Eletrobras

# Programa de Governança em Privacidade das empresas Eletrobras

**Dezembro de 2021**

# Sumário

## INTRODUÇÃO

A Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais - LGPD, que regula as atividades de tratamento de dados pessoais, bem como os direitos dos titulares dos dados pessoais, colocou o Brasil entre os países que contam com uma legislação específica para proteção de dados e da privacidade dos seus cidadãos.

A legislação se fundamenta em diversos valores, como o respeito à privacidade; à autodeterminação informativa; à liberdade de expressão, de informação, comunicação e de opinião; à inviolabilidade da intimidade, da honra e da imagem; ao desenvolvimento econômico e tecnológico e a inovação; à livre iniciativa, livre concorrência e defesa do consumidor e aos direitos humanos de liberdade e dignidade das pessoas.

Desde o ano de 2019, o Grupo de Trabalho LGPD, constituído por diversos empregados das empresas Eletrobras, enfrentaram os mais variados desafios para implementar de maneira integrada, o Projeto de Adequação das empresas à LGPD.

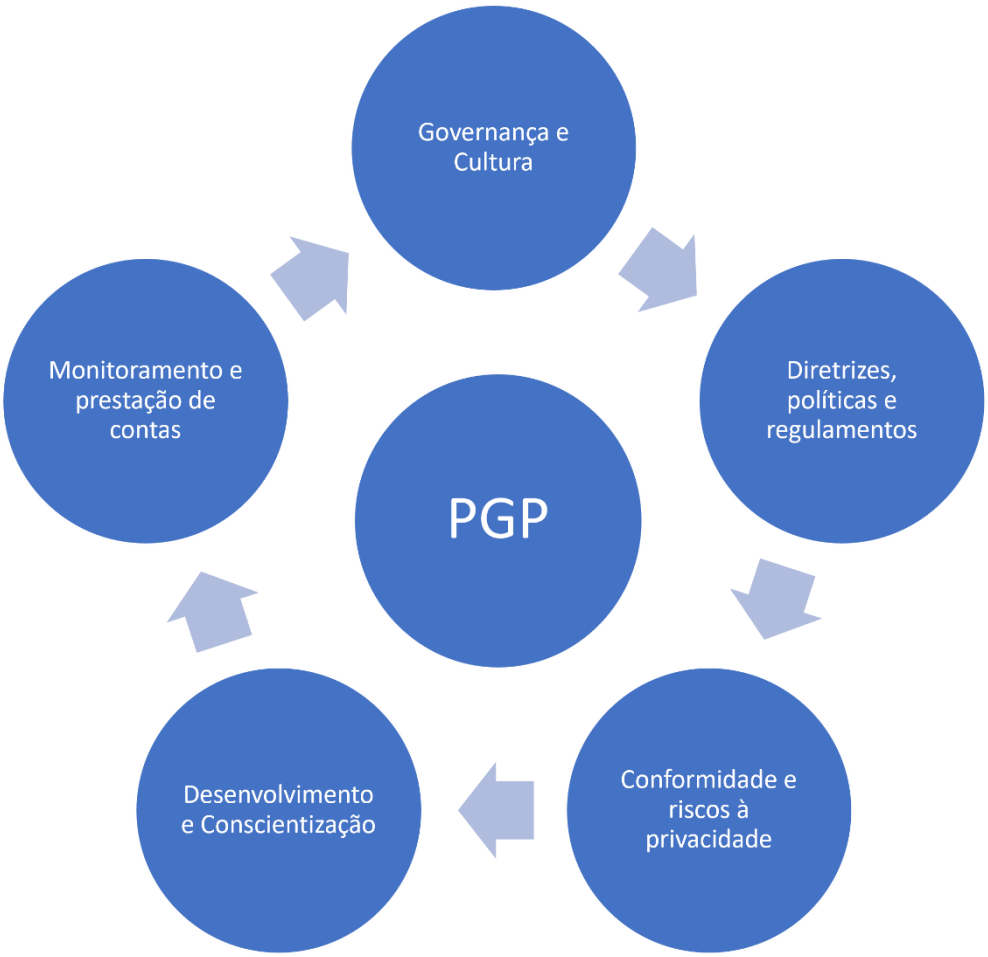
Contudo, a adequação à LGPD extrapola a implementação, pois requer uma mudança cultural no processo de tratamento de dados pessoais. Acrescente-se a isso, o potencial risco à privacidade do titular de dados pessoais, sempre que as atividades empresariais envolvem o tratamento desses dados.

