POLÍTICA DE GESTÃO DE INTELIGÊNCIA ARTIFICIAL DO CEPEL

Versão 1.0

de 11/07/2025

Área responsável pela emissão:

Departamento Jurídico e Compliance (DJC) do Centro de Pesquisas de Energia Elétrica – CEPEL.

Aprovação:

Resolução nº 089.28.2025, emitida na 28ª Reunião da Diretoria Executiva do CEPEL, realizada em 11/07/2025.

Repositório:

Todas as Políticas do CEPEL podem ser encontradas na *Homepage* e na *Intranet* do CEPEL.

Direitos de autor e confidencialidade:

Histórico de Edições:

Versão	Aprovação	Principais Alterações
1.0	11/07/2025	Não se aplica

Sumário

1. Objetivo

Orientar o desenvolvimento, a implementação, o uso e o monitoramento de tecnologias de Inteligência Artificial (IA) no Centro, garantindo a segurança, a ética e a conformidade legal e assegurando que a IA seja desenvolvida e implementada de maneira a respeitar os direitos humanos, promover a justiça social e seguir diretrizes sólidas.

2. Aplicação

Esta Política deve ser observada por todos os profissionais que atuam no CEPEL, pelos membros da Assembleia Geral, do Conselho Deliberativo, do Conselho Fiscal, e da Diretoria Executiva, pelos empregados, prestadores de serviço, bolsistas, estagiários e terceiros, além de quaisquer parceiros de negócio, fornecedores, empresas prestadoras de serviço e colaboradores de parceiros comerciais e *joint ventures*.

3. Conceitos

3.1. Ativo de Informação

Dados, informações e seus meios de armazenamento, transmissão e processamento, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e os recursos humanos que a eles têm acesso.

3.2. Colaborador

Diretores, conselheiros, empregados, contratados, prestadores de serviço, estagiários, bolsistas e jovens aprendizes que atuem no CEPEL.

3.3. Criptografia

Forma de codificar uma informação de maneira que apenas usuários autorizados tenham acesso à informação original.

3.4. Equipamentos de TI

Recursos que processam, armazenam e/ou transmitem informações, tais como aplicações, sistemas de informação e de acesso, estações de trabalho, notebooks, monitores, teclados, mouse, servidores de rede, equipamentos de conectividade e infraestrutura, equipamentos de videoconferência, chips, celulares, tablets e/ou qualquer dispositivos móveis que venham acessar a rede sem fio ou rede estruturada.

3.5. Fallback

Termo usado para descrever uma estratégia ou mecanismo de reserva que entra em ação quando o sistema principal falha ou não consegue completar sua função.

3.6. Incidentes de Segurança da Informação

Qualquer evento adverso, confirmado ou sob suspeita, que afete a proteção dos sistemas de informação e que comprometa ou tenha potencial para comprometer a segurança da informação.

3.7. Informação

Dados, processados ou não, que possam ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato

3.8. IA

Inteligência Artificial.

3.9. Gestor da Informação

Gestores das áreas funcionais do CEPEL responsáveis pela classificação de um conjunto específico de informações, determinando os acessos e os requerimentos de proteção.

3.10. Risco de Segurança da Informação

Possibilidade de que eventos não desejados ocorram com as informações ou com os sistemas de informação.

3.11. Segurança da Informação (SI)

Ações que objetivam viabilizar e assegurar a disponibilidade, integridade e confidencialidade da informação.

3.12. Usuário

Pessoa física, ou responsável por conta de serviço, habilitada para acessar os ativos de informação do CEPEL

4. Referências

- Lei nº 8.078 de 11 de setembro de 1990: Código de Defesa do Consumidor;
- Lei nº 9.296 de 1996: Interceptação das comunicações telefônicas;
- Lei nº 12.737 de 30 de novembro de 2012: Tipificação de delitos informáticos;
- Lei nº 12.965, de 23 de abril de 2014: Marco Civil da Internet;
- Lei nº 13.709, de 14 de agosto de 2018: Lei Geral de Proteção de Dados Pessoais (LGPD);
- Estatuto Social do CEPEL;
- Código de Conduta do CEPEL;
- Política de Segurança da Informação;
- Política de Proteção a Dados Pessoais e Privacidade do CEPEL.

5. Princípios

5.1. Garantia de que o desenvolvimento e o uso da IA estejam em sintonia com os direitos fundamentais, promovendo justiça, inclusão e respeito aos princípios éticos, como a dignidade humana, a transparência e a responsabilidade.

5.2. Garantia de identificação, monitoramento e mitigação de riscos associados ao uso da IA incluindo discriminação algorítmica, violações de privacidade e concentrações indevidas de poder, que possam resultar em impactos negativos à sociedade.

5.3. Garantia de uso da IA para o bem comum, incentivando sua aplicação na resolução de desafios sociais, no fortalecimento de soluções sustentáveis e no desenvolvimento de iniciativas que beneficiem a sociedade como um todo.

