



AP.

**GOV
ERN
ANC**
**DE IA E
DADOS
COM ROI
E VALOR
REAL**

**AP Digital
Services**

**GOV
ERN
ANC
DE IA E
DADOS
COM ROI
E VALOR
REAL**

Sobre a AP

Na AP Digital Services, acreditamos que a verdadeira inovação nasce do equilíbrio entre velocidade e responsabilidade. Em um cenário onde a Inteligência Artificial transforma negócios, produtos e relações humanas em ritmo exponencial, governar dados e algoritmos deixou de ser um tema técnico — tornou-se uma questão estratégica e de confiança.

A AP nasceu com a missão de acelerar a transformação digital de forma ética, inteligente e humana, unindo tecnologia, dados e propósito. Atuando ao lado de empresas líderes em setores como energia, agro, consumo e varejo, a AP construiu um portfólio sólido de soluções em IA, Data, Cloud, Agilidade e Experiência do Cliente, sempre com foco em gerar valor mensurável.

Essa experiência prática mostrou que a governança de IA e Dados não é uma barreira à inovação, mas sim o que a torna sustentável. É ela que permite escalar soluções com segurança, garantir a qualidade e a confiabilidade dos dados, proteger a privacidade dos usuários, mitigar vieses, atender à legislação e, principalmente, construir confiança entre pessoas, negócios e tecnologia.

Com este eBook, a AP compartilha o que aprendeu na implantação de frameworks, políticas e práticas reais de governança em empresas de grande porte — traduzindo o tema em ferramentas aplicáveis, modelos de referência e roteiros práticos.

Nosso objetivo é apoiar organizações que desejam inovar com responsabilidade, conectando compliance, dados e IA de forma fluida, integrada e pragmática.

Acreditamos que o futuro pertencerá às empresas que conseguirem governar para evoluir — que enxergam na governança de IA e Dados não um controle, mas uma vantagem competitiva baseada em confiança, transparência e inteligência coletiva.



Índice

Sobre a AP	03
Introdução	05
Fundamentos	06
Arquitetura de governança	08
Gestão de risco de IA	09
Privacidade e LGPD	11
Ética e Segurança	12
Operação	13
GOV-AI Framework	15
Como A AP Ajuda as empresas	17
Sugestões de KPI	18



Introdução — Por que governança de IA e Dados agora?

A popularização de modelos de linguagem, visão computacional e sistemas de recomendação aumentou a velocidade da inovação — e também os riscos associados ao uso de dados e algoritmos. **Sem governança, organizações enfrentam problemas como vieses não intencionais, decisões inexplicáveis, vazamentos de dados, dependência de fornecedores, uso indevido de propriedade intelectual e falta de conformidade regulatória.**

Este e-book traduz boas práticas de governança em um guia prático para equipes técnicas e de negócio. Você encontrará princípios, papéis, processos, controles, métricas e modelos para acelerar com responsabilidade. O foco é pragmático: “o que precisa existir”, “quem faz o quê” e “como medir”.

Resultados esperados ao adotar este guia

- Reduzir risco jurídico, reputacional e operacional.
- Aumentar a confiança em soluções de IA via transparência e controles.
- Padronizar o ciclo de vida de IA (ideação → avaliação → desenvolvimento → validação → aprovação → operação → aposentadoria).
- Conectar compliance e inovação, evitando bloqueios e retrabalho.



Fundamentos — Princípios, papéis e responsabilidades

Princípios orientadores

Legalidade & legitimidade: alinhar-se às leis aplicáveis (ex.: LGPD) e às expectativas de clientes e sociedade.

Transparência & explicabilidade: documentar finalidade, dados, modelo e limitações.

Equidade & não discriminação: avaliar impacto em grupos protegidos e mitigar vieses.

Privacidade por padrão: minimizar coleta, controlar acesso e registrar consentimento quando necessário.
Robustez & segurança: projetar para falhas, ataques e uso indevido.

Responsabilização (accountability): decisões de IA têm donos, logs e trilhas de auditoria.



Fundamentos — Princípios, papéis e responsabilidades

Papéis essenciais

Patrocinador executivo: define ambição, remove bloqueios, aprova políticas.

Conselho de IA & Dados: fórum de decisão sobre risco, priorização e exceções.