A implementação ampla e inclusiva de um programa direcionado à privacidade pode resultar no aumento da confiança de todas as partes interessadas, pois assegura que o tratamento dos dados pessoais seja realizado de acordo com os princípios definidos na legislação, além de garantir o mapeamento e monitoramento dos riscos ao titular.

Sendo assim, para que a cultura da privacidade e proteção de dados seja incorporada nas empresas e de forma a complementar as ações em andamento, foi desenvolvido o presente Programa de Governança em Privacidade das Empresas Eletrobras (PGP). Sua ampliação e atualização ocorrerão sempre que necessário, de forma que esteja continuamente alinhado com as diretrizes definidas pela Autoridade Nacional de Proteção de Dados (ANPD) e com as diretrizes estratégicas das empresas Eletrobras.

**PROGRAMA DE GOVERNANÇA EM PRIVACIDADE DAS EMPRESAS ELETROBRAS (PGP)**

Com o intuito de sistematizar o Programa para sua implementação e manutenção, ele foi estruturado nos seguintes pilares:




Programa de Governança em Privacidade empresas Eletrobras

A seguir, são apresentadas suas descrições, subdivisões e finalidades, buscando atender às boas práticas de mercado.

## 1. Governança e Cultura

O envolvimento das pessoas é fundamental para o desenvolvimento do programa como meio de promover a conformidade de maneira a prevenir as sanções administrativas e judiciais, e, principalmente, agregar valor à empresa. Sendo assim, este pilar destaca o compromisso da alta administração, assim como a estrutura das equipes para a efetivação do programa.

### 1.1. Compromisso da Alta Administração

O aval explícito e o apoio incondicional da Alta Administração são essenciais para que todos os colaboradores entendam que a privacidade de dados pessoais transcende a ideia de apenas estar em conformidade com legislação e regulamentos, mas abrange aspectos de governança, conduta e transparência.

A Alta Administração, como órgão máximo de deliberação, deve firmar o compromisso em apoiar as regras, políticas e diretrizes instituídas pelo Programa de Governança em Privacidade das Empresas Eletrobras (PGP), através de ações que expressem este posicionamento com comunicações para todos os colaboradores, participação de eventos/treinamentos; sendo exemplo no cumprimento das regras, liberando recursos necessários ao bom andamento do programa.

São exemplos de comprometimento da alta direção:

- Patrocinar o programa de privacidade perante o público interno e externo, ressaltando sua importância para a organização e solicitando o comprometimento de todos os colaboradores e partes interessadas;
- Participar ou manifestar apoio em todas as fases e implementação do programa;
- Aprovar e supervisionar as políticas e medidas de privacidade, destacando recursos humanos e materiais suficientes para seu desenvolvimento e implementação.

Este programa de Governança em Privacidade prevê como um fórum entre as empresas Eletrobras dedicado à governança do tema privacidade e proteção de dados pessoais, o Subcomitê de Privacidade da Eletrobras (SCPE), no âmbito do Comitê Estratégico de Segurança da Informação – CESIE.

### 1.2. Subcomitê de Privacidade da Eletrobras (SCPE)

O SCPE tem atribuições de incorporar novas das novas diretrizes definidas pela Autoridade Nacional de Proteção de Dados – ANPD; manter atualizados a Política de Proteção a Dados Pessoais e à Privacidade e o Regulamento de Governança de Privacidade e Proteção de Dados Pessoais das empresas Eletrobras.