6. Diretrizes

6.1. Transparência

6.1.1. O CEPEL deve garantir que as decisões e processos envolvendo IA sejam compreensíveis e passíveis de explicação, fornecendo informações claras sobre os critérios adotados na tomada de decisões e implementando técnicas eficazes para identificar e remover vieses nos dados utilizados.

6.1.2. O CEPEL deve manter documentação detalhada e atualizada sobre a coleta, o uso e a proteção, tanto na implementação de projetos piloto de IA voltados à solução de problemas reais do Centro, quanto na integração das soluções de IA aos processos e sistemas existentes. Tais documentos precisam conter, de forma precisa, parâmetros de explicabilidade de coleta de dados e dos resultados obtidos por algoritmos, envolvendo dados pessoais, oriundos do direito do indivíduo de obter acesso de forma clara, adequada e ostensiva sobre a forma e a duração do tratamento de seus dados (art. 9º, II da LGPD).

6.1.3. O CEPEL deve garantir que a transparência não seja vista, apenas, como uma obrigação ética, mas também como uma estratégia eficaz para aumentar a satisfação e a lealdade dos usuários.

6.2. Ética

6.2.1. O CEPEL deve assegurar que o uso de IA esteja alinhado com os valores e princípios éticos da Instituição, por meio de avaliações de impacto ético desde a concepção até a implementação das soluções de IA para garantir os cinco principais princípios que são:

- Proteções contra discriminação algorítmica, que significa garantir que os algoritmos não perpetuem desigualdades, em especial aquelas que afetam grupos vulneráveis. Para tanto, é essencial realizar avaliações de impacto e revisões constantes dos dados utilizados para treiná-los;
- Sistemas seguros e eficazes;
- Privacidade dos dados;
- Alternativas humanas, consideração e fallback;

- Aviso e explicação.

6.3. Responsabilidade

6.3.1. O CEPEL deve implementar uma série de medidas para garantir a responsabilidade no uso de IA, incluindo, mas não se limitando a:

- Implementar um sistema de auditoria que registre todas as decisões automatizadas tomadas pela IA, incluindo as justificativas para a aprovação ou rejeição emitidas. Esses registros deverão ser armazenados de maneira segura e acessível para revisões futuras.
- Estabelecer um canal transparente para que os clientes possam contestar decisões que considerem injustas ou incorretas. Quando um cliente solicitar uma revisão, uma equipe especializada analisará o caso e verificará os dados que alimentaram o algoritmo, corrigindo qualquer erro ou viés identificado no processo.
- Os Colaboradores do CEPEL devem receber treinamento regular sobre o uso responsável da IA, enfatizando a importância de entender o funcionamento do sistema e os potenciais impactos sociais de suas decisões, criando, assim, uma cultura de responsabilidade em toda a instituição.

6.4. Conformidade Legal

6.4.1. O CEPEL deve observar integralmente a legislação e as normas regulamentares aplicáveis ao uso de IA, assegurando que o uso de dados esteja em conformidade com a Lei Geral de Proteção de Dados (LGPD) e outras regulamentações aplicáveis.

6.4.2. O CEPEL deve garantir que os sistemas do Centro sejam desenvolvidos de modo a proteger a privacidade dos usuários em interações que possam envolver o compartilhamento de dados pessoais no *prompt.*

6.5. Segurança

6.5.1. O CEPEL deve proteger os dados pessoais e deve garantir a segurança cibernética, em todas as aplicações de IA, utilizando dados relevantes, de alta qualidade, mas com o mínimo necessário de volume para treinamento da IA e obtenção do resultado do processamento.

6.5.2. O CEPEL deve implementar controles de acesso rigorosos para garantir que apenas pessoas autorizadas possam acessar os dados.

6.5.3. O CEPEL deve possuir sistemas de Inteligência Artificial (IA) seguros e resilientes a ataques cibernéticos e outras ameaças, por meio da implementação de medidas de segurança robustas e a realização de testes regulares para garantir que a IA funcione conforme o esperado, mesmo em condições adversas.

6.6. Monitoramento e Auditoria

6.6.1. O CEPEL deve garantir que as soluções de IA sejam desenvolvidas e utilizadas de maneira ética e responsável, fortalecendo a confiança das partes interessadas e mitigando riscos potenciais, por meio das seguintes práticas:

- Implementação de mecanismos para monitorar continuamente o desempenho e o impacto das soluções de IA;

- Desenvolvimento de Normas / Procedimentos para monitoramento contínuo e revisão periódica dos sistemas de IA e da eficácia da Política;
- Realização de auditorias regulares para garantir a conformidade com as Políticas relacionadas à segurança e privacidade, padrões éticos e regulatórios;
- Avaliação de riscos antes da implementação de qualquer solução de IA; e
- Criação de um conselho de revisão para o recebimento de feedback regular dos colaboradores.

