POLÍTICA SEI Nº 25855698/2025 - CAJ.DICAF.GTI.CSIC

Joinville, 23 de junho de 2025.

POLÍTICA DE INTELIGÊNCIA ARTIFICIAL

1. INTRODUÇÃO

A adoção de Inteligência Artificial (IA) no mundo corporativo tem se intensificado significativamente. Desde os primeiros modelos matemáticos apresentados em 1943, a IA evoluiu gradualmente até o início dos anos 2000, com avanços em algoritmos de aprendizado estatístico, aprendizado de máquina e reconhecimento de voz. A partir de 2012, os progressos tornaram-se mais notáveis, especialmente com o reconhecimento de imagens e o aprendizado profundo (Deep Learning). Em 2020, iniciou-se uma fase de impacto massivo com o surgimento da IA Generativa, cujas ferramentas (como o ChatGPT) popularizaram-se globalmente devido à acessibilidade.

Nos últimos cinco anos, a evolução acelerada da IA tem demandado que empresas de diversos setores adotem essas tecnologias para melhorar eficiência, qualidade, redução de custos e automação de processos.

A CAJ reconhece os benefícios da IA, mas também os desafios inerentes a essa inovação. Esta Política de Inteligência Artificial (PIA) estabelece diretrizes para proteger ativos, mitigar riscos e garantir conformidade com leis e regulamentações, alinhando-se a:

I - ISO/IEC 42001:2023 que representa a primeira norma internacional específica para governança de IA.

II - NIST AI RMF (Risk Management Framework) que representa o modelo para gerenciamento de riscos de IA.

III - Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018 e o Marco Civil da Internet, Lei nº 12.965/2014.

IV - Guia de IA Generativa no Serviço Público elaborado pela Secretaria de Governo Digital (SGD) e pelo Serviço Federal de Processamento de Dados (SERPRO).

V - Políticas internas de segurança e proteção de dados pessoais.

2. OBJETIVOS

Esta política tem como objetivo estabelecer diretrizes para a gestão de Inteligência Artificial, permitindo que os colaboradores da CAJ, que se utilizam de recursos de TI, adotem comportamentos alinhados às necessidades do negócio, às oportunidades de inovação, à mitigação de riscos cibernéticos e à conformidade com requisitos legais e regulatórios.

Esta política estabelece diretrizes para o uso ético, seguro e inovador de Inteligência Artificial (IA) na CAJ, alinhando-se com as melhores práticas de governança, proteção de dados (LGPD), segurança da informação e incentivo à inovação responsável.

3. APLICAÇÕES DA PIA

As diretrizes estabelecidas nesta política devem ser seguidas por todos os colaboradores, administradores e terceiros, aplicando-se à informação em meio digital, bem como a qualquer sistema ou processo que utilize Inteligência Artificial.

Para fins de interpretação da presente política, utilizam-se os conceitos que constam no art. 5º da Lei 13.709/2018.

A PIA aplica-se a todos os ambientes de TI, administrativos ou operacionais, com destaque a:

I -Ambientes de IA: Desenvolvimento, treinamento e implantação de modelos (ex.: machine learning, IA generativa).

II - Sistemas críticos: Processos automatizados com impacto em clientes, operações ou conformidade (ex.: análise de crédito, RH).

III - Dados: Uso de dados pessoais, sensíveis ou estratégicos em sistemas de IA (conforme LGPD e ISO 42001).

4. PRINCÍPIOS DA PIA

A implementação e a utilização da Inteligência Artificial (IA) devem observar os seguintes princípios:

I - Legalidade e Conformidade: Todas as soluções de IA devem respeitar as leis aplicáveis, especialmente a LGPD, leis trabalhistas e regulamentos setoriais.

II - Transparência: Decisões tomadas por IA devem ser explicáveis, com registro de processos e responsáveis definidos.

III - Segurança e Privacidade: Dados utilizados em modelos de IA devem ser protegidos contra vazamentos, acessos não autorizados e vieses discriminatórios.