Também é responsabilidade do subcomitê acompanhar, monitorar e gerenciar o Programa de Governança em Privacidade para as empresas Eletrobras, bem como a gestão das ações e medidas a serem implementadas, discussão de boas práticas e soluções para os desafios da proteção de dados pessoais nas empresas Eletrobras.

Neste sentido, é fundamental que o SCPE atue com autonomia, independência e imparcialidade, bem como tenha disponíveis recursos materiais, financeiros e humanos necessários ao desempenho de suas atribuições funcionais.

### 1.3. Demais comitês e a privacidade

Como mecanismo de controle visando garantir a privacidade desde a concepção e por padrão (Privacy by Design e Privacy by Default), é fundamental garantir acesso ao DPO a informações sobre projetos, iniciativas, soluções e sistemas, seja através de reportes periódicos ou através de participação formal em fóruns, comitês e/ou reuniões onde tais iniciativas são avaliadas ou priorizadas, como Comitês de Tecnologia da Informação, Escritórios de Projetos, Reuniões de Pré-Pauta de Diretoria etc.

Também é recomendável que o DPO tenha participação formal no âmbito de cada empresa, em comitês que tratem de temas relacionados à Segurança da Informação, Gestão da Informação, Proteção de Dados e Privacidade.

### 1.4. Encarregado pelo Tratamento de Dados Pessoais - DPO (Data Protection Officer)

O Encarregado pelo Tratamento de Dados Pessoais, também chamado de DPO (Data Protection Officer), deve atuar como um canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados – ANPD. Suas atribuições

são: aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; receber comunicações da autoridade nacional e adotar providências; e orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.

O DPO também deve executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares pela ANPD.

### 1.5. Equipes de Segurança da Informação, privacidade e apoio ao DPO

Nossas empresas não dispõem de equipes exclusivamente dedicadas ao tema da privacidade e da proteção de dados pessoais.

Diante da grande sinergia com a atuação das equipes de Segurança da Informação que atuam na 2ª linha de defesa, recomenda-se que parte da força de trabalho destas equipes possa se dedicar também ao tema da privacidade, garantindo disponibilidade de recursos humanos necessários a execução das ações previstas neste programa.

É fundamental que os gestores responsáveis pelas atribuições de segurança da informação avaliem a necessidade de reforço de suas equipes, visando garantir tal disponibilidade de recursos humanos dedicada a este programa.

### 1.6. Equipes/Unidades Organizacionais / Gestores

Cabe aos gestores de Unidades Organizacionais a elaboração e manutenção dos Registros de Tratamento de Dados – RTD e Relatório de Impacto à Proteção de Dados Pessoais – RIPD, relacionados a atividades sob sua responsabilidade, bem como atender às demandas do DPO e das áreas de segurança da informação, além de executar planos de ação para ajustes de processos e redução de riscos que sejam identificados em processos e atividades sob sua responsabilidade.

### 1.7. Colaboradores

Respeitar a privacidade dos titulares e proteger os seus dados pessoais, em todos os meios utilizados pela empresa, tanto físico, quanto eletrônico, além de participar dos treinamentos e das ações de conscientização promovidas pelas empresas Eletrobras relacionados ao tema da privacidade e proteção de dados.

## 2. Diretrizes, Políticas e Regulamentos

O Programa de Governança em Privacidade das empresas Eletrobras – PGP será guiado por diretrizes regulatórias do tema de Proteção de Dados e pelas diretrizes emanadas pela alta administração das nossas empresas, traduzidas em algumas políticas e regulamentos, destacados neste pilar. Estes normativos devem ser revisados sob a coordenação do Subcomitê de Privacidade da Eletrobras (SCPE).

### 2.1. Política de Proteção a Dados Pessoais e à Privacidade.

O objetivo desta política é estabelecer diretrizes e orientações para o tratamento de dados pessoais, com o objetivo de proteger a privacidade de consumidores, empregados, parceiros ou fornecedores, através da gestão de dados pessoais e da gestão de incidentes de Segurança da Informação com potencial impacto na privacidade dos titulares de dados, seja no ambiente convencional ou de tecnologia das empresas Eletrobras.

