



Eletrobras

**POLÍTICA
DE PROTEÇÃO DE DADOS
PESSOAIS E PRIVACIDADE**

Edição 2.0
20/12/2023



Política de Proteção de Dados Pessoais e Privacidade

Área responsável pela emissão

Vice-Presidência Executiva Governança, Riscos, *Compliance* e Sustentabilidade / Gerência Executiva Segurança da Informação / Gerência Proteção da Informação

Público-alvo

Colaboradores da Eletrobras que realizem atividades que envolvam, de forma direta ou indireta, tratamento de dados pessoais.

Aprovação

Resolução 670/2023, de 18/12/2023, da Diretoria Executiva da Eletrobras.
Deliberação 208/2023, de 20/12/2023, do Conselho de Administração da Eletrobras.

Repositório

As políticas da Eletrobras podem ser encontradas no *site*:
<https://eletrobras.com/pt/Paginas/Estatuto-Politicas-e-Manuais.aspx>

Direitos de autor e confidencialidade

O conteúdo deste documento não pode ser reproduzido sem a devida autorização. Todos os direitos pertencem à Eletrobras.

Prazo máximo de revisão: 5 anos.

Histórico de edições:

Edição	Aprovação	Principais alterações
1.0	DEL-247/2019, de 17/12/2019	não se aplica.
2.0	RES-670/2023, de 18/12/2023 e DEL-208/2023, de 20/12/2023	Atualização da redação padrão e exclusão de referências legais obrigatórias à administração pública federal, em razão da alteração da natureza jurídica da Eletrobras .

Sumário

1 Objetivo	4
2 Referências	4
3 Princípios	4
4 Diretrizes	5
5 Responsabilidades	6
6 Conceitos	7
7 Disposições Gerais	8

1 Objetivo

Estabelecer diretrizes e orientações para o tratamento de dados pessoais, com o objetivo de proteger a privacidade de consumidores, empregados, parceiros ou fornecedores visando à gestão de dados pessoais e à gestão de incidentes de segurança da informação no ambiente convencional ou de tecnologia da Eletrobras.

2 Referências

2.1 Lei n.º 12.813, de 16 de maio de 2013 – Dispõe sobre o conflito de interesses no exercício de cargo ou emprego do Poder Executivo federal e impedimentos posteriores ao exercício do cargo ou emprego (Lei de Conflitos de Interesses).

2.2 Lei n.º 12.965, de 23 de abril de 2014 – Estabelece princípios, garantias, direitos e deveres para o uso da *internet* no Brasil (Marco Civil da *Internet*).

2.3 Lei n.º 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

2.4 Lei n.º 13.853, de 8 de julho de 2019 – Altera a Lei n.º 13.709/2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados (ANPD).

2.5 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.

2.6 Decreto n.º 9.637 de 26 de dezembro de 2018 – Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação.

2.7 Política de Gestão de Documentos e Informações Corporativas da Eletrobras.

2.8 Plano de Classificação de Documentos da Eletrobras.

2.9 Programa de Governança em Privacidade da Eletrobras.

3 Princípios

3.1 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.

3.2 Adequação: compatibilidade do tratamento de dados com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

3.3 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.

3.4 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.

3.5 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.

3.6 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.

3.7 Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

3.8 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.

3.9 Não discriminação: impossibilidade de realização do tratamento de dados para fins discriminatórios ilícitos ou abusivos.

4 Diretrizes

4.1 Base legal de tratamento de dados

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

4.1.2 Quando o tratamento de dados pessoais tiver como base o legítimo interesse do controlador/operador, este deve ser acompanhado de um Relatório de Impacto à Proteção de Dados Pessoais (RIPD).

4.2 Coleta mínima de dados

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

4.3 Consentimento

4.3.1 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 pode ainda ser renovado periodicamente e pode ser revogado a qualquer momento, a pedido do titular.

4.4 Gestão de instrumentos contratuais

4.4.1 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" da Eletrobras em caso de descumprimento da outra parte.

4.5 Gestão de incidentes

4.5.1 Devem ser elaborados e mantidos atualizados pela Eletrobras procedimentos e planos de resposta a incidentes relacionados à privacidade de titulares de dados, a partir de critérios de controle e registro de vazamentos, e de comunicação aos envolvidos e à Autoridade Nacional de Proteção a Dados (ANPD).

4.6 Segurança da Informação

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

4.7 Inventário de dados

4.7.1 O inventário de dados pessoais na Eletrobras deve 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.

4.7.2 O inventário deve ser realizado considerando o contexto de produção ou acúmulo dos documentos e informações, estruturado a partir do Plano de Classificação de Documentos da Eletrobras.

4.8 Governança de privacidade e dados pessoais

4.8.1 O Programa de Governança em Privacidade da Eletrobras 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. Deve organizar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais.

