



Conselho Nacional de  
Proteção de Dados  
Pessoais e da Privacidade

Governança de dados  
no âmbito corporativo  
e privado

GTT 3

2025



**CONSELHO NACIONAL DE PROTEÇÃO DE DADOS  
PESSOAIS E DA PRIVACIDADE**

**Cassio Augusto Muniz Borges**  
**Claudio Eduardo L. de Abreu Rocha**  
**Fernando Antonio Santiago Junior**  
**João Frederico Chagas Maranhão**  
**João Marcos Pereira Vidal**  
**Marcos Vinícius Barros Ottoni (Coordenador Suplente)**  
**Myreilla Aloia Triumpho Pereira da Cruz (Coordenadora  
Titular)**

**SUBSÍDIOS PARA A ELABORAÇÃO DA  
POLÍTICA NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E  
DA PRIVACIDADE**

**Relatório de coleta de subsídios para elaboração  
da Política Nacional de Proteção de Dados  
Pessoais e da Privacidade elaborado pelo Grupo  
de Trabalho nº3 do Conselho Nacional de  
Proteção de Dados Pessoais e da Privacidade.  
Nomeação do GT3: Portaria CNPD Nº 03/2024  
Relatório apresentado à Presidência do CNPD  
em 09/02/2025**

**Brasília  
2025**

## SUMÁRIO

- 1) Contextualização e Introdução
- 2) Histórico das Atividades
- 3) Metodologia
- 4) Referencial Teórico
  - 4.1 Função da Política Nacional de Proteção de Dados Pessoais e da Privacidade
  - 4.2 Definição de Governança de Dados Pessoais
  - 4.3 Benefícios da Governança de Dados Pessoais
  - 4.4 Estrutura da Governança de Dados Pessoais
  - 4.5 Ciclo de Vida dos Dados Pessoais
  - 4.5 Padrões e Frameworks Adotados
  - 4.7 Diretrizes e Boas Práticas
- 5) Conclusão
- 6) Referências

## 1. CONTEXTUALIZAÇÃO E INTRODUÇÃO

A Lei Geral de Proteção de Dados Pessoais (LGPD) dispõe sobre a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade (PNPD), documento este que tem por objetivo fomentar atividades econômicas e tecnológicas que estejam em sintonia com direitos e garantias fundamentais, visando assegurar, no país, um ambiente adequado ao desenvolvimento da sociedade e o fluxo informacional com foco na proteção de dados pessoais.

Assim, para a elaboração da PNPD, a LGPD em seus artigos 55- J, III e 58-B, I, designa como competência da ANPD e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD), respectivamente: I - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; e II - propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD.

Para tanto, através da Portaria CNPD nº 3 de 04/10/2024 foi instituído Grupo de Trabalho nº 3 ("GT3") dedicado a fornecer subsídios, na temática de Governança de Dados (I), para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade, no âmbito do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade.

De acordo com o art. 2º de referida Portaria, é de competência do GT3 realizar análises, estudos e fazer proposições na temática supre mencionada para a elaboração da PNPD.

Ainda, como disposto no Art.3º da mesma Portaria, o GT3 é composto pelos seguintes membros do CNPD:

I - Myreilla Aloia Triumpho Pereira da Cruz, membro titular representante de Confederações Sindicais representativas das categorias econômicas do setor produtivo e coordenadora do GT3;

II - Fernando Antonio Santiago Junior, membro titular representante de outros poderes, órgãos ou instituições públicas;

III - Cassio Augusto Muniz Borges, membro titular representante de Confederações Sindicais representativas das categorias econômicas do setor produtivo;

IV - Claudio Eduardo Lobato de Abreu Rocha, membro suplente representante de entidades representativas do Setor Laboral;

V - Marcos Vinícius Barros Ottoni, membro suplente representante de Confederações sindicais representativas das categorias econômicas do setor produtivo e coordenar suplente do GT3;

VI - João Marcos Pereira Vidal, membro suplente representante de entidades representativas do Setor Laboral; e

VII - João Frederico Chagas Maranhão, membro titular representante de Confederações sindicais representativas das categorias econômicas do setor produtivo.

