 <p>CPFL ENERGIA</p> <p>Uso Interno</p>	Tipo de Documento: Procedimento
	Area de Aplicação: Proteção de Dados
	Título do Documento: Norma de Proteção de Dados

Sumário

1	OBJETIVO	1
2	ÂMBITO DE APLICAÇÃO	1
3	DEFINIÇÕES	1
4	DOCUMENTOS DE REFERÊNCIA	4
5	RESPONSABILIDADES	4
6	REGRAS GERAIS	10
7	CONTROLE DE REGISTROS	25
8	ANEXOS	25
9	REGISTRO DE ALTERAÇÕES	25

1 OBJETIVO

Esta norma tem por objetivo:

- Estabelecer os procedimentos gerais sobre tratamento de dados pessoais para o Grupo CPFL Energia, tendo como base a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018);
- Definir papéis e responsabilidades das gerencias parceiras na integração e manutenção do tema privacidade e proteção de dados; e
- Estruturar o Programa de Governança em Privacidade e Proteção de Dados da Organização.

2 ÂMBITO DE APLICAÇÃO

2.1 Empresa

Esta norma é aplicável ao Grupo CPFL Energia e a todas as suas controladas diretas e/ou indiretas, excetuadas as empresas com modelo de gestão e governança próprio.

2.2 Área


Todas as áreas do Grupo CPFL Energia o que inclui colaboradores, gestores, dirigentes, diretores, conselheiros, prestadores de serviços, parceiros e toda a qualquer pessoa física e/ou jurídica que na execução de sua atividade no Grupo CPFL Energia realize tratamento de dados pessoais de pessoa natural,

3 DEFINIÇÕES

Agentes de tratamento: controlador e operador.

Autoridade Nacional de Proteção de Dados – ANPD: órgão da administração pública responsável por zelar, implementar e fiscalizar as atividades de proteção de dados pessoais e cumprimento à LGPD em todo o território nacional.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
189288	Instrução	1.133	Deise Ramos de Lima	26/04/2023	01 de 28

 Uso Interno	Tipo de Documento:	Procedimento
	Area de Aplicação:	Proteção de Dados
	Título do Documento:	Norma de Proteção de Dados

Banco de dados: conjunto de dados pessoais, estabelecido em um ou vários locais físico ou eletrônico;

Confidencialidade: atributo da segurança da informação que visa garantir que o acesso à informação é restrito a um grupo definido de usuários. A confidencialidade deve prevalecer em todo o ciclo de vida do dado pessoal, ou seja, internamente, na transmissão e no destino.

Controlador: pessoa física ou jurídica que toma decisões relacionadas ao tratamento de dados pessoais por meios próprios.

Custodiante dos dados pessoais: Usuário que possui a posse temporária ou definitiva dos dados pessoais de qualquer natureza.

Dado pessoal: informação relacionada a uma pessoa física identificada ou identificável. Neste documento todas as referências realizadas a este tipo de dado pessoal são aplicáveis a Dados pessoais de criança e dados pessoais sensíveis.

Dado pessoal de criança e adolescente: informação relacionada a uma pessoa física com até 11 anos e 12 meses de idade, sendo que qualquer operação de tratamento de dados para este público somente poderá ocorrer mediante o consentimento de um dos pais ou responsável legal. Utilizaremos esta expressão quando a regra aqui mencionada for exclusivamente aplicável a tal conceito. Já Adolescente é pessoa física com 12 anos completos de idade até 18 anos.

Dado pessoal sensível: dado pessoal sobre 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. Utilizaremos esta expressão quando a regra aqui mencionada for exclusivamente aplicável a tal conceito.

Disponibilidade: é a garantia de que a informação está disponível para o usuário com permissão acesso e para o sistema de informação no momento que o **Grupo CPFL Energia** necessita.

Direitos e Garantias Fundamentais dos titulares de dados: são todos os direitos assim reconhecidos pelo artigo 5º da Constituição Federal Brasileira, tais como a privacidade, a honra, a intimidade, liberdade e personalidade. Direitos estes reconhecidos como inerente a pessoa natural e, portanto, essencial para o seu desenvolvimento pessoal ou coletivo.

Encarregado de dados: pessoa indicada pelo controlador ou pelo operador para atuar como canal de comunicação entre o controlador, titular dos dados e a ANPD.


Grupo CPFL Energia: A CPFL Energia S.A., e todas as suas controladas diretas e/ou indiretas, exceto as empresas com seus próprios padrões de governança e gestão que compartilham controle com outras empresas .

Informação: Toda e qualquer informação dentro do Grupo CPFL Energia que gera valor para a Organização, onde se incluem também os dados pessoais e os dados pessoais sensíveis.

Integridade: é a garantia de que a informação no momento que é acessada está em sua completeza, totalidade, plenitude, sem qualquer alteração em seu conteúdo, quando foi armazenada. Tem por finalidade garantir a autenticidade (certeza que a informação pertence ao autor), o não repúdio (impossibilidade de negar responsabilidade sobre suas ações) e a auditabilidade (permite checar a origem e consistência das informações).

Lei geral de proteção de dados pessoais (LGPD – Lei Federal 13.709/2018): lei geral que trata somente da proteção de dados, mas que para atingir o equilíbrio das relações existentes entre titular de dados e agentes de tratamento, dialoga com outras leis e regulamentações setoriais (ex.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
189288	Instrução	1.133	Deise Ramos de Lima	26/04/2023	02 de 28

 Uso Interno	Tipo de Documento:	Procedimento
	Area de Aplicação:	Proteção de Dados
	Título do Documento:	Norma de Proteção de Dados

Código de Defesa do Consumidor, Código Civil, CLT, Regulamentação da Aneel etc.) para melhor aplicação do Sistema Legislativo Nacional em prol da sociedade civil

Operador: pessoa física ou jurídica que realiza o tratamento de dados pessoais em nome do controlador.

Privacidade: direito fundamental do ser humano, previsto na Constituição Federal Brasileira e que garante ao Titular de Dados o direito de limitar a intervenção de terceiros em sua vida privada sem que haja sua permissão. Este direito aplicado a LGPD, visa assegurar maior controle pelo titular de dados pessoais com relação às operações de tratamento de dados feitas por terceiros em atividades comerciais.

Proprietário do Banco de Dados: pessoa responsável pelos dados pessoais que se encontram em sistemas, ferramentas e diretórios de rede.

Proteção de Dados Pessoais: são regras estabelecidas nas leis e regulamentações que regem o tratamento de dados pessoais de pessoa natural com a finalidade de viabilizar operações de tratamento por terceiros, em atividades comerciais, de forma justa buscando sempre um equilíbrio entre o titular de dados e o terceiro que faz a custódia e utiliza as informações pessoais.

Sub-operador/subcontratado: pessoa física ou jurídica a quem é terceirizado, pelo operador, a realização do tratamento de dados pessoais;

Segurança da informação: proteção da informação contra vários tipos de perigos, ameaças e incertezas para garantir a continuidade do negócio, minimizar os riscos e maximizar o retorno sobre os investimentos e as oportunidades de negócio do Grupo CPFL Energia. São características da Segurança da Informação a confidencialidade, a integridade e a disponibilidade das informações.

Segurança em privacidade e proteção de dados: proteção dos dados pessoais mediante a adoção de medidas técnicas e organizacionais que visam a proteção da privacidade do titular dos dados pessoais contra acessos não autorizados, situações acidentais ou ilícitas, perda, destruição, alteração, comunicação ou qualquer outra forma inadequada de tratamento de dados. As regras e controles adotados por Segurança da Informação são extensivas à privacidade e proteção de dados.

Titular dos dados: pessoa física a quem se refere os dados pessoais que são objeto de tratamento;


Tratamento: toda operação realizada com os dados pessoais, em meio impresso ou digital, de forma presencial ou virtual, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Usuário: nome atribuído à pessoa que tem permissão para interagir com as tecnologias disponibilizadas pelo **Grupo CPFL Energia** para execução de atividades em apoio aos processos de negócio tais como estação de trabalho, sistemas, diretório de rede, provedor de e-mail, dentre outros. Para realizar o controle dos acessos é atribuído a cada usuário, de forma individualizada, uma identificação para acessar ambientes do **Grupo CPFL Energia** o chamado ID.

4 DOCUMENTOS DE REFERÊNCIA

LGPD - Lei Federal 13.709/2018 – estabelece regras a respeito do tratamento de dados pessoais de pessoa natural em atividades econômicas com o objetivo de proteger os direitos fundamentais, as liberdades civis e o livre desenvolvimento da personalidade

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18028	Instrução	1.33	Denise Ramos de Lima	18/04/2023	03 de 28

 Uso Interno	Tipo de Documento: Procedimento
	Area de Aplicação: Proteção de Dados
	Título do Documento: Norma de Proteção de Dados

Marco Civil da Internet (MCI) – Lei Federal 12.965/2014 – estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil

Decreto nº. 8.771/2016 – regulamenta o MCI para indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações

ABNT/ISO 27001-2013

ABNT/ISO 27002-2013

Norma Básica de Segurança da Informação do **Grupo CPFL Energia** (GED 18704)

Norma de Classificação da Informação do **Grupo CPFL Energia** (GED 18744)

Código de Ética e de Conduta Empresarial do **Grupo CPFL Energia** (disponível no Portal Multi em: Quem somos > Programa de Integridade > Nossas diretrizes ou [clikando aqui](#))

Medidas disciplinares e ressarcimento de danos (GED 17055)

Documentos Normativos (“Norma Zero”) (GED 0)

Aviso de Privacidade Laboral (disponível no Portal Multi em: Para você>Central da Proteção de Dados> Acesse o Aviso de Privacidade Laboral e exerça seus direitos ou [clikando aqui](#))


Esta Norma é complementada pela Política e demais Normas e Procedimentos do **Grupo CPFL Energia**.

