POLÍTICA DE GOVERNANÇA DE INTELIGÊNCIA ARTIFICIAL

Aprovação	Data	Ata
Diretoria Colegiada	15/04/2026	15/2026

SUMÁRIO

Centro de Informática e Automação do Estado de Santa Catarina S.A. - CIASC
Rua Murilo Andriani, 327 - Bairro Itacorubi - Florianópolis, SC - CEP 88034-902
www.ciasc.sc.gov.br

1.Introdução

Esta política visa definir diretrizes claras e objetivas para o uso responsável e ético da Inteligência Artificial (IA) nas diversas áreas do Centro de Informática e Automação de Santa Catarina (CIASC). O objetivo é estabelecer, de forma multidisciplinar, a direção da Governança de IA, respeitando a dignidade humana e os direitos fundamentais, alinhado aos direcionadores estratégicos da empresa. Desta forma, possibilita que o CIASC seja reconhecido como uma empresa que considera valores éticos e sociais ao desenvolver ou utilizar soluções de Inteligência Artificial de forma responsável.

1.1. Escopo

Esta política se aplica a todos os empregados, servidores, estagiários, bolsistas, prestadores de serviço e parceiros envolvidos nas atividades da empresa que utilizem, desenvolvam ou interajam com ferramentas, sistemas ou agentes de Inteligência Artificial no exercício de suas funções em dispositivos institucionais.

1.2. Determinações

1. Manter o compromisso com a proteção de dados pessoais e a privacidade, a segurança da informação e a Governança de Dados, bem como com os valores corporativos.
2. Manter o compromisso com todos os requisitos regulatórios aplicáveis.
3. Quaisquer contratações de serviços ou desenvolvedores externos pelo CIASC deverão considerar os critérios aderentes aos termos desta Política.
4. Quaisquer contratações de soluções de IA de terceiros pelo CIASC deverão considerar os critérios aderentes aos termos desta Política.
5. O uso de dados pessoais deve ser autorizado pelo controlador dos dados.

1.3. Objetivos

As metas centrais desta política são:

- Orientar o uso ético, seguro e responsável de ferramentas de IA, alinhando a inovação tecnológica aos valores institucionais.

Centro de Informática e Automação do Estado de Santa Catarina S.A. - CIASC
Rua Murilo Andriani, 327 - Bairro Itacorubi - Florianópolis, SC - CEP 88034-902
www.ciasc.sc.gov.br

- Proteger os dados sensíveis, pessoais e confidenciais da empresa, de seus clientes e dos cidadãos contra vazamentos, acessos não autorizados e usos indevidos.
- Mitigar riscos inerentes à tecnologia, como vieses algorítmicos, geração de informações incorretas ("alucinações"), violações de propriedade intelectual e ataques cibernéticos.
- Promover a conformidade com a legislação vigente, em especial a Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018) e a Lei Estadual Nº 19.450, de 5 de Setembro de 2025.

Para alcançar esses objetivos, a política se fundamenta em princípios que devem nortear todas as iniciativas de IA na empresa.

2.Princípios Fundamentais

Todas as iniciativas de Inteligência Artificial no âmbito desta empresa devem ser regidas por princípios alinhados aos preceitos da administração pública e aos direitos fundamentais dos cidadãos. Estes princípios servem como alicerce para todas as diretrizes e procedimentos detalhados neste documento.

2.1. Legalidade

Toda e qualquer aplicação de IA deve estar em total conformidade com a legislação brasileira vigente, com atenção especial à Lei Geral de Proteção de Dados (LGPD), garantindo que o tratamento de dados pessoais respeite os direitos dos titulares e os requisitos legais.

2.2. Impessoalidade e Equidade

As decisões e os resultados gerados com o auxílio de sistemas de IA devem ser imparciais, baseados em critérios objetivos e livres de vieses discriminatórios. É mandatório identificar e mitigar preconceitos que possam levar a um tratamento injusto ou desigualitário.

2.3. Moralidade e Ética

O uso da IA deve respeitar os direitos humanos, os valores democráticos e os princípios éticos universais. A tecnologia deve ser empregada para promover a dignidade, a

Centro de Informática e Automação do Estado de Santa Catarina S.A. - CIASC
Rua Murilo Andriani, 327 - Bairro Itacorubi - Florianópolis, SC - CEP 88034-902
www.ciasc.sc.gov.br

autonomia e a justiça social, evitando aplicações que possam manipular comportamentos de forma prejudicial ou explorar vulnerabilidades humanas.