Isto posto, de forma introdutória e considerando que no mundo corporativo atual a quantidade de informações cresce exponencialmente, importante ressaltar que a Governança de Dados Pessoais, nitidamente se transformou em medida essencial e uma necessidade estratégica para maior competitividade, assertividade, principalidade dos titulares de dados pessoais, conformidade regulatória e segurança das empresas em um ambiente cada vez mais digital.

Desta forma, a Governança de Dados Pessoais garante a qualidade, segurança e disponibilidade dos dados pessoais dentro das organizações, portanto o presente documento tem como objetivo fornecer subsídios sobre Governança de Dados Pessoais, destacando seu alcance, escopo, importância, benefícios, principais componentes e boas práticas para a implementação.

## **2. HISTÓRICO DE ATIVIDADES**

Cumprir relatar que as atividades do GT3 foram desenvolvidas em 11 (onze) reuniões ordinárias on line de acordo com o Plano de Trabalho apresentado à Presidência do CNPD em 01/11/2024, o qual é parte integrante e inseparável do presente Relatório Final como Anexo I e conforme metodologia abaixo.

## **3. METODOLOGIA**

Para as pesquisas, estudos e mapeamentos de subsídios para PNPD sobre Governança de Dados Pessoais, o GT3 adotou metodologia qualitativa e conceitual com foco em explorar, explicar, correlacionar e descrever uma compreensão aprofundada das informações coletadas e apuradas.

Todas as informações e conceitos foram apurados por intermédio de pesquisas, estudos, mapeamento de normas e regulamentos, análise aprofundada de materiais do setor privado e público. Ainda, foram realizados debates e consultas com os especialistas e profissionais da área abaixo relacionados.

### **Mirian Wimmer**

Doutora em Políticas de Comunicação e Cultura pela Faculdade de Comunicação da UnB, Mestre em Direito Público e graduada em Direito pela UERJ. Certificada como especialista em proteção de dados pessoais (Europa) pela International Association of

Privacy Professionals (CIPP/E). Bolsista do programa internacional da Universidade de Waseda em Tóquio entre 2001 e 2002, com Distinção Acadêmica. Professora do corpo permanente do Mestrado Profissional em Direito, do IDP-Brasília e professora convidada em diversas instituições de ensino de nível superior, em temas relacionados ao direito digital, à tecnologia e à proteção de dados pessoais. É servidora pública desde 2007, integrante da carreira de Especialista em Regulação de Serviços Públicos de Telecomunicações da Anatel. Ocupou diferentes cargos de direção no Ministério das Comunicações - MC e no Ministério de Ciência, Tecnologia, Inovações e Comunicações - MCTIC, onde coordenou a elaboração da Estratégia Brasileira para a Transformação Digital. É, atualmente, Diretora da Autoridade Nacional de Proteção de Dados - ANPD. Desenvolve atividades profissionais e acadêmicas em temas ligados à Internet, às telecomunicações, às políticas digitais e à proteção de dados pessoais.

#### **Carlo Eduardo Passereni Reolon**

Especialista em Tecnologia da Informação e Cybersecurity e Gerenciamento de Projetos Legais e Fiscais na IBM, Coordenador da Comissão de Estudo de IA da ABNT, Expert em Governança de IA e Especializado em Dados.

#### **Fabício da Mota Alves**

Advogado, Sócio Coordenador em Direito Digital e Proteção de Dados do Serur Advogados, Conselheiro Titular no CNPD (1 Mandato) como representante do Senado Federal, Conselheiro e Membro Fundador da Associação Brasileira de Governança Pública de Dados Pessoais, Assessor legislativo sênior do Senado Federal e participou da Comissão de Juristas que elaborou o projeto de lei de regulação da Inteligência Artificial no Brasil. Conselheiro na Anatel.

#### **Mariana Kirmayr Ceridono**

Encarregada de Dados Pessoais da Tempest Security Intelligence. Advogada especialista em Privacidade e Proteção de Dados Pessoais. Certificada pela Exin e pelo Data Privacy Brasil.

Os membros do GT3, com base nos estudos realizados, estruturaram conjuntamente o Relatório Final de Subsídios à PNPd sobre o tema de Governança de Dados.

