# MESTRADO PROFISSIONAL

## EM ADMINISTRAÇÃO PÚBLICA

**ANÁLISE DO ÍNDICE DE ADEQUAÇÃO À PROTEÇÃO DE DADOS PELA POLÍCIA MILITAR DO DISTRITO FEDERAL À LUZ DO ACÓRDÃO Nº 1.384/2022 DO TRIBUNAL DE CONTAS DA UNIÃO**

**PÉRICLES QUEIROZ ARAÚJO**

Brasília-DF, 2025

**PÉRICLES QUEIROZ ARAÚJO**

# ANÁLISE DO ÍNDICE DE ADEQUAÇÃO À PROTEÇÃO DE DADOS PELA POLÍCIA MILITAR DO DISTRITO FEDERAL À LUZ DO ACÓRDÃO Nº 1.384/2022 DO TRIBUNAL DE CONTAS DA UNIÃO

Dissertação apresentada ao Programa de Pós Graduação em Administração Pública, do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, como requisito parcial para obtenção do grau de Mestre.

**Orientador**
Professor Doutor Emmanuel De Nazareth Brasil

Brasília-DF 2025

**PÉRICLES QUEIROZ ARAÚJO**

# ANÁLISE DO ÍNDICE DE ADEQUAÇÃO À PROTEÇÃO DE DADOS PELA POLÍCIA MILITAR DO DISTRITO FEDERAL À LUZ DO ACÓRDÃO Nº 1.384/2022 DO TRIBUNAL DE CONTAS DA UNIÃO

Dissertação apresentada ao Programa de Pós Graduação em Administração Pública, do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, como requisito parcial para obtenção do grau de Mestre.

Aprovado em 07 / 07 / 2025

**Banca Examinadora**

Prof. Dr. Emmanuel De Nazareth Brasil - Orientador

Prof. Dr. Milton De Souza Mendonça Sobrinho

Prof. Dr. Paulo Henrique Ferreira Alves

Código de catalogação na publicação – CIP

A663a Araújo, Péricles Queiroz
Análise do índice de adequação à proteção de dados pela Polícia Militar do Distrito Federal à luz do Acórdão nº 1.384/2022 do Tribunal de Contas da União / Péricles Queiroz Araújo. — Brasília: Instituto Brasileiro Ensino, Desenvolvimento e Pesquisa, 2025.

213 f. : il.

Orientador: Prof. Dr. Emmanuel de Nazareth Brasil

Dissertação (Mestrado Profissional em Administração Pública) — Instituto Brasileiro Ensino, Desenvolvimento e Pesquisa – IDP, 2025.

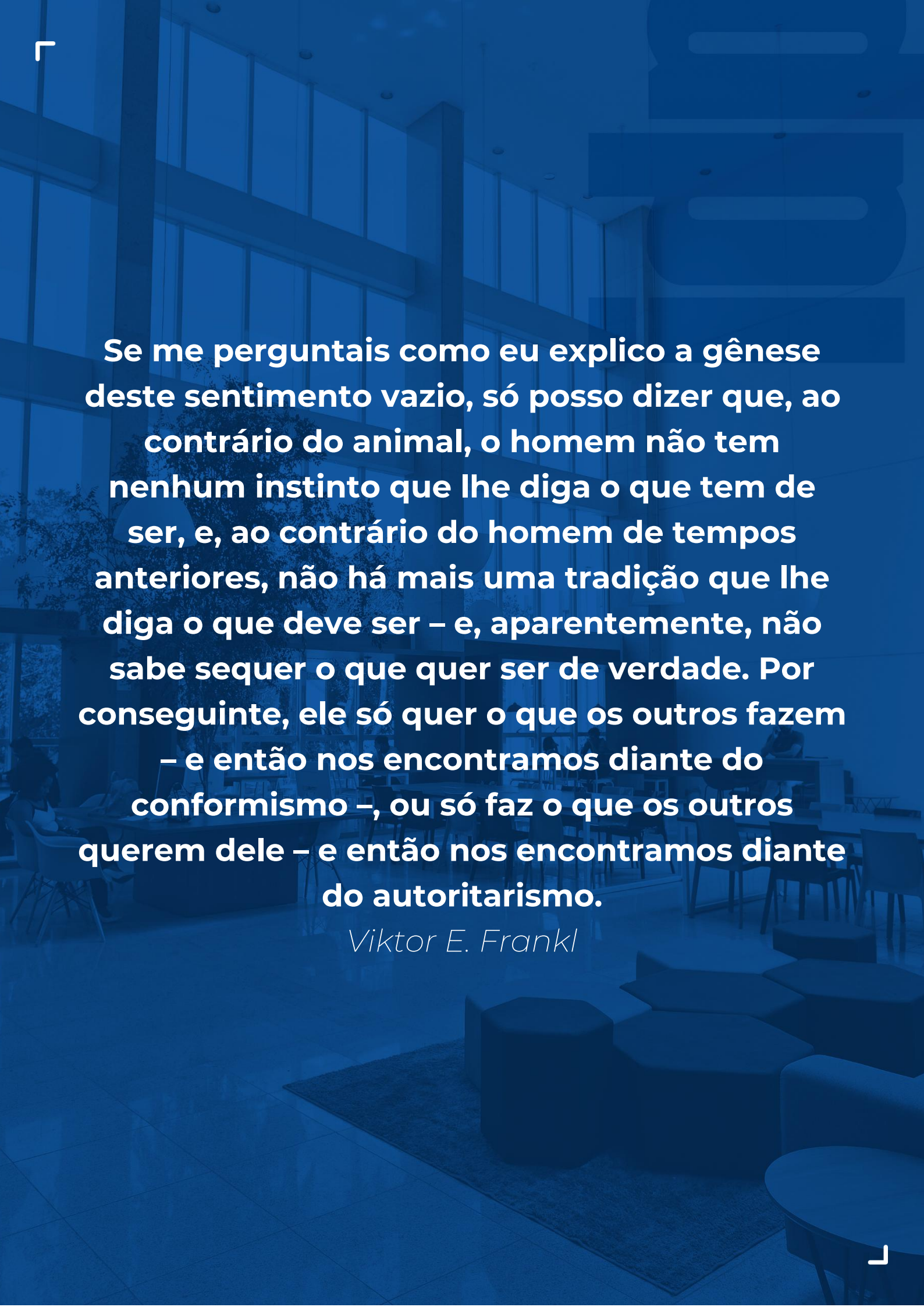
1. Proteção de dados pessoais. 2. Polícia Militar. 3. Indíce. I.Título

CDD 350

Elaborada pela Biblioteca Ministro Moreira Alves

## DEDICATÓRIA

Dedico este trabalho a todos que, de maneira direta ou indireta, me acompanham.



**Se me perguntais como eu explico a gênese deste sentimento vazio, só posso dizer que, ao contrário do animal, o homem não tem nenhum instinto que lhe diga o que tem de ser, e, ao contrário do homem de tempos anteriores, não há mais uma tradição que lhe diga o que deve ser – e, aparentemente, não sabe sequer o que quer ser de verdade. Por conseguinte, ele só quer o que os outros fazem – e então nos encontramos diante do conformismo –, ou só faz o que os outros querem dele – e então nos encontramos diante do autoritarismo.**

*Viktor E. Frankl*

# RESUMO

ARAÚJO, Péricles Queiroz. **Análise do índice de adequação à Proteção de Dados pela Polícia Militar do Distrito Federal à luz do Acórdão nº 1384/2022 do Tribunal de Contas da União**. 2025. Dissertação (Mestrado Profissional em Administração Pública) – Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, 2025.

Esta pesquisa tem por objetivo apresentar o índice de adequação à Lei Geral de Proteção de Dados da Polícia Militar do Distrito Federal, nos termos dos estudos que integram o Acórdão nº 1.384/2022, realizado pelo Tribunal de Contas da União. A necessidade desta conformidade administrativa surge no momento em que a sociedade do século XXI é caracterizada por uma comunicação instantânea e voltada para a utilização massiva dos dados pessoais, seja pelo poder público ou pela iniciativa privada, tudo isso proporcionado pela evolução tecnológica e pela sociedade vigilância. Também, com a vigência da Lei Geral de Proteção de Dados e com a consolidação da Autoridade Nacional de Proteção de Dados, na Política Nacional de Proteção de Dados, impõe-se o dever de que todos os órgãos públicos estejam adaptados e capazes de promover a proteção deste direito fundamental. Assim, com a utilização do método empregado pelo TCU foi possível encontrar o nível de adequação à proteção de dados pessoais da Corporação, no valor de "0,36", equivalente ao estágio "inicial", no ano de 2024. No âmbito da Polícia Militar do Distrito Federal, foram solicitados os artefatos produzidos e que tivessem o escopo de subsidiar e promover a política de Proteção de dados, agregando-se aos resultados obtidos com a pesquisa. Contudo, tais achados não podem ser vistos como positivo pela PMDF, pois a auditoria foi realizada em 2021 e os valores ali descritos se reportam às entidades naquele período. Quanto aos artefatos apresentados pela PMDF, não foram encontrados documentos que tivessem a devida expressão, mas apenas solicitações de reuniões e pedidos de produção de documentos. Desta forma, a obtenção do nível "inicial" de adequação à LGPD, mesmo tendo transcorridos 02 (dois) anos, é razão de preocupação para a Alta Cúpula da PMDF, principalmente quando os dados coletados apresentam deficiências, dentre outras, no que tange ao engajamento, motivação e capacitação, que são qualidades imprescindíveis para uma governança efetiva. Ao final, com suporte na doutrina e nos entendimentos dos

órgãos de fiscalização, quais sejam, a ANPD e TCU, este pesquisador sugeriu medidas, visando a seara estratégica e tático-operacional a serem seguidas para melhorar e tornar mais eficiente a Política de Proteção de Dados na PMDF.

**Palavras chave: PMDF. Proteção de Dados Pessoais. Índice de adequação. TCU.**

## ABSTRACT

ARAÚJO, Péricles Queiroz. **Analysis of the Data Protection Compliance Index by the Military Police of the Federal District in light of Ruling No. 1384/2022 of the Federal Court of Accounts**. 2025. Dissertation (Professional Master's in Public Administration) – Brazilian Institute of Teaching, Development and Research, Brasília, 2025.

This research aims to present the compliance index with the General Data Protection Law of the Military Police of the Federal District, according to the studies that comprise Ruling No. 1,384/2022, carried out by the Federal Court of Accounts. The need for this administrative compliance arises at a time when 21st-century society is characterized by instant communication and the massive use of personal data, whether by the public or private sector, all facilitated by technological evolution and the surveillance society. Furthermore, with the General Data Protection Law in effect and the consolidation of the National Data Protection Authority within the National Data Protection Policy, all public bodies have a duty to adapt and be capable of promoting the protection of this fundamental right. Thus, using the method employed by the TCU (Brazilian Federal Court of Accounts), it was possible to determine the level of adequacy of the Corporation's personal data protection, at a value of "0.36", equivalent to the "initial" stage, in the year 2024. Regarding the Military Police of the Federal District, artifacts produced that had the scope to support and promote the data protection policy were requested, adding to the results obtained from the research. However, these findings cannot be seen as positive by the PMDF (Military Police of the Federal District), since the audit was carried out in 2021 and the values described therein refer to the entities in that period. As for the artifacts presented by the PMDF, no documents with the proper expression were found, only requests for meetings and requests for the production of documents. Thus, achieving the "initial" level of compliance with the LGPD (Brazilian General Data Protection Law), even after two years, is a cause for concern for the PMDF (Military Police of the Federal District) leadership, especially when the collected data presents deficiencies, among others, regarding engagement, motivation, and training, which are essential qualities for effective governance. Finally, based on doctrine and the understandings of oversight bodies, namely the ANPD (National Data Protection Authority) and TCU (Federal Court of Accounts), this

researcher suggested measures, aimed at the strategic and tactical-operational levels, to be followed to improve and make the Data Protection Policy in the PMDF more efficient.

**Keywords: : PMDF. Protection of Personal Data. Suitability index. TCU.**

# LISTA DE ABREVIATURAS E SIGLAS

| | |
|---|---|
| ADI | Ação Direta de Inconstitucionalidade |
| AGU | Advocacia Geral da União |
| ANPD | Autoridade Nacional de Proteção de Dados |
| CGDF | Controladoria Geral do Distrito Federal |
| GDF | Governo do Distrito Federal |
| EBIA | Estratégia Brasileira de Inteligência Artificial |
| IA | Inteligência Artificial |
| LGPD | Lei Geral de Proteção de Dados |
| MP | Medida Provisória |
| LODF | Lei Orgânica do Distrito Federal |
| PL | Projeto de Lei |
| PMDF | Polícia Militar do Distrito Federal |
| SEEDF | Secretaria de Estado de Educação do Distrito Federal |
| RGPD | Regulamento Geral de Proteção de Dados |
| STF | Supremo Tribunal Federal |
| TCU | Tribunal de Contas da União |

# LISTA DE ILUSTRAÇÕES

**Figura 1**
CICLO DE TRATAMENTO DE DADOS PESSOAIS ..... **43**
**Figura 2**
TIPOS DE INCIDENTES ..... **48**
**Figura 3**
DIMENSÕES DO QUESTIONÁRIO ..... **69**
**Figura 4**
IMAGEM DO SITE DA PMDF ..... **71**
**Figura 5**
IMAGEM DO ROL DE NORMAS CONSTANTES NO SITE DA PMDF ..... **72**
**Figura 6**
RELAÇÃO DOS NOMES DOS ENCARREGADOS SETORIAIS DA PMDF ..... **72**
**Figura 7**
NÍVEIS DE ADEQUAÇÃO À LGPD PELO TCU ..... **90**
**Figura 8**
ORGANOGRAMA GERAL DA PMDF ..... **94**
**Figura 9**
GOVERNANÇA E GESTÃO ADMINISTRATIVA ..... **102**
**Figura 10**
MAPA ESTRATÉGICO DA PMDF ..... **106**
**Figura 11**
IMAGEM DE CURSOS DE LGPD PELA ENAP ..... **113**
**Figura 12**
IMAGEM DE CURSO DE LGPD PELA ENAP ..... **114**
**Figura 13**
IMAGEM DE CURSO DE LGPD PELA ENAP ..... **115**
**Figura 14**
ORDEM DE PRIORIDADE PARA CAPACITAÇÃO EM LGPD ..... **116**
**Figura 15**
IMAGEM DE SETE TRILHAS DE APRENDIZAGEM ..... **117**

**Figura 16**
INDICADOR DE SATISFAÇÃO DOS USUÁRIOS
118
**Figura 17**
IMAGEM DO SITE DO TCDF
119
**Figura 18**
IMAGEM DO SITE DO TCDF
120
**Figura 19**
IMAGEM DO SITE DO CBMDF
120
**Figura 20**
IMAGEM DO SITE DO CBMDF
121
**Figura 21**
PROPOSTA DE FLUXO DE COMUNICAÇÃO DE INCIDENTES DE PROTEÇÃO DE DADOS
124
**Figura 22**
FLUXO DE ATENDIMENTO DE REQUISIÇÕES DE TITULARES DE DADOS
127
**Figura 23**
FLUXO DE REQUISIÇÕES DA ANPD
129

# LISTA DE TABELAS

**Tabela 1**
RELAÇÃO DE ARTEFATOS PRODUZIDOS PELO REPRESENTANTE DA PMDF ..... **64**
**Tabela 2**
DESCRIÇÃO DAS QUESTÕES UTILIZADAS PARA O CÁLCULO DO INDICE DE ADEQUAÇÃO À LGPD ..... **74**
**Tabela 3**
PREPARAÇÃO PARA ADEQUAÇÃO ..... **76**
**Tabela 4**
CONTEXTO ORGANIZACIONAL ..... **77**
**Tabela 5**
LIDERANÇA ..... **79**
**Tabela 6**
CAPACITAÇÃO ..... **81**
**Tabela 7**
CONFORMIDADE DE TRATAMENTO ..... **82**
**Tabela 8**
DIREITOS DO TITULAR ..... **83**
**Tabela 9**
COMPARTILHAMENTO DE DADOS PESSOAIS ..... **84**
**Tabela 10**
VIOLAÇÃO DE DADOS PESSOAIS ..... **85**
**Tabela 11**
MEDIDAS DE PROTEÇÃO ..... **86**
**Tabela 12**
ÍNDICE DE ADEQUAÇÃO À LGPD DA PMDF ..... **87**
**Tabela 13**
COMPARATIVO ENTRE PMDF, CBMDF E SERPRO ..... **89**

# SUMÁRIO


**1. INTRODUÇÃO ..... 18**

**2. REVISÃO DE LITERATURA ..... 23**

2.1 FUNDAMENTOS TEÓRICOS DA PROTEÇÃO DE DADOS ..... 23

2.2 GERAÇÃO NORMATIVA DOS DIREITOS DIGITAIS ..... 34

2.3 GOVERNANÇA DE DADOS NA ADMINISTRAÇÃO PÚBLICA ..... 38

2.4 A LGPD COMO POLÍTICA PÚBLICA E O PAPEL DO TCU ..... 45

2.5 ESTUDOS SOBRE A IMPLEMENTAÇÃO DA LGPD EM ÓRGÃOS PÚBLICOS ..... 55

**3. METODOLOGIA ..... 62**

3.1 SOLICITAÇÃO ADMINISTRATIVA DOS ARTEFATOS CONFECCIONADOS PELO SUBCOMITÊ EXECUTIVO DE PROTEÇÃO DE DADOS DA PMDF ..... 64

3.2 ENVIO DO QUESTIONÁRIO DESCRITO NO ACÓRDÃO Nº 1.384/2022 – TCU E COLETA DAS RESPOSTAS PROMOVIDAS PELO SUBCOMITÊ EXECUTIVO DE PROTEÇÃO DE DADOS DA PMDF ..... 65

**4. DIAGNÓSTICO DA SITUAÇÃO ATUAL DA PMDF QUANTO À LGPD ..... 68**

4.1 METODOLOGIA DE DIAGNÓSTICO ..... 68

4.2 ANÁLISE DOCUMENTAL: ARTEFATOS INSTITUCIONAIS DA PMDF ..... 70

4.3 AVALIAÇÃO DIMENSIONAL COM BASE NO QUESTIONÁRIO DO TCU . 74

4.3.1 ESTRUTURAÇÃO PARA A CONDUÇÃO DA INICIATIVA DE ADEQUAÇÃO ..... 76

4.3.1.1 PREPARAÇÃO ..... 76

4.3.1.2 CONTEXTO ORGANIZACIONAL ..... 77

4.3.1.3 LIDERANÇA ..... 78

4.3.1.4 CAPACITAÇÃO ..... 80

4.3.2 MEDIDAS E CONTROLES DE PROTEÇÃO DE DADOS PESSOAIS IMPLEMENTADOS ..... 81

4.3.2.1 CONFORMIDADE DO TRATAMENTO ..... 81

4.3.2.2 DIREITOS DO TITULAR ..... 83

4.3.2.3 COMPARTILHAMENTO DE DADOS PESSOAIS ..... 84

4.3.2.4 VIOLAÇÃO DE DADOS PESSOAIS ..... 85

4.3.2.5 MEDIDAS DE PROTEÇÃO ..... 86

# SUMÁRIO

4.4 SÍNTESE DO DIAGNÓSTICO ..... 87

**5. DISCUSSÃO DOS RESULTADOS E PROPOSTAS DE APRIMORAMENTO 93**

5.1 INTERPRETAÇÃO CRÍTICA DOS RESULTADOS ..... 93

5.2 REFLEXÕES À LUZ DO REFERENCIAL TEÓRICO ..... 100

5.3 PROPOSTAS DE MELHORIA PARA A PMDF ..... 101

5.3.1 AÇÕES EM NÍVEL ESTRATÉGICO ..... 103

5.3.1.1 ENGAJAR A ALTA CÚPULA DA PMDF SOBRE A PROTEÇÃO DE DADOS ..... 103

5.3.1.2 REVISÃO DO PLANEJAMENTO ESTRATÉGICO DA PMDF ..... 104

5.3.1.3 FORMALIZAÇÃO DA POLÍTICA DE PROTEÇÃO DE DADOS NA PMDF ..... 107

5.3.2 AÇÕES EM NÍVEL TÁTICO-OPERACIONAL ..... 109

5.3.2.1 VERIFICAÇÃO DA PERCEPÇÃO DO COMPLIANCE EM PROTEÇÃO DE DADOS ..... 109

5.3.2.2 CRIAÇÃO DE PLANO DE CAPACITAÇÃO ..... 110

5.3.2.3 ALTERAÇÃO DA PÁGINA INICIAL DA PMDF COM DESTAQUE PARA A POLÍTICA DE PROTEÇÃO DE DADOS ..... 117

5.3.2.4 PROCEDIMENTO INTERNO PARA COMUNICAÇÃO DE INCIDENTES ..... 122

5.3.2.5 ESTABELECER A DEVIDA COMUNICAÇÃO COM O TITULAR DE DADOS ..... 125

**6. CONSIDERAÇÕES FINAIS ..... 132**

**REFERÊNCIAS ..... 137**

**APÊNDICES ..... 145**


1

# 1 INTRODUÇÃO

Tratar de Administração Pública, principalmente no que tange a sua eficiência na implementação e execução das políticas públicas, é de extrema importância uma vez que a sua perfeita atuação irá definir os bons resultados em favor do cidadão. Segundo Cavalcante (2020) por esta necessidade é que surgem várias teorias que buscam definir a estrutura de poder executivo que melhor atenda aos propósitos da sociedade, tais como a governança e as agências reguladoras, nos mesmos moldes do que ocorreu no âmbito internacional.

Por seu turno, o Guia de Política de Governança da esfera federal[1], Brasil (2023), descreve acerca do constante aprimoramento do Estado, coordenando as contradições e permitindo os avanços na gestão administrativa, com eficiência, e baseada numa governança consolidada e voltada para o futuro da organização.

O tema se torna denso quando se agrega às funções do Estado a massiva utilização da internet e a consequente proteção de dados pessoais. Acredita-se, assim, que para a implementação da Lei Geral de Proteção de Dados (Lei n° 13.709/2018) exija-se muito conhecimento técnico, atendendo ao princípio da legalidade, e que a sua aplicabilidade seja bastante complexa[2].

Segundo Lima (2020), o cidadão está cada vez mais atento ao tratamento de seus dados pessoais, seja quando comercializa com entidades privadas ou quando os cede para órgãos públicos, a exemplo do que ocorre com a declaração do imposto de renda, em atividades censitárias ou em atuação de segurança pública.

Assim, sabendo-se que o Estado deve atuar com base no princípio da legalidade e na promoção da dignidade da pessoa

[1] Extraído do site file:///C:/Users/user/Downloads/guia_politicadegovernancapublica.pdf. Acessado em 08 de julho de 2024.

[2] Com a criação da Autoridade Nacional de Dados – ANPD surge o braço fiscalizatório e regulatório, no âmbito direito administrativo, que terá a hercúlea tarefa de exercer o controle prévio e posterior das atividades ilícitas praticadas. Ademais, a própria norma trouxe um capítulo “Da Segurança e Boas Práticas” que visa definir o mínimo de governança no tratamento dos dados.

humana, nos termos do artigo 1°, inciso III, da Constituição Federal, e que o TCU já analisou o tema de Proteção de Dados Pessoais nos órgãos públicos da esfera federal, no ano de 2022, caminha-se para a pergunta desta pesquisa: diante do Acórdão n° 1.384/2022 TCU, e de seus fundamentos quanto à Política de Proteção de Dados Pessoais, qual seria o nível de adequação à Lei Geral de Proteção de Dados na Polícia Militar do Distrito Federal?

Para compreender o grau de maturidade, ou seu índice de adequação, em relação à LGPD de uma organização, deve-se atentar que o Tribunal de Contas da União tratou de estabelecer níveis, que variam do inexpressivo ao aprimorado, de adequação à Lei Geral de Proteção de Dados para as entidades jurisdicionadas, pois, apesar da LGPD ter sido sancionada em 2018, ainda não se tinha uma mensuração detalhada de tais índices que pudessem descrever a sua implementação pelas entidades federais.

Entretanto, por ser organizada e mantida pela União, não foi encontrado relatório específico para a Polícia Militar do Distrito Federal, inclusive, compulsando o processo de auditoria, a PMDF está relacionada como “interessada” e não “jurisdicionada”, o que sugere que a pesquisa não foi respondida.

Nesta senda, utilizando-se da mesma metodologia empregada pelo Tribunal de Contas da União - TCU, será possível estabelecer e apresentar o nível atual de adequação da Polícia Militar do Distrito Federal – PMDF para buscar sugerir medidas administrativas que auxiliem na implementação da política de proteção de dados pessoais. Ademais, pretende-se, quiçá, mediante um processo de sensibilização junto aos órgãos de controle interno e externo do Distrito Federal, expandir esta pesquisa para todos os órgãos do Distrito Federal, por intermédio da Controladoria-Geral do Distrito Federal – CGDF.

Em assim sendo, tem-se como hipótese que a Corporação alcançou o nível “Inicial” de adequação à proteção de dados pessoais, conforme será demonstrado em tópico específico, uma vez que a sua estrutura é extremamente complexa e demasiadamente compartilhada, sendo que esta condição dificulta a compilação das informações e o mapeamento dos processos voltados para a proteção de dados.

Para o atingir o escopo desta pesquisa, o objetivo geral se destina a compreender a proteção de dados pessoais como um processo

evolutivo da legislação da própria sociedade, uma sociedade dinâmica e conectada em rede, na qual a Lei Geral de Proteção de Dados se apresenta como um norte para o Estado brasileiro, especialmente para a Polícia Militar do Distrito Federal, que é o foco desta pesquisa.

Quanto aos objetivos específicos podem ser assim estabelecidos: a) estudar os fundamentos teóricos da proteção de dados; b) descrever as gerações normativas dos direitos digitais; c) estudar a governança de dados na administração pública; d) descrever a Polícia Militar do Distrito Federal como um órgão cuja estrutura se volta para a proteção de dados; e) estudar a LGPD como política pública e o papel do TCU; f) apresentar estudos sobre a implementação da LGPD em órgãos públicos; e g) apresentar propostas de melhoria para a PMDF quanto à adequação à LGPD.

Percebe-se a importância desta pesquisa uma vez que o tema de proteção de dados pessoais avança, com mais força e intensidade, ao encontro, também, da Administração Pública brasileira, não restando dúvidas de que as transações de dados, públicas ou privadas, estão cada vez mais presentes na nossa sociedade.

O interesse pela Política de Proteção de Dados na PMDF e a busca pelos resultados deste trabalho se dá pelo fato deste pesquisador contar com mais de vinte oito anos de serviço e conhecer as dificuldades inerentes à gestão administrativa, dos gastos orçamentários e com a qualificação do efetivo para as mais diversas funções. Ademais, no momento de sua criação, este pesquisador contribuiu para a confecção e publicação da norma, quando exercia a função de Subchefe da Seção de Planejamento de Pessoal, Saúde e Legislação, do Estado-Maior da PMDF.

Ressalta-se, portanto, que não se trata de destacar aquela Administração e elevá-la ao patamar de excelência e nem tampouco de inferiorizar os demais entes federativos, mas de buscar paradigmas palpáveis e que tenham certas semelhanças com a Corporação Militar – PMDF. Afinal, como será visto, parte da legislação é da competência da União e isso necessariamente remete às boas práticas na esfera federal no que tange à proteção de dados.

Ciente desta necessidade de adequação à LGPD, é que se encontra no Plano Estratégico da PMDF, aprovado para os anos de 2023 a 2034, o rol de fatores críticos de sucesso corporativo, principalmente

para a implementação de uma política complexa como a proteção de dados:

**a) dotação orçamentária compatível com o atendimento das demandas;**
**b) disponibilidade de recursos humanos em quantidade adequada, capacitados, motivados e disciplinados;**
**c) dotação de recursos logísticos adequados;**
**d) implementação de infraestrutura de informações, tecnologias e inteligência, com uso e gestão apropriados;**
**e) planejamento e tomada de decisão baseada em conhecimento;**
**f) políticas de integração entre os diversos órgãos do setor de segurança pública;**
**g) parcerias estratégicas com os segmentos públicos e privados;**
**h) aprimoramento da comunicação organizacional para fortalecimento da identidade e da imagem corporativas. (DISTRITO FEDERAL, 2023) (grifei)**

Entretanto, apesar das considerações supramencionadas, há fortes indícios de que a implementação da Política de Proteção de Dados Pessoais não avançou na PMDF, sendo tal condição suficiente para se aplicar a metodologia do Tribunal de Contas da União a este caso concreto.

Desta feita, o método será inovador no âmbito da PMDF e servirá como referência para os demais órgãos da Administração Pública do Distrito Federal em pesquisas futuras. Replicar o trabalho realizado pelo Tribunal de Contas da União, com suas dimensões e fórmulas, na Polícia Militar do Distrito Federal é tarefa que resultará bons frutos e uma valiosa autoavaliação da gestão de proteção de dados pessoais da Corporação, sem prejuízo de que outras pesquisas avancem em pontos específicos aqui encontrados.


2

# 2 REVISÃO DE LITERATURA

## 2.1 FUNDAMENTOS TEÓRICOS DA PROTEÇÃO DE DADOS

Vive-se numa sociedade em que as relações são instantâneas e que a cada dia se tornam mais amplas e, na mesma medida, o excesso de informação afeta a todos negativamente, sem distinção de classe social, país ou governo. Paralelamente, para Bauman (2008), às intensas comunicações, a cada dia o consumo exaspera a própria materialidade dos bens, transformando as pessoas em objetos vendáveis e expostos nas vitrines dos sites de comércios e comunidades virtuais.

Assim, da forma como pensado pelo filósofo, o consumo em si proporciona um investimento e insere o indivíduo na sociedade, uma sociedade "líquida" em que tudo acontece num dinamismo jamais visto. Enquanto isso os algoritmos criam perfis, com base nas preferências do próprio indivíduo, representando-o perante a rede mundial em excessos e extravagâncias.

Esta criação virtual do indivíduo, com base em seus perfis comportamentais[3], replica seus desejos, vontades e hábitos que em épocas passadas ficavam adstritos somente ao seu círculo de amigos e parentes mais próximos. A metodologia dos gigantes da internet é simples: acumular o máximo de dados dos navegantes, personalizar as informações e aguardar que o usuário faça o bom uso das mercadorias adquiridas, mesmo que delas não precise.

Pariser (2012, p. 10), por exemplo, descreve que a "Amazon vende bilhões de dólares em produtos prevendo o que cada cliente procura e colocando estes produtos na página principal de sua loja virtual". E é neste sentido que, para Harari (2018), a personalização de ofertas virtuais gera efeitos na sociedade. Contudo, pode ser que a Amazon não

[3] Este é o entendimento da literatura: "Ao mesmo tempo, as facilidades da tecnologia digital deram início a uma espécie de "corrida do ouro", mais conhecida como customização e/ou personalização de serviços e produtos segundo o perfil do usuário/cliente. (...) Acredita-se que, conhecendo o perfil do consumidor, ele possa ser atraído com produtos que atendam exatamente ao que deseja". (COSTA, 2002, p. 32-33)

irá acertar sempre, mas precisará ser apenas melhor que os humanos, uma vez que nem mesmos esses conhecem sobre si mesmos.

Diante deste aglomerado de fatores e submissões do indivíduo é que surge a necessidade de alguma regulamentação pela ciência do direito. Nesta direção, a doutrina de Garbaccio *et al* (2022, p. 04) leciona que muito embora o ordenamento jurídico já fosse contemplado com outras leis que protegessem o indivíduo, principalmente nos contratos e manifestações na internet, a "era tecnológica, com a disposição de dados, da economia digital, através da qual há uma coleta maciça de dados, que muitas vezes não encontra limites e despreza a intimidade e a vida privada dos usuários (...)".

Com o seu traço característico de transnacionalidade, a internet se apresenta como um ambiente de grandes oportunidades para aqueles que a utilizam com sabedoria. Assim, as normas de convivência virtual devem buscar, mesmo que minimamente, o fomento de padrões éticos aceitáveis em todos países que participam desta grande rede de computadores, sendo este o grande dilema.

Para Salama (2017, p. 180) existe uma grande dificuldade em se estabelecer normas jurídicas uma vez que algumas regulamentações se tornam imprevisíveis de se conhecer os resultados, inclusive podendo se tornar indesejáveis aos olhos do próprio legislador.

Desta forma, se uma norma for extremamente detalhista e depender de uma ponderação excessiva por parte do operador do direito para um caso específico, a exemplo do que ocorre com a macroeconomia, esta regra não será de observância impositiva e adequada, pois para todas as opções haverá sempre uma resposta a ser levantada.

Um excelente exemplo de adequação da norma à atualidade tecnológica é a Resolução do Parlamento Europeu[4], de 16 de fevereiro de 2017, destinada à ética na robótica e ao emprego da inteligência artificial que visou, expressamente, o reconhecimento da proteção do homem, tanto para beneficiar quanto para se evitar os efeitos prejudiciais da tecnologia.

