoramento:

- **Avaliação de Desempenho:** Verificar se os sistemas de IA estão cumprindo suas funções de forma eficiente e com os resultados esperados.
- **Identificação de Problemas:** Detectar eventuais falhas, como respostas inadequadas ou resultados tendenciosos.

- **Garantia de Conformidade:** Assegurar que o uso dos sistemas está em conformidade com a legislação, as diretrizes da empresa e os princípios éticos estabelecidos.

Procedimentos de Monitoramento:

Acompanhamento Contínuo:

- Implantar ferramentas ou processos automáticos para monitorar o funcionamento dos portais de IA em tempo real.
- Registrar logs de uso para análise de padrões e identificação de anomalias.

Auditorias Periódicas:

- Realizar revisões detalhadas trimestralmente ou em períodos definidos, avaliando o desempenho e os impactos das ferramentas de IA.
- Avaliar a consistência e a qualidade dos conteúdos gerados pelos sistemas.

Análise de Resultados:

- Comparar os resultados obtidos pelos sistemas de IA com métricas previamente definidas para medir sua eficácia.
- Revisar casos em que decisões ou resultados automatizados foram questionados ou considerados inadequados.

Identificação e Correção de Vieses:

Detecção de Vieses:

- Analisar os resultados gerados para identificar possíveis tendências discriminatórias ou não equitativas.

- Realizar testes regulares com dados diversos para verificar a neutralidade das ferramentas.

Correção Imediata:

- Implementar ajustes nos sistemas sempre que um viés ou falha for identificado.
- Documentar as correções realizadas para garantir transparência e aprendizado organizacional.

Envolvimento de Colaboradores:

Relatos de Incidentes:

Canal acessível para que colaboradores possam reportar problemas ou inconsistências observadas no uso dos sistemas de IA.

inteligencia.artificial@provider-it.com.br

Feedback Ativo:

Incentivar os usuários a fornecerem feedback sobre o desempenho das ferramentas, ajudando na identificação de melhorias necessárias.

Melhorias Contínuas:

Atualização de Sistemas:

Revisar e implementar melhorias nas ferramentas de IA regularmente, acompanhando as atualizações oferecidas pelos fornecedores e as evoluções tecnológicas.

Revisão de Protocolos:

Atualizar os processos internos de uso e monitoramento de IA com base nas lições aprendidas durante as avaliações.

Benchmarking:
Comparar o desempenho das ferramentas internas com melhores práticas e padrões de mercado, identificando oportunidades para inovação e aperfeiçoamento.

Relatórios e Comunicação:

Relatórios Regulares:
Fornecer relatórios periódicos sobre o desempenho, os ajustes realizados e os resultados das auditorias à equipe de governança de IA e à alta gestão.

Transparência:
Compartilhar de forma clara os principais resultados das avaliações com os colaboradores e, quando necessário, com clientes ou parceiros.

Garantia de Conformidade:

Auditorias Externas:
Sempre que necessário, contratar auditorias externas para garantir que os sistemas de IA estejam alinhados às leis e regulamentações, como a LGPD.

Revisões de Impacto:
Avaliar como os sistemas de IA impactam colaboradores, clientes e processos da empresa, promovendo ajustes para reduzir riscos.

11 GESTÃO DE RISCOS E MITIGAÇÃO

O uso de portais de Inteligência Artificial (IA) baseados em Modelos de Linguagem (LLM) traz inúmeras oportunidades, mas também apresenta riscos que precisam ser identificados e gerenciados. Este capítulo descreve os principais riscos associados ao uso dessas ferramentas e as estratégias que a empresa deve adotar para mitigá-los, garantindo um ambiente de trabalho seguro, ético e em conformidade com as normas.

Identificação de Riscos:

A empresa deve monitorar continuamente o uso de IA para identificar potenciais riscos em diferentes áreas. Os principais riscos incluem:

- **Violações de Propriedade Intelectual:**
  1. Uso de conteúdos gerados pela IA que possam infringir direitos autorais ou patentes.
  2. Reprodução indevida de material protegido por terceiros.