## **4. REFERENCIAL TEÓRICO**

### **4.1 Função da Política Nacional de Proteção de Dados Pessoais e da Privacidade**

É crucial esclarecer que políticas são instrumentos importantes para orientar quanto a diretrizes, condutas, ações e formas de atuação das organizações em decorrência de um ato normativo, seja no segmento público ou privado, sendo indispensável interpretar que as políticas não possuem caráter de lei.

Enquanto a lei possui comandos obrigatórios e coercitivos, as políticas definem objetivos, condutas e práticas de atuação, em decorrência daquela, mas não criaram novas regras jurídicas, mas sim orientações para que as organizações operem de forma alinhada com propósitos específicos e em conformidade com os dispositivos regulatórios.

Neste racional, a PNPD será um documento principiológico, a qual deverá dispor sobre as prioridades na vertente de Governança de Dados Pessoais para que as organizações tenham suas próprias políticas, planos e programas institucionais de Governança de Dados Pessoais.

Não é prejudicial ainda mencionar que a PNPD deve acompanhar a evolução do tema de Proteção de Dados Pessoais e da Privacidade no país e no mundo, portanto ser submetida a periódicas atualizações.

## **4.2 Definição de Governança de Dados Pessoais**

Governança de Dados Pessoais refere-se ao conjunto de políticas, processos e estruturas de controle necessários para assegurar a qualidade, integridade, disponibilidade, segurança e uso ético de dados pessoais, garantindo que estes sejam precisos, adequadamente tratados e processados desde sua coleta até o expurgo e exista efetiva gestão dos dados pessoais. Trata-se da modelagem de um conjunto de regras e princípios que permite conciliar os direitos fundamentais dos titulares dos dados pessoais e dos usuários em geral com a emergência de novas iniciativas e modelos econômicos baseados em dados pessoais.

Portanto, indispensável interpretar a importância da existência de uma estrutura de governança de dados pessoais, a qual engloba toda a organização com papéis e responsabilidades claramente definidos quanto a gestão de dados pessoais, administração e supervisão rigorosa quanto as ferramentas utilizadas e quanto ao cumprimento dos procedimentos implantados.

A confiabilidade trazida pela Governança de Dados Pessoais maximiza a qualidade da tomada de decisão e mitiga riscos regulatórios, financeiros e reputacionais, visto:

- ✓ Garantir a conformidade regulatória;
- ✓ Proteger a reputação das organizações;
- ✓ Evitar perdas e penalidades financeiras;
- ✓ Fornecer dados confiáveis e precisos;
- ✓ Otimizar processos;

- ✓ Garantir segurança e privacidade;
- ✓ Aumentar eficiência; e
- ✓ Reduzir custos

### **4.3 Benefícios da Governança de Dados Pessoais**

A implementação de Governança de Dados Pessoais oferece uma série de benefícios relacionados, notadamente, à confiança dos usuários e dos titulares de dados pessoais na economia digital, tais como:

#### **a) Melhor Qualidade dos Dados Pessoais**

Dados pessoais mais confiáveis, precisos, completos e consistentes proporcionam base sólida e assertiva para tomada de decisões em ações estratégicas.

#### **b) Interoperabilidade**

A Governança de Dados Pessoais possibilita a interoperabilidade destes dados e sistemas entre departamentos, empresas do mesmo grupo econômico, parceiros externos, distintos setores, bem como entre os setores públicos e privados de modo que as informações sejam tratadas e reutilizadas de forma mais ágil, eficiente e conforme disposto na legislação.

#### **c) Maior eficiência**

A Governança de Dados Pessoais proporciona processos bem estruturados, os quais evitam duplicidade de atividades e esforços e, de modo associado, minimizam a necessidade de correções e retrabalhos em decorrência de dados pessoais inconsistentes ou incorretos.

Indispensável ressaltar que atividades realizadas com base em dados pessoais organizados e acessíveis são desenvolvidas de forma mais ágil, resultando em ganhos significativos de produtividade e otimização de recursos e tempo.

#### **d) Redução de custo**

A boa qualidade dos dados pessoais consolida decisões personalizadas, assertivas, em menor tempo, de modo a aprimorar ações estratégicas, a segurança e confiabilidade das decisões tomadas resultando em maior satisfação dos clientes aumentando sua principalidade em relação aos produtos e serviços ofertados pelas empresas.