Assim, a preocupação com a existência humana, sua liberdade e sua dignidade, se faz sempre presente no bojo desta Resolução. Igual

[4] Extraído do site: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_PT.html?redirect#title2. Acessado em 20 de junho de 2024.

importância pode ser encontrada na Carta dos Direitos Fundamentais da União Europeia[5] quando tratou da evolução tecnológica, no seu artigo 8º, ao se referir, expressamente, à proteção de dados pessoais[6].

Em uma análise mais ampla de proteção de direitos na internet, nota-se que os países tendem a copiar regras a fim de facilitar as transações comerciais e diplomáticas, como é o caso do Regulamento Geral de Proteção de Dados Pessoais – RGPD da União Europeia. Percebe-se a importância da consolidação, expansão e "viralização"[7] da RGPD, uma vez que os países, mesmo que não pertencentes à União Europeia, passaram a tratar e a dispor desta proteção, com seus conceitos e princípios, de forma bastante similar, não importando a localização da empresa ou do indivíduo, pois, em algum momento, haverá a transferência de economia e isso acarretará no tratamento de dados pessoais pela União Europeia.

Segundo Garbaccio *et al* (2022, p. 05) o que estas leis buscam é a promoção da economia sem a violação de direitos, ou seja, ponderando os princípios inerentes à ordem econômica e da proteção de dados pessoais. Tal pensamento pode ser encontrado, também, na Recomendação sobre Diretrizes que Regem a Proteção da Privacidade e os Fluxos Transfronteiriços de Dados Pessoais, adotada pelo Conselho da OCDE em 23 de setembro de 1980 e revisada em 2013 quando exalta a privacidade e o livre fluxo de dados pessoais[8] com a confiança de que os estados membros possuam salvaguardas suficientes, incluindo mecanismos que garantam a proteção e a utilização segura dos dados pessoais.

---

[5] Batista *apud* Santana (2014, p. 60) esclarece que: "O Tribunal de Justiça da Comunidade Européia (TJCE) e os Tribunais dos Estados-Membros têm reconhecido a autonomia e a individualidade das normas comunitárias. O Direito Comunitário distingue-se, pois, tanto da ordem jurídica internacional quanto da ordem jurídica interna por sua origem (criado por tratados internacionais); finalidade (objetiva a criação de uma autoridade institucional própria que subordine as soberanias – e interesses – dos Estados-Membros para alcançar sua integração social e econômica); destinatários (Estados-Membros da União e instituições comunitárias, ou particulares sujeitos à jurisdição comunitária); e órgãos (para se aplicar e interpretar o Direito Comunitário há um Tribunal de 1ª instância e o Tribunal de Justiça da Comunidade Européia).

[6] Extraído do site: https://op.europa.eu/webpub/com/carta-dos-direitos-fundamentais/pt/. Acessado em 20 de junho de 2024.

[7] Termo empregado pelo advogado Ronaldo Lemos no site https://www.meioemensagem.com.br/midia/a-gdpr-tera-um-efeito-viral. Acessado em 14 de junho de 2024.

[8] Extraído do site https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188. Acessado no dia 10 de maio de 2025.

Sem dúvida os séculos XX e XXI são caracterizados pelas relações sociais mediante a utilização dos equipamentos tecnológicos conectados em rede. Apesar da internet ter possibilitado a divulgação dos direitos humanos ela também é meio para a incidência de suas violações. Para Oliveira e Bittencourt (2020) torna-se, portando, necessário que os Estados reafirmem os direitos conquistados off-line também para os on-line.

Segundo Bobbio (2014) os direitos fundamentais ganham força na medida em que passa a ocorrer um desnivelamento que visa beneficiar e proteger o indivíduo em face de um poder maior, configurando-se numa verdadeira mudança de visão em favor do indivíduo. Em assim sendo, a tecnologia dominante neste século XXI impõe ao legislador novas formas de proteção ao indivíduo e à sua dignidade. Isso aconteceu no âmbito da União Europeia com o Regulamento Geral de Proteção de Dados – RGPD e no Brasil com a Lei Geral de Proteção de Dados – LGPD que, apesar de ter sido sancionada em 2018, somente entrou em vigor em 2020.

O avanço da tecnologia, impõe novos conceitos ou ampliações de conceitos, tal como acontece com a sociedade de vigilância, que tem como atores principais o indivíduo, as grandes empresas de tecnologia e o Estado.

Mas o fato de que a internet tenha ampliado as comunicações e as relações entre pessoas, não impediu a formação de restrições comportamentais ou de obediências irrestritas a certos padrões impostos, que mais se assemelham a prisões, agora sob um novo formato virtual. De maneira semelhante, Deleuze (1990, p. 1) descreve o sistema panóptico, mencionando Foucault, da sociedade de vigilância do século XVIII e XIX na qual os indivíduos eram confinados, separadamente, em celas vazadas e que, ao centro da estrutura panóptica, invisível aos olhos do condenado, estava o carcereiro que poderia observar o preso, ou seu vulto, sabendo o que fazia e como fazia.

Na sociedade de vigilância, pelas lições de Foucault, o indivíduo se torna um corpo dócil, transformado e aperfeiçoado, dentro de uma prisão virtual que o impõe um modo de vida, com limitações e obrigações:

> (...) adestrando as multidões confusas, inúteis de corpos e forças para a multiplicidade de elementos individuais (...) a disciplina fabrica indivíduos; ela é técnica especifica de um

> poder que toma indivíduos ao mesmo tempo como objetos e como instrumentos de seu exercício (...) é um modesto, desconfiado, que funciona a modo de uma economia calculada, mas permanente (...) o sucesso do poder disciplinar se deve sem dúvida ao uso de instrumentos simples: o olhar hierárquico, a sanção normalizadora e sua combinação num procedimento que lhe é específico, o exame. (FOUCAULT *apud* MELLO, p. 350)

Em resumo, na sociedade de vigilância disciplinar, existem dois polos bem definidos, sendo que a assinatura indica o indivíduo e o número da matrícula o seu lugar na massa carcerária. Ao mesmo tempo o poder é individualizante e massificante, moldando o indivíduo como cada membro de seu corpo.

Por seu turno, a atual sociedade de controle é constituída, diferentemente da sociedade de vigilância, de uma cifra, ou seja, de uma senha. Assim, para Deleuze (1990), os indivíduos tornaram-se "'dividuais', divisíveis, e as massas tornaram-se amostras, dados, mercados ou bancos".

Neste contexto, o Estado é o responsável pelo processo de vigilância disciplinar, sendo, ao mesmo tempo, uma peça de fabricação e uma engrenagem na sociedade de controle. Para Mello (2021, p. 351), vive-se a experiência de uma vigilância fluida na qual o poder do Estado é exercido de maneira desapercebida, pois as informações pessoais são repassadas pelos próprios fiscalizados, para os mais diversos fins, mesmo sem saber que estão sendo controlados.

A multiplicidade de redes e a liquidez nas informações fizeram com que se tenha muito mais do que apenas a designação de um sistema panóptico. Segundo Pessoa (2020, p. 46-47), surge a figura do pós-panóptico, do banóptico e o sinóptico. Com suporte em Bauman, inspira-se na imagem de uma nova forma de vigilância do panoptismo com o emprego das tecnologias, "permitindo a volatilidade do olhar do vigilante". Didier Bigo *apud* Pessoa (2020, p. 46) apresenta o viés de segurança nacional e como ela forma perfis dos indivíduos e define quem deverá ser colocado sob vigilância pelos agentes.

Quanto ao sistema sinóptico, o que se verifica é uma inversão da vigilância no sentido de que muitos observem a poucos. Os homens-caramujos carregam suas próprias celas, representadas por suas conchas, possibilitando a autovigilância e a vigilância dos outros. Percebe-se que esta vigilância não é vertical, mas se desenvolve

horizontalmente quando o indivíduo fornece, mesmo sem saber, dados que abastecem o banco global de informações que está pronto para ser usado pelos Estados ou por empresas que gerenciam as redes sociais.

Esta horizontalidade permite que a internet saiba onde está e o que poderia agradar o usuário, em termos de aquisição, serviços ou somente para um simples "gostei". Segundo Bioni (2019, p. 45) esta é a explicação porque a Waze foi adquirida pela Google por US$ 1,3 bilhão, pois a geolocalização é uma ferramenta importantíssima para o market individualizado.

Neste momento faz-se necessário voltar-se ao estudo de Lemes (2021) que traça um singular desenho sobre o emprego de algoritmos por entes governamentais, principalmente com a ampla expansão de programas preditivos em várias áreas do saber. A sua hipótese primária é a de que os algoritmos devem ser usados com transparência, pois podem permitir, em seus códigos, características que o tornem identificável, perante um grupo vulneráveis, e isso pode impedir o exercício de direitos.

As hipóteses secundárias são: de que a captação e utilização pode reproduzir racismo-estrutural; a utilização de algoritmos[9] opacos ressaltam o infamiliar[10]; utilização securitária pode revelar que os algoritmos sejam tendenciosos com viés eugênico.

Apresentadas as condições de sua pesquisa, a autora descreve que os Estados-nação podem estar utilizando as novas tecnologias para o *surveillance* (vigilância-segurança-manipulação de dados e metadados). Neste novo formato de vigilância, sem comparação com o de vigilância panóptico, tem-se a vigilância de pessoas hiperconectadas, que vivem num mundo globalizado revestido por extrema insegurança. Torna-se, assim, num controle social preditivo que torna o poder do Estado mais forte, denominado *new surveillance*.

Desta forma, os dados são produzidos pelas pessoas e o Estado os utiliza, de forma opaca, sob o argumento de que necessita promover

[9] Segundo (Kremer, 2023, p. 10): "algoritmos podem ser entendidos como conjunto de instruções que explicam detalhadamente como realizar uma tarefa qualquer. Seguidas passo a passo, de maneira detalhada e ordenada, essas instruções possibilitam atingir um resultado final, solucionar um problema".
[10] Assim, define: "infamiliar ressoa e reverbera no íntimo, evocando um conhecimento esquecido, oculto. Essa familiaridade perdida atua como vínculo corrompido, causando estranhamento e aversão, inquietação diante do que já não se reconhece". (LEMES, 2021, p. 68)

a segurança da economia, da ordem pública e outras atividades, a fim de obter maiores e melhores resultados. Segundo Lemes (2021, p. 60), os governos têm se apossado dos dados pessoais e empregado em estratégias para realizar análises preditivas de crimes, utilizando-se do comportamento do indivíduo, por intermédio de avaliadores de risco.

Mencionando um caso nos Estados Unidos em que o preso respondeu a um questionário com 137 itens, desenvolvido pela empresa Equivant e comercializado com o nome de COMPAS, o indivíduo teria sido qualificado como de alto risco de reincidência[11]. A defesa, neste caso, recorreu com os argumentos: a) em razão do código fonte ser protegido, teria ocorrido violação ao devido processo legal, pois era ausente a validade do teste; e b) ocorrência de sexismo e racismo, pois o programa leva em conta tais variáveis, mas o juiz do caso não considerou nenhuma das argumentações.

Para Lemes (2021, p. 61-62) existe uma dificuldade na utilização destes programas uma vez que, pelas normas do direto de propriedade, a empresa não é obrigada a fornecer a metodologia sobre os pontos para aferir o risco. Também, como segunda advertência, esta pontuação não tem capacidade de identificação eficiente para identificar indivíduos pela grande especificidade dos grupos a que pertencem. Como terceiro ponto, o COMPAS baseia-se numa amostragem nacional, sem validação que leve em consideração o Estado ou o Condado, bem como que os infratores de crimes insignificantes podem ser pontuados com mais gravidade. Por fim, não se pode perder de vista que o programa foi criado para o Departamento Correcional.

Este caso foi objeto de pesquisa no meio acadêmico e não foi comprovada a possibilidade de satisfazer, simultaneamente, a perfeita adequação aos mínimos de justiça esperados, mas que somente poderia ser aceito para casos excepcionais de crime.

Ainda segundo Lemes (2021, p. 71) a IA pode ser uma importante ferramenta para se alcançar soluções de problemas complexos, num

[11] Segundo o estudo: “Os réus com alta pontuação de risco reincidiram quase 4 vezes mais que aqueles de pontuação baixa (81% do primeiro grupo e, 22% do segundo). Entre os réus com pontuação 7, 60% dos réus brancos reincidiram e, 61% dos réus afrodescendentes, argumento utilizado pela Northpoint em favor da justeza do algoritmo. Entre os réus que não reincidiram, os afrodescendentes tinham 2 vezes mais chance de serem taxados como médio ou alto risco que os brancos, ainda quando não tivessem cometido um crime, estando, ainda, sujeitos a tratamento mais rigoroso por parte dos tribunais”.

momento em que os governos são chamados para atuar de maneira eficiente. Entretanto, nestes novos tempos, a governança deve agir para garantir a responsabilidade ética, com transparência, a fim de se evitar a violação de direitos fundamentais.

No mesmo sentido, Rodotà *apud* Mello (2021, p. 352) descreve que a utilização de tecnologia sob o pretexto de manutenção da ordem é corriqueira e deve ser vista com cautela:

> (...) excluir formas generalizadas de acesso a tais informações significa não apenas deixar nas mãos de grupos privilegiados o poder de tomar tais decisões, mas, sobretudo, impedir a quem não esteja no círculo mágico do verdadeiro poder, a possibilidade criticar tempestivamente as escolhas governamentais e propor alternativas correspondentes à realidade dos fatos. (RODOTÀ *apud* MELLO, 2021, p. 352)

Igualmente, Mello (2021, p. 352) leciona que ao serem inseridas informações e havendo treinamentos por homens brancos, existe uma grande probabilidade de que o programa seja preconceituoso em suas decisões. Neste sentido, a utilização de dados por terceiros pode gerar um "exercício dos poderes baseados na disponibilização de informações, concorrendo assim para estabelecer equilíbrios sócio-políticos mais adequados".

Por fim, buscando entender esta metodologia, descreve-se um caso concreto de emprego de IA na Micareta de Feira de Santana. Segundo Mello (2021, p. 356) a câmera capturou mais de um milhão de rostos de pessoas, gerando 903 alertas, 18 cumprimentos de mandados e 15 prisões, sendo que 96% não resultou em nenhuma medida criminal. Este desempenho deve ser analisado para que se conclua pela eficiência ou não desta atuação em segurança pública[12]. Quanto a isso, em sede de debates no âmbito do Congresso Nacional, a Comissão de Segurança Pública busca, por meio de audiências públicas com a população e especialistas, encontrar uma maneira eficaz de emprego destas câmeras de reconhecimento facial[13].

---

[12] Também, ressalta-se que o Estado do Rio de Janeiro, por autorização da lei nº 7.123/2015, realizava reconhecimento facial nos transportes urbanos intermunicipais, bem como fazia cruzamento de informações com a Interpol e Receita Federal. (Mello, 2021, p. 355)

[13] Extraído do site https://www.camara.leg.br/noticias/1058042-comissao-promove-debate-sobre-o-uso-de-ferramentas-de-reconhecimento-facial-no-combate-ao-crime/. Acessado no dia 15 de julho de 2024.

No que tange à utilização de câmeras para reconhecimento facial, uma vez que não existe uma norma geral, cada Estado brasileiro promove à sua maneira. Segundo dados do Projeto Panóptico, do Centro de Estudos de Segurança Pública e Cidadania (Cesec), mais de 200 municípios estão investindo elevadas cifras para a implementação nas guardas municipais.[14] À título de exemplo, a cidade do Rio de Janeiro concentrou as câmeras de reconhecimento facial no Bairro de Copacabana:

> O projeto foi dividido em duas fases: na primeira, foram instaladas câmeras apenas em Copacabana, durante o carnaval de 2019, e, na segunda, no bairro do Maracanã e nas imediações do Aeroporto Santos Dumont, e foi ampliado o número de câmeras em Copacabana. Em ambas as fases, os acordos de fornecimento de equipamentos e de cooperação técnica foram estabelecidos com a empresa Oi.
> A estrutura de funcionamento do projeto, na primeira fase, consistia na capacitação e no treinamento de quatro policiais militares que coordenaram os monitores e os acessos às 34 câmeras na área de Copacabana, incluindo as saídas do metrô nas estações Siqueira Campos e Arcoverde. (NUNES, 2022, p. 10)

Ainda neste site panóptico consta que dentre 11 casos de pessoas detidas com o uso da tecnologia, sete foram erros da máquina (63% dos casos). Em documento de despesa, no ano de 2019, indicou a solicitação de 10 policiais para suprir as demandas, resultando em R$ 726.789,00. Assim, no âmbito da segurança pública a IA também está promovendo mudanças na administração, sendo que as questões mais importantes estão ocorrendo com a possibilidade de emprego de monitoramento facial, vinculada às plataformas de cidades inteligentes e policiamento inteligente. Agrega-se ao debate a questão de que a IA pode estar impregnada com informações raciais, discriminação de gêneros e outras formas de violações dos direitos fundamentais.

Diante do que se verificou, para a utilização de IA o Estado deve primar pela transparência e respeito aos direitos fundamentais a fim de evitar que ocorram soluções equivocadas ou discriminatórias.

No tocante à governança de IA, deve-se estabelecer mecanismos que permitam evitar e minimizar os danos que possam ocorrer com o emprego de algoritmos ou com a utilização de informações constantes

[14] Extraído do site https://www.conjur.com.br/2024-mai-17/veja-como-cada-estado-usa-o-reconhecimento-facial-para-fins-policiais/. Acessado no dia 15 de julho de 2024.

na base de dados. Assim, o que se exige é a necessidade de encontrar uma prestação de contas eficiente a fim de que:

> (i) a designação de indivíduos ou de grupos específicos dentro da organização para promover a conformidade com os princípios; (ii) a adoção de medidas para aumentar a conscientização interna sobre a necessidade dessa conformidade, inclusive por meio de orientações e treinamentos em toda a empresa; e (iii) a implementação de um processo de escalação por meio do qual os funcionários possam levantar preocupações de conformidade e resolver essas preocupações. Podem, ainda, envolver a criação de selos, certificações e códigos de conduta corporativos ou governamentais. (BRASIL, 2021)

Em interessante estudo, o EBIA apresentou o trabalho realizado pela Fundação Getúlio Vargas – FGV que simulou o impacto da IA no mercado de trabalho brasileiro, para os próximos 15 anos. No estudo foram estabelecidos percentuais de adoção de 5%, 10% e 26%, sendo que em todos os cenários encontrou-se a redução de empregos menos qualificados. Por outro lado, quanto aos empregos mais qualificados, haverá um aumento salarial de 7% e 14,72%.

Com isso, percebe-se a necessidade de criar políticas públicas no campo de IA e proteção de dados, que visem a qualificação ou requalificação de trabalhadores, a fim de que sejam minimizados estes números. Quanto à pesquisa, e o seu desenvolvimento, é inevitável o impacto positivo, mas se faz necessária a realização de políticas públicas para fomentar pesquisas interdisciplinares a fim de evitar discriminações entre áreas do conhecimento.

No campo do poder público, para além do Executivo, a IA se apresenta como uma nova possibilidade de eficiência, promovendo uma superação dos obstáculos burocráticos. No Brasil, já existem vários órgãos que estão fazendo uso da IA na esfera Federal, como exemplos:

> TCU – “Alice” (Análise de Licitações e Editais). Alice, o primeiro dos três robôs do TCU, lê as licitações e editais publicados nos Diários Oficiais trazendo aos membros do Tribunal o número de processos por estado, assim como o valor dos riscos de cada um. Com esses dados, o robô ainda cria um documento apontando se há indícios de fraudes.
> TCU – “Sofia” (Sistema de Orientação sobre Fatos e Indícios para o Auditor). Funciona como um corretor que auxilia o auditor ao escrever um texto, apontando possíveis erros e até sugerindo informações relacionadas às partes envolvidas ou ao

> tema tratado. Sofia cria alertas com dados como a validade de um CPF registrado pelo auditor, a existência e a validade de contratos de uma entidade, se há registro de óbito sobre determinada pessoa, e se o cidadão ou empresa está ou não cadastrado no sistema do TCU.
> TCU – "Monica" (Monitoramento Integrado para Controle de Aquisições). Traz informações sobre as compras públicas na esfera federal, incluindo os poderes Executivo, Legislativo e Judiciário, além do Ministério Público. O robô faz um trabalho mensal de obtenção de dados, com exceção das informações sobre pregões, que são atualizadas semanalmente. Além disso, a tecnologia permite que sejam feitas buscas rápidas por palavras-chave no objeto das aquisições.
> (...)
> CGU: implantou um sistema para encontrar indícios de desvios na atuação de servidores.
> CGU: possui outro sistema baseado em IA usado com o propósito de fiscalizar contratos e fornecedores. A ferramenta elabora uma análise de riscos, incluindo não somente o de corrupção, mas também de outros problemas, como a possibilidade de um fornecedor não cumprir o contrato ou fechar as portas.
> STF – "Victor": a ferramenta tem por objetivo ler todos os Recursos Extraordinários que chegam ao STF e identificar quais estão vinculados a determinados temas de repercussão geral.
> MPF – HALBert Corpus: classifica os pareceres dados em Habeas Corpus quanto a sua admissibilidade (conhecimento, não conhecimento, se está prejudicado, etc) e mérito (concessão, denegação, sem exame de mérito, etc). (BRASIL, 2021)

Percebe-se que a IA e a utilização dos algoritmos vem, a cada dia, fazendo parte da rotina dos indivíduos e do poder público. Para Harari (2018, p. 83) esta situação de mudança de autoridade, dos humanos para algoritmos, não viabiliza mais o entendimento do mundo em que os indivíduos praticavam seus atos com autonomia. Agora, tudo é visto como um fluxo de dados que são processados e analisados pela máquina e que, num futuro, definirá qual será a minha melhor escolha.

Entretanto, mesmo diante de todo este debate, foi apenas em 2022, por intermédio da Proposta de Emenda Constitucional n° 115, de 10 de fevereiro de 2020, que o tema passou a integrar o extenso rol dos direitos fundamentais, nos termos do inciso LXXIX: "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais". Tal condição demonstra que a proteção de dados ainda se encontra dependente de um robusto estudo.

Assim, o direito fundamental à proteção de dados foi previsto no rol do artigo 5°, sendo a lei específica debatida no Congresso Nacional e sancionada pelo Presidente da República no dia 14 de agosto de 2018. Contudo, a complexidade da lei é evidente[15] e demandará esforços dos órgãos públicos e privados para a sua aplicação, conforme verificação das leis alteradoras e que foram decorrentes de medidas provisórias do Executivo Federal.

## 2.2 GERAÇÃO NORMATIVA DOS DIREITOS DIGITAIS

Segundo Rosa (2022, p. 60) a sociedade atual encontra-se na Quarta Revolução Industrial cujo principal combustível é o dado pessoal que é transmitido pela rede de computadores. Entretanto, como qualquer evolução ocorrida na sociedade, esta não pode ser tratada de forma isolada, ou seja, que antes dos dados pessoais existiam outros insumos, tais como aconteceu com o carvão, ferro, com o emprego do vapor, que são característicos da Primeira Revolução Industrial.

Já na Segunda Revolução Industrial, durante o século XIX, houve o domínio da eletricidade, os avanços da química, utilização dos eletrodomésticos e dos aviões. Por fim, a Terceira Revolução Industrial, já no século XX, a informação, os computadores e as telecomunicações foram seus diferenciais, possibilitando ganhos quantitativos e qualitativos no processamento dos problemas complexos que assolavam a sociedade.

Para Meireles (2023) o momento atual, com a nova visão de negócios em que as informações pessoais são disponibilizadas em troca de serviços “gratuitos”, as experiências humanas são matéria-prima para fortalecimento do capitalismo de vigilância.

Assim como ocorreu nas Revoluções Industriais anteriores, com o surgimento de sindicatos que buscavam melhorias para as classes trabalhadoras, com fundamento nos direitos da pessoa humana, o capitalismo de vigilância sofre incidência de normas que visam a proteção do homem. Para Rosa (2022, p. 63) esta violação ao indivíduo surge ao comprar um produto, contratar serviços ou quando somente pesquisamos algo na internet, o indivíduo sofre uma verdadeira

[15] A complexidade se materializa pela quantidade de prorrogações sofridas e acrescentadas ao texto do artigo 65.

intrusão na sua vida privada, uma vez que nossos dados já trafegaram pelas mais diversas empresas que fazem parte da cadeia de consumo.

Com isso, surge o novo ramo do direito digital no momento em que, paulatinamente, as leis que tutelavam a personalidade foram sendo aprimoradas, primeiro no âmbito interno dos países, depois em regiões ou grupos de países e, ao final, de forma bastante ampla e global, pois segundo Pinheiro (2013) "toda mudança tecnológica é uma mudança social, comportamental, portanto, jurídica".

Para Doneda (2020) as primeiras leis nacionais de proteção de dados surgiram na década de 1970, tendo como precursoras a Lei de Hesse (Land alemão) e a da Suécia (1973), sendo que esta última se referia ao banco de dados "Datalog" e à função de inspetor para o uso de dados pessoais. Nesta primeira geração, as leis preocupavam-se com o estado da tecnologia que possibilitava ao poder público coletar indefinidamente os dados dos cidadãos e arquivá-los para uso futuro, militar ou não.

Igualmente, estas leis de primeira geração eram voltadas, quase que exclusivamente, para a concessão e criação de banco de dados sob o controle do Estado. Assim, tais normas faziam parte de um contexto em que não havia muita experiência tecnológica de intercomunicação ou de transferência entre os bancos de dados nem tampouco se pensava na vontade do próprio detentor dos dados pessoais.

Segundo Lugati e Almeida (2020, p. 05) um exemplo de lei desta geração, e que se inseriu num contexto de Estado Moderno, foi a Privacy Act norte americana de 1974 que tinha como característica a centralização do Estado como detentor de dados. Entretanto, com aumento da quantidade de bancos de dados e a dificuldade no controle das concessões pelo Estado, o que demandava rigoroso acompanhamento e fiscalização, estas normas se tornaram obsoletas.

A doutrina especializada de Doneda (2020) estabelece como marco final desta geração a Lei Federal de Proteção de Dados alemã de 1977 (Bundesdatenschutzgesetz). Na segunda metade da década de 1970 as normas estavam mais atentas à privacidade e à proteção de dados pessoais, como uma liberdade negativa que poderia ser exercida pelo cidadão[16].

[16] Esta mesma ideia foi replicada nas constituições portuguesa e espanhola, pois eram reflexos da insatisfação do cidadão pelo emprego de seus dados por terceiros.

Entretanto, não tardou para que as normas tivessem que ser novamente alteradas, pois, agora, o fornecimento de dados pelos cidadãos tornava-se uma condição sem a qual não se poderia viver em sociedade. Estes dados pessoais eram utilizados de forma generalizada e com diversos propósitos, tanto pela iniciativa privada quanto pelo Estado, numa transmissão dinâmica e continuada. Assim, exigir autorização do titular, como condição necessária de tratamento, era uma burocracia desnecessária que prejudicava o próprio indivíduo.

Para Bioni (2020, p. 191) neste momento dava-se ênfase ao titular dos dados pessoais e assegurava a sua autonomia no tocante ao fluxo dos seus dados, mas gerava um paradoxo no sentido de que o excesso de autonomia do titular esbarrava na necessidade de que seus dados eram imprescindíveis para a obtenção de sua sobrevivência na sociedade.

A terceira geração de dados pessoais, portanto, continuava com a manutenção do cidadão como centro das atenções, mas agora não se restringindo a tão somente autorizar ou fiscalizar o tratamento. Segundo Doneda (2020) o cidadão passava a ser mola propulsora da estrutura de dados pessoais, notoriamente conhecida como autodeterminação informativa, apesar de ainda restrita a uma minoria da sociedade.

Por fim, as leis de quarta geração, atualmente existentes nos países mais desenvolvidos, se predispõem a reduzir as desvantagens do enfoque individual, buscando fortalecer a pessoa (indivíduo) em relação às entidades que armazenam e tratam os dados pessoais, mas não se restringido apenas à autodeterminação informacional, conforme previsto anteriormente.

Para esta geração, segundo Bioni (2020), de forma mais enfática, passou-se a prever, expressamente, as competências de uma autoridade de proteção de dados que atuaria de forma independente e técnica.

Ao tratar sobre as autoridades de proteção de dados e da sua importância, Calsing (2019, p. 63) leciona que para que nem sempre as normas são eficazes e se faz necessário criar mecanismos e órgãos de controle que monitorem e sancionem seu descumprimento, pois a força não é o fim do direito, apesar proporcionar a eficácia social, mas

deve vir acompanhada de políticas públicas que viabilizem a atuação segundo os comandos normativos.

Esta progressão de normas, em gerações, que coexistiram em vários países, permite identificar alguns princípios que lhes são comuns, principalmente no tocante a possibilidade de decisão do cidadão e ao uso indevido de seus dados. Segundo Mendes *apud* Lugati e Almeida (2020, p. 14) existe cerca convergência de princípios entre as normas o que proporciona a sua aproximação, mesmo que em ordenamentos jurídicos diversos, como ocorreu nos Estados Unidos, Inglaterra e Alemanha.

Para Malheiros (2017, p. 32) o princípio da publicidade, da transparência, da qualidade de dados, segurança, responsabilidade e o consentimento, sendo que este último é o que confere ao titular dos dados o direito de anuir ou não que seus dados sejam tratados, são sempre presentes nas gerações de proteção de dados.

As leis de quarta de geração buscam proteger os indivíduos de afrontas ao seu direito fundamental à proteção de dados. Desta forma, a LGPD incide nos casos em que a sede da jurídica esteja fora do território, mas os reflexos pelo tratamento repercutam no Brasil, tal como ocorreu com a empresa "Tudo Sobre Todos" que disponibilizava e comercializava dados pessoais de brasileiros pela internet.

Segundo Vainzof (2019) a empresa Top Documentos LCC, que se apresentava como proprietária da aplicação, era localizada na França, o site era sediado nas Ilhas Seychelles, o domínio era registrado na Suécia, bem como não havia identificação do proprietário, entendeu a justiça brasileira para que os servidores de backbone obstaculizassem o acesso eletrônico no Brasil, além de bloquear R$ 2 milhões na conta do proprietário em sede liminar para custear os danos morais coletivos.

Nota-se, na atualidade, uma formatação básica das leis de proteção de dados pessoais que serve para viabilizar as trocas de dados entre países e empresas de forma mais segura e que fossem minimizados os vazamentos e os usos indevidos[17].

[17] Rememore-se o caso do Facebook quando "Em entrevista ao El País, no ano de 2018, o CEO do Facebook, Mark Zuckerberg afirmou que houve vazamento de dados pessoais pela Cambridge Analytica e que teria atingido 87 milhões as contas. No Brasil, o total teria sido de 443.117 conforme mencionou o diretor da empresa Mike Schroepfer. Segundo consta, muitos usuários não teriam configurado o modo referente à privacidade e isso facilitou a tomada de dados". Informações extraídas do

## 2.3 GOVERNANÇA DE DADOS NA ADMINISTRAÇÃO PÚBLICA

Tratar de administração pública é aprofundar no estudo do bem comum e na maneira de tornar os resultados mais eficientes, com ética e transparência. Com isso, inevitavelmente, depara-se com termos que invocam tal qualidade, assim como ocorre com a governança.

Segundo Martins e Marini (2014, p. 43) governança se tornou um "conceito mágico" cuja amplitude de sua interpretação se tornou um problema diante de tantas possibilidades tais quais "bom governo" ou sinônimo contemporâneo de gestão, ou de governar com critérios ou circunstancias. Para tanto, apresenta um conceito de desempenho que se vincula à criação de valor público, ou seja, "conjunto de impactos, produtos e esforços que satisfaçam as expectativas dos beneficiários, promovendo confiança e resiliência com os valores sociais".

Já para Matias-Pereira (2020, p. 79) governança pode ser entendida como a capacidade do governo para formular e implementar suas políticas, sendo que, para tanto, encontram-se presentes a gestão de finanças públicas, no seu aspecto técnico e gerencial, a fim de atender aos anseios de toda a coletividade. Ademais, neste conceito de governança não se enquadram apenas os cidadãos ou a definição de cidadania, mas um prolongamento desta no momento em que os agentes públicos se ocupam de melhor realizar os serviços ao público.

Apesar de não fazer parte diretamente desta pesquisa, ao compulsar o site do Tribunal de Contas da União – TCU, depara-se com o Acórdão n° 588/2018 que analisou com profundidade a maturidade dos órgãos da esfera federal, cujo tema governança foi composto por três mecanismos, dentre eles a Liderança e a Accountability.