2.4. Publicidade e Transparência

Os processos que utilizam IA devem ser transparentes, permitindo auditoria e, quando possível, explicabilidade (XAI - Explainable AI). Deve-se comunicar de forma clara como os sistemas de IA são utilizados, quais dados são processados e como as decisões são tomadas.

2.5. Eficiência

A IA deve ser utilizada como uma ferramenta para otimizar processos, automatizar tarefas repetitivas e aprimorar a qualidade dos serviços. Contudo, a busca pela eficiência não prescinde da revisão humana, que é indispensável para garantir a qualidade, a correção e a adequação dos resultados gerados.

2.6. Responsabilidade e Prestação de Contas *(Accountability)*

A responsabilidade final pelas decisões e pelos resultados gerados com o auxílio da IA é sempre humana. Devem ser estabelecidos mecanismos claros para atribuir responsabilidades, reparar eventuais danos e garantir a supervisão humana em todas as etapas.

2.7. Segurança e Proteção de Dados

A proteção de dados pessoais e sensíveis é prioritária em todas as fases do ciclo de vida das aplicações de IA. Devem ser implementadas medidas robustas para salvaguardar as informações contra acessos não autorizados, vazamentos, ataques cibernéticos e outros usos indevidos.

2.8. Design Centrado no Ser Humano

Os sistemas de IA devem ser projetados para complementar as capacidades humanas e priorizar o bem-estar de cidadãos e colaboradores. A tecnologia deve aprimorar a

Centro de Informática e Automação do Estado de Santa Catarina S.A. - CIASC
Rua Murilo Andriani, 327 - Bairro Itacorubi - Florianópolis, SC - CEP 88034-902
www.ciasc.sc.gov.br

experiência do usuário e servir como uma ferramenta de apoio, em vez de substituir indiscriminadamente a supervisão e o julgamento humano.

3.Diretrizes para o Uso de Ferramentas de IA

É fundamental estabelecer uma distinção clara entre o uso de plataformas de IA internas (aprovadas pela empresa) e plataformas externas (não aprovadas). A segurança, a privacidade e a soberania dos dados institucionais são a prioridade máxima e orientam as seguintes diretrizes.

É obrigatório o uso exclusivo de soluções de IA institucionalizadas pela empresa, sempre que houver o manuseio de:

- Dados internos (emails, projetos, códigos fonte, documentos sigilosos);
- Dados financeiros;
- Dados sensíveis;
- Dados pessoais;
- Dados confidenciais.

O uso de plataformas de IA generativa não institucionalizadas é restrito e só deve ocorrer para tarefas que envolvam exclusivamente dados públicos. Nestes casos, as seguintes proibições devem ser rigorosamente observadas:

- **Proibido:** Inserir dados pessoais de cidadãos, servidores ou terceiros, em conformidade com a LGPD;
- **Proibido:** Inserir informações sigilosas, confidenciais ou de acesso restrito da empresa, como detalhes de projetos, dados financeiros, informações contratuais ou estratégias internas;
- **Proibido:** Inserir qualquer trecho de código-fonte, scripts, senhas, chaves de API, credenciais de acesso, ou quaisquer outros artefatos pertencentes ou cedidos à empresa, ou que estejam sob tutela da mesma, a exemplo de artefatos de clientes;
- **Proibido:** Utilizar endereços de e-mail, credenciais de login ou números de telefone institucionais para criar contas ou acessar essas plataformas. O objetivo é desvincular o uso pessoal ou pontual da relação de trabalho com a instituição;
- **Proibido:** Desenvolver ou implementar soluções voltadas ao público externo que dependam dessas plataformas sem a avaliação de riscos e a aprovação explícita da empresa.

Centro de Informática e Automação do Estado de Santa Catarina S.A. - CIASC
Rua Murilo Andriani, 327 - Bairro Itacorubi - Florianópolis, SC - CEP 88034-902
www.ciasc.sc.gov.br

4.Responsabilidades e Boas Práticas

Embora a Inteligência Artificial seja uma ferramenta robusta, a responsabilidade por seu uso adequado e pelos resultados gerados recai inteiramente sobre o usuário.

4.1. Revisão Humana Obrigatória

Todo conteúdo, código, análise ou decisão gerada por uma ferramenta de IA deve ser obrigatoriamente validado, revisado e corrigido pelo profissional com atribuição pelo uso oficial do conteúdo inserido na solução antes de qualquer uso oficial.

4.2. Validação de Informações e “Alucinações”

As ferramentas de IA generativa podem produzir "alucinações", ou seja, informações factualmente incorretas, inventadas ou sem fonte confiável, embora apresentadas de forma convincente. É dever do usuário sempre verificar fatos, dados, citações e referências em fontes primárias e confiáveis antes de utilizar qualquer informação gerada.