### 2.2. Regulamento de Governança de Privacidade e Proteção de Dados Pessoais das empresas Eletrobras.

As principais diretrizes deste regulamento envolvem orientam sobre o tratamento de dados pessoais, Direitos dos Titulares de Dados e Governança dos Riscos ao Titular de Dados Pessoais. Este regulamento visa a padronização do tratamento de dados pessoais nas empresas Eletrobras, através da definição de modelos para os artefatos para Registro de Tratamento de Dados e de relatório de impacto a proteção de dados pessoais.

### 2.3. Regulamento de Privacidade desde a Concepção das Empresas Eletrobras

Este regulamento tem por objetivo a manutenção das boas práticas de proteção de dados, através do estabelecimento de diretrizes para garantir a aplicação dos conceitos de privacidade desde a concepção nos processos, tecnologias, cultura e governança das empresas Eletrobras.

## 3. Conformidade e Riscos a Privacidade

A gestão de riscos oriundos da LGPD envolve duas perspectivas distintas, sendo uma voltada para o risco regulatório gerado para as empresas Eletrobras de eventualmente não agirem em conformidade com a LGPD, mas também a perspectiva dos riscos gerados aos titulares de dados em razão das atividades realizadas pelas nossas organizações.

### 3.1. Risco regulatório – Conformidade com LGPD

Os riscos gerados para as empresas Eletrobras, em razão da LGPD, devem ser gerenciados e priorizados por meio de eventos e fatores de riscos na Matriz de Riscos das Empresas Eletrobras.

Os riscos regulatórios identificados em razão da LGPD envolvem a possibilidade de impactos financeiros, em razão da previsão legal de possíveis sanções financeiras, e de impactos reputacionais, em razão de sanções que preveem a publicização de eventuais infrações cometidas.

As atividades de monitoramento deste fator de risco envolvem o acompanhamento das regulamentações emitidas pela ANPD – Autoridade Nacional de Proteção de Dados, além da revisão periódica dos Registros de Tratamentos de Dados Pessoais (RTDs) e dos Relatórios de Impacto à Proteção de Dados Pessoais (RIPDs).

#### 3.1.1. Atendimento aos Direitos dos Titulares

As empresas Eletrobras deverão manter em seus canais de comunicação, orientações a respeito dos direitos dos titulares de dados, bem como a maneira de exercê-los.

#### 3.1.2. Declarações de Privacidade

No intuito de atender ao princípio da finalidade, e realizar tratamentos de dados pessoais para propósitos legítimos, específicos, explícitos e informados ao titular, as empresas Eletrobras deverão elaborar e manter atualizadas Declarações de Privacidade, voltadas ao objetivo de comunicar às diversas categorias de titulares de dados, a forma nas quais seus dados são tratados. São exemplos de Declarações de Privacidade as dirigidas aos colaboradores, fornecedores e usuários do website da empresa.

### 3.2. Riscos inerentes ao tratamento de dados

A gestão de riscos para os titulares de dados, gerada a partir dos tratamentos de dados identificados nas empresas Eletrobras, deve utilizar o RTD, que contém identificação, análise e avaliação dos riscos, e o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), que contém as medidas de respostas aos riscos.

Após a identificação dos riscos ao titular, é feita a análise do risco onde são atribuídas, na visão do gestor da atividade, a probabilidade de materialização do risco e impacto gerado ao titular em caso de materialização. Essa análise é feita em uma régua de cinco níveis: Mínima, Baixa, Média, Alta e Crítica.

Após a identificação e análise dos riscos, os dados de probabilidade e impacto são projetados num mapa de calor 5x5, de forma a avaliar o nível de exposição dos titulares ao risco, em razão daquela atividade que envolve o tratamento de seus dados.

Caso os tratamentos de dados exponham o titular de dados a um nível alto ou crítico de risco, sejam baseados no legítimo interesse do controlador/operador, envolvam dados pessoais sensíveis ou ainda gerem riscos às liberdades civis e aos direitos fundamentais do titular, deve ser elaborado o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), com o objetivo de identificar medidas, salvaguardas e mecanismos de mitigação de risco.