Por liderança, aquela Corte, utilizando-se do Referencial Básico de Governança Aplicável a Órgãos e Entidades da Administração Pública (RBG) definiu: "Liderança refere-se ao conjunto de práticas, de natureza ou comportamental, que assegura a existência de condições mínimas para o exercício da boa governança, quais sejam: pessoas íntegras, capacitadas, competentes, responsáveis e motivadas

site https://brasil.elpais.com/brasil/2018/04/04/tecnologia/1522874235_618558.html. Acessado em 11 de junho de 2024.

ocupando os principais cargos das organizações e liderando os processos de trabalho".

França (2006, p. 75) define que a liderança é composta por atributos e práticas para ser considerada eficiente. Os atributos são a capacidade mental, inteligência emocional, conhecimentos técnicos e administrativos, desenvolvimento pessoal e forte senso de si próprio. Por seu turno, as práticas são as que promovem o direcionamento, poder de influenciar outros, fazer com que as coisas aconteçam e construir relações.

Quanto a isso, especificamente na PMDF que tem suas características próprias da vida castrense, a liderança é conceito que colocado em xeque quando se pensa na hierarquia e disciplina, pois, não raras vezes, ocupa-se uma função com base na antiguidade e não por competência ou quaisquer outras qualidades que o cargo exija.

Assim sendo, tendo em vista esta característica militar, a figura do líder é hipervalorizada em razão de sua ascensão hierárquica aos postos mais elevados da carreira, mas que, por muitas vezes, não possui o conhecimento técnico para aquele mister, além da excessiva rotatividade de chefias. Para Caetano (2020, p. 10)[18] a rigidez da caserna não possibilita que os subordinados demonstrem insatisfação, mas a forma como os comandantes transmitem as missões podem ser indicadores motivacionais relevantes, devendo a Alta Cúpula estar atenta aos desvios de conduta ou falhas na eficiência do grupo.

Para Saad-Diniz (2019, p. 172) este conceito tradicional de liderança, representada pelo chefe-superior, termina por ocasionar uma série de danos, principalmente quando se instala numa organização a visão tradicional do "tone at the top" que cria justificativas para uma elite de profissionais que se fundamenta na figura do (leader-centric). Este "super líder" pode viciar toda a eficiência da política pública, seja com objetividade seja com excesso grau de subjetividade. Para tanto, segundo o autor, esta nova liderança (new leadership) é determinada não apenas pelas suas funções na organização, mas pela sua influência emocional, no entusiasmo corporativo e nas novas experiências, e conclui:

[18] Disponível no site https://bdex.eb.mil.br/jspui/bitstream/123456789/7437/1/CGAEM_2020_TC%20CAETANO.pdf. Acessado em 10 de maio de 2025.

> (...) a nova escola de liderança, visionária, carismática, transformadora, autêntica, criando estratégias disruptivas, inspirando todos os stakeholders a incrementar sua performance sob a decisiva orientação do comportamento ético. Assim, o líder é visto como pessoa admirável, detentor de qualidades, valores e habilidades altamente desejáveis e líderes efetivos são considerados aqueles que geram resultados quantitativos e qualitativos superiores. (SAAD-DINIZ, 2019, p. 174)

Logo, a ferramenta liderança, no contexto de governança, é responsável pela motivação, confiança e reforço na ideia de que os desafios devem ser superados por todos. Segundo Newstrom (2008, p. 111), o estabelecimento de metas é um processo motivacional que cria uma discrepância entre o que está sendo realizado e o que se deseja que se realize, ou seja, altera diretamente o desempenho. Não restam dúvidas de que o estabelecimento de um cronograma de atividades com suas respectivas metas auxilia no desejo interno de cada indivíduo em exercer suas tarefas, o que o autor define como autoeficácia.

Corroborando com o estudo acima, Vieira *et al* (2011, p. 14) entendem que metas mais fáceis são mais aceitas que aquelas mais difíceis, entretanto se o gestor conseguir fazer com que a sua equipe busque aquela meta desafiadora, a consequência será perceptível no desempenho final da atividade.

Para Newstrom (2008) o desafio, como elemento do estabelecimento de metas, tem o caráter de motivar os responsáveis para o exercício de sua atividade, entretanto "devem ser factíveis, considerando-se a experiência dos indivíduos e a disponibilidade de recursos". Nesta senda, nota-se que o estabelecimento de metas não significa, por si só, a certeza do empreendimento ou o engajamento da equipe, mas tais propósitos devem ser aceitos pelo responsável da atividade, pois a "simples distribuição de tarefas para os funcionários pode não resultar em seu comprometimento com essas metas, especialmente se a meta for difícil de ser alcançada".

Quanto à accountability, outra ferramenta utilizada pelo TCU para medir a maturidade de governança, a literatura a divide em administrativa e social. A administrativa se define por um processo de prestação de contas e de responsabilização de agentes públicos em face de uma falha na prestação do serviço. Esta prestação de contas, para Ros (2019) pode ser realizada internamente, pela transparência pública ou por auditoria, ou externamente pelos órgãos de controle ou

pelo poder judiciário em devidos processos legais acarretando sanções civis, penais ou administrativas.

Paralelamente ao accountabilty administrativo, surge a conceituação de accountability social que segundo Teixeira *et al* (2024, p. 179) "é identificada como mecanismo de controle vertical não eleitoral que se baseia na ação de atores sociais, incluindo cidadãos, associações e os meios de comunicação, no sentido de controlar o governo". Para a autora, esta forma de accountability possibilita o verdadeiro controle social, contribuindo para a melhoria da gestão pública.

Nota-se que os conceitos supracitados estão incluídos na concepção de Estado democrático de direito no qual a participação da sociedade torna a governança mais eficiente e com resultados mais positivos, pois para Fonseca e Avelino (2020, p. 44) a participação ativa da sociedade na governança reflete em benefícios e torna mais legítima as políticas públicas executadas pela administração, bem como é uma boa prática a ser seguida.

Apresentados conceitos de governança e de suas ferramentas, da liderança e da accoutability, não se pode olvidar de que no estágio atual de tecnologia, e com o avanço da internet, a administração pública passou do governo eletrônico para o governo digital que, segundo a OCDE (2014), se diferenciam no momento em que aquele se utiliza da Tecnologia de informação e comunicação (TIC) como uma ferramenta a fim de alcançar uma melhor gestão governamental enquanto esse se vale das tecnologias digitais para a obtenção de valor público, envolvendo atores do próprio governo, empresas e associações que apoiam a produção e o acesso aos dados e serviços.

De pronto, percebe-se que o estágio de governo digital obriga o desenvolvimento de medidas que permitam à administração pública que priorizem a universalização do acesso às suas funcionalidades, com base em soluções tecnológicas, centradas na necessidade das pessoas[19]. Ainda segundo a OCDE (2014) para criar uma estratégica de

[19] Decreto federal n° 12.069 de 21 de junho de 2024 que "Dispõe sobre a Estratégia Nacional de Governo Digital e a Rede Nacional de Governo Digital – Rede Gov.br e institui a Estratégia Nacional de Governo Digital para o período de 2024 a 2027". Disponível no site https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2024/Decreto/D12069.htm. Acessado em 10 de maio de 2025.

implementação de um governo digital que denote valor público exige-se a observância de três pilares fundamentais.

O primeiro pilar é voltado para a incorporação do princípio da transparência e colaboração da administração pública com os diversos atores. O segundo pilar enfatiza a governança e a coordenação, com destaque para as estruturas eficazes para a plena efetivação da digitalização. O terceiro pilar volta-se para a necessidade de desenvolver competências que possam apoiar a própria implementação do governo digital.

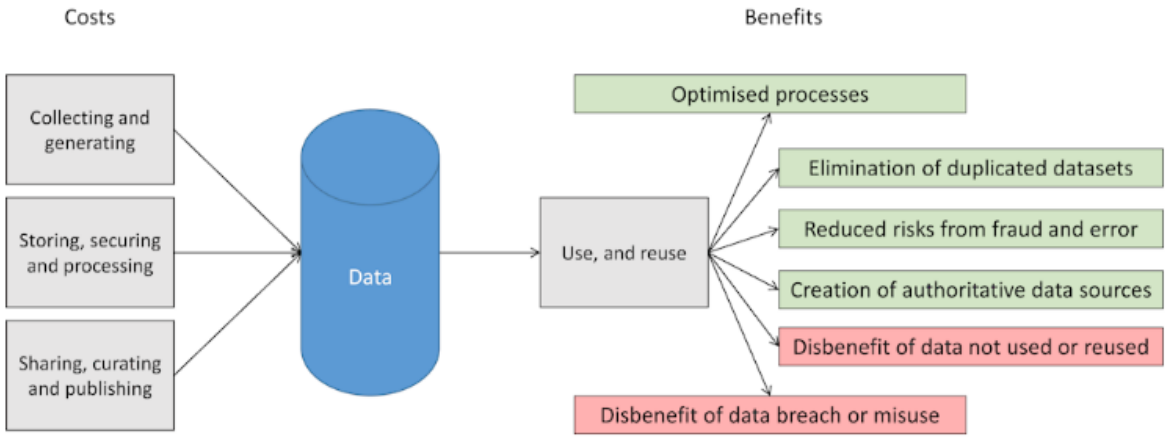
Em continuidade, uma boa governança de dados, no bojo de um governo digital, é crucial para possibilitar a extração do valor ativo dos dados e que terá como reflexo o aumento da eficiência e a responsabilização dos envolvidos no processo digital. Entretanto não acontece isolado ou apenas sob a tutela do setor de tecnologia da informação.

Para se compreender a definição de valor ativo de dados, tanto para a administração pública quanto para a iniciativa privada, deve-se analisar as sete "leis" da informação de Moody e Walsh *apud* OCDE (2019), que dispõe: a primeira lei é que a informação é (infinitamente) compartilhável, ou seja, não se deve acumular ou duplicar dados gerando aumento de custo; a segunda lei é que a informação aumenta com o seu uso, aumentando o retorno sobre o investimento. Assim dados não utilizados geram custo e risco em seu armazenamento.

A terceira lei se refere que a informação é perecível, pois dependendo do dado armazenado ele se desvaloriza ao longo do tempo; a quarta lei dispõe que o valor do dado aumenta com a precisão que ele contém; a quinta lei descreve que o valor da informação aumenta quando esta é combinada com outras, ou seja, a interoperabilidade é crucial para diminuir custos e aumentar tal valor; a sexta lei refere-se a que nem sempre mais dados é o melhor e torna mais eficiente o serviço público ou privado; a sétima e última lei estabelece que a informação não é esgotável, denotando que os dados derivados não são menor valorosos do que os originais coletados.

De forma resumida e didática, a figura abaixo descreve o ciclo de valor dos dados governamentais, bem como identifica o seu valor para a administração pública:

**Figura 1 –** ciclo de tratamento de dados pessoais




Fonte: OCDE (2019): O caminho para se tornar um setor público orientado por dados

Torna-se evidente, neste ambiente digital, que os medos e as desconfianças da população sobressaem nos casos de escândalos de corrupção e de utilização indevida de dados pessoais, exigindo, portanto, um robusto sistema de governança pública que esteja protegido por compliance digital.

Segundo Mathias (2020, p. 121) a confiança na administração pública e a proteção do interesse público são cruciais para que os indivíduos participem da vida pública, bem como no processo político, buscando seus direitos e eficiência dos serviços públicos, apesar de que a percepção de confiança está bastante voltada para ações de corrupção.

Desta forma, para que exista esta confiança na administração pública, deve-se implementar uma cultura de compliance para que seus agentes públicos possam agir com ética e respeito às normas que configuram proteção aos direitos humanos. Bertoccelli (2020, p. 43) leciona que não basta a existência de um código de conduta ou um conjunto de normas que descrevam políticas corporativas, mas não realize ações concretas para prevenir, detectar e punir atos que não estejam de acordo com o programa de compliance.

Para Magacho e Trento (2021, p. 7) o programa de compliance deve possuir um mínimo de elementos para ser efetivo como, por exemplo, a avaliação de análise de risco da atividade que anteciparia ocorrências prejudiciais e responsabilidades que poderiam ser evitadas.

Também para Garcia *et al* (2020, p.292) o programa de compliance para ter efetividade deve contar com o comprometimento

da Alta Gestão, investimento no setor, com recursos humanos capacitados a fim de que se obtenha o resultado esperado. No mesmo sentido, a Controladoria-Geral da União – CGU, menciona, em seu Programa de Integridade: diretrizes para empresas privadas[20], cinco pilares: comprometimento e apoio da alta gestão, instancia responsável pela integridade, análise de perfil e risco, estruturação das regras e instrumentos e monitoramento contínuo.

Aprofundando neste estudo e voltando-se para o governo digital, para Artese (2020, p. 456) o compliance digital é uma derivação do direito digital que surge com o emprego de tecnologia, possuindo um emaranhado de normas que se destinam à ética e conformidade, e que tem um pano de fundo digital. Ademais, segundo o autor, em matéria de compliance deve-se estabelecer prioridades uma vez que é impossível a conformidade plena, sendo a de fundo digital a escolha perfeita por alguns motivos: a) urgência em adequação para a LGPD; b) existência de riscos reputacionais da empresa ou órgão público, em razão das falhas de proteção de dados; c) possibilidade de sanções administrativas pela Autoridade Nacional de Proteção de Dados; e d) necessita de muito tempo para a sua implementação.

Para Calsing (2019, p. 64) os mecanismos de compliance em proteção de dados atuam para o gerenciamento de cumprimento de regras e evitar ou reduzir sanções penais. Assim, não implantar o compliance em direito digital, ou mais especificamente em proteção de dados, pode gerar impacto financeiro, resultante de danos morais, prejuízos à imagem da empresa ou órgão público, bem como sancionamento ao responsável pela falta de diligência com o tema.

Assim, para Magacho e Trento (2021), a complexidade do compliance voltado para proteção de dados exige uma postura enérgica da Alta Gestão para a sua implementação, pois existem três fatores que devem ser levados em consideração: o primeiro é que a LGPD torna necessária a adaptação na coleta e tratamento dos dados; o segundo é que há em cada dispositivo da norma uma gradação de níveis de exigência que se diferenciam, evitando que as atividades sejam interrompidas; o terceiro fator consiste na concretude da LGPD uma vez que existem dispositivos que são passíveis de interpretação

[20] Disponível em https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/integridade/arquivos/programa-de-integridade-diretrizes-para-empresas-privadas.pdf. Acessado em 10 de maio de 2025.

diversa, o que pode gerar equívocos por parte dos setores de compliance.

Diante do que foi visto, percebe-se que a governança de dados é formada por liderança, accountability, motivação de todos os que participam do processo, bem como de um sólido e efetivo programa de compliance voltado para a proteção de dados.

## 2.4 A LGPD COMO POLÍTICA PÚBLICA E O PAPEL DO TCU

A Lei Geral de Proteção de Dados (Lei n° 13.709/2020) surgiu no país, diferentemente do que ocorreu na União Europeia, com o Regulamento Geral de Proteção de Dados, de forma rápida e sem muito conhecimento por parte do poder público. Este desconhecimento, pela sociedade e pelos próprios parlamentares, pode ser corroborado pela forma como a lei foi alterada, antes mesmo de sua vigência, denotando o estado de dúvida perene que afeta diretamente os direitos fundamentais mais importantes:

> Apesar dos questionamentos que são levantados, a proteção de dados pessoais é importante, pois seu tratamento pode afetar direitos e liberdades fundamentais, entre os quais a lei brasileira destaca a liberdade, a privacidade e o livre desenvolvimento da personalidade. (CALSING, 2019, p. 01)

Em sua configuração, a LGPD trouxe bastante do Regulamento Geral de Proteção de Dados da União Europeia cujo escopo se destina a uma fórmula eficiente que possibilite trocas de informações amplas entre os países daquele continente. Apesar da LGPD ter sido econômica na conceituação de dado pessoal, o Regulamento Geral de Proteção de Dados Pessoais[21], em seu artigo 4°, dispõe que:

> (...) «Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular; (...) (UNIÃO EUROPEIA, 2018)

[21] Extraído do site https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acessado em 24 de junho de 2024.

Percebe-se a preocupação do legislador em adequar os conceitos aos tempos atuais em que a velocidade das informações ultrapassa as fronteiras e cuja proteção, outrora exclusivamente restrito às pessoas físicas ou aos meios tradicionais de correspondência, se volta para a coleta dos dados que, muitas das vezes, se referem à própria intimidade do indivíduo.

Compulsando a LGPD, em seu artigo 55-J, inciso III, definiu competência para a Autoridade Nacional de Proteção de Dados – ANPD para elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade.

Para Calsing (2019, p. 89) a LGPD atribuiu diversas competências para a ANPD para tornar mais efetiva a política de proteção de dados, dentre elas a possibilidade de articular com outros órgãos que atuam em setores específicos de fiscalização. Para que isso aconteça, a LGPD propõe que a ANPD mantenha um "fórum permanente de comunicação, inclusive por meio de cooperação técnica", promovendo o monitoramento de inovações e tecnologias, incentivando boas práticas e diretrizes de proteção de dados.

Como parte da consolidação da política de proteção de dados, constante na LGPD, a ANPD vem atuando bastante. Nota-se que entre os anos de 2021 a 2023 o número de servidores aumentou de 50 para 121, ainda sem quadro próprio, o que aparenta ser um número reduzido em razão das suas atribuições, nos termos do que consta no site oficial da ANPD.

As decisões da ANPD são confeccionadas em formato de Resoluções e são cogentes para todas as esferas de poder, tanto para órgãos públicos quanto para a iniciativa privada. Também, são encontrados os guias, estes sem força cogente, que servem para auxiliar na aplicação dos programas de proteção de dados, servindo, portanto, como recomendações importantes para serem estudadas e aplicadas.

Nos anos de 2021 e 2022, após o estabelecimento da agenda regulatória, foram firmadas as prioridades e as necessidades para uma maior orientação no que tange à proteção de dados pessoais. No site mencionado constam aos links de acesso para todos os documentos abaixo citados:

a) **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado.**
b) **Cartilhas segurança para a internet.**
c) **Guia como proteger seus dados pessoais.**
d) **Guia orientativo segurança da informação para agentes de tratamento de pequeno porte.**
e) **Regulamento do processo de fiscalização e do processo administrativo sancionador.**
f) **Guia orientativo aplicação da LGPD por agentes de tratamento no contexto eleitoral.**
g) **Regulamento aplicação da LGPD para agentes de tratamento de pequeno porte.**
h) **Guia orientativo tratamento de dados pessoais pelo poder público.**
i) **Guia orientativo cookies e proteção de dados pessoais.**
j) **Agenda regulatória da ANPD para o biênio 23/24.**
k) **Regulamento de dosimetria e aplicação de sanções administrativas.**
l) **Agenda de avaliação do resultado regulatório – 2023/2026.**
m) **Enunciado sobre hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes.**
n) **Guia orientativo tratamento de dados pessoais para fins acadêmicos e para a realização e estudos e pesquisas.**
o) **Modelo de registro simplificado de operações com dados pessoais para agentes de tratamento de pequeno porte (ATPP).**

No tocante às ações de fiscalização, verifica-se que são de quatro espécies: a) monitoramento; b) orientação; c) atuação preventiva; e d) atuação repressiva. Encontra-se consignado que a ANPD recebeu 237 (duzentos e trinta e sete) comunicados de incidentes, sendo que destes 97 (noventa e sete) foram casos de ransomware[22]. Quanto aos tipos de incidentes relatados, podem ser assim descritos:

[22] Segundo o documento da ANPD, ransomware "é um tipo de malware que criptografa os arquivos de um computador ou sistema, tornando-os inacessíveis ao usuário. Em alguns casos, é cobrado um valor para que seja fornecida uma senha para descriptografar os arquivos".

**Figura 2 –** tipos de incidentes


Fonte: ANPD (2024)

De igual importância neste contexto da política de proteção de dados encontra-se o TCU. Com previsão constitucional, no artigo 71[23] e seguintes, o Tribunal de Contas da União é responsável por auxiliar o Congresso Nacional, na atividade de controle externo, no que tange à fiscalização da administração direta e indireta na esfera federal.

Para Grin (2020), de início, cabe ressaltar que a atuação do Tribunal de Contas não é pacifica quando o assunto é a implementação de políticas públicas. A ampliação das funções do TCU, mesmo que sejam para propor recomendações, acabam por direcionar a administração e impedir o exercício da discricionariedade e a opção por uma resolução democrática. É justamente por não ter sido eleito, que o TCU não teria a legalidade para avaliar e estabelecer regras para a execução de políticas, bem como suas metas.

No entanto, em entendimento diametralmente oposto, para Fernandes (2012, p. 40) e Medeiros (2023, p. 08) a atividade de controle pode ser entendida como um próprio direito fundamental, apesar de não constar expressamente no texto da Constituição Federal. Assim, ao exercer a fiscalização e fomentar a eficiência administrativa, o Tribunal de Contas da União dissemina boas práticas, orienta quanto à governança administrativa, incentiva a redução de gastos públicos e aplica sanções administrativas. Ademais, ao receber petições ou

[23] Assim dispõe o art. 70: "A fiscalização contábil, financeira, orçamentária, operacional e patrimonial da União e das entidades da administração direta e indireta, quanto à legalidade, legitimidade, economicidade, aplicação das subvenções e renúncia de receitas, será exercida pelo Congresso Nacional, mediante controle externo, e pelo sistema de controle interno de cada Poder". (BRASIL, 1988)

denúncias, encaminhadas pelos cidadãos, força a transparência e a integridade daqueles que lidam com a coisa pública.

Em estudo voltado para a atuação dos Tribunais de Contas, na seara das políticas públicas, Medeiros (2023, p. 05) descreve que estas instituições seguem uma metodologia proposta pela Organização Internacional das Entidades Fiscalizadoras Superiores (INTOSAI) cujo objetivo é a promoção de alinhamento dos trabalhos de auditorias públicas.

Verifica-se que as auditorias do setor público podem ter objetivos distintos, mas o escopo é sempre o de contribuir para a boa governança baseada em evidências, aperfeiçoar o accountability e a transparência, fortalecer a efetividade dos órgãos dentro do ordenamento constitucional e criar incentivos para mudanças comportamentais dos gestores no trato com a coisa pública[24].

Quanto ao Tribunal de Contas da União, via de regra, suas fiscalizações são seguidas com bastante atenção pelos entes federativos e pelos poderes que os compõem. A questão se reforça, ainda mais, quando existe o repasse de verbas federais, por meio de Convênios ou Acordos de Cooperação Técnica, quando os entendimentos e decisões daquela Corte se tornam obrigatórios.

Em razão das atividades de fiscalização, para fins desta pesquisa, podem ser descritos os interessantes trabalhos de fiscalização do TCU e que são de ampla divulgação na jurisprudência administrativa. Um deles, encontra-se delimitado no Acórdão n° 1.139/2022 – Plenário que tratou de identificar os riscos associados e o conhecimento dos impactos da Estratégia Brasileira de Inteligência Artificial – EBIA[25], instituída pela Portaria Ministério da Ciência, Tecnologia e Inovação n° 4.979/2021.

Naquele trabalho de auditoria, o relatório apresentou robustos conceitos acerca da inteligência artificial e, voltando-se para a

[24] Extraído do site https://nbasp.irbcontas.org.br/wp-content/uploads/2022/11/NBASP-100-Principios-Fundamentais-de-Auditoria-do-Setor-Publico.pdf. Acessado no dia 20 de agosto de 2024.

[25] Extraído do site https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/*/NUMACORDAO%253A1139%2520ANOACORDAO%253A2022%2520COLEGIADO%253A%2522Plen%25C3%25A1rio%2522/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0. Acessado em 20 de agosto de 2024.

Administração Pública Federal, descreveu vários programas de IA que estão sendo utilizados pelos órgãos públicos.

Em suas conclusões a Corte de Contas descreveu que grande parte das organizações da Administração Pública Federal não planeja utilizar IA em seus processos internos e nem mesmo para a disponibilização de serviços para o cidadão. Também, verificou que 48% das organizações não realizaram capacitação de seus servidores e que, de forma comparativa, o poder judiciário está em estágio mais avançado de IA. Já quanto ao próprio EBIA, o TCU apontou várias irregularidades, tanto formais quanto de monitoramento, e que a ausência de mecanismos de governança pública fragiliza a implementação do plano estratégico.

Avançando no tema proteção de dados pessoais, destaca-se o Acórdão n° 1.384/2022 – Plenário, originado de uma fiscalização do próprio TCU que tinha como foco a Segurança da Informação (SegInfo) e Segurança Cibernética (SegCiber), nos termos do Acórdão n° 4.035/2020[26], que já fazia a previsão de futura "auditoria sobre a LGPD".

É importante notar que para o TCU a segurança da informação é tema que se relaciona com a proteção de dados pessoais, uma vez que, mesmo após a sanção da LGPD, constatou-se o vazamento de dados referentes a mais de 200 milhões brasileiros, por conta de uma falha no Ministério da Saúde, e o incidente denominado "mega vazamento" no qual mais de 223 milhões de dados de titulares foram expostos, bem como informações de veículos e CNPJ's[27].

Esta fragilidade no trato das informações, principalmente nos dados pessoais, alertou o TCU para a importância em se avaliar a Administração Pública, também, quanto à adequação à LGPD no que tange a sua estrutura organizacional, capacitação de servidores, implementação de medidas para controle e, também, da Autoridade

[26] Naquela fiscalização do Tribunal, contida no Acórdão n° 4.035/2020, no bojo do TC 001.873/2020-2, encontram-se números interessantes que reproduziram a gestão da segurança da informação e da segurança cibernética na Administração Pública Federal: 59% das organizações implementavam, ainda que de forma parcial, a gestão de informação; 24% se encontravam no estágio de capacidade aprimorada; 35% no estágio de capacidade intermediária; e 41% ainda se encontravam nos estágios de capacidade inicial ou inexpressiva.

[27] Extraído do site https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml. Acessado em 20 de agosto de 2024.

Nacional de Proteção de Dados e Conselho Nacional de Proteção de Dados.

O trabalho de análise da adequação à LGPD se deu pela aplicação de questionário, no total de 60 (sessenta) questões, com 09 (nove) dimensões, contemplando temas que eram de interesse para os auditores. O preenchimento das questões se deu por um link, encaminhado por e-mail para as 382 organizações, e contou com a utilização de plataforma Lime Survey.

Compulsando o relatório de auditoria que acompanha o Acórdão n° 1.384/2022, notam-se números alarmantes e que merecem a devida atenção neste momento. Assim, para cada dimensão analisada segue um trecho das observações do TCU que possibilitará uma visão específica dos achados, nos seguintes termos: Primeira dimensão (preparação): "verificou-se que apenas 45% das organizações respondentes concluíram a preparação (identificação e planejamento) das medidas necessárias para a adequação à LGPD".

Para a segunda dimensão (contexto organizacional) aquele Tribunal descreveu que:

> (...) 77% dos respondentes não identificaram todas as categorias de titulares de dados pessoais com as quais mantém relacionamento; 51% não conduziram iniciativa para identificar os controladores; 70% não avaliaram a existência de controladores conjunto; 17% identificaram todos os processos de negócios que realizam tratamento de dados; e apenas 14% das organizações identificaram todos os dados pessoais que tratam. (BRASIL, 2022)

No que se refere à terceira dimensão (liderança), de suma importância para a condução de qualquer política de proteção de dados:

> (...) uma em cada quatro organizações não possui política de segurança da informação e 65% não possuem política de classificação da informação, sendo que apenas 57% dessas políticas abrangem diretrizes para classificação de dados pessoais e somente 18% abrangem diretrizes para identificar dados pessoais sensíveis e de crianças e de adolescentes; apenas 18% possuem política de proteção de dados pessoais; e 31% ainda não nomearam encarregado pelo tratamento de dados pessoais. (BRASIL, 2022)

Na quarta dimensão (capacitação dos colaboradores), número que corresponde ao grau de ensino e aprendizagem da proteção de dados:

> (...) o resultado também é preocupante, pois apenas a minoria das organizações, 29%, possui plano de capacitação que abrange a proteção de dados pessoais, sendo que somente 54% desses planos consideram que pessoas que exercem funções com responsabilidades essenciais relacionadas à proteção de dados pessoais devem receber treinamento diferenciado. Ademais, apenas 10% das organizações treinaram todos os colaboradores diretamente envolvidos em atividades que realizam tratamento de dados pessoais. (BRASIL, 2022)

Para a quinta dimensão (conformidade do tratamento com os ditames da LGPD):

> (...) verificou-se que somente 46% das organizações identificaram e documentaram as finalidades das atividades de tratamento de dados pessoais (11% identificaram todas as finalidades e 35% identificaram apenas algumas finalidades), sendo que, dentre essas organizações, 51% não avaliaram se coletam apenas os dados estritamente necessários e 61% não avaliaram se os dados pessoais são retidos (armazenados) durante o tempo estritamente necessário. (BRASIL, 2022)

A sexta dimensão (direitos do titular), segundo o TCU: "constatou-se que 75% das organizações ainda não elaboraram política de privacidade e que somente 14% implementaram mecanismos para atender todos os direitos dos titulares elencados no art. 18 da LGPD".

Para a sétima dimensão (dados compartilhados) a Corte de Contas definiu que: "somente 14% das organizações identificaram todos os dados pessoais compartilhados com terceiros e que 42% delas sequer realizaram iniciativa para identificar possíveis compartilhamento".

Quanto ao controle sobre os sinistros, descrito na oitava dimensão (gestão de incidentes):

> (...) constatou-se que 84% das organizações não possuem plano de resposta a incidentes que abrange o tratamento de incidentes de violação de dados pessoais; 72% não possuem sistema para registro de incidentes que envolvem violação de dados pessoais e 75% não possuem sistema para registro das ações adotadas para solucionar tais incidentes; 66% não monitoram proativamente a ocorrência de eventos associados

> à violação de dados pessoais; e 88% não estabeleceram procedimentos de comunicação à ANPD e ao titular. (BRASIL, 2022)

Por fim, a nona dimensão (medidas de proteção aos dados pessoais) finaliza com os seguintes números:

> (...) 54% das organizações declararam que não são capazes de comprovar que adotaram medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais; apenas 16% implementaram controle de acesso em todos os sistemas que realizam o tratamento de dados pessoais; 7% registram eventos de todas as atividades de tratamento de dados pessoais; 43% não utilizam criptografia para proteger os dados pessoais; e 85% não adotaram medidas para assegurar que processos e sistemas sejam projetados, desde a concepção, em conformidade com a LGPD (de acordo com os conceitos de Privacy by Design e de Privacy by Default). (BRASIL, 2022)

Com isso o TCU entendeu pela existência de uma situação de alto risco que envolve a privacidade dos cidadãos que tem seus dados coletados e tratados pela Administração Pública Federal, sendo necessário o acompanhamento e novas fiscalizações.

Em continuidade, a auditoria do TCU também versou sobre a natureza jurídica da ANPD que na época integrava a Presidência da República. Para a Corte de Contas aquela configuração administrativa não permitia a independência necessária para que a Autoridade de Proteção de Dados exercesse suas atividades, principalmente quanto à isenção das suas decisões em face das influências externas.

Ainda segundo o TCU, apenas a estrutura integrante da Administração Indireta poderia alcançar a autonomia e independência necessária para lidar com proteção de dados pessoais. Para esta fragilidade na estrutura organizacional, o TCU confeccionou expediente para a Casa Civil da Presidência da República a fim de que fosse alterada a natureza jurídica da ANPD. Entretanto, demonstrava-se no processo que, no dia 13 de junho de 2022, tinha sido editada a Medida Provisória nº 1.124/2022, que alterava a Lei nº 13.709/2014, e transformava a ANPD em autarquia de natureza especial vinculada ao Ministério da Justiça e Segurança Pública.