- **Discriminação Algorítmica:**
  1. Resultados tendenciosos que possam prejudicar grupos específicos de pessoas com base em gênero, raça, idade ou outras características.

Privacidade e Proteção de Dados:

- Inserção de dados sensíveis em sistemas de IA que não garantem a segurança e a conformidade legal.
- Vazamento de informações devido a falhas no processamento ou no armazenamento de dados.

Decisões Errôneas:
Dependência excessiva de resultados gerados pela IA, levando a conclusões incorretas ou inadequadas.

Reputação e Confiança:
Impactos negativos na reputação da empresa caso a IA seja usada de forma inadequada, como no envio de conteúdos inadequados ou enganosos.

Estratégias de Mitigação:
Para minimizar os riscos identificados, a empresa adota as seguintes estratégias:

Prevenção de Violações de Propriedade Intelectual:

- Revisar todo o conteúdo gerado pela IA antes de utilizá-lo ou publicá-lo.
- Garantir que as ferramentas de IA utilizadas estejam licenciadas e em conformidade com as leis aplicáveis.

Correção de Discriminação Algorítmica:

- Realizar testes periódicos para identificar e corrigir vieses nos resultados gerados pela IA.
- Treinar os colaboradores para reconhecerem e evitarem vieses nos sistemas.

Garantia de Privacidade e Proteção de Dados:

- Não inserir informações confidenciais ou sensíveis em ferramentas de IA, a menos que sejam autorizadas e seguras.
- Implementar protocolos de segurança para proteger os dados processados pela IA.

Validação de Decisões Automatizadas:

- Revisar e validar manualmente decisões importantes geradas pela IA.
- Usar a IA como ferramenta de apoio, não como substituto completo para o julgamento humano.

Proteção da Reputação da Empresa:

- Estabelecer políticas claras de comunicação para gerenciar conteúdos gerados pela IA.
- Agir rapidamente para corrigir erros ou falhas que possam impactar a confiança de clientes e parceiros.

Monitoramento Contínuo:

Auditorias de Risco: Realizar auditorias regulares para avaliar os riscos associados ao uso de IA e revisar as estratégias de mitigação existentes.
Relatórios de Incidentes: Criar um processo estruturado para relatar e analisar incidentes relacionados ao uso de IA garantindo que lições aprendidas sejam aplicadas.

Capacitação para Gestão de Riscos:

Treinamento: Capacitar os colaboradores para identificar riscos e aplicar medidas de mitigação.

Guias Práticos: Disponibilizar orientações claras sobre como lidar com situações de risco relacionadas ao uso de IA.

Governança de Riscos:

Responsabilidades Definidas: Designar equipes específicas, como o Comitê de Governança de IA e o Departamento de Compliance, para supervisionar e gerenciar riscos.
Revisões Periódicas: Atualizar regularmente as políticas e práticas de mitigação com base em mudanças tecnológicas, legais ou operacionais.

Plano de Resposta a Incidentes:

Ação Rápida: Criar um plano detalhado para responder rapidamente a incidentes de risco, reduzindo danos e corrigindo falhas.
Comunicação Transparente: Informar de forma clara os stakeholders sobre incidentes relevantes, medidas tomadas e ações preventivas futuras.

12 INCIDENTES ÉTICOS DE IA

O uso de sistemas de Inteligência Artificial pode ocasionar incidentes éticos que impactem colaboradores, clientes ou a sociedade. Este capítulo estabelece procedimentos para identificação, resposta e prevenção de incidentes éticos relacionados ao uso de portais de IA baseados em Modelos de Linguagem (LLM) na empresa.

Definição de Incidente Ético de IA:

Consideram-se incidentes éticos de IA as situações onde:

- Sistemas de IA produzem resultados discriminatórios, preconceituosos ou que violem direitos fundamentais
- Decisões automatizadas causem danos injustificados a indivíduos ou grupos,
- Haja uso indevido de dados pessoais em processamentos de IA,
- Conteúdos gerados por IA violem direitos autorais ou propriedade intelectual,
- Sistemas de IA sejam utilizados para desinformação ou manipulação,
- Ocorram falhas de transparência que comprometam a confiança dos usuários.