5 RESPONSABILIDADES

5.1 Gerência de Proteção de Dados

- Desenvolver, implementar, manter e monitorar o **Programa de Governança em Privacidade e Proteção de Dados**.
- **Orientar** o Grupo CPFL Energia com relação a coleta, distribuição, utilização e qualquer operação de **tratamento de dados pessoais de pessoa natural** que realize seja ela decorrente de **atividades, processos, produtos, serviços, novas tecnologias e infraestrutura**, observando as leis e regulamentações que regem a proteção de dados pessoais.
- **Estabelecer políticas, normas, procedimentos e orientações em privacidade e proteção dos dados pessoais**, mantendo-as atualizadas de acordo com as leis e regulamentações vigentes.
- Realizar a **gestão e o monitoramento dos registros das atividades de tratamento de dados pessoais** (data mapping).
- Fomentar a **cultura de proteção de dados** na Organização e promover boas práticas de privacidade e proteção de dados pessoais.
- **Avaliar riscos em privacidade e proteção de dados** em atividades, processos, produtos, serviços, infraestrutura, novas tecnologias, bem em como em todas as situações em que houver o tratamento de dados pessoais de pessoa natural.
- **Recomendar mitigadores e planos de ação** corretivos para redução ou eliminação dos riscos em privacidade e proteção de dados, mediante alinhamento com os departamentos e atividades de negócio impactadas.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18928	Instrução	1.33	Daniel Ramos de Lima	26/04/2023	04 de 28


	Tipo de Documento:	Procedimento
	Area de Aplicação:	Proteção de Dados
	Título do Documento:	Norma de Proteção de Dados
Uso Interno		

- **Comunicar riscos e obter compromissos com relação a planos de ação** estabelecidos os departamentos observando a tabela de alçadas estabelecidas pela Organização.
- **Realizar a classificação dos incidentes** envolvendo dados pessoais com base nos impactos gerados aos direitos e garantias fundamentais dos titulares de dados pessoais, registrar o seu entendimento e informar às partes interessadas.
- **Comunicar a ANPD e ao titular de dados pessoais** na hipótese de **violação de dados pessoais** classificados como de **risco ou dano relevante aos direitos e garantias fundamentais** dos titulares de dados pessoais.
- **Estabelecer os requisitos de privacidade e proteção de dados** a serem implementados pela Gerência de Segurança da Informação com vistas a **assegurar o cumprimento das regras de segurança e sigilo necessárias para garantir a proteção adequada aos dados pessoais**.
- Apoiar a Gerência Jurídica e as demais gerências que realizam a defesa dos direitos da Organização ou ainda que possuem canal específico de contato com consumidores, recursos humanos e relacionamento com investidores na construção de **resposta aos titulares de dados e apresentação de evidências** relacionadas ao tema privacidade e proteção de dados.
- **Contribuir com o plano anual de Auditoria Interna** subsidiando a Gerência de Auditoria com informações baseadas nas avaliações de riscos e situações identificadas na execução do Programa de Governança em Privacidade e Proteção de Dados.
- **Reportar ao canal de ética situações em que a violação de dados pessoais possa ter ocorrido por meio de ação ou omissão do colaborador** a fim de que esta possa ser investigada/avaliada pelo Comitê de Ética do Grupo CPFL Energia.
- Dar conhecimento a alta administração sobre o **Programa de Governança em Privacidade e Proteção de Dados**.
- Dar conhecimento a **Diretoria de Negócios e responsável pela atividade de tratamento de dados sobre riscos ou danos relevantes aos titulares de dados pessoais**;
- **Endereçar temas de privacidade e proteção de dados com relação ao pilar de segurança e sigilo, para conhecimento e discussão junto ao Comitê de Segurança da Informação.**

5.2 Gerência Jurídica

- **Orientar** a Gerência de Proteção de Dados quanto **as leis, normas, procedimentos e entendimentos jurisprudências** que impactam o **negócio e/ou evento** analisado e que devem ser também consideradas nas orientações e entendimentos do Encarregado de Proteção de Dados.
- Apoiar na integração da **avaliação de riscos em privacidade e proteção de dados** nos processos, serviços, produtos, infraestrutura e gestão de terceiros que contenham operações de tratamento de dados, endereçando consultas à Gerência de Proteção de Dados sempre que entender necessário.
- Integrar as **políticas, normas, procedimentos e orientações de proteção de dados** na **avaliação, orientação e defesa** dos interesses do Grupo CPFL Energia.
- Apoiar no acompanhamento da **efetividade do Programa de Governança em Privacidade e Proteção de Dados** participando a Gerência de Proteção de Dados, de forma quantitativa e qualitativa, os procedimentos judiciais e/ou administrativos envolvendo dados pessoais, se houve ou não êxito na defesa da Organização, e, sempre que possível, indicar pontos de melhoria na

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18028	Instrução	1.3	Denise Ramos de Lima	18/04/2023	05 de 28

 Uso Interno	Tipo de Documento:	Procedimento
	Area de Aplicação:	Proteção de Dados
	Título do Documento:	Norma de Proteção de Dados

documentação e/ou no programa de proteção de dados baseados nas decisões judiciais ou administrativas.

5.3 Gerência de Segurança da Informação


- Estabelecer, implementar e monitorar **medidas de segurança aptas a proteger os dados pessoais contra acessos não autorizados, situações acidentais** (cometidas por culpa, negligência, imprudência ou imperícia) **ou ilícitas** (cometidas voluntaria e intencionalmente) que possam evitar a destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
- Assegurar que as **políticas, regras e procedimentos de proteção de dados sejam integrados a Gestão de Segurança da Informação**.
- Adotar medidas de segurança em dados pessoais observando os **requisitos de privacidade e proteção de dados**
- Garantir as medidas e ferramentas adequadas visando a **gestão de acesso, exclusão, pseudoanonimização, anonimização e portabilidade** de dados pessoais.
- Conceder acesso a dados pessoais em sistemas e ferramentas da Organização somente após autorização do Gestor da Informação, realizar o monitoramento dos acessos concedidos e manter o registro adequado das ações realizadas pelos Usuários em ambiente monitorado garantindo a rastreabilidade das ações executadas no ambiente.
- Adotar **medidas de segurança mais restritivas** em ambientes (físico ou eletrônico) que possuam **dados pessoais sensíveis e dados pessoais de criança e/ou adolescentes**.
- Assegurar tecnicamente que os **dados pessoais foram classificados, rotulados e tratados de acordo com os requisitos de privacidade** definidos pela Gerência de Proteção de Dados.
- Disponibilizar **ferramentas homologadas e orientação para compartilhamento** de dados pessoais com empresas externas;
- Pautar no **Comitê de Segurança da Informação**, temas relacionados ao pilar de segurança e sigilo da LGPD orientados pelo Encarregado de Proteção de Dados ou à sua ordem, incluindo-o como participante necessário.

5.4 Gerência de Tecnologia

- Implementar **ferramentas e soluções técnicas com vistas** a garantir o cumprimento dos requisitos de privacidade e proteção de dados.
- Integrar **requisitos de privacidade e proteção de dados** pessoais na **infraestrutura de tecnologia da informação**.
- Apoiar a Gerência de Proteção de Dados a **manter atualizado o inventário de sistemas, ferramentas e bancos de dados** utilizados pelo Grupo CPFL Energia, contendo tratamento de dados pessoais de pessoa natural.
- Assegurar que os sistemas, serviços e equipamentos utilizados para o tratamento de dados pessoais estejam dentro dos **padrões aceitáveis definidos por Proteção de Dados e Segurança da Informação** e conforme normas do Grupo CPFL Energia.
- Informar a Gerência de Proteção de Dados sempre que houver **mudanças relevantes em tecnologias ou utilização de novas tecnologias** para o **tratamento de dados pessoais**.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18028	Instrução	1.3	Denise Ramos de Lima	18/04/2023	06 de 28

- Apoiar a Gerência de Proteção de Dados, prestando a orientação e as informações técnicas

 Uso Interno	Tipo de Documento: Procedimento
	Area de Aplicação: Proteção de Dados
	Título do Documento: Norma de Proteção de Dados

necessárias para o desempenho das atividades relacionadas à Proteção de Dados Pessoais, bem como da **implementação de planos de ação** acordado com as áreas de negócio e requisitos de privacidade necessário para execução de atividades de tratamento de dados pessoais.

5.5 Gerência de Riscos, Controles Internos, Ética e Compliance

- Integrar o **tema privacidade e proteção de dados nos pilares do Programa de Integridade** do Grupo CPFL Energia e compartilhar aspectos de riscos e processos para atuação do time da PAP conforme incidência de desvios de conduta ou potenciais riscos relacionados que tenham sido identificados durante as atividades da área.
- Apoiar a Gerência de Proteção de Dados na **identificação de controles para monitoramento de riscos a privacidade e proteção de dados** em processos críticos do Grupo CPFL Energia, bem como compartilhar os resultados dos testes de efetividade e planos de remediação em andamento com as áreas de negócio que remetem ao tema.
- Integrar a **privacidade e a proteção de dados na gestão de riscos** do Grupo CPFL Energia, por meio de indicadores e sensibilização dos modelos de risco do Mapa Corporativo de Riscos e nas diretrizes de gestão de crise.
- Apoiar a Gerência de Proteção de Dados na identificação de riscos relacionados a privacidade e a proteção de dados, por meio da avaliação de riscos de **projetos de M&A e projetos internos da cia.**

5.6 Gerência de Auditoria

- Realizar avaliação independente do ambiente de Riscos e Controles sobre:
 - Programa de Governança e Privacidade de Dados da Cia;
 - Cumprimento das normas e procedimentos de Privacidade e Proteção de Dados;
 - Política de privacidade, normas e procedimentos em conformidade com os regulamentos.
- Consultivamente subsidiar com discussões e recomendações relacionadas à privacidade e proteção de dados.


5.7 Gerência de Comunicação

- Integrar o tema privacidade e proteção de dados nos Planos de Comunicação da Organização;
- Apoiar a Gerência de Proteção de Dados nas **comunicações a serem realizadas aos titulares de dados e à imprensa**, quando necessário e alinhados às diretrizes de GCN (Gestão de Continuidade dos Negócios);
- Observar as regras de privacidade e proteção de dados nas **ações de publicidade e pesquisas** envolvendo dados pessoais.