IV - Inovação Responsável: A empresa incentivará o uso de IA para otimização de processos, desde que alinhada a critérios de ética e riscos controlados.

5. REQUISITOS DA PIA

Para garantir o uso ético, seguro e alinhado aos objetivos estratégicos da empresa, todas as atividades inerentes ao cumprimento da PIA deverão observar os requisitos de:

I - Comunicação e Adesão: Ser formalmente comunicada a todos os colaboradores e terceiros que utilizem ou desenvolvam soluções de IA na empresa, aplicando-se a sistemas internos e externos.

II - Governança e Responsabilidade: A gestão da IA será responsabilidade da Comissão de Segurança da Informação e Comunicação, composto por um grupo multidisciplinar, que será encarregado por:

a - Implementar, revisar e supervisionar a aplicação da PIA.

b - Avaliar riscos de vieses, privacidade e segurança em projetos de IA.

c - Aprovar o uso de ferramentas de IA generativa (ex.: ChatGPT, Copilot).

III - Revisão e Atualização: A PIA e suas normas complementares deverão ser revisadas e atualizadas periodicamente ou de forma antecipada nos casos de mudanças regulatórias ou eventos relevantes, conforme análise e decisão da Comissão de Segurança.

IV - Treinamento e Conscientização: Todos os colaboradores e terceiros que interajam com sistemas de IA receberão treinamento sobre:

a - Ética no uso de IA.

b - Limitações e riscos de ferramentas generativas.

c - Proteção de dados pessoais (LGPD) e sigilo corporativo.

V - Contratação de Terceiros: Prestadores de serviço que desenvolvam ou acessem sistemas de IA da empresa deverão:

a - Assinar termos de confidencialidade e conformidade com a PIA.

b - Submeter-se a auditorias de segurança (ex.: verificação de vazamento de dados em modelos treinados).

VI - Gestão de Incidentes: Qualquer incidente que IA (ex. vazamento de dados, decisão discriminatória) deve ser comunicado imediatamente à Gerência de Tecnologia da Informação, que, se necessário, encaminhará o caso ao Comissão de Segurança da Informação e Comunicação para análise e medidas corretivas.

VII - Integração em Projetos: Requisitos de segurança e ética em IA devem ser incluídos no escopo de projetos desde o levantamento inicial, com: documentação de fontes de dados e validação humana para decisões de alto impacto.

VIII - Controles de Segurança: Serão implementados controles técnicos para sistemas de IA, como:

a - Auditoria: Logs de uso de ferramentas generativas.

b - Acesso restrito: Dados de treinamento e modelos críticos.

c - Ambientes isolados: Segregação entre desenvolvimento e produção (ex.: sandbox para testes de IA).

IX - Isenção de Responsabilidade: A CAJ não se responsabiliza pelo uso indevido da IA, entretanto, diante da sua reponsabilidade perante terceiros (art. 37, §6º da Constituição Federal), poderá responsabilizar internamente o colaborador por:

a - Uso indevido de ferramentas de IA (ex.: inserção de dados confidenciais em ChatGPT).

b - Decisões tomadas por sistemas de IA sem supervisão humana exigida pela PIA.

X - Padronização de Ferramentas: A CAJ, mediante instrução normativa, especificará as soluções internas ou externas de IA a serem utilizadas no âmbito corporativo, visando:

a - Redução do número de soluções: Manter o mínimo necessário de plataformas para atender às demandas corporativas, priorizando versatilidade e integração.

b - Padronização técnica: Garantir compatibilidade com a infraestrutura existente e políticas de segurança.

c - Otimização de custos: Evitar redundâncias e negociar condições comerciais centralizadas.

XI - Proibições:

a - Uso de versões gratuitas ou versões de amostras antes da aquisição (trial) de ferramentas não homologadas.

b - Assinar ou publicar conteúdos gerados por IA sem revisão humana.