Classificação de Severidade:

Nível 1 - Baixo:

- Vieses menores em conteúdos gerados
- Falhas pontuais de transparência
- Uso inadequado sem consequências significativas

Nível 2 - Médio:

- Discriminação detectada em processos automatizados,
- Violações de privacidade sem exposição massiva de dados,
- Conteúdos inadequados compartilhados internamente.

Nível 3 - Alto:

- Discriminação sistemática afetando grupos específicos,

- Vazamento de dados pessoais processados por IA,
- Desinformação ou conteúdo prejudicial divulgado publicamente,
- Violações significativas de direitos autorais.

Nível 4 - Crítico:

- Danos massivos à reputação da empresa
- Violações legais com possíveis sanções regulatórias
- Impactos societais negativos significativos
- Comprometimento da segurança de indivíduos.

Procedimentos de Resposta:

Detecção e Reporte:

- Qualquer colaborador deve reportar imediatamente incidentes éticos observados.
- *Canal direto com o Comitê de Governança de IA.*
- Sistema de reporte via e-mail: inteligencia.artificial@provider-it.com.br.
- Monitoramento proativo através de auditorias regulares.

Resposta Imediata:

- Interrupção do sistema/processo causador do incidente (se necessário),
- Ativação da equipe de resposta a incidentes éticos,
- Avaliação preliminar de impactos e severidade,
- Comunicação inicial às partes interessadas.

Investigação:

- Análise detalhada das causas do incidente,
- Identificação de todos os afetados,

- Documentação completa do ocorrido,
- Avaliação de conformidade legal e regulatório.

Correção e Mitigação:

- Implementação de correções nos sistemas afetados,
- Comunicação transparente com usuários impactados,
- Ações de remediação para danos causados,
- Ajustes nos processos para prevenir recorrência.

Equipe de Resposta a Incidentes Éticos

Membros do Comitê de Governança de IA

Prevenção e Aprendizado

Análise Post-Incidente:

- Revisão completa das causas e respostas,
- Identificação de falhas nos controles existentes,
- Recomendações para melhoria dos processos,
- Atualização da política e procedimentos.

Medidas Preventivas:

- Fortalecimento dos controles de qualidade,
- Aprimoramento dos treinamentos,
- Revisão dos sistemas de monitoramento,
- Implementação de salvaguardas adicionais.

Registro e Documentação:

Todos os incidentes éticos de IA devem ser registrados em sistema específico contendo:

- Data, hora e circunstâncias do incidente,

- Classificação de severidade e impactos identificados,
- Ações tomadas e responsáveis,
- Resultados das investigações,
- Medidas preventivas implementadas.

13 RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)

A elaboração e manutenção do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) para projetos envolvendo Inteligência Artificial (IA) é uma etapa imprescindível para garantir a conformidade com a Lei Geral de Proteção de Dados (LGPD) e as melhores práticas internacionais de governança de dados.

Quando o RIPD deve ser elaborado

O RIPD deverá ser obrigatoriamente produzido sempre que os projetos de IA envolverem:

- **Tratamento de dados pessoais sensíveis**, conforme definido pela LGPD;
- **Análise automatizada de dados pessoais** para fins de decisões com impactos significativos sobre os titulares (ex.: automação de crédito, triagem de currículos, avaliações de desempenho);

- **Compartilhamento de dados pessoais com terceiros** ou transferência internacional de dados;
- **Inovações em modelos ou sistemas de IA** que possam aumentar riscos à privacidade ou aos direitos dos titulares;
- Sempre que houver **exigência por parte de autoridades regulatórias** ou solicitação formal da Autoridade Nacional de Proteção de Dados (ANPD).

Em caso de dúvida quanto à obrigatoriedade, a questão deverá ser encaminhada ao Comitê de Governança de IA para deliberação.