6.7. Fallback

6.7.1. O CEPEL deve garantir que os fallbacks em IA sejam implementados para garantir que os sistemas possam lidar com falhas ou incertezas de maneira robusta e eficaz. Sua importância pode ser resumida em:

- Resiliência: Melhora a resiliência do sistema, garantindo que ele possa continuar funcionando, mesmo quando partes dele falham.
- Experiência do Usuário: Fornece uma experiência mais fluida e menos frustrante para os usuários, minimizando interrupções.
- Segurança: No contexto de segurança, fallbacks podem ajudar a manter a integridade e a confidencialidade dos dados, mesmo em caso de falhas.

6.8. Educação e Treinamento

6.8.1. O CEPEL deve treinar os colaboradores para lidar com questões éticas e entender a importância da responsabilidade social, além das melhores práticas de segurança e de privacidade de dados, seguindo os seguintes pontos:

- Conscientizar com exemplos práticos de como a IA pode ser aplicada nas tarefas diárias e nos processos do Centro, abordando os dilemas éticos associados ao uso de IA, como viés e transparência;
- Ensinar as melhores práticas para garantir o uso ético e responsável da IA, incluindo a conformidade com regulamentos como a LGPD;
- Demonstrar as ferramentas e plataformas específicas de IA que serão usadas pelo Centro, como softwares de análise de dados, chatbots etc;
- Oferecer sessões práticas, onde os colaboradores possam experimentar e se familiarizar com as ferramentas de IA; e
- Garantir que os colaboradores estejam bem-preparados para usar a IA de maneira eficaz e segura em suas funções diárias.

7. Responsabilidades

7.1. Diretoria Executiva

- Aprovar o texto base da Política de Gestão de Inteligência Artificial e apoiar sua efetiva implementação.
- Aprovar os documentos normativos derivados que permitam sua implementação.

- Determinar, uma vez aprovadas no nível hierárquico competente, a ampla divulgação das Políticas, disponibilizando-as na homepage do CEPEL, na intranet e no Gerenciador Eletrônico de Documentos (GED).

7.2. Diretorias

- Incentivar, apoiar e revisar a utilização da IA, no seu âmbito de atuação.
- Supervisionar o uso responsável da IA dentro do CEPEL, assegurando que todas as práticas e iniciativas estejam em conformidade com os padrões éticos e regulatórios estabelecidos.

7.3. Departamento Jurídico e Compliance (DJC)

- Elaborar o texto base das Políticas, a partir de informações técnicas, dados, instruções existentes ou boas práticas observadas no ambiente técnico e/ou corporativo interno e externo.
- Atuar com as áreas gestoras desta Política.
- Monitorar a atualização desta Política no CEPEL.

7.4. Departamentos de Tecnologia da Informação (DTI)

- Assegurar que a IA seja desenvolvida, implementada e utilizada de maneira a minimizar riscos, proteger dados sensíveis e garantir que as decisões automatizadas respeitem os direitos e a privacidade de indivíduos e organizações.
- Implementar controles apropriados para proteger o acesso e o uso da IA em conformidade com esta Política.
- Desenvolver a estratégia de segurança da informação para o CEPEL.

7.5. Gestores das áreas do CEPEL

- Implementar e monitorar o uso responsável da Inteligência Artificial (IA) dentro da Instituição, garantindo que a IA seja utilizada de forma ética, segura e eficiente nos processos operacionais.
- Supervisionar o impacto da IA em suas áreas de atuação, promovendo a conformidade com as Políticas internas e as leis aplicáveis.

7.6. Colaboradores do CEPEL

- Cumprir esta Política e os demais instrumentos regulamentares relacionados à mesma, por meio do uso de forma responsável, profissional, ética e legal das informações corporativas, respeitando os direitos e as permissões de uso concedidas para a utilização de IA.

8. Disposições Gerais

8.1. As diretrizes aqui estabelecidas devem nortear a atuação de todos os colaboradores e, destacadamente, do Departamento de Tecnologia e Informação e do Comitê de Tecnologia da Informação, contribuindo para uma visão única e integrada.

8.2. O CEPEL deve adequar seus documentos normativos e os controles que se fizerem necessários em consonância com o estabelecido nesta Política, no prazo máximo de 180 dias a partir da aprovação pela Diretoria Executiva do Centro.

8.3. Deve ser assegurado pelo CEPEL que esta Política e seus documentos normativos complementares, sejam amplamente divulgadas aos seus colaboradores, visando a sua disponibilidade para todos que se relacionam com a organização e que, direta ou indiretamente, são impactados.

8.4. Esta Política pode ser desdobrada em documentos normativos internos específicos, sempre alinhados aos princípios e diretrizes aqui estabelecidos.

8.5. Esta Política, e demais instrumentos regulamentares subordinados a ela, devem ser atualizados sempre que houver necessidade, visando garantir que os requisitos técnicos e legais de segurança implementados estejam sendo cumpridos, atualizados e em conformidade com a legislação vigente e alinhados às diretrizes que conduzem o desenvolvimento dos nossos negócios, presentes no nosso planejamento estratégico.