5.8 Proprietário do Banco de Dados

- Realizar a **Classificação da informação diretamente nos bancos de dados, sistemas, diretórios de rede ou em qualquer outro meio** que a informação esteja sendo tratada, observando o disposto na **Norma de Classificação da Informação GED 18744**.
- Analisar, aprovar e manter registro do uso e/ou compartilhamento de dados pessoais sob sua

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
189228	Instrução	1.13	Deise Ramos de Lima	26/04/2023	07 de 28

 Uso Interno	Tipo de Documento:	Procedimento
	Area de Aplicação:	Proteção de Dados
	Título do Documento:	Norma de Proteção de Dados

- responsabilidade para outras áreas e/ou empresas externas.
- Manter o **registro de todas as operações de tratamento** de dados pessoais realizadas, o que inclui **declaração sobre a origem, local, data e hora da coleta; qualidade dos dados; autorizações de acesso e compartilhamentos internos e externos; regras de anonimização e exclusão da informação; algoritmo de avaliação eletrônica; dentre outros.**
- Na **autorização de acesso ou compartilhamento de dados pessoais** é de **responsabilidade do Proprietário da Informação** dar ciência aos Usuários sobre o tipo de classificação da informação e fazer referência a Norma de Classificação da Informação.
- **Implementar as regras, procedimentos e normas relacionadas a privacidade e proteção de dados pessoais** em qualquer operação de tratamento de dados pessoais realizada no **exercício de suas atividades laborais, bem como na função de proprietário da informação.**
- Implementar, durante todo o ciclo de vida dos dados pessoais, o **uso apropriado das medidas de segurança e privacidade designadas pela Organização** para dados pessoais observando a norma de classificação da informação.
- Seguir expressamente as **orientações da Gerência de Segurança da Informação** com relação as medidas de segurança necessárias para controlar os riscos às informações classificadas como dados pessoais, dados pessoais sensíveis, dados pessoais de criança, dados pessoais de adolescentes.
- Realizar a **gestão dos acessos e permissões relacionadas aos dados pessoais** de sua responsabilidade buscando sempre **limitar o acesso a dados pessoais de acordo com a finalidade de uso e a necessidade do Usuário**, sempre buscando que este somente tenha acesso a dados essenciais para o exercício de sua atividade.
- Assegurar que os **dados pessoais serão utilizados apenas para finalidades compatíveis** com o que foi informado ao titular do dado pessoal.


5.9 Custodiante de dados pessoais

- Zelar pelo armazenamento das informações: datacenters, administradores de banco de dados, administradores de servidores de arquivo, cofres, entre outros aplicando as regras e procedimentos de proteção de dados e privacidade aplicáveis.
- Seguir expressamente as orientações das Gerências de Proteção de Dados e de Segurança da Informação com relação as **medidas de segurança e sigilo necessárias para proteção da privacidade das informações pessoais custodiadas.**
-

5.10 Embaixadores de Privacidade

- **Disseminar o conhecimento com relação às políticas, procedimentos e normas** relacionados a privacidade e proteção de dados.
- Manter atualizado o **mapeamento de dados pessoais** da área que representa.
- Buscar **aprovação da Gerência N2** com relação aos processos de tratamento de dados pessoais realizados pela área;
- **Aprovar os mitigadores** orientados pela Gerência de Proteção de Dados observando as alçadas de aprovação da Organização;
- **Identificar situações de riscos e informar tempestivamente** a Gerência de Proteção de

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18928	Instrução	1.33	Denise Ramos de Lima	26/04/2023	08 de 28

 Uso Interno	Tipo de Documento: Procedimento
	Área de Aplicação: Proteção de Dados
	Título do Documento: Norma de Proteção de Dados

Dados.

- Acompanhar **planos de ação** estabelecidos pela área que representa e a Gerência de Proteção de Dados.


5.11 Colaboradores

- Observar as **Políticas, procedimentos e normativos internos** relacionados a **proteção de dados, a privacidade e a segurança da informação** extensivas a proteção de dados pessoais.
- Realizar o **tratamento de dados pessoais somente quando necessários e no estrito cumprimento de suas atividades laborais** observando as regras internas da Grupo CPFL Energia.
- **Tratar** os dados pessoais e informações de terceiros com **sigilo e observando as regras de acesso a informação do Grupo CPFL Energia**, nesta incluída a Norma de classificação da informação (GED 18744).
- **Utilizar os dados pessoais e informações de terceiros** a que tiver acesso no exercício de sua função somente para **a execução de tarefas internas** e que importem para a execução das demandas relacionadas ao seu contrato de trabalho.
- **Não realizar o compartilhamento dos dados pessoais com terceiros**, inclusive outros colaboradores, que não tenham autorização para receber ou utilizar tal informação.
- Na hipótese de **perda, roubo ou comprometimento de equipamentos ou documentos que contenham dados pessoais** a gerência de Segurança de Informação deve ser imediatamente informada a fim de que possa tomar as medidas necessárias para evitar prejuízo aos titulares.
- Tomar todas as **medidas necessárias para manter em segurança os dados pessoais**, independentemente da sua forma ou formato, incluindo àqueles que se encontram armazenados nos equipamentos utilizados para a execução das suas atividades tais como bloquear a tela do computador ao sair da estação de trabalho, não compartilhar senhas ou deixa-las anotadas em local de fácil acesso, não deixar documentos contendo dados pessoais na impressora, realizar a guarda de documentos impressos contendo dados pessoais em armário com chave, dentre outros.
- Realizar o **descarte seguro dos arquivos eletrônicos e impressos** observando as políticas, normas e procedimentos do Grupo CPFL Energia.
- Na hipótese de ter **acesso a dados pessoais por engano**, **informar imediatamente o remetente e destruir de forma segura os dados recebidos sem qualquer tratamento posterior**.
- O **compartilhamento de dados pessoais entre as áreas ou empresas do Grupo CPFL Energia ou mesmo para fornecedores/terceiros somente poderão ocorrer se necessário para o desenvolvimento de alguma atividade interna ou de suporte ao Grupo CPFL Energia** e desde que observadas as políticas e procedimentos corporativos, tais como proteção de dados, segurança da informação, gestão de acesso, dentre outras.
-

5.12 Liderança

- **Orientar a equipe sobre a importância de conhecer e seguir as regras de privacidade e**

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
189228	Instrução	1.03	Deise Ramos de Lima	26/04/2023	09 de 28

 Uso Interno	Tipo de Documento: Procedimento
	Area de Aplicação: Proteção de Dados
	Título do Documento: Norma de Proteção de Dados

proteção de dados da Organização.

- indicar representantes da área (principal e suplente) com conhecimento nos processos e atividades para ocupar a posição de embaixadores de privacidade, mantendo tais indicações atualizadas.
- Definir os acessos a sistemas, ferramentas e bancos de dados do Grupo CPFL Energia de acordo com a função exercida e as atividades desenvolvidas pelo colaborador/terceiro alocado, sempre buscando que o colaborador tenha acesso somente àquelas informações pessoais essenciais para a execução da atividade.
- Manter o **descritivo de função compatível com as atividades** e operações de tratamento de dados realizadas pelo colaborador;
- Na hipótese do colaborador ou terceiro alocado, para o exercício de sua atividade, não necessitar ter acesso às informações de forma a identificar o seu real titular de dados, buscar com a Diretoria de Tecnologia, sempre que possível, os mecanismos para que o acesso a informação seja realizado de forma menos identificada.

6 REGRAS GERAIS

O Grupo CPFL Energia institui as seguintes regras e procedimentos com a finalidade de assegurar o cumprimento das normas jurídicas e de boas práticas direcionadas à privacidade e proteção de dados, bem como a gestão contínua, responsável e preventiva de riscos, constituindo este o seu Programa de Privacidade e Proteção de Dados Pessoais.

As regras aqui disciplinadas se aplicam a dados pessoais de pessoa natural tratados em formato digital e processados através de sistemas e da rede corporativa, como também para dados tratados em formato convencional, armazenados de forma centralizada ou distribuída, em meio físico ou soluções não corporativas.

6.1 Das regras básicas de tratamento


O tratamento de dados pessoais deve observar as leis e regulamentações que regem a proteção de dados pessoais, bem como as políticas, normas e procedimentos internos do Grupo CPFL Energia, em especial, aqueles aplicáveis à proteção de dados.

Todas as operações de tratamento de dados pessoais devem ter **propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com as finalidades a ele informadas.**

São **premissas para o tratamento de dados pessoais** pelo Grupo CPFL Energia:

- a **transparência com o titular dos dados** operacionalizada através de informação adequada com relação aos dados e as operações de tratamento realizadas previamente a coleta ou utilização dos dados;
- a **manutenção do aviso de privacidade institucional e laboral atualizados** com base nas atividades de tratamento realizadas;
- o cumprimento de todos os **direitos garantidos pela LGPD** e demais leis e regulamentações correlatas;
- o **registro atualizado das atividades de tratamento de dados pessoais** para uma gestão adequada de riscos em privacidade e proteção de dados;

N.Documento: 18928	Categoria: Instrução	Versão: 1.33	Aprovado por: Denise Ramos de Lima	Data Publicação: 26/04/2023	Página: 10 de 28
-----------------------	-------------------------	-----------------	---------------------------------------	--------------------------------	---------------------

 Uso Interno	Tipo de Documento: Procedimento
	Área de Aplicação: Proteção de Dados
	Título do Documento: Norma de Proteção de Dados

(v) **delimitação do tempo de tratamento dos dados**, bem como o monitoramento adequado para garantir o seu cumprimento;

(vi) **avaliação de privacidade e proteção de dados em processos, produtos, serviços, tecnologia e infraestruturas** novas e nas já existentes (se e quando em processo de atualização), sempre com vistas a reduzir os riscos à privacidade e proteção de dados.

(vii) assegurar o **menor impacto a privacidade de titulares no tratamento de dados pessoais**, executando a minimização de dados ou acessos em todas as operações de tratamento, sempre que possível.

(ix) promover a **segurança e prevenção no tratamento de dados pessoais** que realiza observando **a estrutura, a escala, o volume, a sensibilidade dos dados tratados, além da probabilidade e gravidade dos danos para os titulares de dados**.

(x) **monitoramento contínuo** de ameaças e vulnerabilidades das operações de tratamento de dados pelo Grupo CPFL Energia com vistas a garantir gestão de riscos em privacidade e proteção de dados na Organização.

6.2 Classificação dos dados pessoais à luz da LGPD e seu relacionamento com a Norma de Classificação da Informação

Os **dados pessoais serão classificados observando** a Norma de classificação da informação (**GED 18744**), disponibilizada pela área de Segurança da Informação.

A classificação da informação levará em conta a promoção da prevenção e segurança dos dados pessoais e observará os seguintes critérios: a estrutura, a escala, o volume, a sensibilidade dos dados tratados, além da probabilidade e gravidade dos danos para os titulares de dados.