Um adequado programa de Governança de Dados Pessoais evita investimentos desnecessários e racionaliza a gestão financeiras das organizações.



### **e) Segurança e Privacidade**

A proteção de dados pessoais e a segurança da informação são vertentes fundamentais da Governança de Dados Pessoais, pois através de estruturado plano de Governança de Dados Pessoais define-se quem tem acesso a quais informações, estabelecendo controles rigorosos sobre o armazenamento, o compartilhamento e o processamento de dados pessoais. Isso garante que os dados pessoais estejam protegidos contra acessos não autorizados e tratamentos indevidos.

### **f) Redução de riscos regulatórios, financeiros e reputacionais**

Como consequência dos benefícios anteriores há garantia de atuação das organizações quanto a conformidade com a legislação, evitando assim perdas financeiras e penalidades, bem como risco de danos à imagem e marca das organizações.

## **4.4 Estrutura da Governança de Dados Pessoais**

A estrutura de Governança de Dados Pessoais diz respeito à pessoa ou grupo de pessoas responsáveis, em cada organização, por analisar os tratamentos de dados pessoais realizados, refletir e zelar pela sua conformidade. Considerando os inúmeros perfis e características de cada organização, não é possível determinar a sua forma ou organização, sendo comum encontrar, a título exemplificativo:

- i. Estrutura Organizacional: Encarregado, Gestor de Dados Pessoais, Detentor de Dados Pessoais
- ii. Comitê de Governança de Dados Pessoais e Fóruns de Aprovação: grupo multidisciplinar, o qual define políticas e diretrizes, monitora o ciclo de vida dos dados pessoais, supervisiona a implementação de toda a governança e garante a conformidade.
- iii. Equipe de Segurança da Informação.

No pilar de estrutura de Governança de Dados Pessoais deve-se observar todo o disposto na Resolução CD/ANPD nº 2 de 27.01.2022, a qual aprova o Regulamento de aplicação da LGPD para agentes de tratamento de pequeno porte.

## **4.5 Ciclo de Vida dos Dados Pessoais**

Toda organização deve compreender e analisar os elementos relacionados ao ciclo de vida dos dados pessoais tratados sob sua responsabilidade. Adota-se, para fins da

presente exposição, a decomposição do ciclo de vida dos dados pessoais em sete (7) etapas a saber: a coleta, o tratamento, a validação, o armazenamento, a difusão, as reutilizações e o arquivamento definitivo<sup>1</sup>:

## **1. Fase de Coleta**

Trata-se da fase inicial de aquisição dos dados pessoais, sejam eles criados, coletados, gerados ou produzidos. Nessa etapa examina-se o fundamento jurídico que torna legítima a detenção do dado, seja ele pela obtenção no respeito das condições exigidas LGPD ou, eventualmente, fundamentada em outra regra jurídica (ex: direito contratual, autoral, etc).

## **2. Tratamento**

Esta etapa diz respeito à legitimidade do tratamento segundo as finalidades definidas e indicadas antes da coleta. O tratamento do dado pode, eventualmente, prescindir do consentimento para sua legitimidade, mas sempre requer a observância do dever de informação e da fidelidade às finalidades informadas. O tratamento deve sempre observar as regras jurídicas que tornam lícitas a sua realização (LGPD), assim como as práticas apropriadas assimiladas à ética (regulamentos profissionais, projeto de lei sobre inteligência artificial), etc.

Em determinados, casos o tratamento deve ser precedido de etapas anteriores que o legitimam, como privacy by design, minimização, ou teste de um algoritmo de inteligência artificial antes da realização do tratamento principal.

## **3. Validação**

A governança dos dados pessoais exige a capacidade de justificar a prova de um fato ou de uma situação jurídica que assegure a licitude do tratamento. Essa prova pode, segundo o caso, revestir diversas formas, como um contrato, um consentimento, um registro de tratamento, ou até mesmo um processo técnico (assinatura eletrônica, blockchain, reconhecimento facial, etc).