XII - Critérios para Adoção de Novas Ferramentas: Qualquer nova solução de IA, que não esteja contemplada no catálogo de ferramentas homologadas, deverá passar por:

a - Análise de Necessidade: Justificativa técnica e de negócios que comprove a insuficiência das ferramentas já existentes.

b - Avaliação de Riscos: A CAJ, mediante instrução normativa, especificará os critérios de classificação e níveis de riscos da IA, adequado às exigências conforme o potencial impacto dos sistemas.

c - Aprovação da Comissão de Segurança da Informação e Comunicação.

XIII - Catálogo de Ferramentas Homologadas de IA: A Gerência de Tecnologia da Informação manterá um registro centralizado com:

a - Ferramentas em uso, classificadas por criticidade (alto/médio/baixo risco), conforme estabelecido em instrução normativa.

b - Casos de uso permitidos e restrições (ex.: proibição para dados pessoais).

XIV - Geração de Conteúdo com IA: Todo conteúdo institucional gerado por IA deve passar por revisão humana antes da publicação. Ferramentas de IA não podem ser usadas para produzir documentos legais ou respostas oficiais sem validação prévia do autor.

XV - Declaração de Uso de IA: Todo conteúdo institucional gerado com auxílio de IA, que envolva a emissão de documentos de cunho decisório ou que impacte economicamente nos negócios da CAJ devem declarar o uso da ferramenta, incluindo a identificação do responsável pela validação humana.

6. DIRETRIZES DA PIA

O uso de ferramentas de IA em processos de trabalho no âmbito da CAJ deverá observar as seguintes diretrizes:

I - Para Uso de Ferramentas Internas de IA: Nos processos que envolvam o tratamento de dados pessoais, dados sensíveis ou estratégicos (ex. dados de clientes, colaboradores ou projetos ainda não divulgados), deve-se priorizar o uso de soluções de IA instaladas em infraestrutura CAJ que permitam total gerenciamento pela equipe interna da Gerência de Tecnologia da Informação.

II - Para Uso de Ferramentas Externas de IA: Todas as ferramentas de IA externas (aplicações de IA instaladas fora da infraestrutura de TI gerenciada pela CAJ) devem ser previamente aprovadas pelo Comissão de Segurança da Informação e Comunicação, considerando:

a - Critérios de segurança: Avaliação de vazamento de dados (ex.: políticas de retenção do fornecedor).

b - Conformidade legal: Alinhamento com LGPD e regulamentos setoriais.

c - Casos de uso permitidos: Definição clara de aplicações autorizadas conforme disposto no item 5, inciso X desta política.

d - Uso de credenciais corporativas: Só podem ser usadas em ferramentas adquiridas e gerenciadas pela Gerência de Tecnologia da Informação.

7. USUÁRIOS DE INFORMÁTICA

São reconhecidos como usuários da infraestrutura de TI da CAJ todos os colaboradores, administradores, profissionais autônomos, temporários ou prestadores de serviços que obtiverem a devida aprovação do gestor responsável e da área de TI para o acesso aos recursos computacionais da empresa, inclusive recursos de IA.

8. DAS RESPONSABILIDADES ESPECÍFICAS

São responsabilidades:

8.1 – DA ALTA DIREÇÃO

I - Aprovar recursos para projetos de IA e assegurar alinhamento com a estratégia da empresa.
II - Aprovar a Política de IA (PIA).

8.2 - DOS USUÁRIOS DE INFORMÁTICA

I - Respeitar e cumprir integralmente a Política de Inteligência Artificial (PIA) da CAJ, bem como as normas e procedimentos relacionados.

II - Não inserir dados confidenciais ou dados pessoais em ferramentas de IA generativa não homologadas ou não autorizadas.

III - Reportar vieses ou erros em decisões automatizadas.

IV - Buscar continuamente conhecimento e capacitação para o uso correto e seguro dos recursos de IA da CAJ, em conformidade com as normas internas.

V - Relatar imediatamente à área de TI qualquer incidente ou ameaça aos recursos de IA, bem como falhas de segurança, vulnerabilidades, mau funcionamento de sistemas, viés discriminatório ou qualquer outro risco relacionado a IA.