6.3 Do registro das operações de tratamento de dados pessoais


O Grupo CPFL Energia manterá registradas e atualizadas as operações de tratamento de dados pessoais de pessoa física que realiza e para tanto a Gerência de Proteção de Dados contará com o apoio de pontos focais nos departamentos corporativos e locais que terão a responsabilidade de manter o inventário de dados pessoais da sua respectiva gerência atualizado (“data mapping”).

Todos os departamentos que realizarem operações de tratamento de dados na execução de suas atividades deverão estar de acordo com as regras de proteção de dados adotadas pelo Grupo CPFL Energia, e na hipótese de serem verificados riscos relevantes as garantias e liberdades fundamentais dos titulares de dados medidas remediadoras deverão ser implementadas a fim de atingir a conformidade legal necessária para a atividade de tratamento realizada.

Todos os produtos, serviços, processos, sistemas e ferramentas que contemplem operações de tratamento de dados pessoais de pessoa natural devem estar de acordo com as regras de privacidade e proteção de dados adotadas pelo Grupo CPFL Energia, sendo obrigatória a integração da avaliação de riscos a privacidade e proteção de dados previamente a criação ou alteração de qualquer atividade da área que contemple o tratamento de dados pessoais.

O Grupo CPFL Energia adota procedimento específico para registro das atividades de tratamento de dados pessoais (*Data Mapping* – GED 18834), bem como para avaliação de riscos de privacidade e proteção de dados no desenho e redesenho de produtos, serviços, processos e infraestrutura de TI (*Privacy by design/by default* – GED 18835).

N. Documento: 18928	Categoria: Instrução	Versão: 1.3	Aprovado por: Denise Ramos de Lima	Data Publicação: 19/04/2023	Página: 11 de 28
------------------------	-------------------------	----------------	---------------------------------------	--------------------------------	---------------------

 Uso Interno	Tipo de Documento:	Procedimento
	Area de Aplicação:	Proteção de Dados
	Título do Documento:	Norma de Proteção de Dados

6.4 Dados Pessoais tratados com base no consentimento do titular

Consentimento é a autorização do titular de dados pessoais para que a Grupo CPFL Energia realize o tratamento de dados para uma finalidade específica e deve ser obtido de forma livre, expressa e informada, e dentre as informações essenciais e que antecedem ao tratamento deve-se esclarecer ao titular as consequências relacionadas a sua não autorização.

Quando forem tratados dados pessoais sensíveis ou dados de menores de 18 anos, além das informações relacionadas no parágrafo anterior, o termo de consentimento deve ser separado e em destaque.

Ao estabelecer um tratamento de dados pessoais com base no consentimento a área responsável pelo processo, produto ou serviço deverá considerar a Gestão do Consentimento, qual seja, estabelecer fluxo para que o titular de dados pessoais possa, a qualquer tempo, desautorizar o tratamento de dados pessoais.

O Grupo CPFL Energia adota procedimento específico para para tratamento de dados lastreado no consentimento (GED 18831)

6.5 Segurança e sigilo da Informação em privacidade e proteção de dados


Os dados pessoais são considerados informações que agregam valor aos negócios do Grupo CPFL Energia, e, portanto, também integram, em termos de segurança e sigilo, as informações geridas por políticas, normas e procedimentos estabelecidos pela Gerência de Segurança da Informação.

As **medidas de segurança técnicas e administrativas** relativas ao tratamento de dados pessoais devem ser suficientes para evitar o acesso indevido e situações que possam gerar a destruição, alteração, perda, comunicação ou qualquer outra forma de tratamento de dados ilícita ou acidental, e ainda adequadas à **categoria de dados (comuns, sensíveis e de vulneráveis); categoria de titulares; volume de dados processados; quantidade de titulares de dados afetados; a facilidade de identificação dos titulares por terceiros não autorizados e potencial de ocasionar danos as liberdades e garantias fundamentais dos titulares.**

Entre as **medidas de segurança que se recomenda** sejam adotadas para cumprimento dos princípios da segurança e da prevenção previstos na LGPD, destacam-se, mas sem limitação a:

- Anonimização dos dados (utilização de meios técnicos razoáveis, que possibilite a não identificação do titular. Ex: dados estatísticos);
- Pseudonimização dos dados (tratamento por meio do qual o dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. Ex.: utilização apenas do número de instalação de clientes em documentos);
- Criptografia de dados em execução (recurso de segurança que protege os dados durante o seu tráfego);
- Criptografia de dados em repouso;
- Canais seguros de trânsito dos dados (utilização de ferramentas que garantem a segurança de dados no momento do compartilhamento e/ou armazenamento. É necessário sempre verificar com a área de Segurança da Informação – SI quais são as ferramentas homologadas para a utilização);
- Gestão de acessos segura (gerenciamento de acessos dos colaboradores em ferramentas internas, como forma de segurança);

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
188288	Instrução	1.13	Deiseu Ramos de Lima	28/04/2023	12 de 28

 Uso Interno	Tipo de Documento: Procedimento
	Área de Aplicação: Proteção de Dados
	Título do Documento: Norma de Proteção de Dados

- Desenvolvimento seguro (utilização de ferramentas que garantem a segurança de dados. É necessário sempre verificar com a área de Segurança da Informação – SI quais são as ferramentas homologadas para a utilização);
- Registro de Logs de Aplicações (coleta de dados não estruturados para registro em trilhas de auditoria e possibilidade de rastreamento das ações internas);
- Compartilhamento seguro e monitorado (utilização de ferramentas que garantem a segurança de dados no momento do compartilhamento. É necessário sempre verificar com a área de Segurança da Informação – SI quais são as ferramentas homologadas para a utilização).

Com relação a **gravidade dos danos aos titulares de dados** será considerado o potencial de ocasionar danos materiais ou morais aos direitos e garantias fundamentais do titular de dados tais como discriminação, violação dos direitos à imagem e à reputação, fraudes financeiras, roubo da identidade, dentre outros.

Internamente, **recomenda-se**


- (i) a segregação de acessos a dados pessoais, com foco na minimização de dados (somente o essencial para o exercício da atividade, seja para colaboradores, seja para terceiros, prestadores de serviços, parceiros e quaisquer terceiros que em apoio ao exercício das atividades de negócio realizam operações e tratamento de dados pessoais);
- (ii) avaliação de riscos à privacidade e proteção de dados dos titulares, bem como a mitigação de eventuais violações das leis, normas de autoridades reguladoras, políticas, normas e procedimentos internos do Grupo CPFL Energia relacionados a privacidade, proteção de dados pessoais e segurança da informação; e
- (iii) investimentos em ferramentas e processos de segurança sejam lastreados e priorizados a partir de estudos técnicos que observem o disposto nesta Norma, sendo priorizados, na medida do possível, àqueles necessários para atingimento da conformidade legal a proteção de dados pessoais e/ou a relevância do potencial de danos as liberdades e garantias fundamentais dos titulares.

6.6 Compartilhamento de dados pessoais

O compartilhamento de dados pessoais somente é possível se houver uma razão, uma finalidade legítima e justificável, além de enquadramento legal adequado, **sendo de responsabilidade de quem as compartilha, no mínimo:**

- Assegurar que a **atividade de compartilhamento está registrada no mapeamento de dados** do Grupo CPFL Energia de acordo com as normas de governança de dados vigentes;
- Utilizar apenas **ferramentas homologadas pela Gerência de Segurança da Informação** (isto assegura que estaremos seguindo regras de segurança necessárias e adequadas de acordo com a classificação da informação);
- Manter **registro sobre o compartilhamento dos dados**, tanto interno quanto externo, de maneira a garantir a trilha de auditoria;
- Ter **embasamento legal para o compartilhamento**, ou seja, mais do que ter uma finalidade
- é ter uma hipótese legal que autoriza o compartilhamento (daí a importância de ter o data

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
189228	Instrução	1.33	Daniel Ramos de Lima	26/04/2023	13 de 28

	Tipo de Documento: Procedimento
	Área de Aplicação: Proteção de Dados
	Título do Documento: Norma de Proteção de Dados
Uso Interno	

mapping atualizado e de consultá-lo previamente ao compartilhamento dos dados pessoais);

- Com relação as informações compartilhadas é de **responsabilidade do remetente**, considerando o rol das informações compartilhadas: **(i) delimitar a finalidade** do tratamento, evidenciando a restrição de uso da informação; **(ii) identificar a classificação da informação** e o seu conceito; **(iii) informar o prazo para devolução dos dados ou para exclusão segura da informação** com orientações sobre a forma e tipo de documento comprobatório do cumprimento desta obrigação; **(iv) sempre que possível, proteger a informação com senha e compartilhá-la apenas com o seu destinatário final** por canais homologados pela Gerência de Segurança da Informação.
- Em se tratando de **compartilhamento de dados sensíveis**, estes deverão ter a **aprovação expressa e registrada do Proprietário da informação**, além de ser **obrigatório a adoção de medidas de segurança mais robustas que garanta a segurança de ponta-a-ponta** cuja orientação técnica se dará por meio da **Gerência de Segurança da Informação**;

Todo o **compartilhamento de dados pessoais** (externo ou entre Empresas do Grupo CPFL Energia) **deve ser registrado contendo no mínimo**: remetente, receptor, data, hora, canal de compartilhamento, classificação da informação, tipo de titular, relação de dados compartilhados, bem como o nº SAP do contrato ao qual o compartilhamento está atrelado.

Os registros de compartilhamento de dados pessoais realizados por meio de ferramenta segura homologada pela Gerência de Segurança da Informação devem ser realizados de maneira a **gerar trilha de auditoria** para verificação do cumprimento das regras dispostas nessa norma, execução dos direitos dos titulares, bem como não repúdio das informações.

Compartilhamento de dados pessoais entre áreas e/ou empresas do Grupo CPFL Energia somente serão admitidos se não houver meios mais seguros de se obter a mesma informação e ainda somente na hipótese de os dados pessoais serem essenciais para a realização de atividades daquela área, incluindo atividades de gestão.


Ao **colaborador que compartilha a informação caberá verificar se o destinatário tem autorização do Proprietário da Informação** antes de realizar o envio dos dados requeridos, e também sempre que possível minimizar o acesso aos dados pessoais considerando a finalidade das atividades que serão executadas. Para tanto, poderá contar com os documentos e informações disponíveis na Central da Proteção de Dados, as normas e procedimentos da Organização e ainda com a equipe da Gerência de Proteção de Dados Pessoais.