Estrutura mínima do RIPD

O RIPD deverá, no mínimo, conter:

- **Descrição detalhada do projeto ou tratamento realizado** (incluindo fluxos de dados pessoais e informações técnicas relevantes);
- **Base legal para o tratamento dos dados** (consentimento, obrigação legal, execução de contratos, legítimo interesse, etc.);
- **Mapeamento dos dados pessoais tratados** (tipos de dados, titulares envolvidos, fontes, volume e finalidade);
- **Análise e classificação dos riscos aos titulares de dados**, com identificação de ameaças e potenciais impactos;
- **Medidas e salvaguardas adotadas para mitigação de riscos**, indicando as soluções técnicas, organizacionais e jurídicas aplicadas (ex.: anonimização, restrição de acesso, revisões humanas, etc.);
- **Planos de resposta a incidentes e monitoramento contínuo dos riscos**;

- **Indicação dos responsáveis técnicos pelo projeto e elaboração do RIPD**, com contatos para esclarecimento de dúvidas;
- **Referências legais e normativas consideradas**;
- **Cronograma de revisão e atualização do próprio relatório**.

Periodicidade de revisão do RIPD

O RIPD deve ser revisado:

- **Anualmente**, nas revisões ordinárias da política de IA;
- **Sempre que houver alteração significativa no projeto**, fluxo de tratamento de dados, base legal, tecnologias utilizadas ou nos riscos identificados;
- **Após ocorrência de incidentes relevantes** envolvendo privacidade ou segurança da informação nos projetos abrangidos.

Responsáveis Técnicos

A elaboração e atualização do RIPD é responsabilidade conjunta:

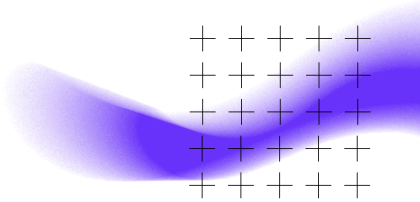
- Do **encarregado de Proteção de Dados (DPO)**;
- Da **área de Governança de IA**;
- Do **departamento Jurídico**;
- Dos **gestores dos projetos de IA envolvidos**, que devem fornecer informações técnicas e operacionais detalhadas.

O Comitê de Governança de IA é o órgão consultivo e deliberativo para casos complexos ou divergentes, garantindo alinhamento com as melhores práticas e requisitos regulatórios.

Disponibilidade e guarda

O RIPD deverá estar à disposição da alta gestão e da ANPD mediante solicitação, respeitando requisitos de confidencialidade e sigilo.

14 DIREITOS DOS USUÁRIOS



O uso de sistemas de Inteligência Artificial (IA), como os portais baseados em Modelos de Linguagem (LLM), deve respeitar os direitos de todos os usuários impactados por essas tecnologias. Este capítulo assegura que os usuários estejam cientes quando estão interagindo com sistemas de IA, e que tenham ferramentas para questionar ou contestar decisões automatizadas que possam afetá-los.

Transparência para os Usuários

A empresa deve monitorar continuamente o uso de IA para identificar potenciais riscos em diferentes áreas. Os principais riscos incluem:

- **Identificação da IA:** Sempre informando claramente quando um sistema de IA está sendo utilizado para gerar respostas, realizar análises ou tomar decisões. O usuário saberá quando está interagindo com uma máquina e não com uma pessoa.

- **Finalidade da IA:** Será explicado de forma simples e acessível o motivo pelo qual a IA está sendo utilizada em cada caso, como:

1. Apoio à tomada de decisões;
2. Automação de processos;
3. Geração de conteúdo.

- **Acesso a Informações:** Será fornecido, quando solicitado, informações básicas sobre como a IA funciona, os dados utilizados e os critérios que influenciam suas decisões, sempre respeitando as normas de proteção de dados.

Direito de Questionar Decisões Automatizadas

Revisão Humana: Os usuários têm o direito de solicitar revisão manual e imparcial de decisões automatizadas.