4.3. Segurança de Dados

Reitera-se a proibição absoluta de inserir dados pessoais, sensíveis ou confidenciais em ferramentas de IA externas não aprovadas pela empresa. Todos os usuários devem seguir as normas de segurança da informação da empresa e os preceitos da LGPD para proteger os dados sob sua responsabilidade.

4.4. Propriedade Intelectual

É proibido utilizar resultados gerados por IA que contenham material suspeito de violar direitos autorais ou de propriedade intelectual de terceiros. Os usuários devem ter cautela para não reproduzir textos, imagens ou códigos protegidos sem a devida autorização.

4.5. Mitigação de Vieses

Os usuários devem avaliar criticamente o conteúdo gerado pela IA para garantir que não haja a perpetuação de vieses, estereótipos ou qualquer forma de linguagem discriminatória

Centro de Informática e Automação do Estado de Santa Catarina S.A. - CIASC
Rua Murilo Andriani, 327 - Bairro Itacorubi - Florianópolis, SC - CEP 88034-902
www.ciasc.sc.gov.br

com base em raça, cor, religião, sexo, nacionalidade ou qualquer outra característica protegida por lei.

5.Disposições Finais

O cumprimento desta política é mandatório e essencial para garantir a segurança jurídica, a integridade operacional e a reputação da empresa na era da Inteligência Artificial.

5.1. Capacitação e Conscientização

A empresa promoverá treinamentos contínuos para todos os colaboradores. A capacitação abordará não apenas o uso eficaz da IA, mas também a mitigação de riscos, com módulos específicos sobre:

- **Identificação de vieses:** Treinamento prático para que os usuários possam analisar criticamente os resultados da IA.
- **Validação de "alucinações":** Métodos para verificação de fatos e fontes, garantindo a integridade da informação.
- **Engenharia de prompt para segurança:** Formulação de instruções que exijam saídas de código seguras (com validação de entrada e tratamento de erros) e que minimizem a exposição de dados.

5.2. Revisão da Política

Esta política tem caráter dinâmico e será revisada sempre que avanços tecnológicos significativos, novos marcos regulatórios ou a identificação de novos vetores de risco exigem uma atualização imediata para garantir sua relevância e eficácia contínuas.

A compreensão comum dos termos utilizados é fundamental para a correta aplicação desta política.

Centro de Informática e Automação do Estado de Santa Catarina S.A. - CIASC
Rua Murilo Andriani, 327 - Bairro Itacorubi - Florianópolis, SC - CEP 88034-902
www.ciasc.sc.gov.br

Anexo A: Exemplos de Casos de Uso por Vertical

Para ilustrar como as soluções de IA podem ser aplicadas de forma prática e segura nas diferentes verticais do CIASC, apresentamos a seguir alguns exemplos de casos de uso. Estes exemplos não são exaustivos, mas servem como um guia para inspirar a inovação responsável.

Desenvolvimento de Software

- **Geração de Código e Testes Unitários:** Utilizar agentes de IA para gerar trechos de código, scripts e testes unitários, acelerando o ciclo de desenvolvimento. **Diretriz chave:** Todo código gerado deve ser revisado e validado por um desenvolvedor sênior antes de ser integrado ao projeto.
- **Refatoração e Otimização de Código:** Empregar agentes de IA para analisar o código existente e sugerir melhorias de performance, legibilidade e segurança. **Diretriz chave:** As sugestões de refatoração devem ser avaliadas criticamente para garantir que não introduzam novos bugs e vulnerabilidades.
- **Análise de Vulnerabilidades:** Utilizar agentes de IA para identificar potenciais vulnerabilidades de segurança no código, complementando as ferramentas de análise estática (SAST) e dinâmica (DAST). **Diretriz chave:** Os alertas de segurança gerados pela IA devem ser investigados e validados por um especialista em segurança da informação.

.

Infraestrutura e Data Center

- **Automação de Tarefas de Rotina:** Utilizar agentes de IA para automatizar tarefas como provisionamento de máquinas virtuais, gerenciamento de backups e aplicação de patches de segurança. **Diretriz chave:** A automação deve ser implementada com mecanismos de supervisão humana e pontos de verificação para evitar falhas em cascata.
- **Análise Preditiva de Falhas:** Empregar agentes de IA para analisar logs e métricas de desempenho de servidores e sistemas de armazenamento, prevendo falhas de hardware e evitando interrupções no serviço. **Diretriz chave:** Os alertas preditivos devem ser correlacionados com outras fontes de informação e validados por um analista de infraestrutura antes de qualquer ação de manutenção.