## **4. Armazenamento**

A governança dos dados pessoais deve integrar necessariamente a relação entre o detentor dos dados pessoais e um terceiro (ou diversos) responsáveis pelo armazenamento dos dados pessoais em seus sistemas de informação e/ou servidor. Esse relacionamento dá origem a uma relação jurídica que deve ser construída segundo os requisitos previstos pela lei, integrando, entre outros, medidas adequadas de proteção contra acesso não autorizado e perda de dados pessoais, e também as disposições específicas sobre transferência internacional de dados pessoais.

---

<sup>1</sup> Sobre o tema, ver : CASSAR B., La gouvernance des données, Enc. Dalloz, Rép. NTIC et IP/IT, 2022

## **5. Modalidades de Acesso e Compartilhamento de Dados Pessoais**

Esta fase trata das políticas e procedimentos visando que o acesso e o compartilhamento de dados pessoais entre diferentes entidades sejam controlados e realizados de maneira segura e conforme as regulamentações aplicáveis. Cada detentor de dados pessoais tem, em função dos direitos dos quais dispõe, a possibilidade de definir as modalidades do seu acesso. No entanto, o compartilhamento requer a implementação de medidas de proteção dos titulares que devem acompanhar os dados pessoais compartilhados.

## **6. Reutilização e Análise Estatística**

A reutilização de dados pessoais - coletados de forma lícita - para fins diversos da finalidade principal deve ser prevista no momento da coleta. São as denominadas "finalidades secundárias" que podem ser importantes para diversas atividades de pesquisa e desenvolvimento ou de inovação. No setor público o dado pode ser, ainda, objeto de políticas de Open Data ou tratados para fins de análise estatística. Tais finalidades secundárias podem proporcionar insights valiosos, mas devem ser sempre realizadas segundo os princípios preconizados nas normas de privacidade e proteção de dados pessoais.

## **7. Arquivamento Eletrônico**

O arquivamento eletrônico difere-se do armazenamento na medida em que envolve a preservação de dados pessoais a longo prazo, passando de um estatuto de ativo e explorável a um estatuto perene cujo acesso é reduzido e limitado a determinadas finalidades. Na maior parte das vezes, o arquivamento tem por finalidade a gestão e o exercício de direitos ou a pesquisa.

Geralmente, esse arquivamento tem características distintas segundo a sua natureza pública ou privada. O primeiro caso pode ser regido por normas especiais que determinam a conservação da memória da ação estatal e a prestação de contas. O segundo caso, considerando a noção de término do tratamento veiculado pela LGPD, o arquivamento deve, na maior parte dos casos, ser eliminado. Ressalte-se que a lei pode enquadrar o prazo de arquivamento desses dados pessoais, razão pela qual a governança dos dados pessoais deve considerar mecanismos que permitam o controle desses prazos.

Esses tópicos podem servir como base para a elaboração de uma Política Nacional de Proteção dos Dados Pessoais que incite à reflexão sobre todas as fases do ciclo de vida dos dados pessoais, garantindo assim uma melhor proteção e o amadurecimento das práticas relacionadas ao tema.

## 4.6 Padrões e Frameworks Adotados

Padrões e frameworks utilizados pelas organizações para orientar a governança dos dados pessoais. Esses padrões permitem que as empresas adotem uma abordagem sistemática, permitindo ser auditável, e alinhada às melhores práticas internacionais.

Entre referenciais, o DAMA-DMBOK (Data Management Body of Knowledge), define Governança de Dados Pessoais como a execução de autoridade, controle e tomada de decisão compartilhada (planejamento, monitoramento e fiscalização) sobre o gerenciamento de ativos de dados pessoais.

A governança de dados pessoais, integrada à governança corporativa e de TI, é abordada pela ISO/IEC 38505, que foca no valor, risco e conformidade associados aos dados pessoais. A norma fornece princípios orientadores para a governança de dados pessoais dentro das organizações. Ela é uma adoção da norma internacional ISO/IEC 38505-1:2017 e foi elaborada para ajudar as estruturas de governança a utilizarem dados pessoais de forma eficaz, eficiente e aceitável. O foco principal da norma é assegurar que as organizações possam maximizar o valor dos dados pessoais enquanto gerenciam os riscos associados a eles.