O **colaborador que compartilha os dados pessoais é o responsável por zelar pelo cumprimento das normas e procedimentos internos de proteção de dados, privacidade e segurança**, incluindo mais não se limitando a exclusão dos dados ao final do tratamento.

6.7 Mídias removíveis somente poderão ser utilizadas mediante autorização expressa do Proprietário da Informação e da Gerência de Segurança da Informação, que tomará todas as providências necessárias para o registro do compartilhamento, contendo, no mínimo: remetente, receptor, data, hora, canal de compartilhamento, classificação da informação, tipo de titular e o nº SAP do contrato ao qual está atrelado o compartilhamento. Gestão de Terceiros - regras para tratamento de dados pessoais e due diligence em privacidade

Toda a atividade de tratamento de dados pessoais que tiver a participação de fornecedores, parceiros, prestadores de serviços ou qualquer terceiro (aqui identificados como “terceiros”) estará registrada no Data Mapping com todas as informações pertinentes ao compartilhamento de dados realizado.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18928	Instrução	1.3	Denise Ramos de Lima	19/04/2023	14 de 28

 Uso Interno	Tipo de Documento: Procedimento
	Área de Aplicação: Proteção de Dados
	Título do Documento: Norma de Proteção de Dados

É obrigatória a avaliação de riscos a privacidade e proteção de dados do Terceiro previamente a sua contratação, o que se dará através de questionário específico disponibilizado pela Gerência de Proteção de Dados.

Havendo objeção da Gerência de Proteção de Dados na contratação ou estabelecimento de negócio jurídico com o terceiro, o tema seguirá a tabela de alçadas de riscos de privacidade e proteção de dados adotada pelo Grupo CPFL Energia.

Os terceiros que realizarem o tratamento de dados pessoais em negócios jurídicos celebrados com o Grupo CPFL Energia estão sujeitos ao cumprimento das regras gerais de proteção de dados estabelecidas neste normativo.

O Grupo CPFL Energia disponibiliza na área pública do site institucional, na página dedicada aos fornecedores, as regras de tratamento de dados pessoais para terceiros a chamada Norma de Proteção de Dados para fornecedores, parceiros e prestadores de serviços (GED18836), como premissa para o estabelecimento de qualquer negócio jurídico com terceiros. Também poderá, a seu critério estabelecer, em instrumento escrito (ex. contrato, acordo, termo de confidencialidade etc.), de forma complementar a GED 18836, outras regras de proteção de dados e privacidade, a depender da operação de tratamento de dados pessoais realizadas na execução do negócio jurídico firmado entre as Partes. Requisitos mínimos para a seleção de fornecedores podem ser encontrados no Anexo III deste documento.

O Gestor do Contrato será responsável por assegurar o cumprimento das regras de proteção de dados do Grupo CPFL Energia desde o processo de eleição do terceiro até a extinção do negócio jurídico ajustado entre as Partes.

O inverso também é verdadeiro, ou seja, o Gestor do Contrato também deverá assegurar que o Grupo CPFL Energia cumprirá com as regras de proteção de dados estabelecidas no GED 18836 ao tratar dados pessoais de seus fornecedores, parceiros e prestadores de serviços.

Ao final do negócio jurídico celebrado entre Grupo CPFL Energia ou qualquer empresa à ele vinculada, deverá o gestor atentar para a **regra de exclusão ou retenção de dados adota pela Organização**. Sempre que a regra for exclusão de dados, a área deverá seguir a regra estabelecida nesta norma geral ou no instrumento jurídico que sustenta o negócio entabulado entre as Partes. Em caso de dúvida a Gerência Jurídica deverá ser consultada.

O compartilhamento de dados pessoais entre o Grupo CPFL Energia e o Terceiro, e vice-versa deverá se dar observando as regras definidas no item 6.6 acima.


É de responsabilidade do Gestor do Contrato **identificar se o fornecedor, parceiro e/ou prestador de serviços utiliza provedor de serviços em nuvem, e se afirmativo deverá incluir no mapeamento de dados relacionados à atividade de tratamento que utiliza o fornecedor o país onde as informações são processadas e/ou armazenadas**. Para estes parceiros será necessária a aplicação da **due diligence em privacidade e proteção de dados**.

Quando o Grupo CPFL Energia realizar o tratamento de dados pessoais com a participação de parceiros, fornecedores e prestadores de serviços, deverá o fornecedor responder a *due diligence* em privacidade e proteção de dados, a fim de que seja avaliado se os critérios exigidos para o tipo de tratamento de dados por ele realizado estão sendo por ele observados.

6.8 Transferência Internacional

A transferência internacional de dados pessoais só será possível mediante garantias do atendimento as regras de proteção de dados no destino, e devem estar baseadas em contratos ou obrigações legais.

N. Documento: 18928	Categoria: Instrução	Versão: 1.3	Aprovado por: Denise Ramos de Lima	Data Publicação: 26/04/2023	Página: 15 de 28
------------------------	-------------------------	----------------	---------------------------------------	--------------------------------	---------------------

 Uso Interno	Tipo de Documento: Procedimento
	Área de Aplicação: Proteção de Dados
	Título do Documento: Norma de Proteção de Dados

Além disso, a transferência internacional dos dados pessoais também deve ser informada de maneira clara ao titular de dados e feita com atenção à finalidade do tratamento, adequação e necessidade do compartilhamento à atividade desempenhada e medidas de segurança adequadas.

As medidas de segurança da informação para o compartilhamento dos dados devem ser definidas pela Segurança da Informação e seguidas pelo Proprietário da Informação e por todos àqueles que de alguma forma participam da atividade de transferência internacional.

Qualquer transferência internacional de Dados Pessoais só pode ser efetuada pelos meios e/ou ferramentas homologadas e com respeito às normas de segurança da informação.

Caberá ao Proprietário da Informação ou à sua ordem manter o registro dos dados pessoais transferidos contendo, no mínimo, as seguintes informações: área/colaborador remetentes, prestador de serviços, país de destino, data, hora, canal de compartilhamento, classificação da informação, tipo de titular, nº SAP do contrato ao qual está atrelado o compartilhamento (informação a ser passada pelo gestor do contrato), finalidade da transferência internacional.

A transferência internacional de dados pessoais deve sempre estar atualizada no registro oficial de tratamento de dados pessoais conforme Norma de Governança de Dados.

6.9 Retenção dos dados pessoais tratados com base na LGPD

O Grupo CPFL Energia poderá manter dados pessoais de pessoa natural em sua base de dados após o término do prazo de tratamento estipulado para fins de auditoria, segurança, controle de fraudes, preservação de direitos ou cumprimento de obrigação legal, regulatória ou judicial que justifique sua retenção.

O tempo de guarda dos dados deverá respeitar a tabela de temporalidade constante no Anexo I deste documento ("Tabela de Temporalidade").

Caso, não haja a previsão do tempo de guarda do dado na Tabela de Temporalidade, o Grupo CPFL Energia utilizará os seguintes critérios para definição do tempo de guarda:


- Área de negócio juntamente com o Proprietário da Informação informarão o prazo de tratamento de dados pessoais com justificativas relacionadas a sua utilização (lembrando que o prazo de retenção está atrelado a finalidade de uso informada ao titular dos dados no momento da coleta);
- A Gerência Jurídica, na ausência de prazo de retenção estabelecido em norma própria, avaliará as justificativas enviadas pela área de negócio/proprietário da informação e recomendará o prazo de retenção a ser aplicado;

Definido o prazo de prescricional este será incluído na Tabela de Temporalidade do Grupo CPFL Energia, constante no Anexo I deste documento.

Cumprido o prazo definido na Tabela de Temporalidade os dados pessoais poderão ser excluídos ou anonimizados conforme definição da área de negócio e observado o disposto na LGPD e demais normas correlatas e setoriais, sendo realizado o seguinte fluxo: (i) área de negócio é avisada sobre a expiração do tempo de guarda com 60 (sessenta) dias de antecedência para que decida sobre a:

(i) eliminação de dados por meio seguro com emissão de certificado de eliminação dos documentos impressos ou dados eletrônicos (quando realizado por empresa terceirizada) ou termo de responsabilidade de eliminação de documento ou instrumento equivalente (quando realizado por equipe própria); ou

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18028	Instrução	1.3	Denise Ramos de Lima	18/04/2023	16 de 28

 Uso Interno	Tipo de Documento: Procedimento
	Area de Aplicação: Proteção de Dados
	Título do Documento: Norma de Proteção de Dados

(ii) anonimização de dados sistêmicos, ou seja, 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. Nesta hipótese a área de tecnologia emitira Termo de Responsabilidade de Anonimização de Dados assegurando que as informações mantidas, considerando o estado da técnica, não possuem possibilidade razoável para que sejam revertidas a ponto de identificar o seu real titular.

Em se tratando de dados armazenados em bancos de dados eletrônicos, a Gerência de Tecnologia da Informação será responsável por garantir ao Grupo CPFL Energia que o backup não retornará as informações eliminadas ou anonimizadas quando utilizado.

Pedidos de eliminação de dados pessoais realizados pelo titular somente serão atendidos se, na data do requerimento, a finalidade de uso tiver sido cumprida e não houver obrigação legal, regulatória ou judicial que justifique a retenção dos dados.

6.10 Sistemas, ferramentas e bancos de dados

O Grupo CPFL Energia manterá inventário de sistemas, ferramentas e bancos de dados contendo dados pessoais de indivíduos atualizado identificando no mínimo: nome do sistema, descrição do sistema, responsável de informática (titular e suplente), responsável de negócio N1 (Diretor), responsável de negócio N2 (titular e suplente), processo de negócio, categoria de titular do dado pessoal, categoria de dados pessoais, lista de dados pessoais, finalidade de tratamento, tempo de retenção do dado pessoal, Tipo do Sistema (EX. Técnico/Corporativo), Plataforma EX. (WEB), Local do Sistema(ex. OnPremesse / Cloud), Permite Exclusão e Restore.

O acesso aos dados pessoais, seja por colaboradores ou terceiros alocados, em sistemas, ferramentas e/ou bancos de dados somente poderá ocorrer quando as informações acessadas forem essenciais para o exercício da atividade e função, devendo quem autoriza o acesso sempre prezar pela minimização de dados e responsabilidade na disponibilização dos dados pessoais, bem como no cumprimento de todas as regras de gestão de acesso do Grupo CPFL Energia.

6.11 Violação de Dados Pessoais

O Grupo CPFL Energia adota as melhores medidas para evitar incidentes de segurança envolvendo dados pessoais.