Centro de Informática e Automação do Estado de Santa Catarina S.A. - CIASC
Rua Murilo Andriani, 327 - Bairro Itacorubi - Florianópolis, SC - CEP 88034-902
www.ciasc.sc.gov.br

- **Otimização de Recursos:** Utilizar agentes de IA para analisar o consumo de recursos (CPU, memória, armazenamento) e sugerir otimizações para reduzir custos e melhorar a eficiência energética do data center. **Diretriz chave:** As recomendações de otimização devem ser implementadas de forma gradual e monitorada para garantir a estabilidade dos sistemas.

.

Redes

- **Detecção de Anomalias de Tráfego:** Utilizar agentes de IA para monitorar o tráfego de rede em tempo real e detectar anomalias que possam indicar ataques cibernéticos ou problemas de desempenho. **Diretriz chave:** Os alertas de anomalia devem ser investigados por um analista de redes para determinar a causa raiz e tomar as medidas corretivas adequadas.
- **Gerenciamento de Configurações:** Empregar agentes de IA para gerar e validar configurações de roteadores, switches e firewalls, reduzindo o risco de erros humanos e garantindo a conformidade com as políticas de segurança. **Diretriz chave:** As configurações geradas pela IA devem ser testadas em ambiente de homologação antes de serem aplicadas em produção.
- **Análise de Logs de Segurança:** Utilizar agentes de IA para analisar logs de firewalls, sistemas de detecção de intrusão (IDS) e outros dispositivos de segurança, identificando padrões de ataque e gerando relatórios de segurança. **Diretriz chave:** Os relatórios gerados pela IA devem ser revisados por um especialista em segurança para extrair insights acionáveis e aprimorar as defesas da rede.

.

Data Lake e IA

- **Qualidade e Limpeza de Dados:** Utilizar agentes de IA para automatizar o processo de limpeza e enriquecimento de dados no Data Lake, garantindo a qualidade e a consistência das informações. **Diretriz chave:** Os processos de limpeza de dados devem ser configurados com regras claras e supervisionados por um engenheiro de dados para evitar a perda ou a corrupção de informações importantes.
- **Análise Exploratória de Dados:** Empregar agentes de IA para realizar análises exploratórias em grandes volumes de dados, identificando padrões, tendências e correlações que possam gerar insights de negócio. **Diretriz chave:** Os insights gerados pela IA devem ser validados por um cientista de dados e contextualizados com o conhecimento de negócio para garantir sua relevância e aplicabilidade.
- **Desenvolvimento e Monitoramento de Modelos:** Utilizar agentes de IA para acelerar o desenvolvimento de modelos de machine learning, automatizando tarefas como seleção de algoritmos, ajuste de hiperparâmetros e monitoramento de

Centro de Informática e Automação do Estado de Santa Catarina S.A. - CIASC
Rua Murilo Andriani, 327 - Bairro Itacorubi - Florianópolis, SC - CEP 88034-902
www.ciasc.sc.gov.br

desempenho. **Diretriz chave:** Os modelos desenvolvidos com o auxílio da IA devem ser rigorosamente testados e validados em relação a métricas de acurácia, justiça e robustez antes de serem implantados em produção.

Centro de Informática e Automação do Estado de Santa Catarina S.A. - CIASC
Rua Murilo Andriani, 327 - Bairro Itacorubi - Florianópolis, SC - CEP 88034-902
www.ciasc.sc.gov.br

Assinaturas do documento

Código para verificação: **FF0R608L**

Este documento foi assinado digitalmente pelos seguintes signatários nas datas indicadas:

GUSTAVO MADEIRA DA SILVEIRA (CPF: 806.XXX.630-XX) em 10/05/2026 às 09:23:59
Emitido por: "SGP-e", emitido em 13/07/2018 - 14:02:49 e válido até 13/07/2118 - 14:02:49.
(Assinatura do sistema)

Para verificar a autenticidade desta cópia, acesse o link https://portal.sgpe.sea.sc.gov.br/portal-externo/conferencia-documento/Q0lBU0NfMjIwOV8wMDAwMTIzNV8xMjQ5XzIwMjVfRkYwUjYwOEw= ou o site https://portal.sgpe.sea.sc.gov.br/portal-externo e informe o processo **CIASC 00001235/2025** e o código **FF0R608L** ou aponte a câmera para o QR Code presente nesta página para realizar a conferência.