CDO / Head de Dados: qualidade, catálogo, linhagem e uso ético de dados.

DPO/Encarregado: orientação sobre LGPD, DPIA e direitos dos titulares.

Owner de Produto de IA: requisitos, riscos, métricas de sucesso e aceite.

Líder de MLOps/LLMOps: plataforma, segurança do modelo e monitoramento.

Engenharia & Ciência de Dados: desenvolvimento, validação e documentação técnica.

Segurança da Informação: controles de acesso, segredos, avaliação de fornecedores.



Arquitetura de governança — Fóruns, políticas e controles

Fóruns e cadência

Conselho de IA & Dados (mensal): aprova políticas, define apetite de risco e acompanha indicadores.

Comitê de Risco de IA (quinzenal): avalia Avaliações de Impacto de IA (AIA) e exceções.

Change Advisory Board de Modelos (semanal): libera versões de modelos e prompts.

Políticas e padrões

Política de Uso Responsável de IA

Política de Dados (classificação, retenção, compartilhamento, anonimização)

Padrão de Documentação (model cards, data sheets, avaliações)

Padrão de Segurança (segredos, dependências, provedores, sandbox)

Controles mínimos por fase

Ideação: triagem de risco, objetivo de negócio, expectativas de desempenho e ética.

Dados: catálogo, base legal, minimização, avaliação de qualidade e representatividade.

Desenvolvimento: versionamento, reprodutibilidade, testes de robustez e de segurança.

Validação: performance, fairness, explicabilidade, privacidade e ataque/red teaming.

Liberação: aprovação do comitê, plano de rollback e proprietário definido.

Operação: monitoramento de drift, incidentes, feedback humano, auditoria periódica.



Gestão de riscos de IA — Avaliação de impacto e controles técnicos

Categorias de risco

Vieses e discriminação(dados históricos, proxies, seleção de variáveis)

Privacidade e confidencialidade (PII, reidentificação, vazamento via prompts)

Segurança e abusos (prompt injection, data poisoning, supply chain de modelos)

Conformidade & propriedade intelectual (origem dos dados, direitos autorais, licenças)

Confiabilidade e robustez (alucinações, drift, generalização)

Sustentabilidade e custo (uso de energia, custo por requisição)

Operacional e terceiros (SLAs, dependência de provedores, continuidade de negócio)

Avaliação de Impacto de IA (AIA)

Uma AIA documenta finalidade, dados, riscos, salvaguardas e plano de mitigação. Use o checklist anexo para padronizar a análise. Registre hipóteses, testes, limites de uso e plano de resposta a incidentes.



Gestão de riscos de IA — Avaliação de impacto e controlos técnicos

Controlos técnicos (exemplos)

Documentação: model cards, datasheets, sistema de rastreio de experimentos.

Privacidade: minimização, anonimização, controle de acesso, logs, retenção.

Segurança: segregação de ambientes, revisão de dependências, proteção de segredos, rate limiting.

Qualidade & fairness: conjuntos de teste estratificados, métricas por subgrupo, testes contrafactuais.

LLMOps: biblioteca de prompts versionada, guardrails, filtro de conteúdo, testes de regressão.



Privacidade & LGPD — Bases legais, DPIA, minimização e retenção

Mapeie dados pessoais: identifique categorias, finalidades e agentes de tratamento.

Defina base legal: consentimento, execução de contrato, legítimo interesse etc.

Implemente DPIA quando necessário: avalie riscos ao titular e salvaguardas.

Minimização & retenção: colete o mínimo necessário e defina prazos claros.

Direitos do titular: acesso, correção, anonimização, portabilidade e eliminação.

Transferências internacionais: avalie requisitos e salvaguardas contratuais.



Ética, segurança e conformidade contínua

Princípios éticos aplicados: justiça, autonomia, não maleficência, beneficência.

Safeguards humanos: revisão humana quando impacto for alto.

Segurança da cadeia de modelos: avaliação de fornecedores, versões e licenças.

Auditoria contínua: revisões periódicas de métricas técnicas e de negócio.



Operação — MLOps/LLMOps, monitoramento e auditoria

Registro de modelos: versões, datasets, hyperparâmetros, objetivos, owners.

Monitoramento: qualidade dos dados, drift, latência, custo, incidentes e SLIs/SLOs.

