

POL – 0024 – Política de Proteção do Usuário e Uso Ético da Tecnologia



Histórico de Versões

Data	Versão	Descrição	Autor
27/07/2026	1.0	POL – 0024 Política de Proteção do Usuário e Uso Ético da Tecnologia_V1	Área de Compliance
28/07/2026	2.0	Revisão conforme Parecer Jurídico nº 043/2026 (Vilanova Advocacia & Assessoria Jurídica)	Área de Compliance

Introdução

A Política de Proteção do Usuário e Uso Ético da Tecnologia da Plano Consultoria tem como objetivo estabelecer diretrizes para o desenvolvimento, a contratação e o uso responsável de soluções tecnológicas — incluindo sistemas de inteligência artificial (IA) — de forma a proteger os usuários, garantir transparência, prevenir discriminação e assegurar o uso ético da tecnologia em todas as atividades da organização. Esta política é parte integrante do Programa de Compliance da Plano Consultoria e deve ser interpretada em conjunto com o POL-0010 Política de Proteção de Dados Pessoais e o POL-0021 Política de Segurança da Informação.

Abrangência

Esta política se aplica a todos os colaboradores da Plano Consultoria (incluindo sócios, estatutários, celetistas, estagiários e prestadores de serviços) e terceiros (fornecedores, parceiros de negócio, entre outros) que desenvolvam, operem, contratem ou utilizem soluções tecnológicas em nome da organização ou de seus clientes.

Glossário

Para os fins desta política, aplicam-se as seguintes definições:

- **Inteligência Artificial (IA):** sistema baseado em máquina projetado para operar com níveis variados de autonomia, capaz de gerar saídas como previsões, recomendações ou decisões.
- **IA Generativa:** sistemas de IA capazes de gerar textos, imagens, códigos ou outras mídias em resposta a comandos (prompts).



- **Decisão Automatizada:** decisão tomada unicamente com base no tratamento automatizado de dados, sem envolvimento humano significativo, sujeita às regras do art. 20 da LGPD.
- **Incidente de Inteligência Artificial:** evento em que o comportamento de um sistema de IA cause ou possa causar dano, incluindo anomalias comportamentais sistêmicas, alucinações severas, outputs tóxicos e ataques de injeção de prompt (prompt injection).
- **Desvio de Modelo (Model Drift):** degradação ou variação de performance e de comportamento de modelos ao longo do tempo, inclusive enviesamento temporal, que exige monitoramento contínuo.
- **Supervisão Humana:** capacidade de intervenção, revisão e reversão, por pessoa natural competente, das saídas e decisões produzidas por sistemas automatizados.

1. Referências Legais e Normativas

- POL-0010 Política de Proteção de Dados Pessoais
- POL-0021 Política de Segurança da Informação
- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), em especial o art. 20
- Nota Técnica nº 12/2025 da ANPD – Decisões automatizadas e explicabilidade
- Lei nº 12.965/2014 – Marco Civil da Internet
- Lei nº 8.078/1990 – Código de Defesa do Consumidor
- ISO/IEC 42001 – Sistema de Gestão de Inteligência Artificial
- Regulation (EU) 2024/1689 (EU AI Act) – referência de melhores práticas em abordagem baseada em risco
- NIST AI RMF (NIST.AI.100-1) – Framework de Gestão de Riscos de IA
- Princípios de IA da OCDE e boas práticas internacionais de IA responsável



2. Objetivos

- Proteger os usuários das soluções tecnológicas desenvolvidas, contratadas ou operadas pela organização, assegurando segurança, privacidade e respeito aos seus direitos.
- Garantir transparência sobre o funcionamento das soluções tecnológicas, em especial quando houver uso de inteligência artificial ou decisões automatizadas.
- Prevenir tratamento discriminatório, vieses indevidos e usos abusivos da tecnologia.
- Estabelecer responsabilidades e mecanismos de supervisão para o uso ético da tecnologia.