#### 3.2.1. Cláusulas contratuais

Os instrumentos contratuais firmados pelas empresas Eletrobras deverão conter cláusula padronizada sobre proteção de dados, dedicada aos compromissos assumidos pelas partes em relação aos tratamentos de dados que façam parte do objeto do instrumento contratual.

As cláusulas padronizadas poderão sofrer acréscimos conforme a necessidade de mitigação de riscos identificada na atividade relacionada ao escopo do instrumento contratual.

### 3.2.2. *Due Diligence* de Privacidade

As empresas Eletrobras buscarão inserir em suas rotinas de diligência prévia de fornecedores, a captura de dados que indiquem o nível de maturidade de seus parceiros em relação ao tema da privacidade e proteção de dados.

Os dados de *due diligence* de privacidade serão utilizados para medir o nível de risco de determinado parceiro em relação a atividade exercida, e poderão resultar em medidas adicionais de resposta a riscos, como cláusulas adicionais, aumento de alçada para aprovação de instrumentos contratuais, além de assinatura de termos de compromisso.

### 3.2.3. Acordo de Compartilhamento de dados

As empresas Eletrobras deverão providenciar acordos de compartilhamento de dados, com o objetivo de regular o compartilhamento de dados pessoais entre a Holding e as empresas controladas por meio da utilização de soluções ou estruturas que promovam tratamento de dados pessoais de maneira compartilhada.

### 3.2.4. Incidentes de violação de privacidade

Os incidentes de segurança da informação que envolvam dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, ou ainda aqueles que possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais, devem ser encaminhados para tratamento pelo DPO (Data Protection Officer – Encarregado pelo Tratamento dos Dados Pessoais) de cada empresa, que deve se orientar pelo Regulamento de Tratamento de Incidentes de Segurança da Informação das Empresas Eletrobras.

## 4. Desenvolvimento e Conscientização

O sucesso deste Programa de Governança em Privacidade depende da capacidade que as empresas Eletrobras tem de promover campanhas de disseminação da cultura da privacidade, bem como da realização de treinamentos para públicos segmentados, de acordo com seu nível de atuação e responsabilidade na proteção de dados pessoais. O planejamento de desenvolvimento e capacitação com foco no tema da privacidade e proteção de dados, deverá ser parte do Planejamento de Educação e Conscientização em Segurança da Informação das empresas Eletrobras, a ser revisto anualmente.

### 4.1. Comunicação

As empresas Eletrobras devem manter canais de comunicação permanentes para abordar os assuntos relacionados aos dados pessoais tratados pela empresa, visando um relacionamento transparente com os seus stakeholders. Tais canais podem, visando maior eficácia, serem segmentados por público e/ou categorias de titulares de dados. Fazem parte de mecanismos de comunicação os Portais de Privacidade, as declarações de privacidade, seções em ambientes de intranet e boletins periódicos dos serviços internos de comunicação.

### 4.2. Sensibilização

Ações e campanhas de sensibilização sobre o valor da privacidade e a responsabilidade no tratamento de dados pessoais devem ser priorizados quando se buscar atingir o público geral de colaboradores da empresa, ou ainda públicos externos. Web series, eventos periódicos com fornecedores, patrocinados, estagiários, eventos em datas relevantes ao tema, são exemplos de ações de sensibilização que devem ser realizados anualmente visando aumento da maturidade em proteção de dados nas empresas Eletrobras.

### 4.3. Treinamentos

Os Encarregado pelo Tratamento de Dados Pessoais - DPO (Data Protection Officer), colaboradores que atuam diretamente no tratamento de dados pessoais com maior frequência, bem como os colaboradores das equipes de Segurança da Informação, privacidade e apoio ao DPO, deverão realizar treinamentos formais e periódicos sobre o tema, visando a obtenção de subsídios para o aprimoramento contínuo deste Programa de Governança em Privacidade - PGP.