Diante dos resultados encontrados, que demonstraram a relevância do acompanhamento nas políticas de proteção de dados

pessoais, foram sugeridos os seguintes encaminhamentos pela Corte de Contas:

> 5) execução de auditorias de conformidade em amostra das organizações que responderam ao questionário, considerando critérios de relevância e risco, incluindo o nível de adequação à LGPD computado com base nas respostas autodeclaradas pelas organizações;
>
> (ii) acompanhamento contínuo da evolução das organizações públicas federais em relação ao nível de adequação à LGPD, **realizado por meio da disponibilização permanente de um questionário online, similar ao utilizado nesta fiscalização, o qual poderia ser respondido voluntariamente a qualquer momento para obtenção de diagnóstico a respeito da evolução da organização respondente quanto à adequação à LGPD**; e
>
> (iii) construção de um painel de informações a ser alimentado, inicialmente, com os dados referentes às respostas ao questionário coletadas por meio desta fiscalização e, posteriormente, com as respostas do questionário online, de modo a demonstrar de forma atualizada a evolução da adequação à LGPD das organizações públicas federais. (BRASIL, 2022) (grifei)

Após a sanção da Lei Geral de Proteção de Dados, e a criação da ANPD, nota-se que o TCU encontra restrições quanto ao tema de proteção de dados pessoais, sem ter perdido a competência constitucional para fiscalizar e apontar falhas na Administração Pública, principalmente quando está em risco este direito fundamental:

> 47. É forçoso ressaltar, entretanto, as limitações impostas à atuação do TCU nesse tema, uma vez que, nos termos do art. 30 da LGPD, compete à Autoridade Nacional de Proteção de Dados o estabelecimento de normas complementares sobre o uso compartilhado de dados pessoais, a exemplo do Guia Orientativo do qual consta o atual entendimento daquele órgão sobre a definição dos agentes de tratamento de dados pessoais.
> 48. Por outro lado, ressalto igualmente que não pode o Tribunal de Contas da União se omitir diante de assunto de tamanha relevância, diante dos prejuízos causados à eficiência da Administração Pública pela falta de compartilhamento e integração de dados entre órgãos e entidades do Estado, conforme sobejamente demonstrados em múltiplos Acórdãos desta Corte.
> 49. Diante do exposto, sugiro ao eminente Relator a inclusão de recomendação adicional direcionada à ANPD no item 9.4

> do Acórdão proposto por Sua Excelência, transformando a deliberação já proposta por Sua Excelência no subitem 9.4.1 e acrescentando o subitem 9.4.2, nos seguintes termos: (...) (BRASIL, 2022)

Desta forma, pode-se entender que o TCU participou ativamente no primeiro momento de implementação da Lei Geral de Proteção de Dados no Brasil quando avaliou riscos, fases de adequação e outros fatores em 382 organizações da Administração Pública Federal.

## 2.5 ESTUDOS SOBRE A IMPLEMENTAÇÃO DA LGPD EM ÓRGÃOS PÚBLICOS

No âmbito do Distrito Federal, a LGPD foi, primeiramente, regulamentada pelo decreto distrital n° 42.036, de 27 de abril de 2021, o qual estabelecia competências e apresentavam conceitos fundamentais quanto à matéria. Atualmente, o decreto distrital n° 45.771[28], de 08 de maio de 2024 regula a proteção de dados, sem grandes alterações em relação ao normativo anterior.

Destaca-se a figura do Encarregado Governamental, em seu artigo 11, como sendo pessoa física, lotada na Casa Civil do Distrito Federal, e tem como responsabilidade, dentre outras, a de atuar como canal de comunicação com a ANPD, orientar os controladores e encarregados setoriais, manter o portal atualizado e consolidar relatórios recebidos pelos encarregados setoriais.

No Portal distrital da LGPD pode-se encontrar vários documentos, tais como Manual da Lei Geral de Proteção de dados, Cartilha de Proteção de dados no GDF, bem como outras informações importantes. Também, ressalta-se que é possível acessar a relação de todos os Encarregados Setoriais e seus Suplementes (nome, e-mail e caixa SEI) que compõem o Governo do Distrito Federal.

Adentrando especificamente no que tange à instrução administrativa sancionatória, objeto de estudo deste subtópico, descreve-se o processo gerado pela Autoridade Nacional de Proteção de Dados – ANPD a fim de apurar irregularidades no tratamento de

[28] Disponível no site https://www.sinj.df.gov.br/sinj/Norma/2d779a53407041f7b899c348124f2cdb/exec_decc_45771_2024.html#capVI_art29. Acessado em 14 de março de 2025.

dados vinculados à Secretaria de Estado de Educação do Distrito Federal – SEEDF.

Consta no processo administrativo, SEI nº 00261.001192/2022-14[29], o auto de infração nº 06/2022, de 08 de julho de 2022, em que a CGF tinha apurado que a Secretaria de Educação estaria expondo indevidamente os dados pessoais de estudantes em virtude de:

> (...) uma falha de segurança no formulário de inscrição do Programa Educação Precoce, construído com a ferramenta Google Forms. As respostas enviadas pelos cidadãos estariam publicamente disponíveis, mostrando dados cadastrais e de saúde de 3.030 crianças e adolescentes, bem como de seus responsáveis, conforme evidenciado pelo Anexo SEE-DF Lista Espera Educação Especial (0045693). (BRASIL, 2022)

Notificado pela ANPD, o Encarregado Governamental do Distrito Federal solicitou manifestações do responsável pela proteção de dados da Secretaria, sendo esclarecido que:

> Nessa ocasião, a autuada informou que o serviço de inscrição no Programa Educação Precoce não estava disponível no i-Educar ou em qualquer outro sistema informatizado da Secretaria de Educação. Ao detectar inconsistências na espera de crianças para ingressar no Programa – como a duplicidade de inscrição em mais de uma unidade escolar, extenso tempo de espera, falta de transparência quanto aos critérios de classificação para o chamamento e ingresso e demanda represada –, a autuada optou pela criação do formulário de inscrição em lista de espera on-line. Essa iniciativa, portanto, teve o objetivo de assegurar os direitos dos estudantes; favorecer a lisura, unificação, validação dos dados, organização da oferta e diminuição do tempo de espera em lista; favorecer a acessibilidade, a clareza do processo de classificação e ordenamento e aumento da oferta, visto que as famílias poderiam se inscrever em mais de uma opção; organizar a demanda; e diminuir o tempo de espera. (BRASIL, 2022)

Ainda no mesmo ofício, a Secretaria de Educação informou que a falha ocorreu por uma "uma alteração de 'viewform' para 'viewanaly' (...)". Acrescentou que "(a) possibilidade de acesso aos dados, verifica-se na configuração do google forms, que traz no seu 'default' essa opção automaticamente selecionada".

[29] Extraído do site https://www.gov.br/anpd/pt-br/documentos-e-publicacoes. Acessado em 12 de julho de 2024.

Neste sentido, ainda segundo aquela Secretaria, tão logo tomou ciência, tratou de solucionar o problema e "alteraram a configuração do link de inscrição para não permitir a visualização das respostas, conforme impressão de página Anexo Lista Espera Educação Especial (0045697), e passaram a fazer o download e a exclusão das respostas diariamente".

Em análise, a ANPD entendeu que o incidente foi grave e emitiu a Nota Técnica n° 40/2022:

> (...) a SEEDF não identificou adequadamente os riscos relacionados ao incidente de segurança e as medidas técnicas e administrativas necessárias para garantir a segurança da base de dados afetada. Por esse motivo, reiterou à autuada que apresentasse: i) a comprovação da comunicação individual do incidente a todos os titulares de dados afetados; ii) o RIPD da atividade de tratamento relacionada ao incidente; iii) o registro da operação de tratamento de dados pessoais (ROT) relacionada ao incidente; e iv) o plano de gestão de incidentes de segurança da informação e privacidade, caso tivesse. (BRASIL, 2022)

Com isso, houve a fixação dos dispositivos violados no art. 48, art. 49, art. 37 e art. 38, todos da LGPD. Intimada para apresentar alegações finais, a Secretaria pediu prorrogação do prazo, para produzir a resposta, e foi atendida. Após o incidente ser devidamente apurado, passou a Autoridade Nacional de Proteção de Dados a discorrer sobre os pontos importantes, sendo um deles:

> A ANPD solicitou à autuada o envio do ROT na Nota Técnica n° 40/2022/CGF/ANPD (0045705) (ver [item 5.10]), **pedido nunca respondido no âmbito do PAI**. Na defesa apresentada neste PAS, contudo, a autuada enviou o documento acima mencionado, intitulado "Registro de Operação de Tratamento dos Dados Afetados pelo Incidente, conforme previsto no art. 37 da LGPD" (Anexo defesa administrativa (0049052), pp. 3-5) (BRASIL, 2022) (grifei)

Também, nota-se que a ANPD estava disposta a atender os pedidos de auxílio técnico e de informações para a confecção dos relatórios, conforme abaixo:

> Importante destacar que, caso a autuada tivesse apresentado o documento quando foi instada para tanto no âmbito do processo anterior ao presente PAS (ou seja, em eventual resposta à Nota Técnica n° 40/2022/CGF/ANPD (0045705)), a ANPD teria oferecido orientações sobre como construir um

> ROT aderente à LGPD, ao invés de sancioná-la pela ausência desse registro. **Isso porque o processo de fiscalização, quando ainda não iniciada a atividade repressiva, prioriza a adoção de medidas de orientação e de prevenção**, nos termos da atuação responsiva indicada no art. 15 do Regulamento de Fiscalização, em especial em seus §§ 2º e 3º. Regulados que dialogam com a ANPD e apresentam postura colaborativa se beneficiam de orientações voltadas a conduzir à conformidade o tratamento de dados que realizam. Isso porque a Autoridade pode valer-se das medidas preventivas, listadas no art. 32 do Regulamento de Fiscalização, para oferecer ao regulado a oportunidade de corrigir eventuais desconformidades à LGPD. **O objetivo maior da LGPD e, por conseguinte, da ANPD é que os dados pessoais sejam tratados de acordo com os parâmetros legais; e o diálogo, a interação e a construção dialética com os regulados, por seu caráter educativo e colaborativo, estão entre as maneiras mais efetivas para assegurar que essa finalidade seja alcançada**. (BRASIL, 2022) (grifei)

Entretanto, pela infração de não manter Registro das Operações de Tratamento (ROT), constante, no artigo 37 da LGPD, a Autoridade de Proteção aplicou a sanção de advertência (leve). Por não elaborar o RIPD após a solicitação da ANPD, nos termos do artigo 38 da LGPD, foi aplicada a sanção de advertência (leve).

No que tange a comunicação aos titulares dos dados quanto ao incidente de segurança, constante no artigo 48 da LGPD, a justificativa da Secretaria foi no sentido de que:

> (...) não precisaria realizar a comunicação do incidente aos titulares porque o formulário não havia sido divulgado ou disponibilizado em canal de comunicação ou rede social de sua responsabilidade; ademais, não teriam sido identificados prejuízos aos titulares ou à Administração Pública decorrentes do incidente (Ofício Vazamento de Dados – Portal I-Educar (0045725)). A suposta ausência de prejuízo é utilizada, pela autuada, como argumento para a não aplicação de penalidade no caso em apreço (Alegações Finais – Ofício nº 3592/2023 – SEE/GAB/AESP (0049066)) (BRASIL, 2022)

Estas alegações da Secretaria de Educação não foram aceitas, e, por isso, restou configurada a violação do artigo 48 da LGPD, sendo classificado como grave, mas foi aplicada a sanção de advertência.

Também, foi analisada a conduta de não utilizar sistemas que atendam aos requisitos de segurança conforme os padrões de boas

práticas e de governança e aos princípios da LGPD – art. 49 da LGPD (incidente de segurança). Esta incidência foi alterada pela ANPD, passando a ser o que prevê no artigo 46, mas a sua incidência foi afastada por rompimento do nexo causalidade.

Por fim, pela conduta de não apresentar informações relevantes para a avaliação das atividades de tratamento de dados pessoais, no prazo estabelecido pela ANPD – art. 5º do Regulamento de Fiscalização, foi aplicada a sanção de advertência, por não ter outra punição possível.

Após a publicação de todas as sanções, a ANPD encaminhou o processo para conhecimento e manifestação da Controladoria-Geral do Distrito Federal a fim de que fossem apuradas as condutas, sob o viés administrativo, dos agentes públicos envolvidos.

Diante de tudo o que foi analisado, deve-se considerar que: a) se faz necessária a efetividade do tratamento de dados pessoais, sendo uma atribuição legal do Encarregado Setorial; b) a comunicação com a Autoridade Nacional de Proteção Dados deve ser a mais transparente possível e as respostas devem ser confeccionadas dentro do prazo estabelecidos; e c) utilizar ferramentas que sejam reconhecidamente seguras e que os seus operadores passem por treinamentos constantes.

Em sede de conclusões para este referencial teórico, pode-se afirmar que a administração pública deve atuar com base na governança, ou seja, apropriar-se de mecanismos que auxiliem na busca da eficiência, com ética e respeito aos direitos humanos.

A liderança é ferramenta imprescindível para todo o suporte administrativo, uma vez que, por intermédio desta é que conseguirá motivar e superar os desafios, principalmente numa sociedade digital do século XXI.

Por seu turno, a prestação de contas dos serviços e a transparência são cruciais para que o indivíduo participe ativamente das políticas públicas e, com isso, fomente os melhores resultados. De igual importância, encontram-se outras peças fundamentais que também promovem a accountability, dentre elas a ANPD e o Tribunal de Contas da União.

Como determinação legal, seguindo o RGPD europeu, a LGPD criou a Autoridade Nacional de Proteção de Dados - ANPD, que, no bojo

da política nacional de proteção de dados, tem o mister de orientar, fiscalizar e impulsionar as boas práticas para o tratamento de dados pessoais no Brasil.

Viu-se que, por intermédio de suas auditorias, as Cortes de Contas dialogam com os demais poderes da república e incentivam a boa governança pública, principalmente diante de um cenário que se movimenta por dados pessoais e algoritmos que representam pessoas. Mais uma vez, a ética e o foco nas melhores práticas, bem como o respeito e a obediências às normas farão a diferença neste complexo problema gerado pela tecnologia.

Corroborando com a importância da adequação à LGPD nos órgãos públicos, apresentou-se um estudo de caso no qual a Secretaria de Estado de Educação do GDF sofreu penalidades administrativas por não cumprir o que foi preconizado pela norma de proteção de dados. Desta forma foi possível concluir que a exposição dos dados pessoais de pais e estudantes, somados ao desconhecimento e ausência de respostas para a ANPD foram as maiores responsáveis pelo ocorrido.

Por fim, a segurança pública não está alheia ao avanço. Na mesma medida em que os programas de IA podem economizar tempo e salvar vidas, eles podem segregar, discriminar e promover a maior das violações dos direitos humanos. Como exemplo, tem-se que as câmeras de reconhecimento facial, cuja matéria ainda se encontra em debate no Congresso Nacional, estão sendo utilizadas para as mais diversas finalidades. Então, somente com um efetivo programa de compliance, com o comprometimento da Alta Gestão, poderá tornar ética a utilização destas ferramentas que estão à disposição de todos, inclusive da Administração Pública.

A PMDF, integrante do Sistema de Segurança Pública do Distrito Federal, deve buscar o aprimoramento de sua governança, a fim de que não sofra reflexos decorrentes de sua inércia administrativa. Adequar-se às novas ferramentas tecnológicas não é somente uma questão orçamentária, mas depende de forte mudança cultural de seus integrantes e, inclusive, uma gestão de riscos estratégica que seja capaz de demonstrar as prioridades exigidas pela sociedade e pelos órgãos de fiscalização.


3

# 3 METODOLOGIA

A fim de se obter as respostas aos objetivos elencados esta pesquisa utilizou de método misto em que uniu a abordagem qualitativa e quantitativa. Houve a necessidade da abordagem qualitativa, uma vez que se baseia em fenômenos únicos e que não podem ser separados do seu contexto.

Segundo Creswell (2004) a pesquisa qualitativa torna o mundo visível em dados que os representa, mas dentro de uma perspectiva que envolve seu contexto natural. Ainda, segundo o autor, a coleta é realizada no ambiente a ser estudado, envolvendo múltiplos métodos e um raciocínio complexo que gira entre a dedução e a indução, bem como focado na perspectiva dos participantes.

Da mesma forma, Gil (2021) define a pesquisa qualitativa como aquela frequentemente empregada quando existe a dificuldade em obter resultados quantitativos em certos contextos, como por exemplo investigar casos de forma mais profunda.

Por seu turno, a abordagem quantitativa serve para analisar indicadores produzidos pela Polícia Militar do Distrito Federal, incluindo artefatos que estejam relacionados à implementação da LGPD. Desta forma, a junção das informações obtidas qualitativamente com aquelas obtidas quantitativamente auxiliará na compreensão do estado atual de adequação da LGPD na PMDF.

No que tange à natureza, esta pesquisa é enquadrada como aplicada, uma vez que busca a solução de problemas concretos, no caso os existentes na Polícia Militar do Distrito Federal. Sob o viés da epistemologia, a adequação da Lei Geral de Proteção de Dados foi analisada da forma como se encontra atualmente, sem qualquer interferência ou indução, apesar do pesquisador ser integrante da Corporação.

Trata-se, também, Segundo Gil (2021) de uma pesquisa exploratória uma vez que seu objetivo visa uma maior familiaridade com o problema, aprimorando ideias, possuindo um planejamento que assume a forma de pesquisa bibliográfica ou estudo de caso.

Por fim, não se pode olvidar que a pesquisa apresentou um estudo de caso, como integrante de uma pesquisa exploratória, e que possui vantagens por estimular novas pesquisas, possibilita a superação de um problema muito comum, simplicidade dos seus procedimentos quanto à coleta e análise de dados.

O objeto analisado foi a Política Militar do Distrito Federal, mantida e organizada pela União, porém integrante da Administração direta do Distrito Federal, ou seja, pertencente ao Governo do Distrito Federal – GDF e que teve como unidade-chave de resposta o Subcomitê Executivo de Proteção de Dados.

No que tange ao instrumento e procedimentos de coleta de dados para a realização da pesquisa, foi utilizado o questionário aplicado no ano de 2021 pelo Tribunal de Contas da União, estruturado com base no Acórdão n° 1.384/2022, apenas com as perguntas fechadas, e que foi anexado ao trabalho, mas que não foi respondido pela PMDF no prazo estabelecido pela Corte de Contas.

Visando à obediência aos ditames internos da PMDF a pesquisa foi submetida ao Departamento de Educação e Cultura – DEC que, por intermédio de Parecer, autorizou o encaminhamento do questionário para a Encarregada Setorial, no caso a Auditora da PMDF. Por seu turno, aquela autoridade designou um integrante daquela Auditoria para que respondesse o questionário, nos termos do que consta no Anexo.

Com isso, as respostas foram realizadas por intermédio formulário google.com/forms aos responsáveis do Subcomitê Executivo, nos termos do que consta no processo de Sistema Eletrônico de Informações – SEI n° 0054-00166772/2024-08. À título de complementação, no dia 03 de dezembro de 2024, foi solicitada informações acerca dos artefatos produzidos pelo Colegiado, no que tange à implementação da LGPD.

Também, houve a coleta de documentos normativos constantes em dados abertos, no site da PMDF, bem como artefatos produzidos e disponibilizados pelos setores competentes, conforme Anexos.

Investiga-se, portanto, o grau de adequação da Política de Proteção de Dados Pessoais na PMDF, ressaltando-se que a confecção da Portaria interna, datada do ano de 2022, contou com a participação deste pesquisador e, ao que tudo indica, não conseguiu êxito.

De forma resumida, com a possível inércia do Subcomitê Executivo, o Comitê de Gestão (integrado pelo Alto Comando da PMDF) não teve o que apreciar. Também não se pode olvidar para o fato de que, em caso de ocorrência de vazamentos dos dados pessoais, fora o efeito desastroso no âmbito do Distrito Federal, isso deverá ser submetido aos rigorosos tratamentos e contenções, nos termos da regulamentação estabelecida pela Autoridade Nacional de Proteção de Dados.

## 3.1 SOLICITAÇÃO ADMINISTRATIVA DOS ARTEFATOS CONFECCIONADOS PELO SUBCOMITÊ EXECUTIVO DE PROTEÇÃO DE DADOS DA PMDF

Como mencionado, com o escopo de aprofundar na pesquisa e verificar o grau de maturidade da proteção de dados na PMDF, foi encaminhado documento interno a fim de que o Colegiado informasse e encaminhasse, se existentes, para análise crítica por parte deste pesquisador. Assim, foi obtido o documento que descreveu o memorando nº 21/2024, de forma suscinta:

**Tabela 1 – Relação de artefatos produzidos pelo representante da PMDF**

| PROVIDÊNCIAS TOMADAS PELO SUBCOMITÊ | DOC. SEI/GDF | FUNDAMENTAÇÃO |
|---|---|---|
| Pedido de divulgação no âmbito da Corporação de informações sobre a privacidade de dados pessoais | Memorando Nº 4/2024 – PMDF/DCC/AUD/SAF/CH (144985970) destinado ao CCS | Art. 29 da Portaria PMDF nº 1.279, de 23 de junho de 2022 |
| Pedido de adoção de medidas de educação continuada atinentes à Lei Geral de Proteção de Dados (LGPD) | Memorando Nº 5/2024 – PMDF/DCC/AUD/SAF/CH (144991318) destinado ao DEC | Art. 41 da Portaria PMDF nº 1.279, de 23 de junho de 2022 |
| Pedido de nomeação de Comissão/Grupo de Trabalho com o desígnio de propor a alteração/revogação da Portaria PMDF nº 1.279, de 23 de junho de 2022, de acordo com as necessidades | Memorando Nº 6/2024 – PMDF/DCC/AUD/SAF/CH (145228362) destinado ao Estado-Maior | Decreto nº 45.771, de 08 de maio de 2024 |

| | | |
|---|---|---|
| institucionais, tendo em vista o advento do Decreto nº 45.771, de 08 de maio de 2024 | | |
| Solicitação de agendamento de reunião com o Comitê Gestor de Proteção de Dados Pessoais – CGPDP / Comitê Interno de Governança da Polícia Militar do Distrito Federal – CIG, com o fim de tratar de assuntos atinentes à Política de Proteção de Dados Pessoais no âmbito da PMDF | Memorando Nº 11/2024 – PMDF/DCC/AUD/SAF /CH (146564818) destinado ao GCG | Art. 15, inciso III, da Portaria PMDF nº 1.279, de 23 de junho de 2022 |
| Solicitação de informações aos Operadores Internos para fins de elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) | Memorando Circular Nº 2/2024 – PMDF/DCC/AUD/SAF (157153161) | Art. 25, inciso IX, da Portaria PMDF nº 1.279, de 23 de junho de 2022 |
| Orientações sobre o cumprimento da LGPD e boas práticas de governança, bem como solicitação de informações acerca da ocorrência de incidentes de segurança | Memorando Circular Nº 1/2024 – PMDF/DCC/AUD/SAF (157136192) | Art. 9º, V; o art. 11, I, da Portaria PMDF nº 1.279, de 23 de junho de 2022 |
| Elaboração das respostas ao questionário do TCU referente ao ano de 2024, acerca dos controles implementados pela PMDF para assegurar a conformidade com a LGPD. | Processo SEI/GDF nº 00054-00096313/2024-41 | Auditoria do TCU para avaliar a adequação das organizações públicas federais à LGPD |

Fonte: tabela confeccionada pelo representante do Subcomitê Executivo da PMDF (2024)

Para favorecer a didática e não comprometer o desenvolvimento do trabalho, todos os documentos relacionados foram incluídos no Anexo. Ademais, as considerações críticas acerca de cada artefato serão realizadas em tópico específico.

## 3.2 ENVIO DO QUESTIONÁRIO DESCRITO NO ACÓRDÃO Nº 1.384/2022 – TCU E COLETA DAS RESPOSTAS PROMOVIDAS PELO SUBCOMITÊ EXECUTIVO DE PROTEÇÃO DE DADOS DA PMDF

Para o atendimento deste subtópico foi encaminhado o documento ao Departamento de Educação e Ensino da Polícia Militar do Distrito Federal (DEC/PMDF), no dia 21 de novembro de 2024, a fim

de comprovar a importância da pesquisa para a instituição (Apêndice I).

Nestes termos, aquele Departamento emitiu o Parecer Técnico nº 35/2024 afirmando acerca da importância e dando caráter itinerante para o Subcomitê Executivo de Proteção de Dados da PMDF (Anexo I).

No âmbito do Subcomitê Executivo, por intermédio da sua Presidente e Encarregada Setorial, foi dada a autorização para que a pesquisa fosse respondida, nos termos do que consta no despacho de 03 de dezembro de 2024 (Anexo II). Neste ponto, deve ser acrescido que não houve uma resposta por parte do Colegiado, mas de um representante e integrante da Auditoria o que dificulta a análise e deixa impressões de que não existe uma estrutura consolidada sobre a implementação da LGPD na Polícia Militar do Distrito Federal.

Entretanto, mesmo diante desta circunstância, o questionário foi incluído no processo do Sistema Eletrônico de Informações – SEI e disponibilizado para as devidas análises críticas que serão realizadas no tópico seguinte, bem como foi incluída no Anexo.


4

# 4 DIAGNÓSTICO DA SITUAÇÃO ATUAL DA PMDF QUANTO À LGPD

A pesquisa, atendendo-se ao que foi estabelecido na metodologia, buscou encontrar o índice de adequação à LGPD na Polícia Militar do Distrito Federal, a partir das informações exaradas pelo Subcomitê Executivo de Proteção de Dados, num dos níveis fixados pelo TCU, que são: a) inexpressivo; b) inicial; c) intermediário; e d) aprimorado

.

## 4.1 METODOLOGIA DE DIAGNÓSTICO

As técnicas de análise se deram segundo o cálculo do índice de adequação, conforme fórmula do TCU, que possibilitaram uma análise descritiva dos resultados por dimensão, bem como viabilizaram a comparação com outras instituições avaliadas no mesmo Acórdão. Para o cálculo do índice do TCU foram consideradas as respostas enviadas pelo Subcomitê Executivo e seu representante, nos mesmos termos do que aconteceu com os órgãos respondentes na pesquisa original do TCU. A variação se dará para "sim", "parcialmente" e "não", respectivamente (1; 0,5 e 0), sendo que o valor obtido em cada uma das respostas será somado e dividido por 42:

$$indicador = \frac{\sum_{i=1}^{42} notaResposta(i)}{42}$$

Ainda, seguindo o método estabelecido pelo TCU alcançou-se os quatro índices:

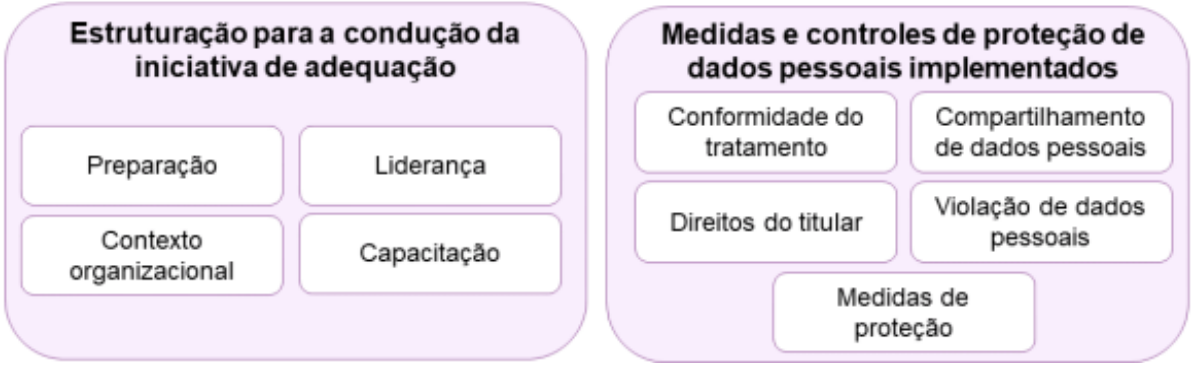
> (...) 293. A partir do cálculo do indicador, foram definidos quatro níveis de adequação à LGPD: 'Inexpressivo' (indicador menor ou igual a 0,15), 'Inicial (indicador maior do que 0,15 e menor ou igual a 0,5), 'Intermediário' (indicador maior do que 0,5 e menor ou igual a 0,8) e 'Aprimorado' (indicador maior do que 0,8). Assim, conforme o valor do indicador obtido, as organizações foram enquadradas em um desses níveis. (BRASIL, 2022)

Esta metodologia aplicada na pesquisa e teve o condão de apontar o nível de adequação em que se encontra a Polícia Militar do

Distrito Federal,[30] nos termos do Acórdão n° 1.384/2022, nota-se que o questionário foi dividido em nove dimensões, a seguir: 1. Preparação (3 questões); 2. Contexto organizacional (11 questões); 3. Liderança (13 questões); 4. Capacitação (4 questões); 5. Conformidade do tratamento (8 questões); 6. Direitos do titular (5 questões); 7. Compartilhamento de dados pessoais (5 questões); 8. Violações de dados pessoais (6 questões); e 9. Medidas de proteção (5 questões), conforme a figura abaixo:

**Figura 3 –** dimensões do questionário

***Figura 1** - Dimensões do questionário*




Fonte: TCU (2022)

De igual forma, menciona-se que o método empregado pela Corte de Contas da União foi o de autoavaliação da instituição, conforme descrito abaixo:

> 19. O método utilizado para avaliar as organizações foi o de autoavaliação de controles (do inglês Control Self-Assessment – CSA), por meio do qual foi disponibilizado um questionário eletrônico para que os gestores preenchessem as respostas que melhor refletiam a situação das respectivas organizações com relação aos controles relacionados à LGPD. Além de permitir que as organizações verificassem quais controles associados à LGPD foram implementados, as questões também podem ser utilizadas como referência para a condução de futuras iniciativas de adequação.

[30] Assim dispõe: "SUMÁRIO: AUDITORIA. DIAGNÓSTICO DO GRAU DE IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS NA ADMINISTRAÇÃO PÚBLICA FEDERAL. 382 ORGANIZAÇÕES AVALIADAS. NOVE DIMENSÕES: **PREPARAÇÃO, CONTEXTO ORGANIZACIONAL, LIDERANÇA, CAPACITAÇÃO, CONFORMIDADE DO TRATAMENTO, DIREITOS DO TITULAR, COMPARTILHAMENTO DE DADOS PESSOAIS, VIOLAÇÃO DE DADOS PESSOAIS E MEDIDAS DE PROTEÇÃO**. MAIOR PARTE DAS ORGANIZAÇÕES EM ESTÁGIO INICIAL. ESTRUTURA DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. RECOMENDAÇÕES". (BRASIL, 2022) (grifo nosso)

> 20. As perguntas do questionário tiveram como referência a própria LGPD e a norma técnica ABNT NBR ISO/IEC 27701:2019 (extensão da ABNT NBR ISO/IEC 27.001 e da ABNT NBR ISO/IEC 27.002 para gestão da privacidade da informação – Requisitos e diretrizes). Também foram consultadas boas práticas oriundas de materiais disponibilizados pelo ICO (Information Commissioner's Office) e pelo CNIL (Commission Nationale de l'Informatique et des Libertés), que são organizações equivalentes à ANPD, a primeira do Reino Unido e a segunda da França, e que são reconhecidas por conduzirem bons trabalhos relacionados à proteção de dados pessoais no continente europeu. (BRASIL, 2022)

Em complemento, para a obtenção do índice de adequação deve-se observar que a coluna dos valores da organização foi preenchida levando-se em conta o somatório de cada pontuação por questão (1, 0,5 e 0), divididas pela quantidade de questões utilizadas em cada dimensão. O valor de adequação foi encontrado somando-se os valores parciais e dividindo-se por 09 (nove), que é a quantidade total de dimensões do questionário.

## 4.2 ANÁLISE DOCUMENTAL: ARTEFATOS INSTITUCIONAIS DA PMDF

Os documentos descritos pelo Subcomitê Executivo de Proteção de dados da PMDF não se constituem de normas publicadas ou de medidas administrativas que sirvam para direcionar os integrantes da Corporação ou de seu público externo. Como se observa, são expedientes que reforçam o que já consta na Portaria PMDF n° 1.279/2022, ou solicitam reunião com o Alto Comando, não servindo de norma ou facilitador para os operadores/controladores de dados pessoais. Ademais, serão apresentados na mesma sequência disposta pelo representante do Subcomitê Executivo.

A partir deste momento, serão acrescentados comentários com a necessária visão crítica acerca dos artefatos apresentados pela PMDF. O primeiro deles é o memorando n° 04, de 02 de julho de 2024, destinado ao Centro de Comunicação Social da PMDF para que seja dada publicidade ao que consta no artigo 29[31] da Política de Proteção de Dados Pessoais, constante em Anexo a este trabalho.

[31] Extraído do site https://portal.pm.df.gov.br/wp-content/uploads/2024/11/PORTARIA-No-1279_2022-%E2%80%93-Intranet.pdf. Acessado em 19 de fevereiro de 2025.

Em seu bojo, o supracitado documento reforça que as informações necessárias sejam disponibilizadas no site oficial da Corporação. Entretanto, ao acessar o site https://portal.pm.df.gov.br/ não foi possível visualizar nenhuma referência à LGPD, mas apenas os links para as matérias de saúde, educação e concursos, conforme abaixo:

**Figura 4 –** Imagem do site da PMDF


Fonte: site da PMDF

Apenas quando o usuário desce o cursor e clica no link "transparência" e, posteriormente, em "base jurídica" é que se verifica a menção à Portaria PMDF nº 1.279/2022, sem qualquer outro detalhe ou informação, conforme se verifica abaixo:

**Figura 5 –** imagem do rol de normas constante no site da PMDF

i) Decreto n° 10.443, de 28 de julho de 2020, que dispõe sobre a organização básica da Polícia Militar do Distrito Federal;

j) Portaria PMDF n° 1.279, de 23 de junho de 2022, que aprova a Política de Proteção de Dados Pessoais – PPDP no âmbito do Polícia Militar do Distrito Federal e estabelece a aplicação dos preceitos da Lei federal n° 13.709, de 14 de agosto de 2018, concernente à Lei Geral de Proteção de Dados Pessoais e dá outras providências;

l) Lei Federal nº 14.751, de 12 de dezembro de 2023, que institui a Lei Orgânica Nacional das Polícias Militares e dos Corpos de Bombeiros Militares dos Estados, do Distrito Federal e dos Territórios, nos termos do inciso XXI do caput do art. 22 da Constituição Federal, altera a Lei nº 13.675, de 11 de junho de 2018, e revoga dispositivos do Decreto-Lei nº 667, de 2 de julho de 1969.