É possível que, apesar de todos os esforços, ocorram incidentes em decorrência de ação maliciosa de terceiros ou ainda em decorrência de negligência, imprudência ou imperícia do próprio usuário/cliente.

Todos os colaboradores devem relatar violações de dados pessoais ou possíveis violações das diretrizes das políticas, normas e procedimentos de proteção de dados pessoais e de segurança da informação através dos canais disponibilizados pelo Grupo CPFL Energia.

Para mais informações sobre o tema consultar Norma Básica de Segurança da Informação (GED 18704) e Procedimento de Gestão de Incidentes de Segurança da Informação (GED 14368).

Na hipótese de roubo ou furto de equipamentos do Grupo CPFL Energia ou ainda de equipamentos próprios com informações relacionadas a execução de sua atividade na CPFL Energia, que possa pôr em risco dados pessoais de indivíduos, o Colaborador ou Terceiros alocado deverá entrar em contato imediatamente com os Serviços Corporativos de Tecnologia através do número (19) 3756-8002 para comunicar a ocorrência e receber orientações.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18928	Instrução	1.3	Denise Ramos de Lima	19/04/2023	17 de 28
18928	Instrução	1.3	Denise Ramos de Lima	26/04/2023	17 de 28


 Uso Interno	Tipo de Documento: Procedimento
	Área de Aplicação: Proteção de Dados
	Título do Documento: Norma de Proteção de Dados

Na hipótese de violação de dados pessoais, interno ou externo, a depender do risco aos direitos e garantias fundamentais do titular, medidas mitigatórias serão tomadas em conjunto com a área de negócio, tecnologia e segurança da informação observando o disposto na orientação de riscos de LGPD cumulada com o Plano de Respostas a Incidentes de Segurança da informação (GED 14368) e a Orientação para comunicação a ANPD e aos titulares de dados afetados (GED 18860).

6.12 Direitos dos titulares

São direitos de todos os titulares de dados pessoais, garantidos pelo Grupo CPFL Energia e que deverão sempre ser garantidos em todos os processos de tratamento de dados pessoais realizados pela Organização:

Confirmação de tratamento de dados	Confirmar se temos ou não dados pessoais sobre titulares em nosso banco de dados.
Declaração completa de dados pessoais	Obter todas as informações que o Grupo CPFL Energia tem sobre o titular, sua origem e finalidade de uso.
Correção de dados incompletos, inexatos ou desatualizados	Retificar seus dados pessoais. O Grupo CPFL Energia poderá pedir documentação comprobatória por questões de segurança e prevenção a fraude.
Anonimização, bloqueio ou eliminação de dados pessoais	Interromper o tratamento de dados pessoais excessivos, desnecessários ou em desconformidade com a LGPD. Eliminação/anonimização somente serão executados quando não houver lei ou regulamentação específica que justifique o tratamento no Grupo CPFL Energia.
Oposição ao tratamento de dados	Discordar e apresentar razões pelas quais entende que os seus dados não devem ser tratados.
Revogação e suspensão do consentimento	Retirar (revogar) ou suspender seu consentimento com o tratamento de seus dados pessoais.
Suspensão do tratamento de dados sem o consentimento	Quando a base para o tratamento for o consentimento, caso este não tenha sido pedido de acordo com o previsto na LGPD, o titular poderá pedir que seus dados sejam excluídos da base de dados do Grupo CPFL Energia.
Revisão de decisões automatizadas	Quando decisões forem tomadas pelo Grupo CPFL Energia apenas com base em análise eletrônica de dados pessoais, o titular poderá pedir revisão da decisão tomada.

 Uso Interno	Tipo de Documento: Procedimento
	Area de Aplicação: Proteção de Dados
	Título do Documento: Norma de Proteção de Dados
Portabilidade de Dados	Encaminhamento dos dados pessoais, a pedido do titular, a outro fornecedor. Aguardamos regulamentação da ANPD para que o exercício desse direito seja possível.
Informação sobre compartilhamento de dados com terceiros	Salvo segredo industrial ou comercial o titular de dados pessoais tem o direito de saber com quem seus dados foram compartilhados e para qual finalidade.
Informações/dúvidas/comunicações	Obter informações e esclarecer dúvidas a respeito do cumprimento das leis e regulamentações relacionadas a proteção de dados, comunicar eventuais incidentes de dados pessoais, dentre outros temas relacionados ao tratamento de dados pessoais realizados pelo Grupo CPFL Energia.
Direito à Explicação sobre Decisão Automatizada	Requerer informações a respeito dos critérios e procedimentos utilizados para a decisão automatizada, ressalvadas as informações de segredo de negócio.

O Grupo CPFL Energia disponibiliza canal eletrônico específico e destacado dos demais, com gestão realizada pela Gerência de Proteção de Dados, para que os titulares de dados pessoais exerçam os direitos decorrentes da LGPD e os mantém atualizado no Portal da Privacidade, no site institucional, nas Agências e especialmente para colaboradores do Grupo CPFL Energia na Central da Proteção de Dados e no Portal Multi RH. Os procedimentos e orientações para atendimento destes direitos estão disponibilizados em normativo específico (GED 18865).

Demandas realizadas por titulares baseadas na LGPD devem ser compartilhadas com a Gerência de Proteção de Dados a fim de que possa avaliar os riscos relacionados a LGPD, compartilhar evidências e tomar as medidas necessárias visando a mitigação de eventuais riscos em processos, pessoas e tecnologias sempre visando a mitigação de riscos as liberdades e garantias fundamentais dos titulares.

6.13 Comunicação com a Autoridade Nacional de Proteção de Dados, demais autoridades e Associações de Classe


São prerrogativas do Encarregado de Proteção de Dados a comunicação com a Autoridade Nacional de Proteção de Dados e a comunicação com o titular de dados, independente do canal escolhido por este para reivindicar direitos decorrentes da LGPD.

Para responder às autoridades ou aos titulares de dados, o Encarregado envolverá tantas áreas quantas se façam necessárias na busca da apuração do evento e com foco na melhor defesa dos interesses e direitos dos titulares e do Grupo CPFL Energia.

Assim, na eventualidade do **recebimento de ordem ou comunicação da ANPD**, todo **colaborador fica obrigado a contatar o Encarregado de Proteção de Dados** e, a encaminhar a ordem ou comunicação recebida, tão breve quanto possível, através do canal privacidade@cpfl.com.br.

Adicionalmente, **ao receber ordem que envolva ou que pareça envolver dados pessoais em poder do Grupo CPFL Energia**, emanada de autoridade judicial, policial ou administrativa, ou ainda de associações de classe, **o colaborador que recebeu a ordem deverá contatar o**

N.DOCUMENTO: 18928	Categoria: Instrução	Versão: 1.3	Aprovado por: Denise Ramos de Lima	Data Publicação: 26/04/2023	Página: 19 de 28
-----------------------	-------------------------	----------------	---------------------------------------	--------------------------------	---------------------

 Uso Interno	Tipo de Documento:	Procedimento
	Área de Aplicação:	Proteção de Dados
	Título do Documento:	Norma de Proteção de Dados

Encarregado de Proteção de Dados tão breve quanto possível, **através do canal privacidade@cpfl.com.br**.

6.14 Comunicação e Treinamento

As políticas, normas e procedimentos relacionadas a proteção de dados e privacidade são comunicadas aos colaboradores de forma consistente, regular e documentada.

Novos colaboradores devem tomar conhecimento sobre a proteção de dados na integração, e no decorrer da execução do seu contrato de trabalho a Gerência de Proteção de Dados tomara as ações necessárias para que as políticas, normas e procedimentos de privacidade sejam reforçadas

A Gerência de Proteção de Dados adotará as medidas necessárias para disseminar conhecimento sobre o tema privacidade e proteção de dados na Organização, e sempre que possível direcionado ao planejamento estratégico do Grupo CPFL Energia. Os departamentos da Organização com maior volume de acesso a dados pessoais, sempre que possível, receberão orientação sobre proteção de dados de forma mais específica considerando o tratamento de dados por eles realizados.

A Gerência de Proteção de Dados mantém um canal dedicado sobre o tema privacidade e proteção de dados (Central da Proteção de Dados) e que concentra as orientações, políticas, procedimentos, manuais orientadores, documentos padrão, avisos de privacidade, dentre outras notícias, a fim de facilitar que os colaboradores, além dos treinamentos, workshops e palestras que participam, tenham acesso facilitado a informações que os apoiem a integrar, da melhor forma, o tema proteção de dados pessoais e privacidade em suas atividades diárias. O conteúdo desta página é gerido e produzido pela Gerência de Proteção de Dados e fica disponível na intranet para todos os colaboradores, no seguinte caminho:

<https://cpflenergia.sharepoint.com/sites/PortaldaPrivacidade>

Os colaboradores que para entrega de suas atividades realizarem o tratamento de dados pessoais em médio e alto volume deverão realizar treinamento de proteção de dados específico, de preferência anualmente.


Já os colaboradores que não realizam baixo volume de tratamento de dados pessoais ou mesmo que não tenham acesso a dados pessoais na execução de suas atividades participaram do treinamento em proteção de dados que é conferido juntamente com o treinamento básico em segurança.

6.15 Gestão de Riscos em Privacidade e Proteção de Dados

Os riscos de proteção de dados e privacidade, corporativamente, integram de forma transversal o mapa de riscos do Grupo CPFL Energia.

A avaliação de riscos em privacidade e proteção de dados para cálculo do risco leva em consideração: a categoria de dados (comuns, sensíveis e de vulneráveis), categoria de titulares, volume de dados processados, a quantidade de titulares de dados afetados no tratamento, a facilidade de identificação dos titulares por terceiros não autorizados, potencial de ocasionar danos materiais ou morais e possibilidade de sanção ao Grupo CPFL Energia pela ANPD.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
189288	Integração	1.13	Deise Ramalho de Lima	28/04/2023	20 de 28

 Uso Interno	Tipo de Documento: Procedimento
	Area de Aplicação: Proteção de Dados
	Título do Documento: Norma de Proteção de Dados

Políticas, normas e procedimentos são implementados para cobrir todos os aspectos relevantes para assegurar a privacidade e a proteção de dados dos titulares, sendo selecionados os controles a serem monitorados, bem como a frequência com base em avaliação de riscos relacionadas ao tema.

