☆ Plano Centralizado de Uso de IA — Manager Systems

CNPJ 80.750.714/0001-56 • ~50 colaboradores • 6 lideranças • ISO/IEC 27001 • ISO/IEC 27701 • ISO/IEC 20000-1 • ISO 9001

Alternar edição | Salvar local | Carregar | Exportar JSON | Importar JSON | Imprimir / PDF

Use o botão “Alternar edição” ou Ctrl + E

Sumário

1. Sumário executivo
2. Diagnóstico do estado atual
3. Estado-alvo e princípios
4. Arquitetura de referência
5. Políticas e SOPs
6. Controles e trilhas de auditoria
7. Riscos, DPIA, ROPA
8. Onboarding e catálogos
9. Métricas e OKRs
10. Roadmap 90 dias
11. Evidências para auditoria

A. Política corporativa (1 pág.)

B. Matriz RACI

C. Fluxo BPMN

D. Checklist fornecedores & DPA

E. Modelo DPIA

F. Classificação de dados

G. Playbook incidentes

H. Mapa LGPD ↔ ISO

Contexto

Empresa: MANAGER CONSULTORIA EM INFORMATICA (CNPJ 80.750.714/0001-56). **Site:** managersystems.com.br.

Perfil: ~50 colaboradores, 6 lideranças funcionais, software house com certificações ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 20000-1 e ISO 9001.

Problema: uso disperso de ferramentas de IA por contas individuais, risco de não conformidade com LGPD e com requisitos das ISOs.

Objetivo: projetar uma *solução centralizada de IA* com governança, segurança, conformidade e custo previsível.

1) Sumário executivo

- Adotar plataforma de IA corporativa com SSO, RBAC, DLP/CASB e *gateway de prompts*.
- Padronizar políticas, classificação de dados e revisão humana por risco.
- Implantar trilhas de auditoria e mapeamento LGPD↔ISO.
- Reduzir *shadow AI* em 90 dias. Custo sob controle via limites e orçamentos.

2) Diagnóstico do estado atual

▶ **Inventário de usos e dados**

▶ **Riscos prioritários**

3) Estado-alvo e princípios

- Privacidade por padrão e por design.
- Menor privilégio e segregação de funções.
- Observabilidade, mensuração e melhoria contínua.

4) Arquitetura de referência

Descreva até 3 opções com prós/contr as e TCO resumido. Inclua SSO, RBAC, DLP/CASB, gateway de prompts, logging, retenção, criptografia e KMS.

Opção	Descrição	Prós	Contras	TCO (resumo)
SaaS corporativo	Plataforma gerenciada com SSO e controles nativos.	Rápida adoção; menor esforço operacional.	Menor controle de dados; dependência de fornecedor.	Assinaturas por usuário + add-ons de segurança.
On-prem/privado	Modelos hospedados em VPC; KMS próprio.	Maior controle; residência de dados.	Capex/opex altos; equipe especializada.	Infra + licenças + MLOps.

Opção	Descrição	Prós	Contras	TCO (resumo)
Híbrido	SaaS para uso geral; privado para dados sensíveis.	Equilíbrio custo/risco; flexível.	Complexidade de governança.	Tiers de uso + custos de trânsito.

5) Conjunto de políticas e SOPs

- Política de Uso Aceitável de IA.
- Classificação e tratamento de dados.
- Gestão de fornecedores e DPAs.
- Engenharia de prompts segura e revisão humana.
- Treinamento e conscientização.
- Resposta a incidentes.

6) Controles e trilhas de auditoria

Mapeie ISO/IEC 27001 (ex.: A.5, A.8, A.12, A.18), ISO/IEC 27701, ISO/IEC 20000-1 e ISO 9001. Registre referência a artigos da LGPD.

Requisito	Referência	Evidência	Responsável
Gestão de ativos	ISO 27001 A.5/A.8	Inventário de ferramentas/contas	Segurança da Informação
Logs e monitoramento	ISO 27001 A.12	SIEM + retenção	Infra/SecOps
Privacidade	ISO 27701	DPIA/ROPA	DPO

7) Avaliação de riscos, DPIA e ROPA

- DPIA simplificada por caso de uso de IA.
- Registro de Operações de Tratamento (ROPA).
- Minimização, anonimização e bases legais.