Fonte: site da PMDF (2024)

Por seu turno, compulsando o site[32] do Governo do Distrito Federal destinado aos Encarregados Setoriais de Proteção de Dados das Pastas que compõem a administração direta e indireta, nota-se que as informações da PMDF estão desatualizadas, pois a Encarregada setorial da PMDF é a CEL QOPM Jucilene, conforme se observa dos Anexos produzidos pela responsável, e não o CEL QOPM Carlos André:

**Figura 6 –** relação dos nomes dos encarregados setoriais da PMDF

LGPD/DF
LEI GERAL DE PROTEÇÃO DE DADOS

A LGPD ▼ Autoridades ▼ Publicações Legislação

ATENÇÃO

É de responsabilidade do Controlador encaminhar os nomes dos Encarregados Setoriais para publicação no DODF, de acordo com o processo SEI nº 00002-00002617/2021-46.

15 resultados por página

Pesquisar: pmdf

| ORGÃO | ENCARREGADO SETORIAL | MATRICULA | SUPLENTE | MATRICULA | CAIXA SEI |
|---|---|---|---|---|---|
| PMDF | CARLOS ANDRÉ DA SILVA | 50285-5 | LEONARDO SIQUEIRA DOS SANTOS | 50526-9 | |
| E-MAIL | carlos.silva@pmdf.df.gov.br | | leonardo.santos@pmdf.df.gov.br | | |

Mostrando de 1 até 2 de 2 registros (Filtrados de 310 registros) 1

Fonte: site do GDF (2025)

[32] Informações extraídas do site https://lgpd.df.gov.br/tabela-encarregados/. Acessado em 19 de fevereiro de 2025.

Como se percebe, não existe efetividade na apresentação das informações que se referem à Política Pública de Proteção de Dados na PMDF uma vez que se encontram desatualizadas e difíceis de serem visualizadas.

O próximo documento informado pelo representante do Subcomitê Executivo foi o memorando n° 05, de 02 de julho de 2024, que visa dar efetividade ao que dispõe o artigo 41 da Portaria PMDF n° 1279/2022, ou seja, de que haja processo de educação continuada sobre LGPD na Corporação que vem a atender aos princípios da LGPD.

Para esta demanda, este pesquisador não teve acesso ao documento que incorporou a matéria de proteção de dados aos cursos e especializações, apesar deste pesquisador ter sido convidado para ministrar palestra para o Curso de Altos Estudos – CAE no dia 09 de janeiro de 2025, conforme QTS n° 14 (de 06 a 10 de janeiro).

O memorando n° 06, de 04 de julho de 2024, solicita reunião para estabelecer Grupo de Trabalho ou Comissão para estudar a possibilidade de alterações na Portaria n° 1.279/2022, entretanto não se tem informações sobre o seu andamento ou resultados.

O memorando n° 11, de 22 de julho de 2024, trata de solicitação de reunião do Subcomitê Executivo com o Comitê Gestor de Proteção de Dados Pessoais que, pela Portaria[33] é o Alto Comando da PMDF, nos termos do que consta no artigo 12.

Quanto ao deslinde desta reunião, este pesquisador não sabe informar o que foi resolvido e quais providências foram ajustadas. Já o memorando circular n° 1, de 27 de novembro de 2024, descreve a necessidade de que seja dada publicidade das responsabilidades dos operadores internos da PMDF, bem como a necessidade de informar ao Encarregado Setorial sobre qualquer incidente de segurança.

Por fim, o memorando circular n° 2, de 27 de novembro de 2024, descreve a necessidade de elaborar e manter atualizado o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) e solicita que cada unidade encaminhe para o Subcomitê Executivo de Proteção de Dados Pessoais. Quanto às respostas, este pesquisador não obteve informações sobre os encaminhamentos ou seus desenvolvimentos,

[33] Extraída do site https://portal.pm.df.gov.br/wp-content/uploads/2024/11/PORTARIA-No-1279_2022-%E2%80%93-Intranet.pdf. Acessado em 19 de fevereiro de 2025.

nem tampouco quais foram as orientações para a confecção dos documentos solicitados.

Nota-se que, apesar da Política de Proteção de Dados da PMDF ter sido materializada em 2022, não houve uma produção de artefatos por parte do Colegiado que direcionasse a atuação dos integrantes da corporação. Desta forma, os documentos somente foram produzidos no ano de 2024 e de forma apenas que reiterasse o que já existe da Portaria interna ou que sugerisse reunião com o Alto Comando.

## 4.3 AVALIAÇÃO DIMENSIONAL COM BASE NO QUESTIONÁRIO DO TCU

Neste tópico, busca-se o quadro atual da proteção de dados pessoais na Polícia Militar do Distrito Federal – PMDF, utilizando-se a metodologia empregada pelo Tribunal de Contas da União – TCU, ou seja, do total de 60 (sessenta) questões apenas foram qualificadas e pontuadas um subgrupo de 42 (quarenta e duas), divididas em dois vetores: "Estruturação para condução da iniciativa de adequação" e "Medidas e controles de proteção de dados pessoais implementados". Cada vetor foi divido em dimensões num total de 09 (nove).

A fim de tornar mais didática a apresentação das questões pontuadas pelo TCU, apresenta-se o seguinte quadro, demonstrando as dimensões, as questões que foram utilizadas para comporem o índice e a relação entre o total pelo quantitativo utilizado:

**Tabela 2 – descrição das questões utilizadas para o cálculo do índice**

| Dimensões | Questões utilizadas | Utilizadas/total de questões objetivas |
|---|---|---|
| Preparação | 2.1 e 2.2 | 2/2 |
| Contexto organizacional | 3.1; 3.2; 3.3; 3.4; 3.5; 3.5.1; 3.6; 3.6.1 e 3.7 | 9/11 |
| Liderança | 4.1; 4.2; 4.2.1; 4.2.1.1; 4.2.1.2; 4.3; 4.4; 4.4.1; 4.4.3 | 9/10 |
| Capacitação | 5.1; 5.1.1 e 5.2 | 3/3 |

| | | |
|---|---|---|
| Conformidade de tratamento | 6.1; 6.1.1; 6.1.2; 6.2; 6.3 | 5/7 |
| Direitos dos titulares | 7.1; 7.1.1 e 7.2 | 3/3 |
| Compartilhamento de dados pessoais | 8.1 | 1/5 |
| Violação de dados pessoais | 9.1; 9.2; 9.3; 9.4 e 9.5 | 5/5 |
| Medidas de proteção | 10.1; 10.2; 10.3; 10.4 e 10.5 | 5/5 |
| Total | ---------- | 42/51 |

Fonte: confeccionado pelo autor (2025)

No questionário original (Anexo), aplicado pelo TCU, existem 61 (sessenta e uma) questões, contando com a identificação do respondente, para o preenchimento pelo respondente.

Com o escopo de destacar as dimensões, foi atribuída a cor vermelha para aquelas em que o TCU valorou na sua integralidade, ou seja, utilizou totalidade das questões. Na cor amarela, destacaram-se as dimensões que o TCU se utilizou de uma gradação, ou seja, deixou de considerar algumas questões. Por fim, a cor verde foi utilizada para destacar a dimensão em que a questão utilizada foi apenas uma, de um total de 05 (cinco).

Entretanto, para os fins desta pesquisa, e por não pontuarem para a obtenção do índice, não foram incluídas as perguntas que serviam para avaliar o conteúdo dos programas ou instrumentos da organização, constantes nas questões de números: 1.1 (nome, e-mail, telefone e cargo/função); 2.2.1 (anexe do plano de ação, plano de projeto ou documento similar que foi elaborado pela organização); 4.1.1 (anexe a Política de Segurança da Informação (ou instrumento similar) da organização; 4.2.2 (anexe a Política de Classificação da Informação (ou instrumento similar) da organização; 4.3.1 (anexe a Política de Proteção de Dados Pessoais (ou documento similar) da organização; 5.1.2 (anexe o Plano de Capacitação (ou instrumento similar) da organização; 6.3.1 (anexe o arquivo que representa o registro das atividades de tratamento de dados pessoais (e.g: inventário)); 7.1.1.1 (favor informar o endereço da internet (URL) onde a política está publicada; 7.1.2 (anexe a Política de Privacidade (ou instrumento similar) da organização; 9.1.1 (anexe o plano de respostas a incidentes (ou documento similar) da organização.

Apresentadas estas condições, passa-se à descrição dos valores apresentados pelo representante do Subcomitê Executivo e dispostos no Anexo deste trabalho.

### 4.3.1 ESTRUTURAÇÃO PARA A CONDUÇÃO DA INICIATIVA DE ADEQUAÇÃO

Neste subtópico serão apresentados os valores respondidos pela PMDF, separados por dimensões, sendo que os números da PMDF inferiores aos valores médios (TCU-2022) foram destacados na cor vermelha.

#### 4.3.1.1 PREPARAÇÃO

O questionário, idêntico ao utilizado pelo TCU, inicia com o tópico "Preparação" e, assim, apresenta o tema ao respondente:

> Antes de iniciar o processo de adequação à LGPD, a organização deve adotar medidas para construir um ambiente propício para o sucesso da iniciativa. As questões desta seção abordam aspectos relacionados à identificação e ao planejamento das medidas necessárias à adequação. (BRASIL, 2022)

**Tabela 3 – preparação para adequação à LGPD**

| Preparação para adequação à LGPD | Valores da PMDF | Valores médios obtidos pelo TCU |
|---|---|---|
| Questões | | |
| **2.1 A organização conduziu iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD?** | 1,00 | 0,67 |
| **2.2 A organização elaborou plano de ação, plano de projeto ou documento similar para direcionar a iniciativa de adequação à LGPD?** | 1,00 | 0,51 |

Fonte: elaboração própria (2024)

Nesta dimensão a Corporação informa que foram tomadas medidas para planejar a adequação e que confeccionou o documento necessário para direcionar a conformidade com a LGPD, obtendo valores bem acima da média. Nota-se que está sendo referenciada a

Portaria PMDF n° 1.279/2022 que se encontra publicada no site da Corporação, mas não foi encaminhado qualquer documento que informasse sobre um plano de ação para a sua implementação.

### 4.3.1.2 CONTEXTO ORGANIZACIONAL

A terceira parte do questionário versa sobre o "Contexto organizacional", que assim apresenta ao respondente:

> Para alcançar os resultados pretendidos pela iniciativa de adequação à LGPD, a organização deve avaliar questões internas e externas que são relevantes para atingir os objetivos. As questões desta seção abordam aspectos relacionados à identificação de normativos correlatos à proteção de dados pessoais que devem ser respeitados pela organização, à identificação das partes interessadas e à análise dos dados pessoais tratados pela organização e dos processos organizacionais que tratam esses dados. (BRASIL, 2022)

**Tabela 4 – contexto organizacional**

| Contexto organizacional | Valores da PMDF | Valores médios obtidos pelo TCU |
|---|---|---|
| Questões | | |
| **3.1 A organização conduziu iniciativa para identificar outros normativos, além da LGPD, que abrangem comandos relacionados à proteção de dados pessoais e que também devem ser respeitados?** | 1,00 | 0,76 |
| **3.2 A organização identificou as categorias de titulares de dados pessoais com os quais se relaciona?** | 0,50 | 0,46 |
| **3.3 A organização conduziu iniciativa para identificar os operadores que realizam tratamento de dados pessoais em seu nome?** | 1,00 | 0,42 |
| **3.4 A organização avaliou se há tratamento de dados que envolva controlador conjunto?** | 0,00 | 0,30 |
| **3.5 A organização identificou os processos de negócio que realizam tratamento de dados pessoais?** | 0,00 | 0,39 |

| | | |
|---|---|---|
| **3.5.1 A organização identificou quem são os responsáveis pelos processos de negócio que realizam tratamento de dados pessoais e que já foram identificados?** | 0,00 | 0,38 |
| **3.6 A organização identificou quais são os dados pessoais tratados por ela?** | 0,50 | 0,43 |
| **3.6.1 A organização identificou os locais onde os dados pessoais identificados são armazenados?** | 0,00 | 0,44 |
| **3.7 A organização avaliou os riscos dos processos de tratamento de dados pessoais que foram identificados?** | 0,00 | 0,20 |

Fonte: elaboração própria (2024)

Nos quesitos 3.1 (identificação de outros normativos), 3.3 (iniciativa para identificar operadores) a PMDF respondeu “sim”. Para o quesito 3.2 (categorias de titulares) e 3.6 (identificou quais são os dados tratados) afirmou que “parcialmente”. E quanto aos 3.4 (controlador conjunto), 3.5 (processos de negócios), 3.5.1 (responsáveis pelos processos de negócios), 3.6.1 (locais onde os dados são armazenados) e 3.7 (riscos dos processos de tratamento) a PMDF respondeu que “não”.

Apesar de ter afirmado “sim” tais medidas não foram encontradas no site ou mencionadas na resposta que foi enviada a este pesquisador. Desta forma, caso existam, sugere-se a inclusão no site da Corporação.

### 4.3.1.3 LIDERANÇA

O quarto tópico trata da “Liderança”, sendo observado o seguinte:

> A alta direção deve demonstrar liderança e comprometimento com a iniciativa de adequação à LGPD. A existência e a elaboração de políticas relacionadas à proteção de dados pessoais e a nomeação de um encarregado que tenha autonomia para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) são fundamentais para o processo de adequação.
> As questões desta seção são relacionadas à nomeação do encarregado e à existência de políticas que buscam assegurar a segurança das informações e a proteção dos dados pessoais. (BRASIL, 2022)

| Tabela 5 – liderança | | |
|---|---|---|
| **Liderança** | **Valores da PMDF** | **Valores médios obtidos pelo TCU** |
| Questões | | |
| **4.1 A organização possui Política de Segurança da Informação ou instrumento similar?** | 0,00 | 0,76 |
| **4.2 A organização possui Política de Classificação da Informação ou instrumento similar?** | 0,00 | 0,35 |
| **4.2.1 A Política de Classificação da Informação (ou instrumento similar) abrange diretrizes para a classificação de dados pessoais?** | 0,00 | 0,20 |
| **4.2.1.1 A Política de Classificação da Informação abrange diretrizes para identificar dados pessoais sensíveis e relacionados a crianças e adolescentes?** | 0,00 | 0,04 |
| **4.2.1.2 A Política de Classificação da Informação (ou instrumento similar) abrange diretrizes para identificar dados pessoais de crianças e de adolescentes?** | 0,00 | 0,02 |
| **4.3 A organização possui Política de Proteção de Dados Pessoais?** | 1,00 | 0,18 |
| **4.4 A organização nomeou o encarregado pelo tratamento de dados pessoais?** | 1,00 | 0,69 |
| **4.4.1 A nomeação do encarregado foi publicada em veículo de comunicação oficial?** | 1,00 | 0,52 |
| **4.4.3 A identidade e as informações de contato do encarregado foram divulgadas na internet?** | 1,00 | 0,46 |

Fonte: elaboração própria (2024)

No que tange a dimensão de liderança, a PMDF respondeu aos quesitos 4.3 (possui política de proteção de dados), apesar de responder duas vezes (“sim” e “não”) será considerado como “sim” uma vez que a Política existe e encontra-se devidamente públicada, 4.4 (nomeou o encarregado), 4.4.1 (nomeação foi publicada), 4.4.3 (informações de contato na internet) como “sim”. Para os quesitos 4.1 (política de segurança da informação), 4.2 (classificação da informação), 4.1.1

(política de classificação), 4.2.1.1 (identificar dados sensíveis) a PMDF respondeu que “não”.

Apesar das respostas afirmarem “sim”, percebe-se que os dados do Encarregado Setorial se encontram desatualizados no site do GDF, como visto em tópico anterior, o que fragiliza o valor atribuído no questionário. Em assim sendo, recomenda-se a atualização urgente para não incorrer em sanções pela ANPD.

De igual forma, quanto à classificação da informação ou instrumento similar, este pesquisador encontrou no site da PMDF o link para “informações classificadas e desclassificadas”[34]. Nele é possível encontrar o fundamento legal, ou seja, a lei distrital n° 4.990, de 12 de dezembro de 2012, e o decreto distrital n° 34.276/2013 e o decreto distrital n° 35.832/2014, bem como relações de documentos classificados pela PMDF nos anos de 2020 a 2023.

Compulsando o teor do decreto n° 34.276/2013 nota-se o Capítulo VI “Das Informações Pessoais”, dispõe sobre os procedimentos inerentes às informações pessoais relativas à vida privada, honra detidas pelo poder público. Desta forma, faz-se necessário que a PMDF regule internamente o acesso à informação aos documentos classificados e publique em seu site a fim de promover a devida transparência dos atos públicos.

### 4.3.1.4 CAPACITAÇÃO

O quinto tópico trata da capacitação da organização respondente, entendido pelo TCU da seguinte forma:

> A organização deve conduzir iniciativas para conscientizar e capacitar os colaboradores em proteção de dados pessoais. A conscientização é importante para que os colaboradores conheçam as políticas organizacionais relacionadas à proteção de dados pessoais e para que reconheçam como suas ações são importantes para a preservação da privacidade dos titulares.
> As ações de capacitação devem considerar diferentes níveis de envolvimento dos colaboradores no tema, de forma que aqueles que ocupam funções com responsabilidades essenciais relacionadas à proteção de dados pessoais recebam treinamento diferenciado, além do nível básico fornecido aos

[34] Disponível no site https://portal.pm.df.gov.br/informacoes-classificadas-e-desclassificadas/. Acessado em 18 de março de 2025.

demais. Nesta seção são abordadas questões para avaliar o planejamento e a realização de ações de conscientização e de capacitação. (BRASIL, 2022)

| Tabela 6 – capacitação | | |
|---|---|---|
| **Capacitação** | **Valores da PMDF** | **Valores médios obtidos pelo TCU** |
| Questões | | |
| **5.1 A organização possui Plano de Capacitação que abrange treinamento e conscientização dos seus colaboradores em proteção de dados pessoais?** | 0,00 | 0,29 |
| **5.1.1 O Plano de Capacitação considera que pessoas que exercem funções com responsabilidades essenciais relacionadas à proteção de dados pessoais devem receber treinamento diferenciado?** | 0,00 | 0,15 |
| **5.2 Colaboradores da organização que estão diretamente envolvidos em atividades que realizam tratamento de dados pessoais receberam treinamentos relacionados ao tema?** | 0,00 | 0,37 |

Fonte: elaboração própria (2024)

Quanto à dimensão capacitação a PMDF respondeu “não” para todas as questões, permanecendo abaixo da média. Como mencionado, somente um dos artefatos apontava para a inclusão do tema proteção de dados pessoais nos currículos de cursos, mas não se tem uma resposta sobre a sua efetividade. Desta forma, convém que a PMDF elabore um cronograma de capacitação a fim de adequação na LGPD.

## 4.3.2 MEDIDAS E CONTROLES DE PROTEÇÃO DE DADOS PESSOAIS IMPLEMENTADOS

### 4.3.2.1 CONFORMIDADE DO TRATAMENTO

O sexto tópico do questionário trata da “Conformidade do tratamento, sendo assim apresentado:

A organização deve ser capaz de provar que os tratamentos de dados pessoais que realiza são lícitos. Para isso é fundamental demonstrar que os princípios estabelecidos pela LGPD são seguidos e que os tratamentos são fundamentados em, ao menos, uma das bases legais descritas na legislação.
Nesta seção são abordadas questões para avaliar se os tratamentos estão em conformidade com alguns dos princípios e se estão fundamentados em alguma base legal. Também será avaliado se a organização possui um registro para documentar detalhes das atividades de tratamento. (BRASIL, 2022)

| Tabela 7 – conformidade de tratamento | | |
|---|---|---|
| **Conformidade de tratamento** | **Valores da PMDF** | **Valores médios obtidos pelo TCU** |
| Questões | | |
| **6.1 A organização identificou e documentou as finalidades das atividades de tratamento de dados pessoais?** | 0,50 | 0,29 |
| **6.1.1 A organização avaliou se coleta apenas os dados estritamente necessários para cumprir com as finalidades de tratamento de dados pessoais que foram identificadas?** | 0,00 | 0,23 |
| **6.1.2 A organização avaliou se os dados pessoais são retidos (armazenados) durante o tempo estritamente necessário para cumprir com as finalidades de tratamento de dados pessoais que foram identificadas?** | 0,00 | 0,18 |
| **6.2 A organização identificou e documentou as bases legais que fundamentam as atividades de tratamento de dados pessoais?** | 0,50 | 0,35 |
| **6.3 Há um registro (e.g.: inventário) instituído para consolidar informações relacionadas às características das atividades de tratamento de dados pessoais?** | 0,00 | 0,18 |

Fonte: elaboração própria (2024)

Quanto a esta dimensão conformidade de tratamento, a PMDF nos quesitos 6.1 (identificou e documentou as finalidades) e 6.2 (identificou e documentou as bases legais) afirmou que “parcialmente”. Quanto aos quesitos 6.1.1 (avaliou se coleta apenas o estritamente

necessário), 6.1.2 (armazenamento pelo tempo necessário), 6.3 (inventário) respondeu que “não”.

As respostas como “parcialmente” realizado não foram mencionadas como artefatos, o que podem sugerir que estão em fase de confecção ou de encaminhamento. Ressalta-se que consta um memorando aos departamentos para que elaborem os Relatórios de Impactos de Proteção de Dados, mas este pesquisador não obteve outras informações, e nem se houve orientação, por parte do Subcomitê Executivo, para a confeccção dos documentos solicitados.

### 4.3.2.2 DIREITOS DO TITULAR

O sétimo tópico versa sobre os “Direitos do titular” e tem a seguinte menção inicial:

> A organização deve assegurar que os titulares tenham acesso a informações relacionadas ao tratamento de seus dados pessoais. Para isso, a organização deve publicar, de maneira clara e concisa, informações relativas ao tratamento de dados pessoais.
> A organização também deve estar preparada para atender todos os direitos dos titulares que são elencados na LGPD. Nesta seção são abordadas questões relacionadas à elaboração da política de privacidade e ao atendimento dos direitos dos titulares. (BRASIL, 2022)

**Tabela 8 – direitos do titular**

| Direitos do titular | Valores da PMDF | Valores médios obtidos pelo TCU |
|---|---|---|
| Questões | | |
| **7.1 A organização possui Política de Privacidade?** | 1,00 | 0,25 |
| **7.1.1 A Política de Privacidade está publicada na internet?** | 0,00 | 0,20 |
| **7.2 Foram implementados mecanismos para atender os direitos dos titulares elencados no art. 18 da LGPD e aplicáveis à organização?** | 0,50 | 0,30 |

Fonte: elaboração própria (2024)

Quanto aos direitos dos titulares a PMDF respondeu nos quesitos 7.1 (possuir política de privacidade) “sim”. Para 7.2 (implementação de mecanismos para atender aos titulares) respondeu que “parcialmente”. Para 7.1.1 (publicação da política de privacidade) respondeu que “não”.

Percebe-se que houve menção à existência de uma Política de Privacidade mas que não se encontra publicada, impedindo que a população acesse tal documentos, o que vai de encontro à LGPD. Ademais, apesar de ser mencionado, o atendimento dos direitos dos titulares, esse não foi apresentado.

### 4.3.2.3 COMPARTILHAMENTO DE DADOS PESSOAIS

O oitavo tópico trata do “Compartilhamento de dados pessoais”, sendo assim iniciado:

> A organização deve documentar detalhes relacionados ao compartilhamento de dados pessoais com terceiros. A realização de compartilhamento demanda a adoção de controles adequados para mitigar riscos que possam comprometer a proteção dos dados pessoais.
> Diante disso, a LGPD defende que as precauções a serem adotadas entre as partes envolvidas no compartilhamento sejam formalizadas em contrato e que cuidados especiais devem ser adotados no caso de transferência internacional desses dados. Nesta seção são abordadas questões relacionadas à identificação dos dados pessoais que são compartilhados, ao registro de eventos correlatos aos compartilhamentos e à transferência internacional de dados pessoais. (BRASIL, 2022)

**Tabela 9 – compartilhamento de dados pessoais**

| Compartilhamento de dados pessoais | Valores da PMDF | Valores médios obtidos pelo TCU |
|---|---|---|
| Questões | | |
| **8.1 A organização identificou os dados pessoais são compartilhados com terceiros?** | 0,00 | 0,42 |

Fonte: elaboração própria (2024)

Quanto à dimensão de compartilhamento de dados pessoais a PMDF respondeu que “não”, permanecendo abaixo da média obtida

pelo TCU. Diante desta informação, faz-se necessário que a Corporação realize, pelo menos minimamente, de que forma os dados são compartilhados bem como o seu fundamento legal.

### 4.3.2.4 VIOLAÇÃO DE DADOS PESSOAIS

O tópico nove foi destinado para as "Violações de dados pessoais", sendo assim iniciado:

> A organização deve gerenciar incidentes de segurança da informação que envolvem a violação de dados pessoais. Nesta seção são abordadas questões relacionadas à identificação, ao registro e ao tratamento de incidentes de violação de dados pessoais.
> Também será avaliado se a organização dispõe de mecanismo para notificar a Autoridade Nacional de Proteção de Dados e os titulares nos casos de incidentes que possam acarretar risco ou dano relevante aos titulares. (BRASIL, 2022)

**Tabela 10 – violação de dados pessoais**

| Violação de dados pessoais | Valores da PMDF | Valores médios obtidos pelo TCU |
|---|---|---|
| Questões | | |
| **9.1 A organização possui Plano de Resposta a Incidentes que abrange o tratamento de incidentes que envolvem violação de dados pessoais?** | 0,00 | 0,16 |
| **9.2 A organização possui sistema para o registro de incidentes de segurança da informação que envolvem violação de dados pessoais?** | 0,00 | 0,28 |
| **9.3 A organização possui sistema para registro das ações adotadas para solucionar incidentes de segurança da informação que envolvem violação de dados pessoais?** | 0,00 | 0,25 |
| **9.4 A organização monitora proativamente a ocorrência de eventos que podem ser associados à violação de dados pessoais?** | 0,00 | 0,34 |
| **9.5 A organização estabeleceu procedimentos para comunicar à ANPD e ao titular a ocorrência** | 0,50 | 0,12 |

| | | |
|---|---|---|
| **de incidente de segurança que possa acarretar risco ou dano relevante aos titulares?** | | |

Fonte: elaboração própria (2024)

Nesta dimensão, a PMDF informou “parcialmente” no quesito 9.5 (estabeleceu procedimentos para comunicar à ANPD e ao titular) mas não consta no rol de artefatos confeccionados pelo Subcomitê. Quanto aos demais quesitos a PMDF respondeu “não”, ficando bem abaixo da média. Ademais, não foi encontrada a forma como se dará esta comunicação com a ANPD.

Acredita-se que a simples menção de que a PMDF irá comunicar com o Encarregado Governamental tenha sido o suficiente para o atendimento parcial da questão “9.5” e, por isso, atribuiu valor parcial.

### 4.3.2.5 MEDIDAS DE PROTEÇÃO

O tópico dez versa sobre as “Medidas de proteção”, sendo assim capitaneado:

> A organização deve adotar medidas de segurança, técnicas e administrativas, para proteger os dados pessoais. Para isso, convém que sejam implementados controles capazes de mitigar riscos que possam resultar em violação da privacidade. Nesta seção serão abordadas questões relacionadas à implementação de controles para restringir e rastrear o acesso a dados pessoais e à avaliação de impacto sobre a proteção de dados pessoais. (BRASIL, 2022)

| Tabela 11 – medidas de proteção | | |
|---|---|---|
| **Medidas de proteção** | **Valores da PMDF** | **Valores médios obtidos pelo TCU** |
| Questões | | |
| **10.1 A organização é capaz de comprovar que adotou medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais?** | 0,00 | 0,46 |
| **10.2 A organização implementou processo para registro, cancelamento e provisionamento de** | 0,50 | 0,34 |

| | | |
|---|---|---|
| **usuários em sistemas que realizam tratamento de dados pessoais?** | | |
| **10.3 A organização registra eventos das atividades de tratamento de dados pessoais?** | 0,50 | 0,34 |
| **10.4 A organização utiliza criptografia para proteger os dados pessoais?** | 0,00 | 0,33 |
| **10.5 A organização adotou medidas para assegurar que processos e sistemas sejam projetados, desde a concepção, em conformidade com a LGPD (Privacy by Design e Privacy by Default)?** | 0,00 | 0,15 |

Fonte: elaboração própria (2024)

Quanto às medidas de proteção a PMDF respondeu que "parcialmente" aos quesitos 10.2 (implementação de processo para registro, cancelamento e provisionamento) e 10.3 (registra eventos das atividades). Já para os demais quesitos a resposta foi "não".

Apesar do que consta nesta dimensão, não foi mencionado nenhum artefato que esteja vinculado aos quesitos expostos.

## 4.4 SÍNTESE DO DIAGNÓSTICO

Para encontrar o índice de adequação à LGPD da Polícia Militar do Distrito Federal foi necessário somar as pontuações correspondentes a (1; 0,5 e 0) para as 42 (quarenta e duas) questões do questionário. Assim, para ser mais didático, pode-se resumir da seguinte forma:

**Tabela 12 – índice de adequação à LGPD da PMDF**

| Dimensões do questionário | Valores da organização obtido pelo pesquisador (2024) | Valores médios obtidos pelo TCU (2022) |
|---|---|---|
| Estruturação para condução da iniciativa de adequação | | |
| Preparação | 1,00 | 0,59 |
| Contexto organizacional | 0,33 | 0,42 |
| Liderança | 0,44 | 0,36 |

| | | |
|---|---|---|
| Capacitação | 0,00 | 0,27 |
| Medidas e controles de proteção de dados pessoais implementados | | |
| Conformidade de tratamento | 0,20 | 0,24 |
| Direitos do titular | 0,50 | 0,25 |
| Compartilhamento de dados pessoais | 0,50 | 0,42 |
| Violação de dados pessoais | 0,10 | 0,23 |
| Medidas de proteção | 0,20 | 0,32 |
| **Indicador de adequação à LGPD da PMDF** | 0,36 | 0,35 |

Fonte: elaboração própria (2024)

Assim, pode-se verificar que o indicador de adequação à LGPD da PMDF é de **0,36** que equivale ao nível "Inicial", acima do indicador médio (0,35) apontado pelo TCU em 2022. Entretanto, deve-se levar em conta que no momento em que o questionário foi aplicado (2021) não havia ainda a Portaria que criava a Política de Proteção de Dados Pessoais na PMDF (2022) o que, inevitavelmente, diminuiria o índice de adequação à LGPD.

À título de comparação, acrescenta-se que o Corpo de Bombeiros Militar do Distrito Federal – CBMDF, com as mesmas características legislativas da PMDF, foi submetido à pesquisa, no bojo do Acórdão n° 1.384/2022 TCU, e recebeu valor "0,25" para o indicador de adequação, correspondendo ao nível "Inicial"[35].

De igual importância, e de maneira comparativa, na mesma auditoria realizada pelo TCU, o Serviço Federal de Processamento de Dados – SERPRO obteve o valor "0,85" para o indicador de adequação, o que corresponde ao nível "Aprimorado"[36].

Por fim, verifica-se que os valores alcançados pela PMDF denotam que a Política de Proteção de Dados precisa ser acompanhada pelo Alto Comando a fim de que possa ser eficiente.

[35] Extraído do site https://www.cbm.df.gov.br/lai/sem-categoria/relatorios-auditoriais-orgaos-de-controle-e-fiscalizacao/. Acessado em 10 de junho de 2024.
[36] Extraído do site https://www.serpro.gov.br/privacidade-protecao-dados/OFCIO_02952022TCUSefti.pdf. Acessado em 10 de junho de 2024.