Para identificação de riscos em privacidade e proteção de dados em atividades de negócio a Gerência de Proteção de Dados contará com, no mínimo, os seguintes documentos:

- (i) inventário de dados ou “data mapping” (registro de tratamento de dados pessoais por processos);
- (ii) avaliação de *privacy by design/by default* em processo, produtos, serviços e infraestrutura;
- (iii) *Due diligence* em privacidade e proteção de dados em fornecedores, parceiros e prestadores de serviços;
- (iv) Atendimento aos titulares de dados pessoais;
- (v) Avaliação de vulnerabilidades em privacidade e proteção de dados;
- (vi) Procedimentos administrativos (Senacon, Aneel, MP, Procon) e judiciais;
- (vii) Ações de controles internos e auditoria;
- (viii) Monitoramentos de segurança da informação (blindagem de sistemas, testes periódicos de ambiente, monitoramentos pelo SOC (relatório mensal); Security score (scan on line), dentre outros).

Em conjunto com a Gerência de Riscos, Ética e Compliance, a Gerência de Privacidade adota metodologia adequada a avaliar os impactos da LGPD nas atividades de tratamento de dados realizadas pela Organização, bem como implementa controles a fim de que os riscos possam ser monitorados e plano de remediação adotados para readequação da conformidade quando necessário.

Os procedimentos para gerenciamento de riscos em privacidade e proteção de dados constará em documento apartado, sendo este aprovado em reunião de diretoria do Grupo CPFL Energia.


6.16 Melhoria contínua

Existe processo de monitoramento e avaliação dos efeitos de suas várias iniciativas e a empresa procura continuamente melhorar

O Grupo CPFL Energia realizará monitoramento de conformidade dos processos e procedimentos de proteção de dados para:

- (i) identificar problemas de não conformidade e aplicar planos de remediação para garantir conformidade;
- (ii) melhorar métodos de comunicação e compreensão dos colaboradores e terceiros alocados com relação a integração do tema em suas atividades de trabalho;
- (iii) aprimorar a comunicação e compreensão dos titulares de dados com relação aos tratamentos de dados realizados pelo Grupo CPFL Energia, bem como para que os indivíduos sejam adequadamente informados sobre como entrar em contato com a entidade com indagações, reclamações e disputas;
- (iv) garantir o correto endereçamento dentro de um período de tempo específico dos requerimentos de exercício de direitos garantidos pela LGPD por titulares;
- (v) redesenhar e melhorar a privacidade dos processos internos e garantir que o tratamento de dados pessoais seja realizado de forma ética e de acordo com os preceitos da LGPD;
- (vi) garantir a conformidade contínua e sustentável da governança de dados pessoais de indivíduos baseada nas leis, regulamentações e melhores práticas em privacidade, proteção de dados e segurança;
- (vii) implementar correções, inclusive imediatas (sempre que possível), tanto após revisões

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
189288	Instrução	1.33	Deise Ramos de Lima	26/04/2023	21 de 28

 Uso Interno	Tipo de Documento: Procedimento
	Area de Aplicação: Proteção de Dados
	Título do Documento: Norma de Proteção de Dados

periódicas quanto em avaliações específicas de privacy by design/by default.

6.17 Penalidades

O cumprimento das normas e procedimentos de privacidade e proteção de dados, assim como todas as demais políticas, normas e procedimentos do Grupo CPFL Energia é obrigatório para todos os colaboradores do Grupo CPFL Energia.

O descumprimento de qualquer delas pode gerar a aplicação das penalidades conforme previstas nas políticas, normas e procedimentos da Organização.

6.18 Revisão Periódica

Este documento, assim como os demais documentos correlatos e cujo tema seja proteção de dados pessoais serão revistos, no mínimo, anualmente pelo Encarregado de Proteção de Dados do Grupo CPFL Energia, a fim de que se mantenha atualizado não só com relação a legislação e normas externas aplicadas ao tema, como também com relação as atividades de negócio e planejamento estratégico do Grupo CPFL Energia.

Também, será utilizado como base para revisões periódicas o monitoramento contínuo realizado pela Organização.

O processo de revisão e produção de políticas, normativos, orientações e demais documentos relacionados a privacidade e proteção de dados com relação a alçadas de aprovação seguem a orientação da Norma Zero (GED 0) de gestão da Gerência de Excelência.

6.19 Dados do Encarregado de Proteção de Dados

O **Grupo CPFL Energia** nomeia **como Encarregado de Proteção de Dados** a colaboradora Denise Ramos de Lima - Matrícula r00XX51 (principal).

Na ausência do **Encarregado de Proteção de Dados** assumirá as atividades relacionadas na Lei Geral de Proteção de Dados a colaboradora: **Nadine Emile Prado Marostergan** r00XX30 (**suplente**).

Os dados de contato do encarregado de proteção de dados nomeado será divulgado no Aviso de Privacidade.

Em se tratando de atendimento via formulário eletrônico, recomenda-se a disponibilização do formulário no aviso de privacidade e no Portal da Privacidade no site institucional das empresas que integram o Grupo CPFL Energia.

Já para colaboradores, especialmente no que diz respeito a consultoria e orientação sobre o tema Privacidade e Proteção de Dados o canal a ser utilizados são:


(1) Para atualização do Data Mapping – realizar a revisão ou inclusão de novas atividades envolvendo tratamento de dados pessoais através da ferramenta interna Inventário de Dados, em conjunto com o Embaixador de Privacidade observando procedimento específico disponibilizado no GED;

(2) Para avaliação de privacidade em produtos, serviços, atividades e infraestrutura de TI: formular consulta através da ferramenta Privacy By Design/By Default em conjunto com o Embaixador de Privacidade observando procedimento específico disponibilizado no GED;

(3) Requisições de titulares de dados realizadas por outros canais, tais como Central de Atendimento, SAC e Ouvidoria – utilizar o canal privacidade@cpfl.com.br até que esteja disponível a consulta via CRM.

(4) Procedimentos administrativos (Senacon, Aneel, MP, Procon) e judiciais envolvendo o

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18928	Instrução	1.33	Denise Ramos de Lima	26/04/2023	22 de 28

 Uso Interno	Tipo de Documento: Procedimento
	Area de Aplicação: Proteção de Dados
	Título do Documento: Norma de Proteção de Dados

tratamento de dados pessoais - – utilizar o canal privacidade@cpfl.com.br até que esteja disponível a consulta via CRM.

(5) Dúvidas e demais consultas que não se enquadrem nos itens 1 e 2 acima, utilizar o canal privacidade@cpfl.com.br.

a. **Programa de Governança em Privacidade e Proteção de Dados**

O Grupo CPFL Energia instituiu Programa de Governança em Privacidade e Proteção de Dados baseado em 7 pilares:



- Governança de dados pessoais: contempla o registro das atividades com tratamento de dados pessoais (data mapping), inventário de terceiros que realizam tratamento de dados pessoais para entrega das atividades de cada departamento, o ciclo de vida da informação atrelada aos processos de negócio declarados pelos respectivos responsáveis do departamento (todos estes registrados no data mapping) e inventário de sistemas e bancos de dados contendo dados pessoais (documento mantido pela Gerência de Tecnologia).

- Políticas, Normas e procedimentos: regras internas, baseadas em leis, regulamentações e melhores práticas de proteção de dados e privacidade e que visam criar processos e metodologias para estar em conformidade com a LGPD.

- Transparência com o titular: mecanismos para garantir os direitos estabelecidos na Lei Geral de Proteção de Dados e demais leis e regulamentações que regem o tema.


- Comunicação e Treinamento: aculturação e evolução da maturidade em proteção de dados de colaboradores e terceiros que apoiam a execução do objeto social das empresas que compõe o Grupo CPFL Energia.

- Gestão de Fornecedores. Redução de riscos a privacidade e proteção de dados no tratamento de dados realizados por terceiros (parceiros e fornecedores).

- Riscos e controles. métricas e controles para redução e gestão de riscos em privacidade e proteção de dados, o que inclui a definição da matriz e também o acompanhamento da efetividade dos controles e a recomendação e acompanhamento dos planos de ação necessários;

- Ferramentas de governança. ferramentas de apoio a Gerência de Proteção de Dados para gestão do Programa.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18028	Instrução	1.3	Denise Ramos de Lima	18/04/2023	23 de 28

 Uso Interno	Tipo de Documento: Procedimento
	Area de Aplicação: Proteção de Dados
	Título do Documento: Norma de Proteção de Dados

O acompanhamento do Programa de Governança em Privacidade e Proteção de Dados é de competência da Gerência de Proteção de Dados, cabendo a esta última, na hipótese de identificar nos tratamentos de dados mapeados potencial de risco relevante aos direitos e garantias fundamentais do titular dos dados levar o assunto a conhecimento/decisão da alta direção do Grupo CPFL Energia.

7 CONTROLE DE REGISTROS

Identificação	Armazenamento e Preservação	Proteção (acesso)	Recuperação e uso	Retenção	Disposição
Anexo I	Central da Privacidade	Restrição de Acesso	Por documento	Até a próxima atualização do documento	Substituição
Anexo III	Central da Privacidade	Restrição de Acesso	Por documento	Até a próxima atualização do documento	Substituição

8 ANEXOS

Anexo I – Cartilha de Proteção de Dados Pessoais

Disponível em:

<https://cpflenergia.sharepoint.com/sites/PortaldPrivacidade/Documentos%20Partilhados/Cartilhas/Cartilha%20-%20Prote%C3%A7%C3%A3o%20de%20Dados.pdf>

Anexo II – Tabela de Temporatidade de Dados Lógicos

Anexo III – Requisitos mínimos para a seleção de fornecedores


Disponível em:

<https://cpflenergia.sharepoint.com/:w/s/PortaldPrivacidade/EeygNJO6vchCgOg2kQWcs4sBj3nQjdI5Ezr9DXIfDsT-SA?e=3PpEk6>

9 REGISTRO DE ALTERAÇÕES

9.1 Colaboradores


Empresa	Área	Nome
CPFL Renováveis	PAP	Denise Ramos de Lima
CPFL Renováveis	PAP	Nadine Emile Prado Marostegan
CPFL Brasil	PAP	Thiago Bento dos Santos
CPFL Piratininga	PAG	Bruna Victorelli
CPFL	IJC	Michel Franco de Carvalho
CPFL Paulista	PAP	Rebeca Querido Potestino