Gestão de prompts: versionamento, testes A/B, red teaming e políticas de conteúdo.

Planos de contingência: rollback, feature flags, dupla decisão para alto risco.

Auditoria: logs imutáveis, rastreabilidade ponta-a-ponta, revisões trimestrais.



Como a AP Digital Services estrutura a Governança de IA e Dados

Na AP Digital Services, tratamos governança de IA e Dados como um pilar estratégico da transformação digital – não apenas como um requisito de conformidade.

Nosso propósito é acelerar o uso da inteligência artificial de forma responsável, auditável e alinhada ao negócio, garantindo que a inovação ocorra com segurança, explicabilidade e geração de valor mensurável.

Para isso, desenvolvemos o **GOV-AI Framework**, um modelo exclusivo da AP que integra estratégia, governança, operação e gestão da mudança em torno da IA.

O **GOV-AI** foi criado a partir da experiência prática da AP em grandes programas de transformação digital e de dados em empresas como Raízen, Yara, Converse e Vicunha, unindo práticas de Data Governance, AI Ethics, Agile Delivery e Lean Portfolio Management em um único modelo.



O GOV-AI Framework

O framework da AP é composto por cinco dimensões complementares, que estruturam toda a jornada — da estratégia à adoção viva da IA:

1. Estratégia de Valor

Define onde a IA realmente gera impacto.

Através da **Matriz Valor x Complexidade**, a AP ajuda as organizações a priorizar casos de uso de **alto ROI**, equilibrando ambição com maturidade técnica e cultural.

2. Orquestração de VMO

Garante governança executiva e fluidez entre áreas.

Com Value Streams e Scorecards, a AP conecta as iniciativas de IA aos objetivos estratégicos da empresa, alinhando squads, dados e funding sob uma visão de portfólio.



O GOV-AI Framework

3. Governança de IA

Estabelece os princípios, papéis e controles que sustentam a confiança.

Inclui frameworks de LoA (Level of Automation), Explainability e Prompt Hygiene, além de modelos de Avaliação de Impacto de IA (AIA) e políticas de uso responsável.

É aqui que a AP integra ética, LGPD, segurança e auditoria à prática de desenvolvimento.

4. LPM Modular

Transforma a governança em execução ágil e mensurável. Com Funding orientado a valor e guardrails de investimento, o LPM (Lean Portfolio Management) da AP permite evoluir a IA por ondas, com métricas de negócio e aprendizado contínuo.

5. Gestão de Mudança Viva

Assegura adoção real e cultura de IA no dia a dia. A AP mede KPIs de adoção, promove capacitação adaptada por perfil e sustenta uma governança viva — que evolui junto com os times, tecnologias e regulações.



Como a AP ajuda as empresas

A AP atua de ponta a ponta, desde a definição estratégica até a sustentação operacional, com quatro frentes principais:

1. Diagnóstico e estratégia de governança — avaliação de maturidade, roadmap e arquitetura de IA.
2. Implantação do GOV-AI™ Framework — criação dos fóruns, políticas, papéis e processos.
3. Engenharia e MLOps/LLMOps — integração de dados, versionamento de modelos, monitoramento e explainability.
4. Gestão de mudança e cultura de IA — engajamento, treinamentos e governança viva.

Com esse modelo, ajudamos nossos clientes a governar com inteligência, inovar com segurança e crescer com confiança.

KPIs Sugeridos

KPIs_Sugeridos

Indicador	Fórmula (sugestão)	Meta inicial	Frequência	Responsável	Fonte
Modelos com AIA aprovada (%)	<i>Modelos com AIA / Modelos em produção</i>	95%	Mensal	Conselho IA & Dados	Registro/AIA
Incidentes por 1.000 req	<i>Incidentes / 1.000 requisições</i>	≤ 0,5	Mensal	MLOps	Logs
Tempo de aprovação (dias)	<i>Data liberação - data submissão</i>	≤ 10	Mensal	Comitê	Workflow
Desvio de performance (%)	<i> prod - val / val</i>	≤ 5%	Semana	DS/MLOps	Métricas
Solicitações de titular atendidas (%)	<i>Atendidas / Total</i>	100%	Mensal	DPO	Canal LGPD



AP Digital Services