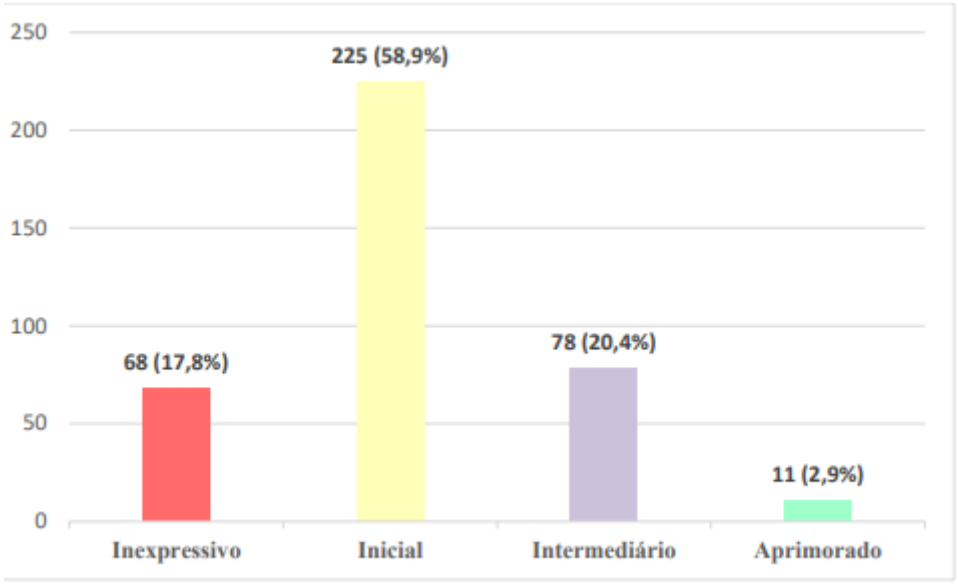
| Tabela 13 – comparativo entre PMDF, CBMDF e SERPRO | | | | |
|---|---|---|---|---|
| **Dimensões do questionário** | **Valores da PMDF no ano de 2024 obtidos pelo pesquisador** | **Valores do CBMDF no ano de 2021** | **Valores do SERPRO no ano de 2021** | **Valores médios obtidos pelo TCU no ano de 2021** |
| Estruturação para condução da iniciativa de adequação | | | | |
| Preparação | 1,00 | 0,25 | 1,00 | 0,59 |
| Contexto organizacional | 0,33 | 0,00 | 0,72 | 0,42 |
| Liderança | 0,44 | 0,00 | 1,00 | 0,36 |
| Capacitação | 0,00 | 0,33 | 1,00 | 0,27 |
| Medidas e controles de proteção de dados pessoais implementados | | | | |
| Conformidade de tratamento | 0,20 | 0,00 | 0,60 | 0,24 |
| Direitos do titular | 0,50 | 0,00 | 1,00 | 0,25 |
| Compartilhamento de dados pessoais | 0,50 | 1,00 | 1,00 | 0,42 |
| Violação de dados pessoais | 0,10 | 0,40 | 0,60 | 0,23 |
| Medidas de proteção | 0,20 | 0,30 | 0,70 | 0,32 |
| **Indicador de adequação à LGPD** | 0,36 | 0,25 | 0,85 | 0,35 |

Fonte: elaboração própria (2024)

Passando-se para algumas considerações acerca do que foi obtido, pode-se, de pronto, concluir que os resultados obtidos pela PMDF estão atualizados, no ano de 2024, enquanto que os demais órgãos tiveram seus dados coletados em 2021, ano em que a auditoria foi realizada, sendo que naquele momento foram estabelecidos quatro níveis de adequação à LGPD: “Inexpressivo” (indicador menor ou igual a 0,15), “Inicial” (indicador maior do que 0,15 e menor ou igual a 0,5),

"Intermediário" (indicador maior do que 0,5 e menor ou igual a 0,8) e "Aprimorado" (indicador maior do que 0,8), conforme a figura abaixo:

**Figura 7 –** níveis de adequação à LGPD pelo TCU




Fonte: TCU (2022)

Pelos valores obtidos em 2024, a PMDF está no nível "inicial", assim como o CBMDF no ano de 2021, e o SERPRO no "aprimorado" no ano de 2021. Neste sentido, por si só, pode-se afirmar que a PMDF teve mais tempo, ao longo destes dois anos, para implementar a LGPD. Entretanto, pelos valores obtidos não é o que se verifica, principalmente no que tange à capacitação, com valor 0,00, enquanto que o CBMDF considerou valor 0,33 e o SERPRO 1,00. Ademais, é possível que as organizações avaliadas em 2021 estejam com suas políticas de proteção de dados bem mais adiantadas do que a auditoria apurou naquele período.

Quanto aos valores obtidos pelo SERPRO estão de acordo com a sua atividade que é a de propor serviços especializados em tecnologia para a iniciativa privada e administração pública.

Em sede de conclusão deste tópico, deve-se ter em mente que a PMDF, apesar de encontrar-se no nível "inicial" está aquém do esperado em razão das oportunidades de evoluir com a Política de Proteção de Dados, com a possibilidade realizar cursos na área e com o próprio resultado da Auditoria divulgada pelo TCU. Neste sentido, com base no que foi respondido e nos artefatos apresentados, seria provável que em

2021 a PMDF estivesse no nível “inexpressivo”, pela ausência da própria Política de Proteção.


5

# 5 DISCUSSÃO DOS RESULTADOS E PROPOSTAS DE APRIMORAMENTO

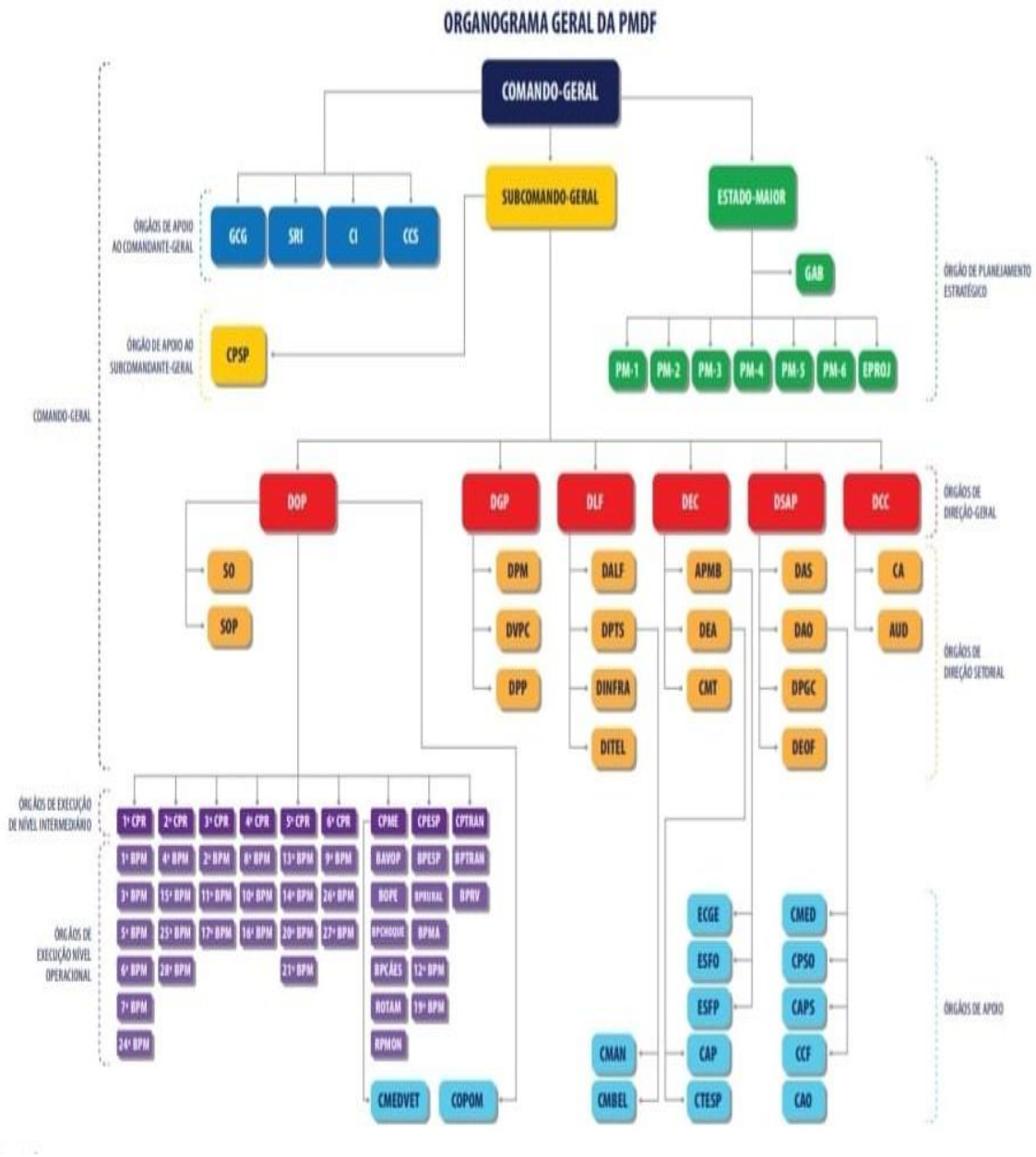
## 5.1 INTERPRETAÇÃO CRÍTICA DOS RESULTADOS

Como verificado, a PMDF encontra-se, atualmente, no nível "inicial" de adequação à LGPD e tal classificação gera preocupações no cenário de proteção de dados. Ressalta-se, mais uma vez, que a auditoria foi realizada em 2021 e divulgada em 2022, impulsionando as entidades avaliadas para uma melhoria de seus índices.

Assim, para este pesquisador, não existe mérito no índice aferido, pois denota que não houve avanço da Política de Proteção de Dados na PMDF. Também, apesar da LGPD dispor, em seu artigo 4°, inciso III, que não se aplica aos fins exclusivamente de segurança pública, existem outras atividades que são realizadas pela PMDF e que sofrem incidência direta da LGPD.

Neste ponto, convém descrever o Decreto Federal n° 10.443/2020 que dispõe expressamente, em rol exaustivo, nos termos do artigo 17, os Departamentos que integram a estrutura da Corporação: I – Departamento de Gestão de Pessoal; II – Departamento de Logística e Finanças; III – Departamento de Educação e Cultura; IV – Departamento de Saúde e Assistência ao Pessoal; V – Departamento de Controle e Correição; e VI – Departamento de Operações, representados na figura abaixo:

**Figura 8 –** organograma geral da PMDF




Fonte: PMDF (2024)

Como se percebe a Administração da PMDF é extremamente complexa e, apesar da enorme diferença entre o efetivo existente e previsto[37], ainda assim exige um esforço de gestão para estar em conformidade com todas as leis e regulamentos que regem a Administração Pública. Especificamente quanto à proteção de dados

[37] Segundo consta na Lei federal nº 12.086/2009, em seu artigo 2º, o efetivo da Corporação "é de 18.673 (dezoito mil e seiscentos e setenta e três) policiais militares". Entretanto, segundo se extrai do Relatório da CPI da CLDF o efetivo atual se aproxima dos dez mil. Disponível no site https://static.poder360.com.br/2023/11/Relatorio-CLDF-29nov2023.pdf. Acessado em 14 de março de 2025.

pessoais, deve-se estabelecer algumas críticas no que tange às suas deficiências.

Na Gestão de Pessoas, com seus dados sensíveis sobre os integrantes e dependentes, faz-se necessário ter precaução na divulgação dos dados pessoais e vazamento para terceiros não autorizados. Também, nos contratos administrativos e processos licitatórios (Departamento de Logística e Finanças) deve-se ter atenção com as informações acerca de pessoas jurídicas e dos colaboradores que as integram.

Nestas pastas, de Gestão de Pessoas e Logística, a Corporação respondeu "0,00" para as questões abaixo (conformidade de tratamento):

> 6.1.1 A organização avaliou se coleta apenas os dados estritamente necessários para cumprir com as finalidades de tratamento de dados pessoais que foram identificadas?
> 6.1.2 A organização avaliou se os dados pessoais são retidos (armazenados) durante o tempo estritamente necessário para cumprir com as finalidades de tratamento de dados pessoais que foram identificadas?
> 6.3 Há um registro (e.g.: inventário) instituído para consolidar informações relacionadas às características das atividades de tratamento de dados pessoais?

Ou seja, nos contratos administrativos, bem como na coleta de informações de pessoas, não existe qualquer mensuração sobre a necessidade dos dados solicitados, gerando um acúmulo de informações e aumento de risco de seu vazamento. Ademais, corre-se sério risco de que exista uma duplicidade de solicitações e guarda de dados em arquivos nos dois departamentos para a realização das atribuições, quando se avaliou com "0,00" para a pergunta: "10.1 A organização é capaz de comprovar que adotou medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais?".

No ensino, com os dados pessoais de jovens e crianças que estudam no Colégio Militar Tiradentes (CMT), bem como os dados dos militares que realizam cursos iniciais e sequenciais de carreira, conforme previsto no decreto distrital n° 37.786, de 21 de novembro de 2016. Esta atividade se torna preocupante, pois a corporação respondeu com nota "0,0" às seguintes perguntas:

> 4.2.1.1 A Política de Classificação da Informação abrange diretrizes para identificar dados pessoais sensíveis e relacionados a crianças e adolescentes?
> 4.2.1.2 A Política de Classificação da Informação (ou instrumento similar) abrange diretrizes para identificar dados pessoais de crianças e de adolescentes?

Seria crucial promover tais medidas a fim de minimizar possíveis ocorrências com os dados tratados, ainda mais que sofre fiscalização direta por parte da ANPD. Neste momento cabe um breve apontamento para tratar de interessante análise voltada ao ensino e os dados pessoais dos estudantes, quando a ANPD se pronunciou quanto à possibilidade do Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira – INEP requerer microdados dos alunos para suas missões de interesse público, dentre eles, o monitoramento do Plano Nacional de Educação (PNE[38]).

Foi no bojo do processo SEI 00261.000730/2022-53[39] que a Autoridade de Proteção de Dados Pessoais confirmou que o INEP tem autorização legal para realizar o tratamento de dados, mas na divulgação dos microdados deve atentar para a LGPD e que não necessariamente deve ser por anonimização. Deve-se, portanto, avaliar os riscos e tomar as seguintes cautelas:

> Após a elaboração do relatório de impacto, deve-se reavaliar os motivos pelos quais concluiu-se pela não divulgação dos microdados dos censos escolares e do Enem, podendo continuar publicando-os caso (i) não tenha sido identificado alto risco para os titulares ou (ii) os riscos identificados tenham sido neutralizados ou adequadamente mitigados com a adoção das salvaguardas apropriadas ao caso. Porém, se houver impacto significativo sobre os direitos dos titulares, deve-se avaliar a amplitude da divulgação ou a aplicação de outras técnicas de anonimização e medidas de mitigação, já

[38] Conforme se extrai do site, tem-se que: "PNE – O Plano Nacional de Educação estabelece 20 metas com o objetivo de orientar, no período de dez anos (contados a partir da sua instituição em 2014), a atuação dos sistemas educacionais do país, do nível básico ao superior. Os objetivos do plano atual (2014-2024) são direcionados à garantia do direito à educação de qualidade, assegurando o acesso e a universalidade do ensino obrigatório, bem como a ampliação das oportunidades educacionais em todos os níveis de ensino. O documento também elenca metas voltadas à redução das desigualdades, à promoção da diversidade, à valorização dos profissionais da educação e à ampliação do investimento em educação". Informação constante no site https://www.gov.br/inep/pt-br/assuntos/noticias/estudos-educacionais/pne-inep-atualiza-painel-de-monitoramento. Acessado em 13 de julho de 2024.

[39] Processo administrativo disponível no site https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_00261-000730_2022_53-nt-46.pdf. Acessado em 13 de julho de 2024.

> mencionadas, para a publicação dos dados. Faz-se necessário, também, verificar a ocorrência de riscos e danos relevantes proveniente da publicação dos microdados em anos anteriores que pudessem justificar a não divulgação ou a sua indisponibilidade. Caso não seja constatado nenhuma ocorrência relevante, os microdados devem ser tornados públicos, após a aplicação das medidas de segurança e de mitigação de risco necessárias, indicadas pelo relatório de impacto à proteção de dados. (BRASIL, 2022, p. 11)

Com isso, torna-se evidente a necessidade de que o Departamento de Educação e Cultura desenvolva procedimentos eficientes para que os dados dos estudantes estejam à salvo de possíveis vazamentos ou que estejam sendo tratados irregularmente.

No que tange a Assistência à Saúde sabe-se que a matéria é de extrema sensibilidade. Com uma carteira com mais de 70.000 vidas, a assistência à saúde da PMDF deve estar voltada para a proteção de dados. Entretanto, preocupa quando a Corporação pontuou com “0,00” às seguintes perguntas:

> 3.7 A organização avaliou os riscos dos processos de tratamento de dados pessoais que foram identificados?
> 5.1 A organização possui Plano de Capacitação que abrange treinamento e conscientização dos seus colaboradores em proteção de dados pessoais?
> 5.1.1 O Plano de Capacitação considera que pessoas que exercem funções com responsabilidades essenciais relacionadas à proteção de dados pessoais devem receber treinamento diferenciado?
> 5.2 Colaboradores da organização que estão diretamente envolvidos em atividades que realizam tratamento de dados pessoais receberam treinamentos relacionados ao tema?
> 6.1.2 A organização avaliou se os dados pessoais são retidos (armazenados) durante o tempo estritamente necessário para cumprir com as finalidades de tratamento de dados pessoais que foram identificadas?
> 6.2 A organização identificou e documentou as bases legais que fundamentam as atividades de tratamento de dados pessoais?
> 6.3 Há um registro (e.g.: inventário) instituído para consolidar informações relacionadas às características das atividades de tratamento de dados pessoais?
> 8.1 A organização identificou os dados pessoais são compartilhados com terceiros?
> 9.1 A organização possui Plano de Resposta a Incidentes que abrange o tratamento de incidentes que envolvem violação de dados pessoais?

> 9.2 A organização possui sistema para o registro de incidentes de segurança da informação que envolvem violação de dados pessoais?
> 9.3 A organização possui sistema para registro das ações adotadas para solucionar incidentes de segurança da informação que envolvem violação de dados pessoais?
> 9.4 A organização monitora proativamente a ocorrência de eventos que podem ser associados à violação de dados pessoais?

As medidas administrativas constantes nos questionamentos são extremamente importantes para resguardar a corporação. A assistência à saúde é um dos setores que mais realiza credenciamentos com pessoas jurídicas (Hospitais, Clínicas e outras) que são atividades de risco em sede de proteção de dados, bem como existe a prestação de serviço nas dependências do Centro Médico da PMDF. Como exemplo, ressalta-se o processo de apuração de incidente pela ANPD, no bojo do processo SEI 00261.001886/2022-51, tendo como violadora a Secretaria de Estado de Saúde de Santa Catarina:

> O controlador alegou terem sido exfiltrados 4GB de dados (1,2 milhão de registros). Teriam sido afetados 48 mil titulares, a base conteria registros duplicados ou referentes a um mesmo titular. Os titulares seriam pacientes e prestadores de serviço, e não haveria dados de crianças ou adolescentes, conforme indicado no Formulário de Incidente de Segurança – ANPD (SEI nº 2837556), Relatório – SEI Relatório Complementar ANPD (SEI nº 3036397), OFICIO Processo SEI/ANPD nº 00261.001020/2021-6 (SEI nº 3279023) e OFICIO Processo SEI/ANPD nº 00261.001020/2021-6 (SEI nº 3279024). 4.6. No entanto, em momento posterior, a SES/SC apresentou Relatório RIPD (SEI nº 3666470) que descreve ser possível que o incidente tenha afetado crianças, adolescentes ou idosos: "Como a gama de pessoas atendidas pelo SUS é grande e irrestrita, são tratados dados de idosos e de menores representados por seus responsáveis legais (pois contamos com um Hospital Infantil Estadual)". (BRASIL, 2023, p.2)

Na decisão, a ANPD justificou a violação do artigo 49 da LGPD, ou seja, de que o sistema não atendeu aos critérios de segurança:

> A obrigação de observar os requisitos de segurança nos sistemas utilizados pelo Estado é ainda mais severa, tendo em vista que os dados pessoais dos titulares afetados são tratados de forma compulsória. O não tratamento de dados pela SES/SC na lista de espera SUS tem como consequência a inviabilidade da garantia do direito à saúde ao cidadão. Logo, o Estado, respeitados os critérios do caso concreto, possui ônus de

> utilizar sistemas em acordo com o previsto na LGPD. (BRASIL, 2023, p. 11)

Quanto às sanções, consta que foram aplicadas advertências por violações ao artigo 38, artigo 48, artigo 49 e artigo 52, todos da Lei Geral de Proteção de Dados. Desta forma, com base no exemplo citado, o DSAP/PMDF deve tomar as providências cabíveis para evitar falhas no tratamento dos usuários da assistência à saúde.

Também, a proteção de dados deve fazer parte da rotina da Corregedoria e de suas atividades de investigação dos delitos e sanções administrativas, que contém, inclusive, os nomes de vítimas de crimes domésticos e outros. Neste setor, mais uma vez, gera preocupação quanto às falhas de proteção de dados quando a corporação pontuou com "0,00" ao questionamento: "8.1 A organização identificou os dados pessoais são compartilhados com terceiros?".

Sabe-se que interessados comparecem à Corregedoria para solicitar documentos, dados sobre investigações e outras atividades que são de sua competência, sendo importante definir quais dados serão solicitados e como será a forma de arquivo. Também, deve-se ter cautela em anonimizar os dados pessoais que constam nos procedimentos de maneira que não sejam disponibilizados para quem não deveria.

Por fim, o Departamento Operacional[40], que é a atividade fim, ou seja, o Departamento responsável pelo policiamento e preservação da ordem pública deve estar adequado ao tratamento de dados pessoais, principalmente quanto às ocorrências policiais e ao programa que arquiva estes dados coletados.

A preocupação quanto à proteção de dados para o Departamento Operacional se faz presente, dentre outras, quando a PMDF pontuou com "0,00" às questões supramencionadas, uma vez que os dados constantes nas ocorrências policiais e que entraram no sistema do COPOM devem ser preservados e seu compartilhamento, para as situações que não sejam exclusivas de segurança pública, devem obedecer à LGPD.

[40] Importante mencionar que no dia 28 de maio de 2024 foi assinada, pelo Ministro da Justiça, a Portaria que estabelece "diretrizes sobre o uso de câmeras corporais pelos órgãos de segurança pública do país". Site https://www.gov.br/mj/pt-br/assuntos/noticias/lewandowski-lanca-diretrizes-sobre-uso-de-cameras-corporais-por-orgaos-de-seguranca-publica. Acessado no dia 29 de maio de 2024.

Diante do que foi analisado, percebe-se que a corporação se encontra em grave risco, no tocante à proteção de dados, quando se analisam as atividades e as compara com as respostas recebidas.

Deve-se, com urgência, promover medidas para a efetiva implementação da política de proteção de dados em todos os setores a fim de evitar sanções. Apesar de não ser possível que a ANPD aplique multa aos órgãos públicos, por expressa previsão legal, existem outras medidas que podem ser praticadas tais como a publicização da infração e a suspensão do exercício da atividade de tratamento de dados, ambas repercutindo negativamente para a imagem e a confiança da população na PMDF.

## 5.2 REFLEXÕES À LUZ DO REFERENCIAL TEÓRICO

Como visto, a sociedade encontra-se numa fase em que os dados são ativos de suma importância, seja para a iniciativa privada ou órgãos públicos e seu tratamento definirá, em grande parte o sucesso nas atividades. Quanto a isso não se pode olvidar que a administração pública, utilizando-se cada vez mais de tecnologia, possa ficar alheia as normas previstas na LGPD.

A sociedade exige, por tanto, que a administração pública seja eficiente no trato da coisa pública. Para tanto, no bojo do estado democrático de direito, existem mecanismos que viabilizem a prestação de contas, ou accountability, dos serviços prestados. Assim a governança é um sistema complexo que possibilita agregar valor aos serviços públicos, com transparência e participação social, ainda mais no bojo de uma sociedade de vigilância.

A administração pública necessita de líderes que estejam capacitados, fomentem a motivação e saibam escutar os anseios da população, e se distanciem do tradicional “tone at the top” e seus conceitos de “super líder”, pois tudo isso faz parte da boa governança.

De igual forma, o estabelecimento de compliance efetivo é medida salutar durante a implementação de uma política pública, uma vez que serve para minimizar e prevenir possíveis riscos à organização. Como visto, a efetividade do compliance é responsabilidade da Alta Cúpula da PMDF quando se compromete e investe no setor de integridade, com no caso da proteção de dados.

Com tais apontamentos, torna-se visível que não basta uma Portaria de Proteção de Dados sem que não exista, minimamente, condições para que seja efetiva. No caso da PMDF, mesmo após a publicação do acórdão do TCU (2022), não houve evolução quanto à esta política o que fica bastante evidente ao observar que não ocorreram as devidas capacitações para o tema.

A LGPD encontra-se vigente e a ANPD vem, a cada dia, mais atuante na fiscalização das melhores práticas de proteção de dados, devendo a corporação concentrar esforços para se adaptar às novas exigências.

## 5.3 PROPOSTAS DE MELHORIA PARA A PMDF

O presente tópico terá como objetivo estabelecer sugestões para a administração castrense que visem às boas práticas em proteção de dados pessoais, logo não tem qualquer cunho impositivo, mas o de aproximar os estudos acadêmicos da prática de gestão pública.

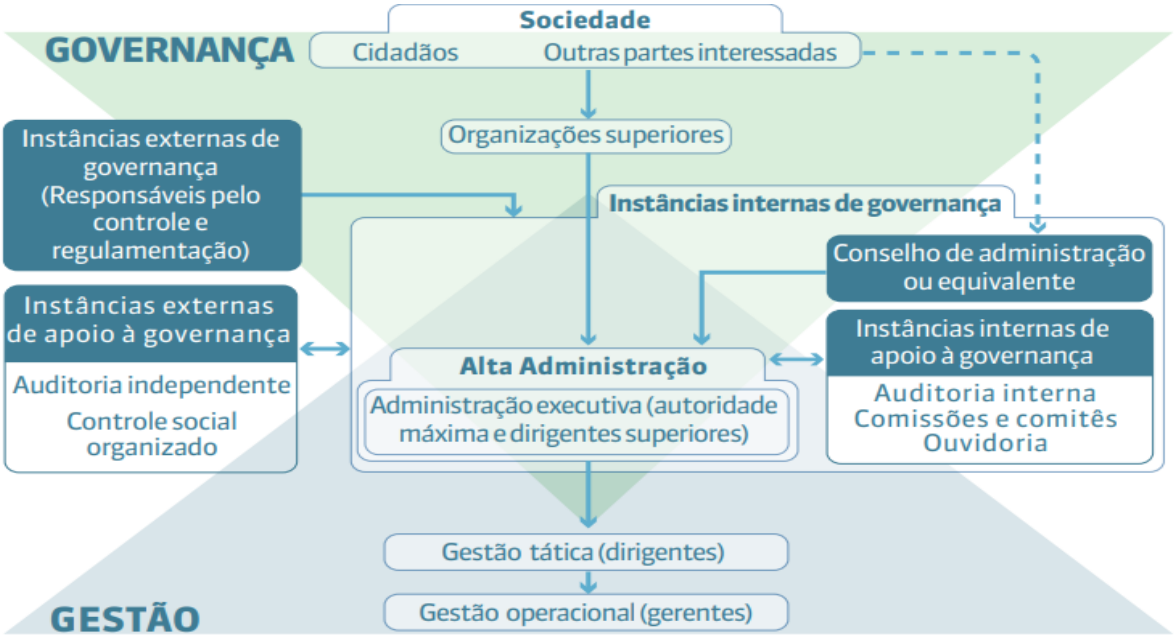
De início cabe ressaltar que as informações obtidas na pesquisa foram prestadas por um representante da Encarregada Setorial e não pelo próprio Colegiado. Tal fato é importante para o debate acerca da Política de Proteção de Dados Pessoais na PMDF pois o tema se refere às mais diversas atividades da Corporação, sendo pouco provável o conhecimento por apenas um representante.

Este trabalho tem como escopo a propositura de sugestões para o estabelecimento de uma governança eficiente na PMDF e que seja voltada para a proteção de dados. Para tanto, cabe mencionar que o TCU sintetizou que a governança pública organizacional compreende "essencialmente os mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a atuação da gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade". (BRASIL, 2020)

Como será visto, as sugestões se baseiam nos pilares da liderança, uma vez que existem necessidades para os gestores, na estratégia com as sugestões no Plano Estratégico, e no controle com as atribuições direcionadas ao Subcomitê Executivo de Proteção de Dados Pessoais.

Os subtópicos a seguir foram divididos em estratégico e tático para fins didáticos para enaltecer o caráter de Alta Administração de um com o de atuação pelo Subcomitê Executivo de outro, buscando-se à excelência das atribuições legais estabelecidas pela Constituição Federal e pelas leis afetas. Com isso, com suporte no Guia Básico de Governança Organizacional – TCU[41], pode-se estabelecer o seguinte fluxo da governança desejada:

**Figura 9 –** governança e gestão administrativa




Fonte: TCU (2025)

Segundo Tajra (2009, p. 66) o nível estratégico está relacionado com a Alta Administração da organização e sua atuação está direcionada para o exterior, para as modulações do mercado e tendências que podem alterar, comprometer ou ampliar as atividades da instituição. Voltando-se os olhares para a PMDF, pode-se compreender que são missões do Alto Comando, nos termos do que consta no decreto federal n° 10.443/2022:

> Art. 45. O Alto-Comando da PMDF é órgão colegiado de assessoramento permanente, de finalidade consultiva quanto aos assuntos relevantes para a PMDF, com vistas a dar suporte ao Comandante-Geral no processo decisório.

[41] Disponível no site https://portal.tcu.gov.br/data/files/FB/B6/FB/85/1CD4671023455957E18818A8/Referencial_basico_governanca_organizacional_3_edicao.pdf. Acessado em 15 de março de 2025.

> Art. 46. O funcionamento do Alto-Comando será definido em ato do Comandante-Geral. (BRASIL, 2020)

Em assim sendo, a tomada de decisão pelo ao Alto Comando direciona os rumos da PMDF, definindo como deverá participar do cenário no Distrito Federal, nacional e internacional. Por seu turno, o nível tático encontra-se delimitado ao ambiente interno da corporação, implementando as diretrizes que foram definidas pelo Alto Comando, fazendo a intermediação entre o nível operacional e estratégico. (TAJRA, 2009, p. 67)

Apesar de não ser tratado neste trabalho, pode-se entender que o nível operacional é o que faz acontecer, ou seja, atua para realizar os produtos oferecidos pela organização. No caso da PMDF, de forma bastante evidente, tem-se que os Batalhões de área exercem este papel com bastante maestria, como definido pelo decreto distrital nº 41.167/2020, na sua "Seção II, Dos Órgãos de Execução de Nível Operacional".

Apresentadas estas considerações iniciais, este trabalho volta-se para a apresentação de sugestões, baseadas nos estudos realizados, que poderão servir de direcionamento para a Política de Proteção de Dados no âmbito da PMDF. Primeiramente, serão delineados aspectos referentes ao Plano Estratégico da PMDF e à estrutura do Subcomitê Executivo de Proteção de Dados que foi criado para subsidiar as decisões do Alto Comando da PMDF. Após, serão apresentadas sugestões para atuação do próprio Subcomitê Executivo com base nos principais valores encontrados na pesquisa, bem.

É sente sentido que serão apresentadas as sugestões a seguir.

## 5.3.1 AÇÕES EM NÍVEL ESTRATÉGICO

### 5.3.1.1 ENGAJAR A ALTA CÚPULA DA PMDF SOBRE A PROTEÇÃO DE DADOS

Tratar de uma política de proteção de dados requer que os agentes que compõem a Alta Cúpula da organização estejam comprometidos com a missão de incorporar o compliance na instituição, uma vez que serão os responsáveis por influenciar os esforços e os comportamentos de seus servidores.

Segundo Pescarmona *et al* (2020, p. 35), acompanhando os principais estudiosos sobre o tema, classificam o *tone at the top* (envolvimento da alta liderança) como o pilar mais importante dos programas de compliance, apesar de que deve ser buscado por todos os integrantes da organização. Quanto a este ponto, a busca pelo envolvimento da Alta Liderança, a Portaria PMDF n° 1279/2022 tratou de forma tímida, quando em seu artigo 40 determina que o Estado-Maior deveria elaborar palestra para os integrantes do Alto Comando.

Entretanto, entende-se que apenas uma palestra não seja suficiente para garantir o devido comprometimento com a política de proteção de dados, com a profundidade e a coragem para efetivar as medidas:

> Garantir o walk the talk não é tarefa simples, pelo contrário. No entanto, esta árdua tarefa é primordial para que uma empresa e seus funcionários sejam reconhecidos pela ética e não pela prática comum de obtenção de resultado a qualquer custo. Para que isso aconteça, é vital que os gestores exercitem, por meio de treinamentos, reuniões e discussões de projetos, o comportamento ético e íntegro que garantirá e demonstrará o compromisso e a efetividade do programa de compliance. (PESCARMONA *et al*, 2020, p. 37)

Assim, para o atingimento do objetivo de engajar a Alta Gestão, deve-se conscientizar das responsabilidades inerentes a cada um dos integrantes em casos de falhas na proteção de dados. Neste ponto, a ABNT ISO/IEC 27.701/2019, no tópico 6.4.2.1, é bastante clara ao dispor sobre danos reputacionais da organização, disciplinares, danos aos titulares dos dados e outras consequências decorrentes.