A norma estabelece que a governança de dados pessoais é um subconjunto da governança de TI e se preocupa com a aplicação de princípios de governança para o uso e proteção de dados pessoais. Isso inclui a responsabilidade pela qualidade, segurança e conformidade dos dados pessoais, além de garantir que as partes interessadas possam confiar na forma como os dados pessoais são geridos.

Além disso, a norma orienta as organizações a desenvolverem uma cultura de dados pessoais que promova o compartilhamento e a proteção adequados, e a implementarem políticas que assegurem o uso responsável dos dados pessoais. Isso é especialmente relevante em um contexto em que o volume de dados pessoais está crescendo rapidamente, e onde a proteção de dados pessoais e a conformidade com legislações são cada vez mais críticas.

Em termos de segurança, o ISO/IEC 27001, uma referência em sistemas de gestão de segurança da informação, estabelece requisitos para proteger os dados pessoais contra ameaças, enquanto o NIST Cybersecurity Framework é amplamente adotado para fortalecer a segurança cibernética. A ISO/IEC 27701, por sua vez, complementa a segurança com diretrizes específicas para privacidade, alinhando-se a regulamentações como a LGPD e o GDPR.

## 4.7 Diretrizes e Boas Práticas

Nos cenários digital, social e econômico atuais, em que os dados pessoais são considerados um dos ativos mais importantes das organizações de todos os

segmentos, a Governança de Dados Pessoais está longe de se resumir a processos burocráticos ou prolixos, mas sim deve estabelecer estrutura que possibilite às organizações aproveitar ao máximo a geração de valor econômico dos dados pessoais no mesmo diapasão em que protege e controla sua integridade, além de assegurar a conformidade em seu uso.

Disto isso, há valor imensurável no desenho de diretrizes e boas práticas que sustentem uma Governança de Dados Pessoais palpável e sustentável tendo em mente, mas não apenas, as condutas abaixo, para assegurar que os dados pessoais sejam, de fato, tratados como recurso estratégico por todas as partes envolvidas.

O objetivo das boas práticas é propor diretrizes factíveis e passíveis de serem efetivamente adaptadas e implantadas pelas mais diversas realidades organizacionais, auxiliando as empresas a inovar fazendo uso da Governança de Dados Pessoais a seu favor, considerando a informação pautar cada vez mais o mundo moderno.

Atualmente está claro que o Estado tem muito a ganhar se puder contar com a colaboração da sociedade para compartilhar a responsabilidade de implementar sua agenda regulatória - em particular diante de todas as complexidades advindas das novas aplicações tecnológicas, despontando como fundamental o apoio da rede de atores privados que fórmula, desenha, utiliza e aplica essas tecnologias.

É nesse sentido que a LGPD traz, de forma inovadora, a possibilidade de realização de códigos de conduta pelo setor privado, nos termos de sua seção II, dedicada exclusivamente às boas práticas e à governança. O seu art. 50, caput, traz a possibilidade de que as empresas individualmente ou por meio de associações formulem regras de boas práticas e de governança, enquanto o parágrafo 3º deste mesmo dispositivo estabelece a possibilidade de que tais regras sejam reconhecidas e divulgadas pela Autoridade Nacional.

Como foco para uma Política Nacional, entendemos que referida inovação legislativa deve ser fomentada, por se constituir em uma grande oportunidade para o setor promover a implementação da LGPD, aplicando as melhores práticas nacionais e internacionais e garantindo os direitos previstos no referido diploma legal, ao tempo que possibilita debater as suas especificidades

Assim, as boas práticas relacionadas a Governança de Dados Pessoais podem abordar diversos temas, tais como:

- ✓ Planejamento Estratégico
- ✓ Definição de Propósito

- ✓ Mapeamento quanto ao Ciclo de Vida dos Dados Pessoais
- ✓ Políticas Claras e Acessíveis
- ✓ Códigos de Conduta
- ✓ Regras de Segurança e Backup
- ✓ Monitoramento Contínuo e Avaliação
- ✓ Capacitação Contínua

## 5. CONCLUSÃO

A Governança de Dados Pessoais é fundamental para organizações que almejam maior competitividade, rentabilidade e principalidade nos clientes e titulares, garantindo conformidade, segurança, eficiência e menor custo.