## 5. Monitoramento e Prestação de Contas

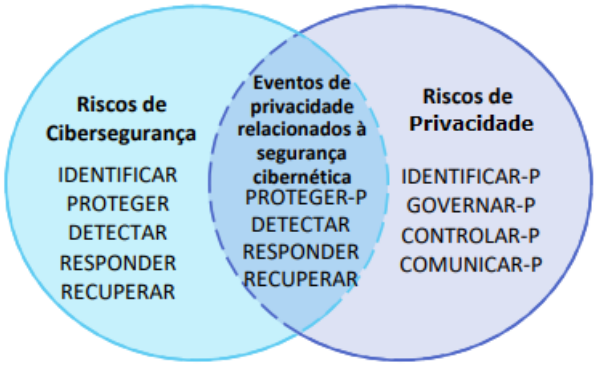
O atingimento dos objetivos deste Programa de Governança em Privacidade – PGP depende de mecanismos de monitoramento, avaliação e aprimoramento contínuos, visando a verificação da efetiva implementação do Programa e identificar pontos falhos que precisem ser corrigidos e/ou aprimorados.

### 5.1. Integração com planejamento de Segurança da Informação

Diante da sinergia e complementariedade entre os temas da Privacidade e da Segurança da Informação, é imprescindível que ambos os temas sejam pensados e monitorados de maneira integrada. Dentre os diversos pontos de conexão entre os temas, podemos citar a presença do Subcomitê de Privacidade no âmbito do Comitê Estratégico de Segurança da Informação – CESIE, o compartilhamento de recursos humanos entre as respectivas equipes, a existência de normas e procedimentos compartilhados, bem como a existência de modelos de gestão e maturidade complementares entre os temas. Desta forma, este programa buscará atuar de maneira conjunta e integrada com o planejamento e as ações do Programa de Segurança da Informação.

### 5.2. NIST Privacy Framework

O Privacy Framework do NIST (National Institute of Standards and Technology) segue a estrutura do Cyber Security Framework do mesmo instituto. A proposta é que a avaliação de maturidade já realizada em Segurança da Informação passe a incorporar funções do framework de privacidade, conforme figura abaixo:




Nesse sentido, as funções previstas no Framework de Privacidade do NIST deverão ser inseridas no atual modelo de avaliação de maturidade em Segurança da Informação, com

objetivo específico de medir o nível de maturidade em privacidade e, desta forma, orientar as priorizações de iniciativas a serem adotadas por este programa.

Com o objetivo de aprimorar a gestão de desempenho das empresas Eletrobras aos processos de privacidade e proteção de dados, alguns indicadores de desempenho poderão ser adotados de forma padronizada entre as empresas, como por exemplo quantidade de incidentes, percentual de processos registrados em RTDs, ou ainda tempo de resposta nos atendimentos a solicitações de titulares de dados.

### 5.3. Reuniões do Subcomitê de Privacidade das empresas Eletrobras

A coordenação deste programa e de suas ações terá como mecanismo de gestão, a reunião de dois tipos de reunião periódica.

As reuniões ordinárias do Subcomitê de Privacidade da Eletrobras (SCPE) serão mensais, terão duração de duas horas, e terão por objetivo o acompanhamento das iniciativas e projetos priorizados neste Programa, bem como o planejamento de novas iniciativas.

Visando uma resposta mais rápida a situações que surjam durante o trabalho dos DPOs e das equipes de privacidade, serão realizadas quinzenalmente reuniões denominadas de PGP, com duração de uma hora e com objetivo compartilhar desafios e buscar padronização no tratamento de situações específicas envolvendo proteção de dados nas empresas Eletrobras.

### 5.4. Reportes a alta Administração

Os relatórios sobre monitoramento dos riscos, planejamento de ações priorizadas, e acompanhamento de iniciativas ligadas ao tema da privacidade deverão compor os relatórios trimestrais encaminhados ao Comitês de Apoio ao Conselho de Administração – CAE.