 <p>Uso Interno</p>	Tipo de Documento:	Procedimento
	Area de Aplicação:	Proteção de Dados
	Título do Documento:	Norma de Proteção de Dados

9.2 Alterações

Versão Anterior	Data da Versão Anterior	Alterações em relação à Versão Anterior
Versão inicial	n/a	n/a
Versão 1.2		<p>Ajustes de redação sem alterar conteúdo: itens 2.2; 6; 6.1;</p> <p>6.3 (atual 6.4); 6.4 (atual 6.5); 6.5(atual 6.6); 6.6 (atual 6.7); 6.7 (atual 6.8); 6.10 (atual 6.11); 6.11 (atual 6.12); 6.15 (atual 6.14)</p> <p>Inclusão de legislação correlata- item 4</p> <p>Inclusão de novas responsabilidades - item 5.1</p> <p>Itens novos: 6.3 (com renumeração dos itens subsequentes); 6.8 (atual 6.9); e 6.20</p>
Versão 1.3		Inclusão dos dados do encarregado de proteção de dados principal e suplente.
Versão 1.4		Inclusão do Anexo III - Requisitos De Proteção De Dados Para Contratação /Seleção De Fornecedores E Parceiros

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18928	Instrução	1.3	Denise Ramos de Lima	20/04/2023	25 de 28

 Uso Interno	Tipo de Documento: Procedimento
	Area de Aplicação: Proteção de Dados
	Título do Documento: Norma de Proteção de Dados


Anexo II – TABELA DE TEMPORALIDADE DE DADOS LÓGICOS

DADOS CADASTRAIS E FINANCEIROS	
Prazo de Armazenamento	Fundamento Legal e âmbito
5 anos após o término da relação de consumo, exceto para cobrança de dívidas, cujo prazo prescricional é de 10 anos, conforme fundamentação abaixo	Art. 27 do Código de Defesa do Consumidor.
10 anos após o término do contrato ou da relação civil.	Art. 205, do Código Civil.
5 anos após o primeiro dia do exercício seguinte àquele em que o lançamento poderia ter sido efetuado; da data em que se tornar definitiva a decisão que houver anulado, por vício formal, o lançamento anteriormente efetuado.	Art. 173, inciso I e II do Código Tributário Nacional.


N.Documento: 18928	Categoria: Instrução	Versão: 1.3	Aprovado por: Denise Ramos de Lima	Data Publicação: 19/04/2023	Página: 25 de 28
-----------------------	-------------------------	----------------	---------------------------------------	--------------------------------	---------------------

OUTROS DADOS	
Prazo de Armazenamento	Fundamento Legal e âmbito
Dado pessoal: enquanto durar a relação e não houver pedido de apagamento, revogação de consentimento ou outra base legal que o mantenha.	Art. 7 (dados pessoais); Art. 9, Inciso II; Art. 11 (dados pessoais sensíveis) e Art. 16 da Lei Geral de Proteção de Dados Pessoais.
Acervo histórico e cultural – guarda permanente	Artigos 215 e 216, da Constituição Federal de 1988, recomendação n. 37 CNJ.
OBSERVAÇÃO	Para fins de fundamentação legal do prazo de guarda adequado, avaliar o contexto no qual o dado está inserido. Para guarda de dados de colaboradores e ex-colaboradores do Grupo CPFL Energia, deverá ser observada a tabela de temporalidade prevista na Instrução nº 16.894 – Processos de Gestão e Guarda Gerenciada de Documentos de RH.

N.Documento: 18928	Categoria: Instrução	Versão: 1.3	Aprovado por: Denise Ramos de Lima	Data Publicação: 28/04/2023	Página: 26 de 28
----------------------------------	------------------------------------	---------------------------	--	---	--------------------------------

 <p>Uso Interno</p>	Tipo de Documento: Procedimento
	Area de Aplicação: Proteção de Dados
	Título do Documento: Norma de Proteção de Dados

CATEGORIA DOS DADOS	DADOS	INÍCIO DO PRAZO	PRAZO LEGAL	FUNDAMENTAÇÃO LEGAL	PRAZO RECOMENDADO	JUSTIFICATIVA
DADOS CADASTRAIS (CLIENTES)	Nome	Após o término do Contrato/relação	10 anos	Art. 205, CC	11 anos (10 +1)	A manutenção dos dados objetiva a preservação de prova da existência da relação contratual, bem como das condições contratuais estabelecidas, ensejando a aplicação do prazo mínimo de 10 anos (cf. art.205, Código Civil).
	RG	Após o término do Contrato/relação	10 anos	Art. 205, CC	11 anos (10 +1)	
	CPF	Após o término do Contrato/relação	10 anos	Art. 205, CC	11 anos (10 +1)	
	Data de nascimento	Após o término do Contrato/relação	10 anos	Art. 205, CC	11 anos (10 +1)	
	Endereço	Após o término do Contrato/relação	10 anos	Art. 205, CC	11 anos (10 +1)	
	Telefone(s)	Após o término do Contrato/relação	10 anos	Art. 205, CC	11 anos (10 +1)	
	E-mail	Após o término do Contrato/relação	10 anos	Art. 205, CC	11 anos (10 +1)	
DADOS CONTRATUAIS (FORNECEDORES)	Dados Cadastrais do representante legal	Após o término do Contrato/relação	10 anos	Art. 205. CC	11 anos (10 +1)	A manutenção dos dados objetiva a preservação de prova da existência da relação contratual, bem como das condições contratuais estabelecidas, ensejando a aplicação do prazo mínimo de 10 anos (cf. art.205, Código Civil).
	Dados bancários de pessoas físicas vinculadas	Após o término do Contrato/relação	10 anos	Art. 205, CC	11 anos (10 +1)	
	Comprovantes de pagamentos feitos aos fornecedores	Após término da contratação	10 anos	Art. 205, CC		
DADOS DE IDENTIFICAÇÃO DIGITAL	Endereço IP e Porta Lógica de Origem	A contar da atividade do usuário no sistema eletrônico	6 meses	Art. 15, Marco Civil da Internet Gerenciamento em conformidade com o domínio 12.4.2 e 12.4.3 da ISO 27001 e 12.1.1 (i), 12.4.2, 12.4.3, 8.3.3 (e) da ISO 27002	18 meses (6 + 12)	O Marco Civil da Internet (Lei nº 12.965) determina que, no caso de provedor que exerça tal atividade de forma organizada, profissionalmente e com fins econômicos, este deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses.
	Informações sobre o dispositivo (versão do sistema operacional)	A contar da atividade do usuário no sistema eletrônico	03 anos	Art. 206, §3º, V, CC. Gerenciamento em conformidade com o domínio 12.4.2 e 12.4.3 da ISO 27001 e 12.1.1 (i), 12.4.2, 12.4.3, 8.3.3 (e) da ISO 27002	04 anos (3 + 1)	
	Geolocalização	A contar da atividade do usuário no sistema eletrônico	03 anos	Art. 206, §3º, V, CC. Gerenciamento em conformidade com o domínio 12.4.2 e 12.4.3 da ISO 27001 e 12.1.1 (i), 12.4.2, 12.4.3, 8.3.3 (e) da ISO 27002	04 anos (3 + 1)	
	Registros de data e horário de cada ação realizada	A contar da atividade do usuário no sistema eletrônico	06 meses	Art. 15, Marco Civil da Internet	18 meses (6 + 12)	
	Telas acessadas	A contar da atividade do usuário no sistema eletrônico	03 anos	Art. 206, §3º, V, CC. Gerenc. em conf. com domínio 12.4.2 e 12.4.3 da ISO 27001 e 12.1.1 (i), 12.4.2, 12.4.3, 8.3.3 (e) da ISO 27002	04 anos (3 + 1)	
	ID da sessão	A contar da atividade do usuário no sistema eletrônico	03 anos	Art. 206, §3º, V, CC. Gerenc. em conf. com dom. 11 da ISO 27002	04 anos (3 + 1)	
	Dados de biometria	A contar da coleta através dos	05 anos	Art.27, CDC	06 anos (5 + 1)	



Uso Interno

Tipo de Documento: **Procedimento**

Area de Aplicação: **Proteção de Dados**

Título do Documento: **Norma de Proteção de Dados**

		ambientes físicos e lógicos				
		A partir do término da Contrato/relação	10 anos	Art. 205, CC	11 anos (10 + 1)	
	Logs de Consentimento	A contar da atividade do usuário no sistema eletrônico	10 anos	Art. 205, CC Gerenciamento em conformidade com o domínio 12.4.2 e 12.4.3 da ISO 27001 e 12.1.1 (i), 12.4.2, 12.4.3, 8.3.3 (e) da ISO 27002	11 anos (10 + 1)	
	Logs dos sistemas eletrônicos	A contar da atividade do usuário no sistema eletrônico	6 meses	Art. 15, Marco Civil da Internet Gerenciamento em conformidade com os itens 12.4.2 e 12.4.3 da ISO 27001 e 12.1.1 (i), 12.4.2, 12.4.3, 8.3.3 (e) da ISO 27002	01 ano e 6 meses (6 meses + 1 ano)	
	Históricos de Navegação	A contar da atividade do usuário no sistema eletrônico	6 meses	Art. 15, Marco Civil da Internet Gerenciamento em conformidade com os itens 12.4.2 e 12.4.3 da ISO 27001 e 12.1.1 (i), 12.4.2, 12.4.3, 8.3.3 (e) da ISO 27002	01 ano e 6 meses (6 meses + 1 ano)	
DADOS FINANCEIROS		A contar da atividade do usuário no sistema eletrônico	6 meses	Art. 15, Marco Civil da Internet Gerenciamento em conformidade com os itens 12.4.2 e 12.4.3 da ISO 27001 e 12.1.1 (i), 12.4.2, 12.4.3, 8.3.3 (e) da ISO 27002	01 ano e 6 meses (6 meses + 1 ano)	
	Dados de pagamento	Após o término do Contrato/relação	10 anos	Art.205, Código Civil	11 anos (10 + 1)	Como a manutenção dos dados objetiva a preservação de prova da existência da relação contratual, bem como das condições contratuais estabelecidas, o prazo mínimo aplicável deve ser de 10 anos (cf. art.205, Código Civil).
	Endereço de cobrança	Após o término do Contrato/relação	10 anos	Art.205, Código Civil	11anos (10 + 1)	
	Comprovantes de pagamento	Após o término do Contrato/relação	10 anos	Art.205, Código Civil	11 anos (10 + 1)	