Um ambiente de negócios confiável, o qual promove a inovação e o respeito à privacidade e segurança de dados pessoais, sem dúvida é respaldado por um programa de Governança de Dados Pessoais bem estruturado pautado em dados pessoais confiáveis, precisos e seguros.

Para atender as demandas de mercado e rigorosas regulações sobre privacidade e proteção de dados pessoais é essencial o compromisso contínuo com a governança.

Dito isto, talvez seja pertinente a ANPD refletir sobre a necessidade de detalhar o tema Governança de Dados Pessoais em documento público específico.

Isto posto, como conclusão dos estudos realizados e considerando como temas prioritários, entendemos que a PNPD no que tange a Governança de Dados Pessoais, deve abordar essencialmente:

- ✓ Entendimento sobre o escopo e abrangência da Governança de Dados Pessoais;
- ✓ Implantação de uma Política de Governança de Dados Pessoais;
- ✓ Implantação de um Plano de Governança de Dados Pessoais nas empresas com foco na transversalidade, ou seja, no envolvimento de diversas áreas, como a Tecnologia da Informação, Jurídico, Compliance, Segurança da Informação, Riscos, CDO e todas as áreas que tratam dados pessoais;
- ✓ Implantação de diretrizes e boas práticas para a Governança de Dados Pessoais abrangendo os temas constantes do item 4.7 do presente Relatório Final;
- ✓ Implantação de métricas e indicadores para medir o desempenho e os resultados das ações de Governança de Dados Pessoais
- ✓ A estrutura organizacional no que tange a atribuições, responsabilidades e processos;
- ✓ O mapeamento e Gestão do Ciclo de Vida dos Dados Pessoais pelas empresas;
- ✓ As organizações devem avaliar se os padrões e frameworks, alguns citados no item 4.6 do presente Relatório Final, podem auxiliar na implantação e monitoramento de uma Política de Governança de Dados Pessoais.

Conclui-se, portanto, que a definição e a implementação de práticas robustas de Governança de Dados Pessoais são essenciais para assegurar o tratamento adequado e a proteção dos dados pessoais, conforme exigido pela LGPD.

A Governança de Dados Pessoais deve ser vista como uma iniciativa transversal e estratégica, em que se espera que as organizações adotem abordagens proativas e sistemáticas para garantir a conformidade, a transparência e a confiança dos titulares de dados, promovendo um ambiente de respeito à privacidade.

Em síntese, a Governança de Dados Pessoais não é apenas um requisito regulatório, mas um diferencial competitivo estratégico no mercado atual. Sua implementação efetiva requer comprometimento das organizações em estabelecer políticas claras, processos bem definidos e práticas alinhadas às questões regulatórias e frameworks disponíveis.

Ao tratar os dados pessoais com segurança, precisão, transparência e responsabilidade, os agentes de tratamento, além de estarem em conformidade com a legislação, fortalecem a confiança dos titulares e promovem a inovação em um ambiente de negócios cada vez mais desafiador.

Assim, a Governança de Dados Pessoais deve ser compreendida como um pilar essencial para a sustentabilidade, a competitividade e a proteção dos direitos fundamentais à privacidade no cenário em constante evolução.

## **6. REFERÊNCIAS**

- Cartilha de Governança de Dados do Poder Executivo Federal
- CASSAR B., La gouvernance des données, Enc. Dalloz, Rép. NTIC et IP/IT, 2022
- Política de Governança de Dados Pessoais do Ministério das Comunicações
- BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais
- General Data Protection Regulation – GDPR
- BRASIL. Lei Complementar nº 131, de 27 de maio de 2009. Lei da Transparência

- BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações
- BRASIL. Lei nº 14.129, de 29 de março de 2021. Dispõe sobre princípios, regras e instrumentos para o Governo Digital
- BRASIL. Lei nº 13.853 de 08/07/2019 – Altera a Lei nº 13.709 de 14.09.2018
- Diretrizes e Política de Governança de Dados Pessoais de grandes empresas do setor privado como Totvs, Leega, SAP, Banco Santander (Brasil) S.A
- Plano de Governança de Dados Pessoais do Banco Santander (Brasil) S.A.
- Subsídios apresentados pelas Instituições Financeiras (Mercantil, Bradesco, Santander e Itaú)
- Subsídios apresentados pelos entrevistados mencionados no item 3 do presente documento.