Processo de Contestação: Disponibilizamos canais claros e acessíveis para que os usuários possam questionar decisões da IA. *inteligencia.artificial@provider-it.com.br*

Correções e Ajustes: Caso um erro seja identificado na decisão automatizada, providenciaremos rapidamente sua correção e comunicaremos o resultado ao usuário.

Direito à Explicação das Decisões Automatizadas

Em consonância com princípios éticos e exigências legais, todo usuário afetado por decisões automatizadas de IA tem direito a:

- Solicitar uma explicação clara, acessível e compreensível sobre os principais critérios, dados e lógica utilizados na decisão automatizada;
- Receber essa explicação em linguagem não técnica, incluindo informações sobre os fatores que mais influenciaram a decisão;
- Ser informado previamente sempre que uma decisão relevante for realizada de forma automatizada, bem como compreender as consequências que tal decisão pode ter sobre seus direitos;
- Saber quando e como pode contestar ou requerer revisão humana dessa decisão.

Privacidade e Proteção de Dados

Controle sobre Dados Pessoais: O usuário será informado sobre quais dados estão sendo utilizados pela IA, podendo solicitar:

- Acesso aos dados processados;
- Retificação ou exclusão de informações incorretas;
- Restrição do uso de dados em situações específicas.

Consentimento: Sempre que necessário, o consentimento do usuário será obtido para o uso de dados pessoais em processos de IA. O consentimento deverá ser livre, informado e revogável.

Comunicação Clara e Simples

Linguagem Acessível: As informações sobre o uso de IA e os direitos dos usuários serão apresentadas em linguagem clara, livre de termos técnicos complicados.

Disponibilidade de Informações: os usuários podem acessar informações sobre seus direitos de forma fácil, solicitando via e-mail para *inteligencia.artificial@provider-it.com.br.*

Inclusão de Usuários no Processo

Feedback dos Usuários: os usuários podem fornecer feedback sobre o uso de IA, apontando preocupações ou sugestões de melhorias através do e-mail: *inteligencia.artificial@provider-it.com.br.*

Participação Ativa: Consideramos a opinião dos usuários ao revisar e ajustar os sistemas de IA, garantindo que eles se sintam ouvidos e valorizados.

15 ATUALIZAÇÃO E REVISÃO DA POLÍTICA

A tecnologia de Inteligência Artificial (IA) está em constante evolução, e a legislação e as melhores práticas também mudam com frequência. Por isso, esta política de utilização de portais de IA baseados em Modelos de Linguagem (LLM) deve ser revisada e atualizada regularmente, garantindo que

continue relevante, eficaz e alinhada aos objetivos da empresa, às leis aplicáveis e às necessidades de nossos colaboradores e clientes.

Periodicidade de Revisão

Revisões Regulares: A política será revisada anualmente para assegurar que está atualizada com:

- Mudanças nas ferramentas e tecnologias de IA utilizadas pela empresa;
- Alterações nas leis e regulamentações aplicáveis, como a LGPD e normas internacionais;
- Melhores práticas do mercado e novos padrões éticos no uso de IA.

Periodicidade: Revisão anual da política

Revisões Adicionais: Revisões extraordinárias poderão ser realizadas a qualquer momento, caso ocorram:

- Introdução de novas ferramentas ou tecnologias de IA na empresa;
- Mudanças significativas na legislação ou nas regulamentações;
- Identificação de falhas ou problemas críticos durante a aplicação da política.

Responsáveis pela Revisão

Diretoria de Inovação
Comitê de Diretoria
Departamento Jurídico

Informação aos Colaboradores

Todas as alterações na política serão comunicadas de forma clara e direta, através dos canais existentes na Provider IT e o documento atualizado sempre está disponível na Intranet.

Registro de Alterações

Emissão da política em 10 fevereiro de 2025

- Responsável: Nedyr Pimenta Filho.

Atualização/ Versão 2 em 30 setembro de 2025

– Responsável: Nedyr Pimenta Filho

Atualização/ Versão 3 em setembro de 2026

– Responsável: Nedyr Pimenta Filho