POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS E PRIVACIDADE DO CEPEL

Versão 2.0

de 25/02/2026

Área responsável pela emissão:

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

Aprovação:

Resolução da 07ª Reunião, de 25/02/2026, item 028.07.2026, da Diretoria Executiva do CEPEL.

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	26/10/2020	Não se aplica
2.0	25/02/2026	Inclusão / revisão de Conceitos, Diretrizes e referências

Sumário

1. Objetivo

Estabelecer diretrizes e orientações para o tratamento de dados pessoais, com o objetivo de proteger a privacidade de colaboradores, parceiros, clientes ou fornecedores, visando à gestão de dados pessoais e à gestão de incidentes de Segurança da Informação no ambiente convencional ou de tecnologia do CEPEL.

2. Aplicação

Esta Política deve ser observada por todos os colaboradores 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 e estagiários, além de quaisquer parceiros de negócio, fornecedores, empresas prestadoras de serviço e colaboradores de parceiros comerciais e *joint ventures*.

3. Conceitos

3.1. Anonimização

Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

3.2. Agência Nacional de Proteção de Dados (ANPD)

Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD).

3.3. Coleta Mínima

Conceito derivado do princípio da finalidade, que define que a coleta de dados só pode ser realizada com finalidade específica e esta deve ser informada aos titulares previamente. Desse princípio, resulta o da minimização da coleta, ou seja, a coleta se restringe aos dados necessários para atingir ao fim específico.

3.4. Controlador

Pessoa natural ou jurídica, de direito público ou privado, que tem competência para tomar decisões referentes ao tratamento de dados pessoais.

3.5. Cookies

São arquivos de dados gerados por um *site* durante a navegação na *internet*, transferidos para o computador ou outro aparelho eletrônico do usuário, registrados e gravados pelo navegador utilizado. Esses arquivos possuem dados que servem para identificação do usuário, para a personalização da página de acordo com as preferências demonstradas pelo usuário durante sua visita ao *site*, e até mesmo para facilitar a navegação entre as páginas em um mesmo *site*.

3.6. Dado anonimizado

Dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

3.7. Dado pessoal

Informação relacionada à pessoa natural identificada ou identificável, que a identifique ou possa identificar, tais como nome, números, códigos de identificação, telefones, endereços.

3.8. Dado pessoal sensível

Dado cujo tratamento pode ensejar a discriminação do seu titular. Diz respeito a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

3.9. Encarregado pelo Tratamento dos Dados Pessoais (*Data Protection Officer* – DPO)

Profissional indicado pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Agência Nacional de Proteção de Dados (ANPD).

3.10. Operador

Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

3.11. Privacidade desde a concepção (*Privacy by Design*)

Metodologia na qual a proteção de dados pessoais é pensada desde a concepção de sistemas, práticas comerciais, projetos, produtos ou qualquer outra solução que envolva o manuseio de dados pessoais.

3.12. Registro de Tratamento de Dados (RTD)

Formulário que o controlador e o operador devem manter com o registro das operações de tratamento de dados pessoais que realizarem, especialmente no caso de tratamento baseado no legítimo interesse.

3.13. Relatório de impacto à proteção de dados pessoais (RPID) (*Data Protection Impact Assessment*)

Documentação do controlador que contém o detalhamento de todos os processos de tratamento pelos quais os dados pessoais passam durante o seu ciclo de vida na operação, assim como as bases legais necessárias e as medidas de segurança adotadas no tratamento desses dados, bem como as medidas, salvaguardas e mecanismos de mitigação de risco.

3.14. Titular de dados pessoais

Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

3.15. Transferência internacional de dados

Transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

3.16. Tratamento de dados pessoais

Toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle de informação, modificação, comunicação, transferência, difusão ou extração.

4. Referências

- Lei nº. 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD);
- Lei nº 13.853, de 8 de julho de 2019 - Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências;
- Lei nº. 12.965/2014 - Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet).;
- Decreto n.º 8.771, de 11 de maio de 2016 – Regulamenta a Lei n.º 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações.
- Decreto nº. 9.637/2018 - Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação;
- Estatuto Social do CEPEL;
- Código de Conduta do CEPEL; e
- Política de Segurança da Informação.

5. Princípios

5.1. Finalidade

Realização do tratamento de dados para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

5.2. Adequação

Compatibilidade do tratamento de dados com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

5.3. Necessidade

Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados informadas.