Neste sentido, a Alta Gestão da PMDF deve estar imbuída do sentimento de liderança e buscar a promoção de medidas que favoreçam a governança: a) escolha de oficiais que tenham experiência com o tema; b) conduzir ações preparatórias para a assunção da função; c) definir formas de avaliar o desempenho dos oficiais que estejam na função de Encarregado Setorial.

### 5.3.1.2 REVISÃO DO PLANEJAMENTO ESTRATÉGICO DA PMDF

De início cabe ressaltar que o Planejamento Estratégico da PMDF 2023-2034 foi alterado em 2024, passando-se, assim, a vigorar a

2ª edição, que pode ser encontrado no site oficial da Corporação[42]. Como se pode verificar, nesta nova versão foram acrescidos pontos de interesse para a Instituição e que devem fazer parte de estudos a fim de que sejam incorporados à rotina castrense.

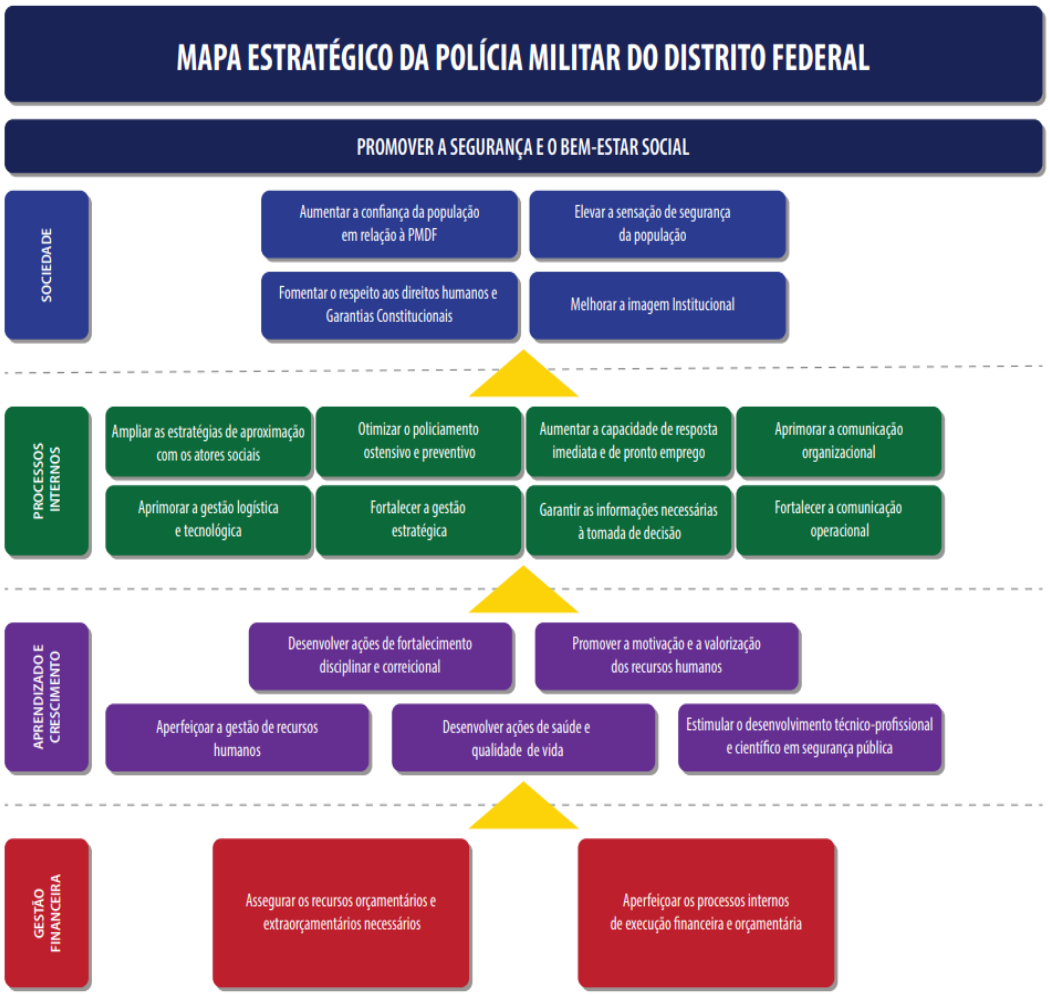
O documento dispõe de uma série de medidas para serem aplicadas tais como a implementação de programas de integridade, em parceria com a Controladoria-Geral do Distrito Federal – CGDF, proteção das mulheres e grupos de vulneráveis, foco na qualidade de vida, bem como:

> Entre os principais focos deste novo plano estratégico, destacam-se:
> • O fortalecimento dos conceitos de Comando, Controle e Inteligência (C3I);
> • Práticas voltadas à ampliação da prevenção e resposta à criminalidade violenta qualificada;
> • O fortalecimento das estruturas policiais para enfrentar crimes complexos;
> • A prevenção à violência doméstica e a outros crimes contra grupos vulneráveis;
> • A intensificação da abordagem comunitária.
> Como destacado pela Comandante-Geral, os eixos dessa nova edição abrangem:
> • Programas educacionais e assistenciais;
> • Um Programa de integridade;
> • A proteção de mulheres e grupos vulneráveis;
> • A promoção de boas práticas institucionais;
> • Um policiamento orientado pela inteligência;
> • E um enfoque nas mídias digitais, radiodifusão e televisiva. (DISTRITO FEDERAL, 2024)

Entretanto, não foi possível encontrar expressamente qualquer menção à proteção de dados pessoais, assim como se encontra na Lei n° 13.709/2018 e sua regulamentação distrital pelo decreto n° 45.771, de 08 de maio de 2024. Desta forma, como primeira necessidade, nota-se que a alteração do Plano Estratégico deve ser quanto à esta questão, atendendo-se a definição do Mapa Estratégico da PMDF:

[42] Nos termos do que consta no site https://portal.pm.df.gov.br/wp-content/uploads/2024/12/Plano_Estrategico_PMDF_2023_2034_2ed_FINAL.pdf. Acessado no dia 26 de fevereiro de 2025.

**Figura 10 –** mapa estratégico da PMDF




Fonte: Plano Estratégico PMDF 2023-2034 – PMDF (2024)

Como mencionado, o tema proteção de dados pessoais é matéria de morada constitucional, logo a Política de Proteção de Dados Pessoais da PMDF deve ser inserida no fomento ao respeito aos direitos humanos e garantias fundamentais (Sociedade), mais especificamente no objetivo 16[43], que teria a seguinte redação:

> 16. Objetivo: Fomentar o respeito aos direitos humanos e às garantias constitucionais.
> Estratégia:
> 16.1 CONSOLIDAR A POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS
> Iniciativas Estratégicas:
> 16.1.1 Promover a efetiva capacitação dos integrantes do Subcomitê Executivo de Proteção de Dados;

[43] Atualmente a redação consta apenas: "16. Objetivo: Fomentar o respeito aos direitos humanos e às garantias constitucionais".

> 16.1.2 Divulgar no âmbito da Corporação a Política de Proteção de Dados da PMDF.

Estas alterações no bojo do Planejamento Estratégico se fazem necessárias para demonstrar que a Alta Gestão está alinhada com a Política. Com base na ABNT ISO/IEC 27.001/2006, no tópico 5 e seguintes, o comprometimento da direção deve ocorrer de forma inequívoca, assegurando a consciência da relevância da atividade a ser exercida em Proteção de dados:

> 5.2.2 Treinamento, conscientização e competência
> A organização deve assegurar que todo o pessoal que tem responsabilidades atribuídas definidas no SGSI seja competente para desempenhar as tarefas requeridas:
> a) determinando as competências necessárias para o pessoal que executa trabalhos que afetam o SGSI;
> b) fornecendo treinamento ou executando outras ações (por exemplo, contratar pessoal competente) para satisfazer essas necessidades;
> c) avaliando a eficácia das ações executadas; e
> d) mantendo registros de educação, treinamento, habilidades, experiências e qualificações (ver 4.3.3).
> A organização deve também assegurar que todo o pessoal pertinente esteja consciente da relevância e importância das suas atividades de segurança da informação e como eles contribuem para o alcance dos objetivos do SGSI. (BRASIL, 2006)

Com tais acréscimos, o Plano Estratégico passará a expressar a necessidade de que a Política de Proteção de Dados Pessoais da PMDF seja verdadeiramente consolidada e observada em todas as atividades inerentes à Corporação.

## 5.3.1.3 FORMALIZAÇÃO DA POLÍTICA DE PROTEÇÃO DE DADOS NA PMDF

No tocante a Portaria PMDF n° 1.279/2022, que Aprovou a Política de Proteção de Dados na Corporação, a sugestão seria no tocante aos integrantes do Subcomitê Executivo de Proteção de Dados.

Percebe-se que a norma, a partir do inciso III, trouxe a possibilidade de indicação bastante ampla e isso pode ocasionar problemas. Primeiro quanto ao “garimpar” oficiais capacitados na matéria e segundo que este oficial escolhido detenha o conhecimento das necessidades do Departamento em que trabalha. Corroborando

com esta linha, tem-se que até o presente momento não constam nenhuma menção aos oficiais que ocupam estas cadeiras.

Neste sentido, a mudança proposta seria para a indicação de oficial que esteja próximo ao Chefe do Departamento e que o assessore diretamente, tenha conhecimento das demandas jurídicas do Departamento e que tenha uma permanência maior na função. Esta última qualidade é de suma importância para que se evite a solução de continuidade dos trabalhos de proteção de dados.

Compulsando o Regimento Interno da Corporação, uma função sobressai com estas características necessárias para o exercício deste colegiado que é o de Chefe da Assessoria Técnico-Jurídica (ATJ). Constando no organograma de todos os Departamentos, a ATJ tem como função o assessoramento do Chefe e objetiva a promoção de pareceres e trabalhos de cunho eminentemente jurídicos sendo este um fator de grande importância para a implementação da Política de Proteção de Dados na PMDF.

Esta mudança é bastante salutar uma vez que estabelece o colegiado de forma mais rígida e de acordo com a qualificação profissional dos seus integrantes. Para Matheson *apud* Matias-Pereira (2020, p. 22) a administração pública moderna requer servidores capacitados e intelectualmente preparados para assessorar os gestores em problemas complexos, compondo equipes suficientemente estáveis de forma que não se alterem com mudanças de políticas governamentais.

Ressalta-se que o colegiado é composto por oficiais de várias áreas, como a comunicação social, tecnologia da informação, inteligência policial (Centro de Inteligência) e direito, reforçando o caráter multidisciplinar da proteção de dados.

Segundo Saavedra e Garcia (2020, p. 116) as equipes formadas apenas por especialistas em direito e de compliance não são suficientes para atuar diante da complexidade que é a transformação da organização, sendo que “fazer a gestão de riscos e os treinamentos necessários são etapas fundamentais, mesmo porque os maiores riscos são os de comportamento humano, mais do que tecnológico”.

Também, não se pode olvidar que a rotatividade dos gestores é algo que atormenta a administração pública, principalmente os cargos de alta gestão. Segundo Pinto (2023, p. 19) esta alta rotatividade resulta

em descontinuidade das ações a serem implementadas, bem como a sua própria eficiência. Da mesma forma, deve ser levada em consideração a curva de aprendizado decorrente dos excessivos casos de substituição do Encarregado Setorial, que deve ser amenizado pelos integrantes do colegiado.

Outra medida importante é a adaptação da estrutura complexa da PMDF às atribuições do colegiado de proteção de dados. Com a inclusão dos Chefes de ATJ's dos Departamentos, nos termos das lições de Alcantara e Júnior (2022), seriam os *Data Protect Office* local ou DPO-local e representariam o Encarregado Setorial naquelas unidades, sendo este o modelo aplicado no SERPRO.

Com isso, entende-se que o colegiado terá maiores condições para exercer suas atividades com grande possibilidade de sucesso.

### 5.3.2 AÇÕES EM NÍVEL TÁTICO-OPERACIONAL

#### 5.3.2.1 VERIFICAÇÃO DA PERCEPÇÃO DO COMPLIANCE EM PROTEÇÃO DE DADOS

Como visto até o presente momento, a proteção de dados é uma incógnita na PMDF e não pode ser implementada sem informações que demonstrem a percepção por parte dos integrantes da Corporação. Segundo Garcia *et al* (2020, p. 301) uma forma de obter esta percepção, além do responsável pelo compliance e pela Alta Gestão, é com a aplicação de pesquisa interna ao lado da concentração no treinamento e na capacitação das pessoas da organização.

De igual forma, para Hencsey *et al* (2020, p. 59) um treinamento efetivo somente será obtido se for possível conhecer o público para o qual está sendo disponibilizado o conhecimento a fim de evitar perda de tempo, retirar o servidor de suas atividades ou, até mesmo, custear cursos que não serão necessários em razão das atividades que ele exerce.

Segundo Leal (2019, p. 160) este mapeamento deve passar por entrevistas com os integrantes da organização, inclusive com a Alta Administração, análise de documentos e contratos e verificação de potenciais impactos na atividade. Em continuidade, ultrapassada a etapa de entrevistas, pesquisas e as demais fases, será possível

encontrar os pontos fracos da cultura de compliance e atuar de forma mais efetiva.

Como sugestão, a Controladoria-Geral do Estado do Paraná disponibiliza em seu site[44] um formulário-diagnóstico que, também, pode ser utilizado para obter de maneira mais ampla a cultura organizacional de proteção de dados, ou seja, nos Departamentos e Diretorias de modo a obter os resultados mais desejados. Desta forma, com os dados obtidos na pesquisa será possível ministrar a palestra de forma mais coerente com o que existe na PMDF.

Evidente que, neste momento inicial de implementação, não seria possível aplicar o questionário para todos os integrantes da PMDF. Entretanto, aconselha-se a sua utilização, de forma anônima, aos oficiais superiores do posto de Coronéis, Tenentes-Coronéis e Majores que exerçam funções gratificadas. Com isso, o colegiado já teria uma interessante visão de compliance de proteção de dados e conseguiria iniciar treinamentos direcionados e individualizados conforme as necessidades de cada Departamento.

Para a realização da pesquisa, sugere-se a utilização da plataforma google forms que é de fácil acesso e sem custo para a PMDF, tomando-se como base o que foi aplicado pela Controladoria-Geral do Estado do Paraná, que está em Anexo.

Entretanto o maior desafio do Subcomitê Executivo, no caso da PMDF, será manter o espírito de compliance em proteção de dados vivo ao longo de toda a fase de implementação e consolidação, sendo, para Ajele *et al* (2020), que o pilar da capacitação "se mostra como principal meio de garantia e principal aliado à manutenção da cultura ética e de integridade, das diretrizes de compliance e dos valores da organização".

### 5.3.2.2 CRIAÇÃO DE PLANO DE CAPACITAÇÃO

O presente subtópico se destina a tentar sanar um dos pontos cruciais da Política de Proteção de Dados que é a capacitação dos seus integrantes, uma vez que foi obtido valor "zero" para todos os quesitos.

Os números denotam a pouca atuação institucional nos procedimentos que se referem à capacitação técnica dos integrantes

[44] Disponível no site https://www.cge.pr.gov.br/sites/default/arquivos_restritos/files/documento/2021-06/manual_implementacao_lgpd.pdf. Acessado em 09 de março de 2025.

da Corporação. Sabe-se das dificuldades orçamentárias para se investir em tais cursos e das inúmeras demandas voltadas para a atividade-fim (policiamento ostensivo e repressivo). Ademais, refletem o entendimento do TCU acerca de que a ausência de um plano de capacitação afeta diretamente a implementação da Política de Proteção de Dados:

> O resultado é preocupante, pois a LGPD é uma legislação técnica e complexa, que exige estudo para que as organizações adquiram maturidade no tema. Para que a maturidade seja alcançada, é fundamental que os colaboradores sejam treinados e conscientizados em proteção de dados pessoais.
> No mesmo sentido, para averiguar a qualidade dos planos de capacitação que foram elaborados, caso a organização afirmasse ter produzido o artefato, era exibida a subquestão 5.1.1 para avaliar se o plano considerava que pessoas que exercem funções com responsabilidades essenciais relacionadas à proteção de dados pessoais deveriam receber treinamento diferenciado. No entanto, constatou-se que quase metade das organizações que elaboraram o plano, 46%, não consideraram essa necessidade (...). (BRASIL, 2022)

Com base nestes apontamentos realizados pela Corte de Contas é que sugere a capacitação como o pilar que deve ser mais trabalhado inicialmente, e que sustentará as demais sugestões.

A importância da capacitação dos integrantes da Corporação, como pilar da implementação, se anuncia quando se observam os artefatos produzidos pelo Subcomitê Executivo de Proteção de Dados da PMDF, conforme debatido em tópico próprio.

Sabe-se que o tema é complexo e, razoavelmente, novo no Brasil, principalmente na administração pública, o que dificulta a implementação de forma natural, espontânea. Este fato de adaptação à LGPD foi relatado pelo TCU, no processo de auditoria da LGPD:

> Por se tratar de tema emergente, técnico e complexo, com o intuito de não surpreender os gestores com a condução do trabalho, três meses antes do início da execução da fiscalização (novembro de 2020) foram enviados e-mails às organizações selecionadas para a auditoria para comunicar que o TCU iniciaria, no primeiro trimestre de 2021, trabalho para avaliar a adequação das organizações públicas à LGPD. Além disso, foram divulgadas notícias sobre o trabalho no Portal do TCU e em mídias especializadas, o que contribuiu para a grande adesão de respostas ao questionário eletrônico (100%) e,

> acredita-se, induziu a adoção das primeiras medidas por várias organizações, devido à expectativa de controle criada. (BRASIL, 2022)

Agrega-se ao tema complexo à dificuldade em se conduzir políticas de proteção de dados numa organização como a PMDF que exerce uma grande quantidade de serviços, tais como saúde, ensino, contratações administrativas, requerendo do gestor um sem número de habilidades profissionais. Corroborando com este entendimento, Artese (2020, p. 458) descreve que:

> É evidente que em matéria não apenas de alta complexidade, mas que também se caracteriza por estar constantemente pressionada pelas rápidas transformações sociais e tecnológicas do nosso tempo, os temas de ponta em discussão e revisão são os mais variados. O papel do compliance (accountability é o termo usual) na proteção de dados pessoais é a discussão do momento. (ARTESE, 2020, p. 458)

Neste sentido, reforça-se a determinação do decreto distrital nº 45.771, de 08 de maio de 2024, em seu artigo 22, para que a administração envide esforços visando a capacitação de seus agentes no que tange à proteção de dados, utilizando-se dos recursos do próprio GDF.

Tendo a capacitação este papel de importância na implementação da política de proteção de dados, a sua não realização acarreta na ineficiência da própria iniciativa. Segundo Assi (2018, p. 103) não se torna mais eficiente e eficaz o negócio baseando-se apenas numa pessoa. A empresa deve funcionar como uma engrenagem e o ato de represar processos não funciona. Para tanto, deve-se definir a fim de que possam ser melhorados. Em outro ponto, o autor, ao tratar de COBIT[45] descreve:

> DS7.2 Entrega de treinamento e ensino – Com base nas necessidades de ensino e treinamento identificadas, definir grupos-alvo e seus membros, mecanismos adequados de ministrar os treinamentos, professores e monitores. Indicar os instrutores e organizar sessões de treinamento de forma oportuna. Registrar inscrições (incluindo pré-requisitos), frequência e participação e avaliações de desempenho. (ASSI, 2018, p. 105)

[45] Segundo explicação do autor, Control Objectives for Information and Related Technology, na prática, significa uma estrutura capaz de fornecer governança de TI.

Com base nestas considerações, nos valores obtidos na pesquisa e na ausência de artefatos produzidos pelo Subcomitê Executivo, é que se entende que a capacitação é o pilar central da política de proteção de dados e que dele derivam os demais.

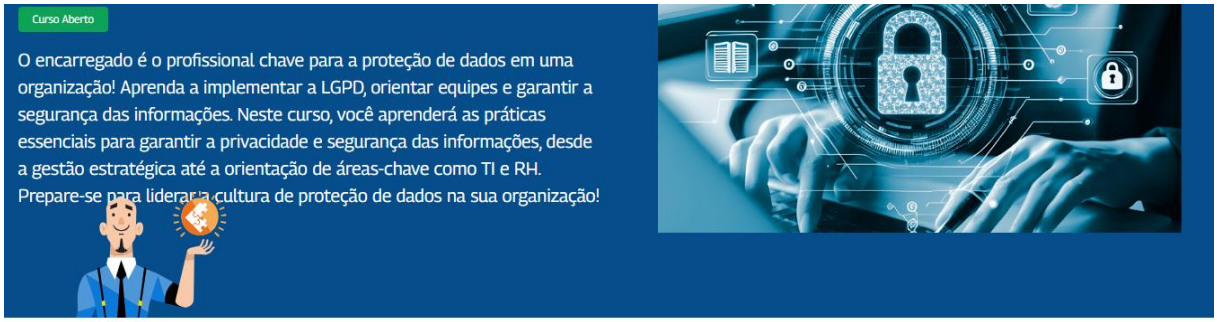
Diante das previsões normativas e margeando a questão da disponibilidade orçamentária, sabe-se que existem bons cursos gratuitos que podem ser fomentados pela PMDF a fim de iniciar esta trajetória de consolidação da proteção de dados. Um deles, pode ser encontrado na Escola Nacional de Administração Pública – ENAP que atenderia, plenamente, aos anseios da Corporação:

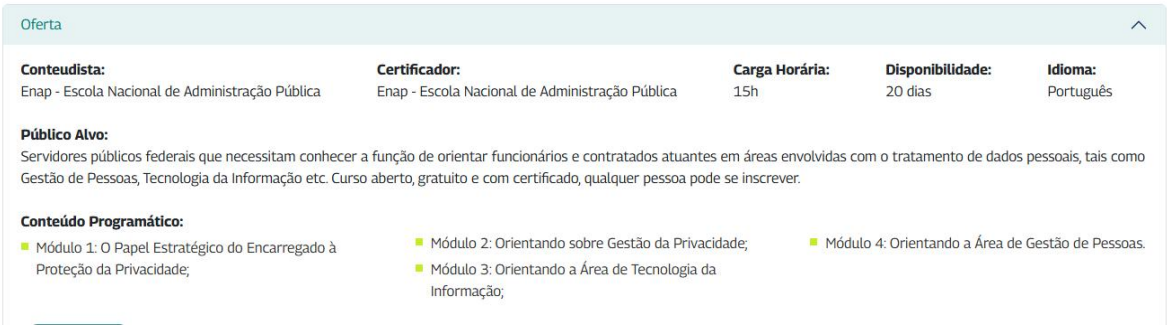
**Figura 11 –** imagens de cursos de LGPD pela ENAP


Fonte: ENAP (2025)

Navegando pela internet no dia 26 de fevereiro de 2025, este pesquisador se deparou com um curso específico para o Encarregado de proteção de dados que pode ser de bastante proveito na PMDF:

**Figura 12 –** imagens de cursos de LGPD pela ENAP



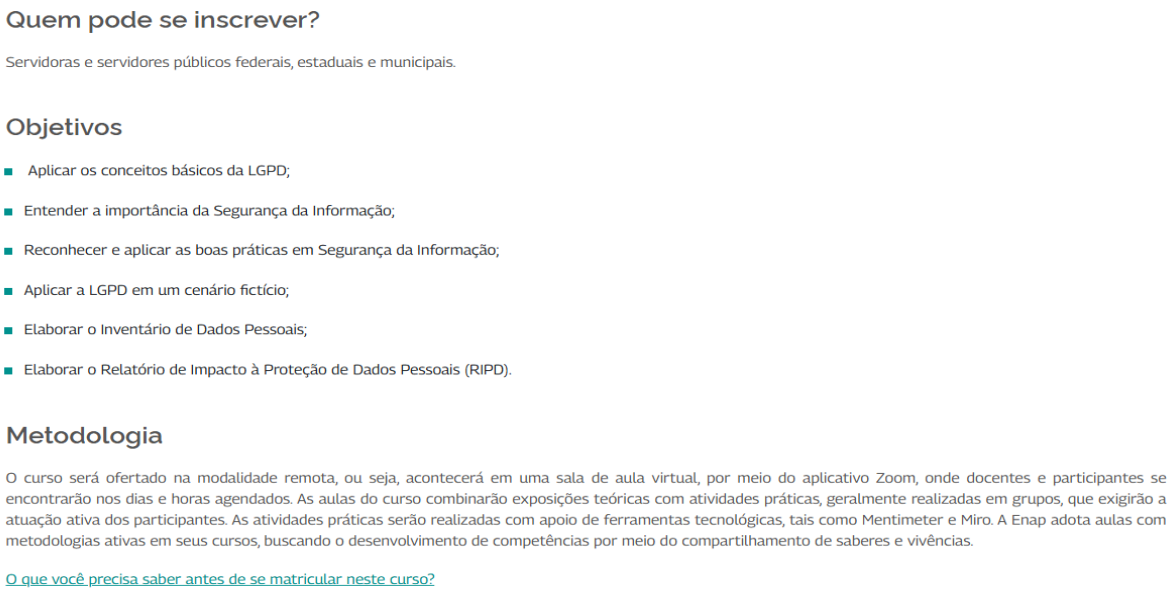

Fonte: ENAP (2025)

Como se percebe, este curso está totalmente direcionado para a atuação do principal responsável pela Política de Proteção de Dados na PMDF e deveria ser obrigatório para o oficial que ocupa aquela função.

Nota-se, também, que a capacitação está intimamente relacionada com outras atividades, dentre elas a elaboração de inventário de dados pessoais (bastante útil para os integrantes do Subcomitê Executivo da PMDF[46]), sendo o objetivo deste outro curso que está disponível pela ENAP (https://suap.enap.gov.br/vitrine/curso/2054/):

[46] Nos termos da Portaria PMDF nº 1279/2022, fazem parte do Subcomitê Executivo: Art. 21º O Subcomitê Executivo de Proteção de Dados Pessoais – SEPDP é composto, minimamente, pelo: I – Conselho Deliberativo; II – Consultoria Técnica; III – Secretaria. Art. 22º O Conselho Deliberativo será presidido pelo Encarregado Setorial (Auditor da PMDF) e composto pelos seguintes membros: I – Subdiretor da DITEL/PMDF; II – Subchefe do CCS/PMDF; III – Subchefe do Centro de Inteligência/PMDF; III – Oficial indicado pelo Departamento de Logística e Finanças. IV – Oficial indicado pelo Departamento de Gestão de Pessoal; VI – Oficial indicado pelo Departamento de Educação e Cultura; VI – Oficial indicado pelo Departamento de Saúde e Assistência ao Pessoal; VII – Oficial indicado pelo Departamento Operacional; VIII – Oficial indicado pelo Departamento de Controle e Correição.

**Figura 13 –** imagens de cursos de LGPD pela ENAP



Quem pode se inscrever?

Servidoras e servidores públicos federais, estaduais e municipais.

Objetivos

- Aplicar os conceitos básicos da LGPD;
- Entender a importância da Segurança da Informação;
- Reconhecer e aplicar as boas práticas em Segurança da Informação;
- Aplicar a LGPD em um cenário fictício;
- Elaborar o Inventário de Dados Pessoais;
- Elaborar o Relatório de Impacto à Proteção de Dados Pessoais (RIPD).

Metodologia

O curso será ofertado na modalidade remota, ou seja, acontecerá em uma sala de aula virtual, por meio do aplicativo Zoom, onde docentes e participantes se encontrarão nos dias e horas agendados. As aulas do curso combinarão exposições teóricas com atividades práticas, geralmente realizadas em grupos, que exigirão a atuação ativa dos participantes. As atividades práticas serão realizadas com apoio de ferramentas tecnológicas, tais como Mentimeter e Miro. A Enap adota aulas com metodologias ativas em seus cursos, buscando o desenvolvimento de competências por meio do compartilhamento de saberes e vivências.

O que você precisa saber antes de se matricular neste curso?

Fonte: ENAP (2025).

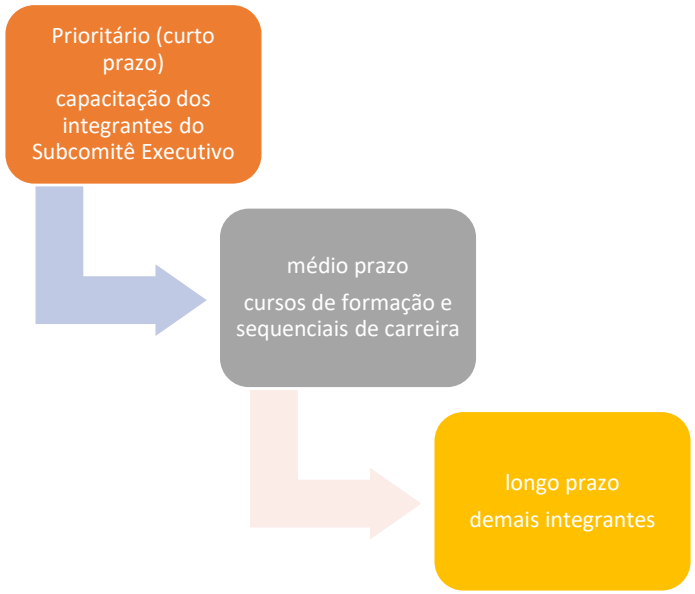
Em assim sendo, ainda no contexto da capacitação, sugere-se que o Subcomitê Executivo estabeleça um cronograma de capacitação de curto, médio e longo prazo, sendo que a prioridade de ser dada para aqueles que atuam diretamente no colegiado ou que estejam lotados nos departamentos orçamentários da PMDF, que são: Departamento de Saúde e Assistência ao Pessoal – DSAP/PMDF, Departamento de Logística e Finanças – DLF/PMDF e Departamento de Gestão de Pessoal – DGP/PMDF. Ademais, reforça-se que cada departamento tem um representante no Subcomitê executivo de proteção de dados pessoais, devendo receber uma capacitação mais especializada.

Estes departamentos supramencionados são os mais sensíveis em termos de proteção de dados pela própria natureza de gestão de contratos e manutenção de dados pessoais de todos os integrantes da Corporação.

No médio prazo, encontram-se aqueles que estão em curso de formação e cursos sequenciais de carreira, tanto para oficiais quanto para praças. Por fim, dentro do cronograma de capacitação, encontram-se os integrantes civis e os demais que não atuam diretamente ou indiretamente na área, como por exemplo os assessores técnicos e recepcionistas do Centro Médico da PMDF.

Desta forma, o cronograma de capacitação em proteção de dados teria esta configuração:

**Figura 14 –** ordem de prioridade para capacitação em LGPD



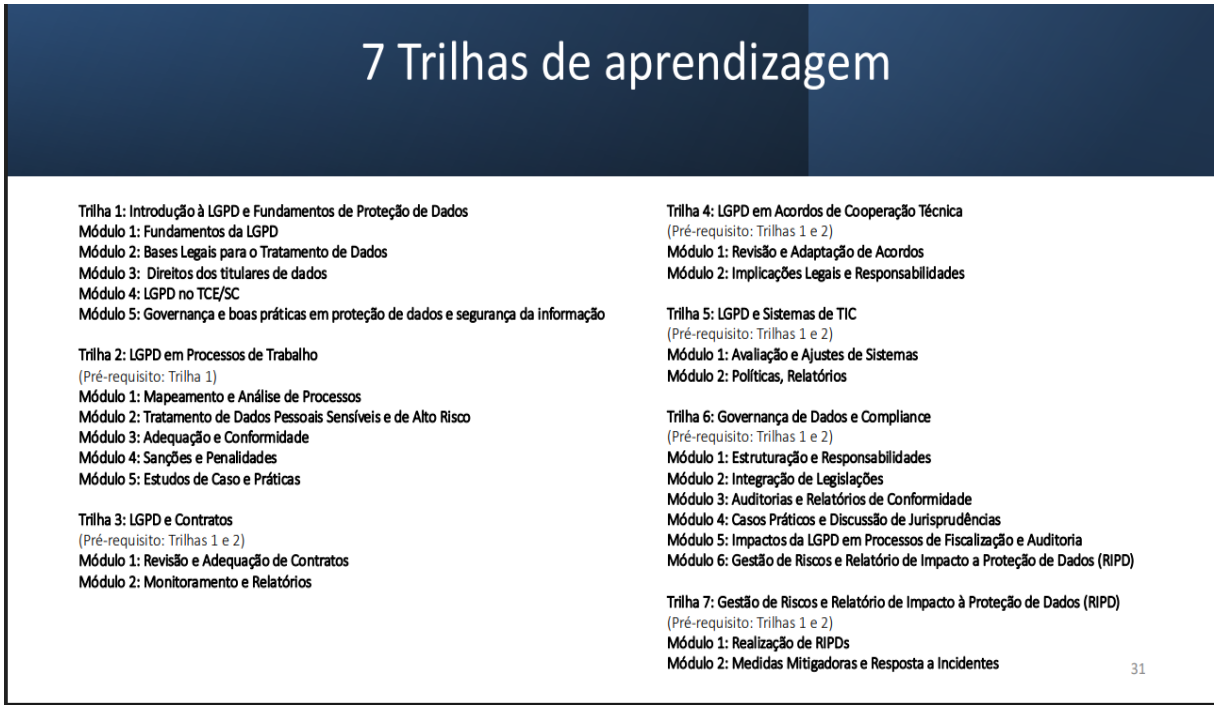

Fonte: elaboração própria (2025).