De São Paulo para Brasília, 30 de janeiro de 2025.

Atenciosamente,



**Myreilla Aloia Triumpho Pereira da Cruz**

Conselheira Titular do CNPD e Coordenadora do GT 3



## **ANEXO I**

### **PLANO DE TRABALHO**



### **Plano de Trabalho do GT3 do CNPD**

#### **Governança de Dados I<sup>2</sup>**

#### **I) Objetivos**

Fornecer subsídios e diretrizes no que tange a Governança de Dados para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade (PNPD).

O GT apresentará proposta para estabelecer, monitorar e aprimorar as práticas de gestão de dados pelos agentes de tratamento, assegurando que os dados sejam tratados de forma ética, eficiente, segura e de acordo com os dispositivos legais vigentes.

No tema objeto do GT3 serão abarcadas também disposições sobre governança de privacidade.

#### **II) Metodologia**

Pesquisas, estudos, mapeamento de normas e regulamentos, análise aprofundada da Cartilha de Governança de Dados do Poder Executivo Federal, do Acórdão nº 390 do TCU, do Relatório Final de Subsídios da Política Nacional de Proteção de Dados elaborado no primeiro mandato do Conselho Nacional de Proteção de Dados, bem como das diretrizes da ISO 38505 e ISO 27001, bem como demais

---

<sup>2</sup>PORTARIA CNPD Nº 03, DE 4 DE OUTUBRO DE 2024

materiais e conteúdos que apresentem insumos importantes ao tema de Governança de Dados. Consultas a especialistas e profissionais da área. Ainda, realização de reuniões internas de alinhamento do GT3, reuniões internas conjuntas de alinhamento entre os GTs 3 e 4, elaboração conjunta do relatório pelos membros do GT e aprovação do texto final.

III) Cronograma das atividades

Considerando os prazos estabelecidos na Portaria CNPD nº 03 de 04/10/2024, conforme subitem III.1, propomos no presente Plano de Trabalho como Cronograma do GT3 o constante no subitem III.2 abaixo:

III.1) Cronograma Oficial - Portaria CNPD nº 03 de 04/10/2024

- ✓ **Duração do GT:** 120 dias a contar da data de entrada em vigor da Portaria CNPD nº 03 de 04/10/2024
- ✓ **Plano de trabalho:** 04/11/2024
- ✓ **Relatório final do GT:** 04/02/2025
- ✓ **Apresentação ao CNPD:** até cinco dias após o término do prazo de suas atividades – 09.02.2025

III.2) Cronograma do GT3

CRONOGRAMA		
Ação	Datas das reuniões	Prazo
Apresentar para discussão a primeira minuta de Plano de Trabalho e estrutura para o Relatório Final	24.10.2024	X
Contribuições dos membros do GT sobre a proposta inicial de Plano de Trabalho e da estrutura para o Relatório Final	30.10.2024	Até 28.10.2024
Finalização do Plano de Trabalho e da estrutura para o Relatório Final com base nas contribuições dos membros do GT para envio ao CNPD	X	Até 03.11.2024
Envio do Plano de Trabalho ao CNPD	X	04.11.2024

Pesquisas, estudos, coleta de subsídios e diretrizes, bem como nova discussão quanto a necessidade de contribuição por parte de entidades e especialistas	13.11.2024	Até 04.12.2024
	27.11.2024	
	04.12.2024	
Estruturação do Relatório Final	11.12.2024	Até 15.01.25
	18.12.2024	
	08.01.2025	
Debates e ajustes do Relatório Final	15.01.2025	Até 24.01.25
	22.01.2025	
Conclusão do Relatório Final	29.01.2025	Até 03.02.25
Apresentação do Relatório Final ao CNPD	05.02.2025	Até 09.02.24

#### IV) Sumário Preliminar para o Relatório Final:

- 7) Contextualização e introdução
- 8) Histórico das Atividades
- 9) Referencial Teórico
- 10) Metodologia
- 11) Apresentação dos Resultados
- 12) Considerações Finais
- 13) Referências

Atenciosamente,



**Myreilla Aloia T P da Cruz**

Conselheira Titular e Coordenadora do GT3 do CNPD