8) Onboarding, aprovação e catálogos

- Workflow de aprovação de casos de uso e modelos.
- Tiers de acesso por sensibilidade de dados.
- Limites de gasto, orçamentos e *rate limits*.
- Integração com ticketing e SIEM existentes.

9) Métricas e OKRs

Métrica	Definição	Meta 90d
Aderência	% de uso via plataforma oficial	≥ 85%
Shadow AI	Ferramentas não autorizadas	−80%
Custos	Gasto por equipe	≤ orçamento mensal
Risco	Incidentes e quase-incidentes	0 crítico

10) Roadmap de 90 dias (6 marcos)

1. **S0** Semana 0–2: Inventário, risk triage, política 1 pág.
2. **S1** Semana 2–4: Escolha arquitetural e SSO/RBAC básicos.
3. **S2** Semana 4–6: DLP/CASB, gateway de prompts, logging.
4. **S3** Semana 6–8: DPIA/ROPA, treinamento, catálogo inicial.
5. **S4** Semana 8–10: Integração ticketing/SIEM, limites e orçamentos.
6. **S5** Semana 10–12: Auditoria interna, ajustes finais e handover.

11) Pacote de evidências para auditoria

- Templates, checklists e registros versionados.
- Relatórios de log, aprovações, DPIAs e ROPAs.
- Mapa de rastreabilidade LGPD↔ISO.

A) Política corporativa de IA (1 página)

Escopo: uso de IA por colaboradores, terceiros e sistemas. **Princípios:** legalidade, finalidade, necessidade, transparência, segurança e responsabilização. **Obrigatório:** uso via plataforma oficial; proibição de dados sensíveis sem autorização; revisão humana por risco; registro de prompts e saídas quando aplicável.

B) Matriz RACI

Atividade	R	A	C	I
Definir arquitetura	Gerência de Produto	Diretoria	Segurança, Infra	Suporte, Jurídico
Políticas e SOPs	Segurança	DPO	Jurídico	Times
Operação plataforma IA	Suporte	Infra	Segurança	Todos

C) Fluxo BPMN do ciclo de vida

Representação textual simplificada:

```
[Solicitação de caso de uso] → [Classificação de dados] → [DPIA] →
[Aprovação DPO/Segurança] → [Implementação no gateway] → [Monitoração/Logs] →
[Revisão periódica] → [Encerramento/Archival]
```

D) Checklist de fornecedores & critérios de DPA

Item	Critério	Status
Residência de dados	País/região e cláusulas contratuais	
Criptografia	Em trânsito e em repouso; KMS	
Logs e retenção	SIEM, retenção mínima 12 meses	
DPA	Assinado; sub-processadores listados	

E) Modelo de DPIA simplificada

Campo	Descrição
Finalidade	Objetivo do tratamento
Base legal	LGPD art. 7º/11
Dados pessoais	Tipos e fonte
Riscos	Impactos e probabilidade
Mitigações	Controles aplicados

F) Classificação de dados e redaction/anonymização

Classe	Exemplos	Regras de uso em IA
Pública	Site, materiais de marketing	Permitido
Interna	Documentação técnica interna	Permitido com gateway
Confidencial	Clientes, contratos	Anonimizar/mascarar
Sensível	Dados pessoais sensíveis	Proibido sem exceção formal

G) Playbook de resposta a incidentes de IA

1. Detecção e triagem.
2. Containment: revogar chaves, bloquear contas, isolar gateway.
3. Eradicação e análise de causa raiz.
4. Notificação conforme LGPD e contratos.
5. Lições aprendidas e reforço de controles.

H) Mapa de Conformidade LGPD ↔ ISO

LGPD	ISO 27001	ISO 27701	Evidência no plano
Art. 6º princípios	A.5, A.8	6, 7	Políticas e classificação
Art. 7º bases legais	A.18	7.4	DPIA/ROPA
Art. 46 segurança	A.12	8	Criptografia, logs, DLP

Critérios de sucesso

- Solução auditável.
- Redução de ferramentas não autorizadas.
- Trilhas de auditoria completas.
- Adequação LGPD e aderência às ISOs citadas.
- Custo sob controle em 3 meses.

Documento interativo local. Edição salva no navegador. Nenhum dado é enviado para servidores.