VI - Assegurar que as informações e dados fornecidos para treinamento dos sistemas de IA sejam dados confiáveis, corretos e livres de vieses discriminatórios.

VII - Assumir total responsabilidade por qualquer prejuízo ou dano causado à CAJ ou a terceiros decorrente do não cumprimento das diretrizes e normas estabelecidas nesta PIA.

VIII - O colaborador que utilizar ferramentas de IA para gerar ou editar conteúdos é o responsável final pela:

a - Revisão crítica do material antes de assinar, publicar ou compartilhar.

b - Verificação de precisão, adequação ao contexto empresarial e conformidade com políticas internas.

c - Citação de fontes quando aplicável (ex.: dados estatísticos, referências técnicas).

8.3 – DOS GESTORES DE PESSOAS E/OU PROCESSOS

I - Exercer uma postura exemplar em relação ao uso de Inteligência Artificial na CAJ, servindo como modelo de conduta para os colaboradores sob sua gestão e assegurando o cumprimento das diretrizes da PIA.

II - Incluir a responsabilidade pelo cumprimento da PIA da CAJ durante a fase de admissão de pessoal, prestação de serviços ou parcerias, garantindo que todos os envolvidos estejam cientes de suas obrigações em relação ao uso de IA na CAJ.

III - Deflagrar processo administrativo sancionatório à luz da Política de Consequências e Medidas Disciplinares, sempre que houver descumprimento de algum dispositivo desta política.

IV - Implementar e adaptar processos sob sua responsabilidade para assegurar conformidade com a PIA, promovendo boas práticas de governança de IA e uso equilibrado das tecnologias na CAJ.

8.4 – DA ÁREA DE TECNOLOGIA DA INFORMAÇÃO

I - Documentar fontes de dados.

II - Implementar controles de acesso a modelos e dados de treinamento.

III - Auditar sistemas de IA contra ataques.

IV - Manter um registro de todos os sistemas de IA em uso, com classificação de risco.

V - Garantir que os modelos utilizados sejam transparentes, auditáveis e que permita a explicabilidade das decisões tomadas pela IA.

VI - Realizar testes suficientes para redução de risco de erros e falhas com sistemas de IA, inclusive com atenção aos conjuntos de dados para treinamento.

VII - Garantir a implementação de recursos que assegurem segurança nos sistemas de IA nos ambientes de TI (Tecnologia da Informação) e TO (Tecnologia Operacional).

VIII - Homologar as ferramentas de IA passível de utilização.

8.5 – DA COMISSÃO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

I - Propor investimentos relacionados a implantação de sistemas de inteligência artificial.

II - Propor alterações nas versões da PIA e revisar continuamente as normas complementares, considerando a evolução das tecnologias, os requisitos de conformidade e a necessidade de integração com as operações de TI e TO da CAJ.

III - Aprovar propostas de utilização de ferramentas de IA não previstas no catálogo de ferramentas homologadas.

9 - DAS DISPOSIÇÕES FINAIS

O uso ético e responsável da Inteligência Artificial é parte integrante da cultura de inovação da CAJ. Qualquer violação desta política configura não apenas um risco operacional, mas uma transgressão aos princípios de governança, transparência e proteção de dados que regem nossa instituição.

Na hipótese de violação desta PIA ou das normas complementares, a Diretoria, com o apoio das áreas de Segurança da Informação, Conformidade e Gestão de Pessoas, determinarão as sanções administrativas que serão aplicadas, sendo que:

I - Para os colaboradores, pode acarretar na aplicação de advertência e/ou suspensão ou desligamento formal conforme previsto na Política de Consequências e Medidas Disciplinares.

II - Para os prestadores de serviços, pode acarretar na aplicação rescisória imediata do respectivo contrato estabelecido violado.

Esta política foi aprovada pelo Conselho de Administração, entra em vigor na data de sua publicação e terá validade indeterminada, podendo ser revisada a qualquer momento.

Nota: Este conteúdo foi produzido com apoio de IA e revisado pelo Comissão de Segurança da Informação em 08/12/2025