5.4. Qualidade dos Dados

Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

5.5. Transparência

Garantia aos titulares de dados, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e seus respectivos agentes de tratamento, observados os segredos comercial e industrial.

5.6. Segurança

Utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

5.7. Prevenção

Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

5.8. Livre Acesso

Garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

5.9. Não Discriminação

Impossibilidade de realização do tratamento de dados para fins discriminatórios ilícitos ou abusivos.

6. Diretrizes

6.1. Público-alvo

6.1.1. Esta política deve ser aplicada a todos os colaboradores do CEPEL que realizem atividades que envolvam, de forma direta ou indireta, tratamento de dados pessoais.

6.2. Base legal de tratamento de dados

6.2.1. O tratamento de dados pessoais, ou seja, a realização de coleta, acesso, exclusão, edição, ou qualquer outra operação, somente deve ser realizada dentro de uma das bases legais dispostas na Lei Geral de Proteção de Dados Pessoais (LGPD).

6.2.2. Quando o tratamento de dados pessoais tiver como base o legítimo interesse do controlador/operador, este deverá ser acompanhado de um Relatório de Impacto à Proteção de Dados Pessoais – RIPD (*Data Protection Impacta Assessment* - DPIA).

6.3. Coleta mínima de dados e Consentimento

6.3.1. Os processos que envolvam coleta de dados pessoais devem ser ajustados pelo CEPEL com base no conceito de coleta mínima, com finalidades específicas e obtenção do respectivo consentimento, quando couber.

6.4. Consentimento

6.4.1. No momento da coleta, o titular do dado pessoal deve consentir e ser informado de forma clara e explícita sobre a finalidade, a natureza obrigatória ou facultativa do fornecimento, e sobre as consequências da negativa em fornecê-los. O consentimento poderá ainda ser renovado periodicamente e pode ser revogado a qualquer momento, a pedido do titular.

6.5. Gestão de instrumentos contratuais

6.5.1. Os contratos, convênios e demais instrumentos contratuais relacionados a atividades que envolvam tratamento de dados pessoais, devem prever de forma explícita a responsabilidade do correto tratamento de dados por parte de terceiros, bem como garantir a realização de diligências, com previsão de "direito de regresso" do CEPEL em caso de descumprimento da outra parte.

6.6. Gestão de Incidentes

6.6.1. Deverão ser elaborados pelo CEPEL os procedimentos e planos de resposta a incidentes relacionados à privacidade de titulares de dados, a partir de critérios de controle e registro de vazamentos, bem como comunicação aos envolvidos e à Agência Nacional de Proteção a Dados (ANPD).

6.7. Segurança da Informação

6.7.1. As medidas contra vazamento de dados, bem como investimentos em ferramentas e processos de segurança, devem priorizar a proteção de dados pessoais sensíveis, bem como daqueles dados cujo tratamento utiliza, como base legal, o legítimo interesse do controlador.

6.8. Inventário de dados

6.8.1. O inventário de dados pessoais deverá ser mantido permanentemente atualizado, identificando os tipos documentais e as informações que os contêm, visando seu tratamento (incluindo eventual obtenção de consentimento do titular) em acordo com a respectiva base legal, com adoção do conceito de coleta mínima.

6.8.2. O inventário deve ser realizado considerando o contexto de produção ou acúmulo dos documentos e informações.

6.9. Governança de privacidade e dados pessoais

6.9.1. O Programa de Governança em Privacidade do CEPEL deve ter por objetivo o estabelecimento de relação de confiança com os titulares de dados pessoais, por meio de atuação transparente, com monitoramento contínuo e avaliações periódicas integradas a sua estrutura geral de governança e devem ter processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais.

6.10. Capacitação e conscientização

6.10.1. Devem ser promovidas, de forma continuada, ações educacionais, de capacitação, sensibilização e conscientização sobre as melhores práticas acerca do tratamento de dados pessoais no CEPEL bem como a ampla divulgação dos riscos e ameaças da não utilização dessas práticas.

6.11. Navegação na web e cookies

6.11.1. O CEPEL pode, mediante mecanismos de obtenção e revogação de consentimento dos usuários, utilizar-se de cookies e tecnologias semelhantes, visando compreender melhor o comportamento dos usuários, informando quais páginas e conteúdo dos sites foram visitados, contribuindo para a eficácia na distribuição de conteúdo.