4.9 Capacitação e conscientização

4.9.1 Devem ser promovidas, de forma continuada, ações educacionais, de capacitação, sensibilização e conscientização sobre as melhores práticas acerca do tratamento de dados pessoais na Eletrobras bem como a ampla divulgação dos riscos e ameaças da não utilização dessas práticas.

4.10 Navegação na web e cookies

4.10.1 A Eletrobras pode, mediante mecanismos de obtenção e revogação de consentimento dos usuários, utilizar-se de *cookies* e tecnologias semelhantes que visem compreender melhor o comportamento dos usuários e contribuir para a eficácia na distribuição de conteúdo, informando quais páginas e conteúdos dos *sites* foram visitados.

4.11 Sistemas de tecnologia da informação

4.11.1 Os sistemas de tecnologia da informação de suporte a processos e atividades que envolvam tratamento de dados pessoais que forem desenvolvidos ou adquiridos pela Eletrobras devem seguir o conceito de *Privacy by Design*. Portanto, sua aderência à LGPD e a esta política deve ser observada desde sua concepção/aquisição.

4.12 Metodologia de projetos

4.12.1 A metodologia de gestão de projetos da Eletrobras deve considerar o conceito de *Privacy by Design*, visando evitar o surgimento de novos processos, atividades, sistemas, práticas, projetos, produtos ou qualquer outra solução que não esteja aderente à LGPD.

4.13 Atendimento a Demanda do Titular de Dados Pessoais (*Data Subject Request – DSR*)

4.13.1 A Eletrobras 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.

4.13.2 O recebimento dos requerimentos de titulares de dados pessoais também poderá ser feito pelo Canal de Ouvidoria, apoiando assim o Encarregado pelo Tratamento de Dados Pessoais (DPO).

5 Responsabilidades

5.1 Conselho de Administração da Eletrobras

5.1.1 Aprovar esta política e deliberar sobre as diretrizes estratégicas da governança de proteção de dados pessoais.

5.1.2 Delegar à Diretoria Executiva da Eletrobras a aprovação de atualizações do Plano de Classificação de Documentos da Eletrobras.

5.2 Diretoria Executiva da Eletrobras

5.2.1 Aprovar esta política e os documentos normativos desdobrados que permitam sua implantação.

5.3 Área responsável pela segurança da informação

5.3.1 Apoiar o Encarregado pelo Tratamento de Dados Pessoais (DPO) em suas atribuições.

5.3.2 Coordenar e apoiar metodologicamente a realização do inventário de dados pessoais, a partir de informações fornecidas pelas áreas da Eletrobras.

5.3.3 Elaborar procedimentos para tratamento e resposta a incidentes relativos à privacidade de titulares de dados.

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

5.4 Encarregado pelo Tratamento dos Dados Pessoais (DPO)

5.4.1 Realizar a interlocução junto aos titulares de dados e junto à Autoridade Nacional de Proteção de Dados (ANPD), incluindo reporte de incidentes e orientando colaboradores e terceiros a respeito das práticas relativas a proteção de dados pessoais e privacidade.

5.5 Gestores das áreas

5.5.1 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, a implantação e a operacionalização de seus controles, fazendo cumprir as diretrizes desta política.

5.6 Colaboradores

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

6 Conceitos

6.1 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.

6.2 Autoridade 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) em todo o território nacional.

6.3 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.

6.4 Controlador – Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

6.5 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*.

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

6.7 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.

6.8 Dado pessoal sensível – Dado vinculado a uma pessoa natural cujo tratamento pode ensejar a discriminação do seu titular, em respeito a: origem racial ou étnica; convicção religiosa; opinião política; filiação a sindicato ou a organização de caráter religioso, filosófico ou político; saúde; vida sexual; genética; ou biometria.

6.9 Eletrobras – *Holding*, suas subsidiárias integrais e empresas nas quais possui controle societário direto e indireto.

6.10 Encarregado pelo Tratamento dos Dados Pessoais (DPO) – (*Data Protection Officer*) Profissional indicado para tratar os incidentes relacionados a violação de privacidade ou que gerem danos aos titulares de dados pessoais e para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

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

6.12 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.

6.13 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.

6.14 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.

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

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

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

7 Disposições Gerais

7.1 Devem ser observadas a legislação correlata ao tema e as determinações e acordos jurídicos específicos vigentes da empresa.

7.2 Tendo em vista o atendimento das especificidades de cada processo, esta política pode ser desdobrada em outros documentos normativos específicos, sempre alinhados aos princípios e diretrizes aqui estabelecidos.

7.3 Esta política substitui a Política de Proteção a Dados Pessoais e Privacidade das Empresas Eletrobras (POL-33) – edição 1.0, aprovada pela DEL-247/2019, de 17/12/2019.

7.4 Revogam-se os documentos normativos e as disposições em contrário a esta política.