3. Diretrizes de Proteção do Usuário

- As soluções tecnológicas devem ser concebidas com privacidade e segurança desde a concepção (privacy by design e security by design), em conformidade com a LGPD.
- Os dados pessoais de usuários somente podem ser tratados para finalidades legítimas, específicas e informadas, conforme o POL-0010.
- Os usuários devem ser informados de forma clara e acessível sobre coleta e uso de seus dados, funcionalidades relevantes e canais de suporte e atendimento.
- Em estrita observância ao art. 20 da LGPD e às diretrizes da ANPD (Nota Técnica nº 12/2025), é garantido aos usuários o direito de solicitar informações claras, adequadas e inteligíveis a respeito dos critérios e procedimentos utilizados para a tomada de decisões automatizadas, bem como o direito inalienável de solicitar a revisão humana dessas decisões.
- A organização assegurará mecanismos ágeis de contestação e reparação de eventuais danos causados aos usuários em virtude de falhas, alucinações algorítmicas ou vieses nos sistemas operados, em consonância com a responsabilidade objetiva prevista no Código de Defesa do Consumidor.



- Incidentes que afetem usuários devem ser tratados conforme os procedimentos de resposta a incidentes da organização, com comunicação transparente aos afetados quando cabível. O plano de resposta a incidentes da organização deve ser atualizado para tipificar e mitigar Incidentes de Inteligência Artificial, compreendendo anomalias comportamentais sistêmicas, alucinações severas, outputs tóxicos e ataques de injeção de prompt.

4. Diretrizes de Uso Ético da Tecnologia e de IA

- É vedado o uso de tecnologia para finalidades ilícitas, abusivas, enganosas ou que violem direitos fundamentais.
- A organização adotará uma abordagem baseada em risco para a classificação de sistemas de IA, sujeitando sistemas de alto risco a processos de due diligence, controle humano e auditorias rigorosas prévias à implementação.
- Sistemas de inteligência artificial devem operar sob supervisão humana adequada, sendo vedada a delegação integral de decisões críticas a sistemas automatizados sem possibilidade de revisão humana.
- Quando houver interação de usuários com sistemas de IA ou decisões automatizadas que os afetem, isso deve ser informado de forma transparente.
- Modelos e algoritmos devem ser avaliados quanto a vieses que possam gerar tratamento discriminatório por raça, gênero, idade, deficiência ou qualquer outro atributo protegido, com medidas de mitigação quando identificados riscos. Conforme os padrões do NIST AI RMF, essa avaliação deve ser contínua ao longo do ciclo de vida da solução, visando garantir a confiabilidade e prevenir desvios sistêmicos de comportamento (model drift).
- A contratação de fornecedores de soluções tecnológicas deverá ser precedida de due diligence prévia, estruturada pelo nível de risco. Os instrumentos contratuais devem vedar expressamente o uso de dados pessoais, sensíveis ou confidenciais da organização para o treinamento ou aprimoramento de modelos fundacionais do fornecedor (data scraping/training), salvo autorização explícita.



- Os sistemas de IA devem garantir a rastreabilidade e a manutenção de logs de interações, decisões automatizadas e acessos, respeitando os prazos legais de guarda estipulados pelo Marco Civil da Internet.
- O uso de ferramentas de IA generativa por colaboradores deve observar a confidencialidade das informações de clientes e da organização, sendo vedada a inserção de dados pessoais ou informações sigilosas em ferramentas não homologadas.
- As soluções tecnológicas devem buscar aderência a diretrizes de acessibilidade digital, de modo a não excluir usuários com deficiência.

5. Responsabilidades

- A área de Compliance é responsável por gerenciar, monitorar e atualizar esta política, apoiar a avaliação ética de novas soluções tecnológicas e realizar a auditoria contínua e periódica dos sistemas em produção, zelando pela governança algorítmica.
- As áreas técnicas são responsáveis por aplicar as diretrizes desta política no desenvolvimento, contratação e operação de soluções tecnológicas, e por manter a documentação técnica rigorosamente atualizada, permitindo a transparência e a explicabilidade (Explainable AI – XAI) das operações.
- Todos os colaboradores são responsáveis por utilizar a tecnologia de forma ética e por reportar usos inadequados.

6. Canal de Integridade

O Canal de Integridade é um meio confidencial e seguro para comunicação de dúvidas, sugestões ou relatos de condutas inadequadas relacionadas a esta política. Todas as denúncias são tratadas com sigilo absoluto, sem risco de retaliação.

7. Medidas Disciplinares

Violações à presente política estarão sujeitas a sanções disciplinares previstas na legislação aplicável, assegurados os direitos ao contraditório e à ampla defesa.

8. Vigência e Revisão





Esta política deve ser revisada periodicamente para garantir sua aderência às leis e regulamentos aplicáveis, bem como às necessidades organizacionais. A vigência é imediata a partir de sua publicação.