6.12. Sistemas de Tecnologia de Informação

6.12.1. Os sistemas de Tecnologia da Informação de suporte a processos e atividades que envolvam tratamento de dados pessoais que forem desenvolvidos ou adquiridos pelo CEPEL devem seguir o conceito de *Privacy by Design*.

6.13. Metodologia de Projetos

6.13.1. A metodologia de gestão de projetos do CEPEL deverá considerar o conceito de *Privacy by Design*, garantindo a aderência à LGPD e a esta Política desde a concepção / aquisição de qualquer nova solução (processo, sistema, produto etc.), prevenindo a criação de iniciativas não conformes.

6.14. Atendimento a Requerimentos do Titular de Dados Pessoais (Data Subject Request – DSR)

6.14.1. O CEPEL deve desenvolver mecanismos para atendimento aos direitos dos titulares de dados previstos na LGPD, com destaque para confirmação e acesso a dados, retificação, restrição de tratamento, revogação de consentimento e exclusão de dados, sempre observando os impactos e os direitos do controlador.

6.14.2. O recebimento dos requerimentos de titulares de dados pessoais será preferencialmente realizado pelo Encarregado pelo Tratamento de Dados Pessoais (DPO) do CEPEL, por meio do e-mail dpo@cepel.br, podendo, alternativamente, ocorrer pelo Canal de Ouvidoria, disponibilizado na *homepage* do CEPEL.

7. Responsabilidades

7.1. Diretoria Executiva

- Aprovar o texto base desta Política e garantir sua implementação.
- Deliberar sobre as diretrizes estratégicas de segurança da informação, norteando todo o processo no CEPEL.

7.2. Departamento Jurídico e Compliance (DJC)

- Elaborar o texto base desta Política, a partir de informações técnicas, dados, instruções existentes ou boas práticas observadas no ambiente técnico e/ou corporativo interno e externo.
- Monitorar permanentemente a atualização dessa Política.

7.3. Departamento de Tecnologia da Informação / Segurança da Informação

- Apoiar o encarregado pelo tratamento de dados pessoais em suas atribuições.
- Coordenar e apoiar metodologicamente a realização do inventário de dados pessoais, a partir de informações fornecidas pelas áreas do Centro.
- Elaborar procedimentos para tratamento e resposta a incidentes relativos à privacidade de titulares de dados.

7.4. Encarregado pelo Tratamento dos Dados Pessoais

- Atuar na interlocução junto aos titulares de dados e junto à Agência Nacional de Proteção de Dados (ANPD), incluindo reporte de incidentes.
- Orientar os colaboradores e terceiros a respeito das práticas relativas à proteção de dados pessoais e privacidade.

7.5. Departamento de Gestão de Pessoas (DGP)

- Promover ações de treinamento e desenvolvimento referentes à proteção de dados pessoais e privacidade, incluindo aspectos técnicos, normativos e comportamentais.

7.6. Departamentos

- Zelar pelas informações produzidas e recebidas por sua equipe em razão das atividades da área, realizando e monitorando o inventário de dados sob sua responsabilidade, sua adequada classificação e autorização de acesso, bem como o mapeamento, implantação e operacionalização de seus controles, fazendo cumprir as diretrizes desta Política.

7.7. Departamento de Comunicação e Marketing (DCM)

- Disponibilizar esta Política na *intranet* e na *homepage* do CEPEL.

7.8. Colaboradores e Parceiros do CEPEL

- Cumprir esta Política e os demais instrumentos que a regulamentam, utilizando do uso de forma responsável, profissional, ética e legal as informações corporativas que contenham dados pessoais, respeitando os direitos e a privacidade dos titulares dos dados.

8. Disposições Gerais

8.1. A divulgação dessa Política deverá seguir uma estratégia proposta pelo Departamento de Comunicação e Marketing (DCM) e aprovada pela Diretoria Executiva.

8.2. Esta política pode ser desdobrada em outros documentos normativos específicos, sempre alinhados aos princípios e diretrizes aqui estabelecidos.

8.3. Devem ser revisados ou reeditados os instrumentos normativos que estejam em desacordo com os princípios, diretrizes e demais disposições estabelecidas nesta Política.

8.4. Esta Política substitui a Política de Proteção de Dados Pessoais e Privacidade do CEPEL – Versão 1.0, aprovada pela RES. 105/2020, de 26/10/2020.