A definição de tempo como prioritário (curto prazo), médio e longo prazo deve ser estabelecido pelo próprio Subcomitê Executivo que estudará as possibilidades logísticas e orçamentárias e submeterá ao Comitê Gestor (Alto Comando da PMDF), atentando-se para o fato de que a proteção de dados é um direito fundamental e deve ser implementado dentro de um prazo razoável.

Por fim, cabe ressaltar que a capacitação deve seguir um caminho planejado, no qual a profundidade e complexidade do conteúdo aumenta conforme a necessidade de conhecimento desejado ao servidor. Neste sentido, o Tribunal de Contas do Estado de Santa Catarina – TCESC pensou na capacitação por trilhas[47] e que pode ser adequado à PMDF, conforme os estudos do Subcomitê Executivo:

[47] Disponível no site https://www.tcesc.tc.br/sites/default/files/apresentacao-doprograma-de-conformidade-a-lgpd-no-tce.pdf. Acessado em 09 de março de 2025.

**Figura 15 –** imagens de sete trilhas de aprendizagem




Fonte: TCESC (2025)

Neste formato a PMDF poderia definir quem frequentaria as trilhas de aprendizagem de acordo com as necessidades da Corporação.

### 5.3.2.3 ALTERAÇÃO DA PÁGINA INICIAL DA PMDF COM DESTAQUE PARA A POLÍTICA DE PROTEÇÃO DE DADOS

Como já mencionado, ao percorrer a página da PMDF verificou-se, com dificuldade, a menção à LGPD. Desta forma, o internauta pode se sentir constrangido em não saber qual será o destino que a PMDF dará aos seus dados pessoais, além de estar na contramão de direção do que prevê a Lei Geral de Proteção de Dados.

A divulgação das atividades realizadas pela PMDF aos seus usuários já foi objeto de análise pelo TCU que, por intermédio do Acórdão n° 2.164/2021[48], promoveu auditoria em Governança e Gestão Públicas em 378 organizações públicas. Nesta auditoria, verifica-se a participação da PMDF na qual respondeu àquela Corte e recebeu o feedback para conhecimento e adequações necessárias.

[48] Disponível no site https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/*/NUMACORDAO%253A2164%2520ANOACORDAO%253A2021%2520COLEGIADO%253A%2522Plen%25C3%25A1rio%2522/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0. Acessado em 09 de março de 2025.

Especificamente para a sugestão deste tópico, vale a pena analisar o gráfico inerente à "capacidade de monitorar a satisfação dos usuários – iGG – Governança Pública Organizacional, conforme abaixo:

**Figura 16 –** indicador de satisfação dos usuários


Fonte: site do TCU (2018)

O gráfico descreve a forma como a PMDF atua em relação à quatro indicadores (3130, 3131, 3132 e 3133), bem como a classificação que varia de "aprimorado" ao "inexpressivo". De todos os indicadores, o 3132 - "A organização assegura que os serviços acessíveis via internet atendam aos padrões de interoperabilidade, usabilidade e acessibilidade, e que as informações pessoais utilizadas nesses serviços sejam adequadamente protegidas" recebeu valor extremamente baixo (entre o inexpressivo e inicial).

Também, o indicador 3133 – "A organização promove a participação dos usuários com vistas à melhoria da qualidade dos serviços públicos prestados", obteve o mesmo valor baixo. Naquele momento, pelo que se verifica, deveria a PMDF ter buscado melhorar o seu site a fim de priorizar o acesso e a divulgação de informações aos seus usuários e aos titulares de dados pessoais.

Dito isso, e compulsando a LGPD, em seu artigo 50, na “Seção II, Das Boas Práticas e da Governança”, nota-se que um dos objetivos do controlador é o de “estabelecer relação de confiança com o titular dos dados pessoais, por meio de uma atuação transparente. Em assim sendo, a sugestão seria dar destaque à LGPD logo no primeiro momento em que se entra na página da Corporação. Como exemplo, pode-se trazer o que consta na página inicial do Tribunal de Contas do Distrito Federal – TCDF (https://www2.tc.df.gov.br/):

**Figura 17 –** imagem do site do TCDF


Fonte: TCDF (2025)

Nota-se que no canto superior direito o internauta se depara de pronto com a sigla “LGPD” facilitando e direcionando o usuário para clicar no link, caso esteja com dúvida sobre o tratamento realizado, se deparando com as seguintes informações:

**Figura 18 –** imagem do site do TCDF


Fonte: TCDF (2025)

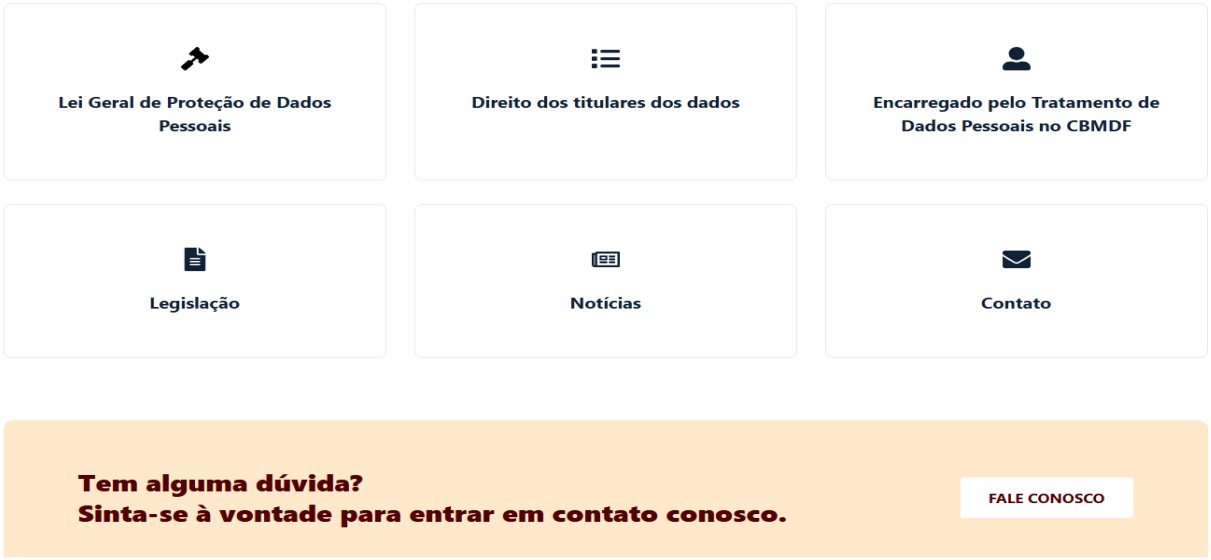
Interessante, também, é a configuração do site do Corpo de Bombeiros Militar do Distrito Federal – CBMDF que possibilita facilmente ao usuário visualizar e acessar informações sobre a proteção de dados:

**Figura 19 –** imagem do site do CBMDF


Fonte: CBMDF (2025)

Ao clicar em “transparência” e após em “LGPD”, abre-se uma janela que apresenta informações importantes ao usuário, bem como o caminho para maiores contatos com o Encarregado Setorial:

**Figura 20 –** imagem do site do CBMDF




Fonte: CBMDF (2025)

Estes dois sites são exemplos que podem servir de referência para a Corporação. Desta forma, a PMDF estaria dando informações precisas e diretas acerca de suas atividades, bem como os nomes dos responsáveis pela Proteção de Dados (Encarregado Setorial e Suplente). A transparência no tratamento de proteção de dados é expressamente descrita na LGPD, como um princípio basilar, nos termos do artigo 6°, inciso VI: "garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;".

A importância da fácil visualização quanto à política de proteção de dados, para muito além da LGPD, vem descrita no Regulamento Geral de Proteção de Dados da União Europeia, nos termos do que consta no considerando 39:

> O princípio da transparência exige que as informações ou comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples. Esse princípio, diz respeito, em particular, às informações fornecidas aos titulares dos dados sobre a identidade do responsável pelo tratamento dos mesmos e os fins a que o tratamento se destina, bem como às informações que se destinam a assegurar que seja efetuado com equidade e transparência para com as pessoas singulares em causa, bem como salvaguardar o seu direito a obter a confirmação e comunicação dos dados pessoais que lhes

> dizem respeito que estão a ser tratados. (UNIÃO EUROPEIA, 2016)

Também, segundo Matias-Pereira (2020, p.86) a transparência é de extrema importância no âmbito da administração pública por possibilitar a mudança do controle burocrático para o da sociedade e complementa:

> Em síntese, a busca permanente da transparência na administração pública deve ser vista como uma condição essencial para que os países, especialmente o Brasil, possam continuar a progredir no processo de desenvolvimento socioeconômico e ambiental e na consolidação da democracia. Neste sentido, a transparência do Estado se efetiva por meio do acesso do cidadão à informação governamental, o que torna mais democráticas as relações entre o Estado e sociedade civil. (MATIAS-PEREIRA, 2020, p. 86)

O que se busca com esta sugestão é proporcionar, à exemplo do que ocorre com a transparência ativa, quando, no dia 04 de dezembro de 2024, a PMDF conquistou o Prêmio Índice de Transparência Ativa (ITA)[49], pelos 100% de transparência em seu site institucional.

### 5.3.2.4 PROCEDIMENTO INTERNO PARA COMUNICAÇÃO DE INCIDENTES

O próximo subtópico trata acerca de sugestões para que a PMDF possa obter, minimamente, a comunicação entre os operadores internos de proteção de dados no momento em que houver um incidente no tratamento dos dados pessoais.

Nota-se que apenas no item 9.5 é que a PMDF obteve “0,50”, ou seja, respondeu que atende parcialmente ao questionamento, entretanto, não foi possível verificar, com base nas informações prestadas pelo representante do Subcomitê de Proteção de Dados, de que forma ou como será realizada tal comunicação.

Neste ponto, a Lei Geral de Proteção de Dados estabelece, em seu artigo 46 e seguintes que o controlador deve valer-se de boas

[49] Extraído do site https://portal.pm.df.gov.br/?post_type=noticias-institucion&p=6077, o citado prêmio foi “Instituído pela Controladoria-Geral do Distrito Federal (CGDF) em 2016, o Prêmio ITA busca promover o cumprimento da LAI, incentivando órgãos e entidades a priorizarem a transparência e a boa governança. Na edição de 2024, a PMDF não apenas manteve sua excelência, mas reafirmou seu papel como referência em gestão pública”. Acessado no dia 05 de março de 2025.

práticas para tal comunicação. Por seu turno, o decreto distrital n° 45.771, de 08 de maio de 2024, em seu artigo 6°, estabelece que o controlador deve comunicar ao Encarregado Governamental e ao titular a ocorrência de incidente de segurança que acarrete risco ou dano relevante.

Por fim, a Portaria PMDF n° 1.279/2022, em seu artigo 10, inciso VIII, dispõe que o Encarregado Setorial deverá "reportar-se ao Encarregado Governamental, que o orientará e supervisionará em caso de comunicação com a ANPD;". Apesar desta previsão, mais uma vez, não foi descrito este artefato indicando como se dará a comunicação interna (fluxo da comunicação), entre os operadores, e a comunicação com o Encarregado Governamental e ANPD, nem tampouco qual instrumento será utilizado para tal.

Existem indícios desta comunicação de incidente de dados, apesar de tudo. Compulsando o site da PMDF, pode-se extrair o recente Edital de Credenciamento n° 1/2024 – DSAP/PMDF, que tem como objeto:

> (...) de serviços de saúde de natureza contínua, na área específica de SERVIÇOS ASSISTENCIAIS CLÍNICOS E CIRÚRGICOS ELETIVOS E DE URGÊNCIA E EMERGÊNCIA, em valor estimado de R$ 401.512.665,41 (quatrocentos e um milhões, quinhentos e doze mil, seiscentos e sessenta e cinco reais e quarenta e um centavos) para um período de 12 (doze) meses consecutivos, de modo a atender os beneficiários do sistema de saúde da PMDF, nas condições estabelecidas neste edital e seus anexos. (DISTRITO FEDERAL, 2024)

Em seu tópico "Da Proteção de Dados Pessoais" o acordo jurídico define que a credenciada deverá:

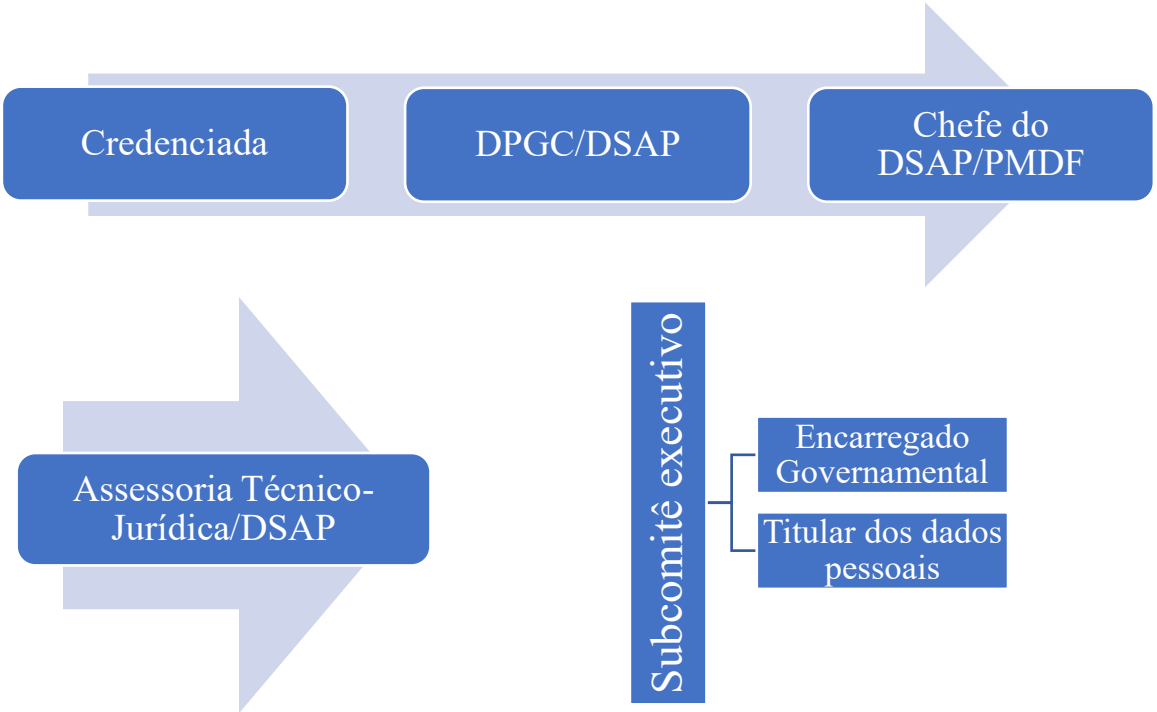
> 13.1.11. O preposto da credenciada manterá contato formal com a Diretoria de Planejamento e Gestão de Contratos - DPGC, por meio de gestores e fiscais de contrato, no prazo de 24 (vinte e quatro) horas da ocorrência de qualquer incidente que implique violação ou risco de violação de dados pessoais, para que se possa adotar as providências devidas, na hipótese de questionamento das autoridades competentes. (DISTRITO FEDERAL, 2024)

Como se percebe, o Edital é claro em estabelecer o dever da credenciada em comunicar o incidente de tratamento de dados pessoais para a Diretoria de Planejamento e Gestão de Contratos – DPGC que faz parte da estrutura do DSAP/PMDF. A dificuldade se

encontra sobre as seguintes perguntas que advém naturalmente: o que fazer com esta comunicação? Qual setor vai encaminhar esta comunicação e para quem? Qual o instrumento ou formulário será utilizado para que se consiga descrever os fatos de acordo com o que requer a norma de proteção de dados?

Para estas questões este pesquisador irá sugerir um fluxo interno que seja simples e eficiente para o atingimento do que descreve as normas para a comunicação de incidente[50]:

**Figura 21 –** proposta de fluxo de comunicação de incidentes de proteção de dados




Fonte: elaboração própria (2025)

A fim de explicar o caminho da comunicação, rememora-se que o Edital já descreve que a credenciada tem o dever de comunicar formalmente o incidente de tratamento de dados pessoais para a DPGC/DSAP, por ser aquela Diretoria a responsável pelo planejamento e gestão de contratos de saúde na PMDF. A partir deste ponto, acrescenta-se que a informação deve ser encaminhada imediatamente para o Chefe do DSAP/PMDF, por ser o ordenador de despesas e o gestor da Pasta de saúde da PMDF.

[50] Cabe esclarecer que a LGPD determina que em casos de incidentes de dados, o controlador informe aos titulares de dados, nos termos do que consta no artigo 48. Entretanto, para o escopo do presente trabalho não serão feitos apontamentos sobre tal comunicação.

Ao ser informado, o Chefe do DSAP/PMDF despacha o relato para o Chefe da ATJ/DSAP[51] para uma breve análise e verificação dos itens necessários para o encaminhamento ao Subcomitê Executivo de Proteção de Dados da PMDF. Naquele colegiado, seriam agregadas mais algumas informações e o devido encaminhamento para o Encarregado Governamental, em prazo razoável, conforme estabelece a LGPD. Estabelecidas as balizas fundamentais para o fluxo da comunicação de incidentes, ele pode ser aplicado para todos os demais Departamentos da Corporação.

Resta, portanto, sugerir algum modelo de documento que possa ser empregado pela PMDF, até que outro seja definido pelo Encarregado Governamental. Aqui, também a simplicidade deve ser utilizada, pois a padronização já foi realizada pela ANPD.

Compulsando a página oficial da ANPD[52], encontra-se o Formulário de Comunicação de Incidentes de Segurança com Dados Pessoais que tem o escopo de esclarecer às autoridades competentes detalhes acerca do sinistro e que já se apresenta no formato word para o preenchimento do responsável pelas informações, sendo possível que a PMDF utilize até que não haja padronização pelo Encarregado Governamental.

### 5.3.2.5 ESTABELECER A DEVIDA COMUNICAÇÃO COM O TITULAR DE DADOS

Por fim, em sede de sugestões, cabe tratar de ponto importante e que tem ligação direta com a primeira sugestão do capítulo, ou seja, alterações no site oficial da PMDF. Por coerência lógica, no momento em que a organização desenvolve sua Política de Proteção de Dados, deixando-a transparente e pública, bem como demonstrando a confiança para com o usuário dos serviços, deve-se pensar na maneira como tais titulares irão exercer seus direitos, dentre eles o de requerer a confirmação de que seus dados estão sendo tratados.

---

[51] A Assessoria Técnico-Jurídica (ATJ) é o órgão à disposição dos Chefes de Departamento cuja competência é assessorar quanto aos aspectos jurídicos que estejam na alçada daquela Pasta. Normalmente, a ATJ é chamada para dar parecer de cunho eminentemente jurídico e proporciona segurança na decisão do Chefe.

[52] https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-inicia-processo-de-regulamentacao-sobre-incidentes-de-seguranca-com-tomada-de-subsidios. Acessado em 02 de março de 2025.

Segundo Fontoura e Rodrigues (2022, p. 100) a comunicação efetiva se concretiza quando o controlador exerce a comunicação ativa e a passiva. A comunicação ativa ocorre quando a organização a realiza em deferência aos princípios da finalidade, adequação, necessidade e transparência. Por seu turno, a comunicação passiva é aquela que surge no momento em que o titular do direito provoca o Encarregado para esclarecimentos ou outras medidas inerentes aos seus dados pessoais.

Visando a comunicação passiva, a LGPD, em seu artigo 19 determina que, mediante requerimento do titular, a PMDF deve confirmar se existe tratamento de dados. A norma determina que a resposta seja providenciada dentro do prazo de 15 (quinze) dias, sendo que, caso a organização não esteja preparada para fazê-lo, pode acarretar em sanção administrativa por parte da ANPD. Como não foi percebido nenhum artefato neste sentido, ou seja, de proporcionar resposta ao titular dos dados pessoais, é que se sugere um fluxo de comunicação interno para a PMDF, como se verá a seguir.

Primeiramente, com a finalidade de facilitar e direcionar as demandas, cujos tratamentos podem ser diversos de acordo com as finalidades de sua coleta, parte-se do princípio de que o Subcomitê Executivo de Proteção de Dados será o órgão recebedor deste requerimento, sob a orientação do Encarregado Setorial.

Ao receber, deve analisar sobre que matéria o pedido se refere e incluir no Sistema Eletrônico de Informações – SEI do GDF/PMDF. Por exemplo: caso seja um requerimento questionando sobre dados de saúde, o responsável será o DSAP/PMDF; caso seja de dados tratados por conta do ensino, o responsável será o Departamento de Educação, e assim por diante. Esta primeira triagem é necessária para encurtar caminhos e tornar mais célere a resposta ao interessado.

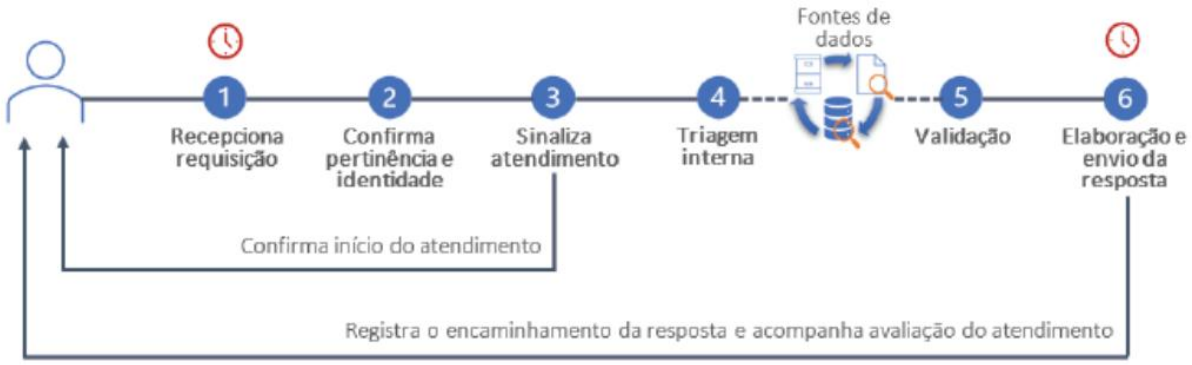
Após tal providência, o requerimento será analisado pelo Departamento específico que confeccionará a minuta de resposta que será encaminhada para o Subcomitê Executivo. Naquele colegiado, serão verificadas e validadas a identidade do requerente, evitando dar conhecimento de dados pessoais de forma indevida, e encaminha a resposta ao interessado.

A grande dificuldade é que o tratamento de dados pode ser tanto em meio físico quanto em meio eletrônico, apesar de que a comunicação está a cada dia mais tendenciosa para este último. Assim,

cabe à organização estabelecer métodos eficazes para alcançar a excelência no trato das informações a fim de conseguir responder tempestivamente.

Fontoura e Rodrigues (2022, p. 111) adaptaram de Gartner (GARTNER, 2021) um exemplo de fluxo de atendimento às requisições de titulares de dados:

**Figura 22 –** fluxo de atendimento de requisições de titulares de dados




Fonte: elaborada pelos autores (2022)

Percebe-se que este fluxo pode ser adaptado e empregado na PMDF a fim de tornar mais célere o atendimento da demanda pelo titular de dados.

1. **Recepção da requisição pelo Subcomitê Executivo;**
2. **O colegiado confirma a pertinência com a matéria e a identidade do requerente;**
3. **Ocorre a sinalização do atendimento ao interessado;**
4. **O Subcomitê Executivo verifica qual o Departamento responsável pelo tratamento de dados, conforme as competências definidas pelo decreto federal nº 10.443/2020 e abordadas nesta pesquisa;**
5. **O Departamento providencia as informações necessárias e confecciona a minuta de resposta ao interessado;**
6. **A validação das informações será realizada pelo Subcomitê Executivo e enviada ao titular dos dados pessoais.**

Para a efetividade deste processo é necessário que ele seja confeccionado e divulgado no site da PMDF. A promoção de respostas não é um processo novo na PMDF, pois com base no decreto distrital nº 36.462/2015, que estabelece a Ouvidoria como órgão responsável por receber e dar os devidos encaminhamentos, dentro do prazo estabelecido na norma, já existe este caminho de coleta de

informações. Isso é o que consta no site da PMDF (https://portal.pm.df.gov.br/carta-de-servicos-ouvidoria-da-pmdf/) as atividades exercidas:

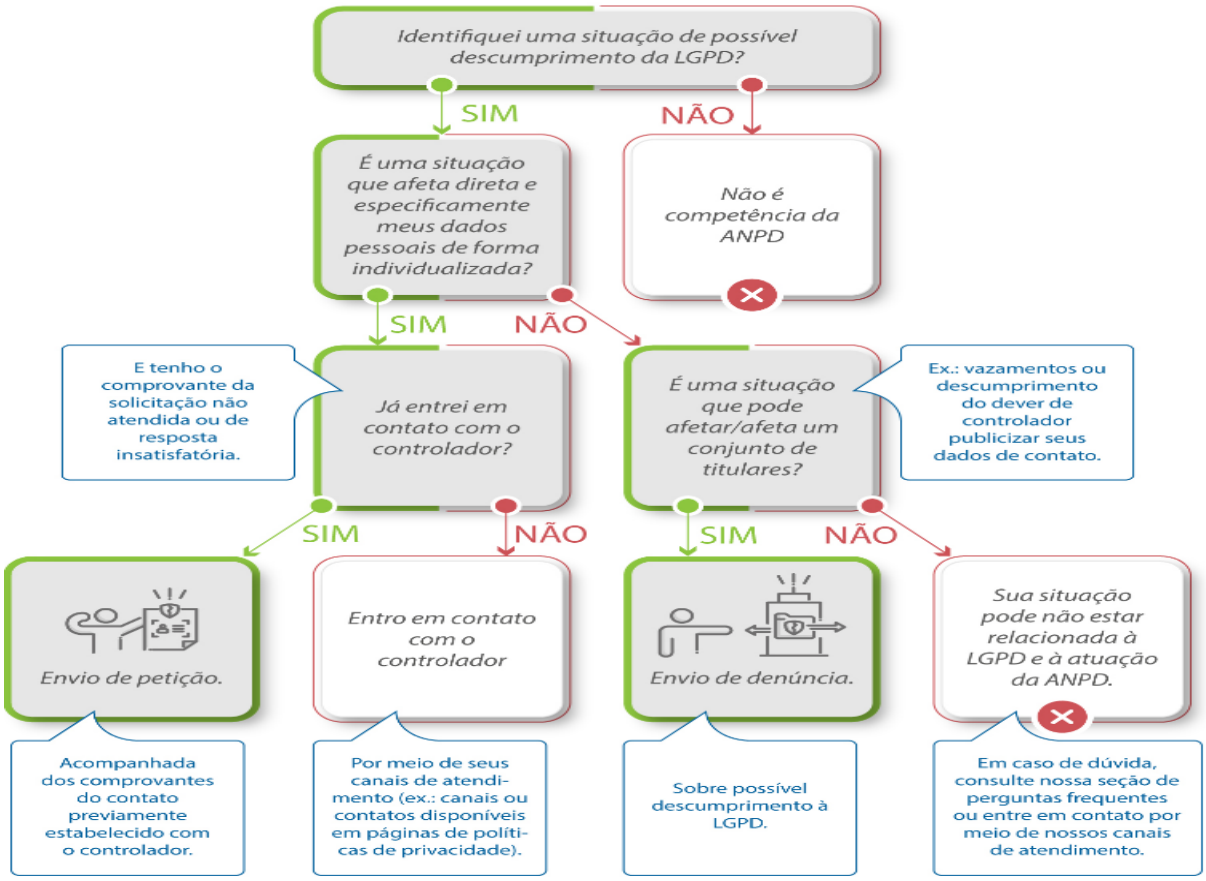
> Dessa forma, a Ouvidoria Geral do Distrito Federal recebe as manifestações registradas e, após triagem, as encaminham para os Órgãos responsáveis.
> **A Ouvidoria da Polícia Militar do Distrito Federal recepciona suas demandas encaminhadas pelo Ouv-DF e, após análise, distribui para as Unidades responsáveis para a averiguação dos fatos e possíveis providências.**
> A Ouvidoria da Polícia Militar tem como incumbência a recepção das demandas oriundas do OUV-DF, encaminhamento para as Unidades, controle de prazos, monitoramento da qualidade da resposta e inserção destas no sistema Ouv-DF.
> São também responsabilidades da Ouvidoria da PMDF: produção de relatórios acerca do trabalho desenvolvido; a recepção, encaminhamento e inserção das respostas no sistema de Informação ao Cidadão-SIC; atualização e monitoramento da Carta de Serviços e a atualização de algumas abas e o monitoramento das publicações e atualizações acerca da Transparência Ativa da Corporação.

Desta forma, deve o Subcomitê Executivo ajustar-se para promover nos mesmos moldes as demandas pertinentes aos dados pessoais, facilitando o exercício deste direito fundamental aos titulares de dados pessoais.

A importância de se estabelecer um fluxo para a comunicação passiva é que o titular dos dados pessoais, ao não ser atendido ou ter sua resposta insatisfatória, pode peticionar ou denunciar diretamente à ANPD, gerando possíveis reflexos sancionatórios. Compulsando o site da ANPD, pode-se encontrar, de forma didática[53], o fluxo exigido para que as petições e as denúncias sejam tratadas diretamente por aquela Autoridade de Proteção de Dados:

[53] Importante ressaltar que o modelo pode ser plenamente utilizado pela PMDF uma vez que facilita o entendimento dos trâmites necessários para o interessado.

**Figura 23 –** fluxo de requisições da ANPD




Fonte: ANPD (2025)

Como se verifica do fluxograma acima, a ANPD diferencia o encaminhamento de "denúncia" de um "direito do titular" ao devido tratamento de dados. A denúncia não se refere necessariamente a uma situação específica de um dado titular de dados, mas que tenha o condão de atingir um conjunto de titulares ou que inviabilize o exercício de vários titulares, como é o caso do tratamento discriminatório dos dados pessoais, a coleta excessiva de dados pessoais, a ausência de encarregado pelo tratamento dos dados pessoais, a não existência de canal de comunicação para o exercício de direitos e outros.

Já a petição diz respeito aos direitos inerentes ao titular, tais como a confirmação de existência de tratamento de dados pessoais pelo controlador, direito de acessar seus dados pessoais, de pedir correção de informações, de revogar consentimento e outros.

Quanto à fiscalização da ANPD para os casos de denúncia ou petição, ela é regulamentada pela Resolução CD/ANPD nº 1[54], de 28 de

[54] Disponível no site https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-1-de-28-de-outubro-de-2021-355817513. Acessado em 05 de março de 2025.

outubro de 2021, que se compõe de atividade de orientação, atividade preventiva e atividade repressiva que pode acarretar em sanções administrativas à PMDF.

Portanto, é de suma importância que o Subcomitê Executivo promova a elaboração de um fluxo de comunicação passiva para com os titulares e dados a fim de evitar denúncias ou peticionamentos decorrentes da falta de aplicação da LGPD.


6

# 6 CONSIDERAÇÕES FINAIS

A tecnologia aproximou países e disseminou a informação, proporcionou qualidade de vida e melhoria nos serviços públicos com a digitalização. Assim, os dados são coletados e transmitidos, quase que simultaneamente, entre os órgãos públicos para a concretização das políticas públicas e outras finalidades previstas nas legislações. Da mesma forma, os dados também são transmitidos entre empresas para as mais diversas finalidades, inclusive a de buscar lucro, pois o dado passou a ser a nova moeda.

Com a LGPD, que acompanhou o Regulamento europeu, vários setores tiveram que se adaptar à proteção de dados pessoais, fazendo ressurgir conceitos como governança corporativa ou governança pública que já a algum tempo vem sendo tratado pela literatura especializada. Ocorre que tais ferramentas foram sendo atualizadas a fim de que lhe coubesse a inovação tecnológica que ganhou espaço na sociedade, trazendo os algoritmos, a inteligência artificial e outras facilidades que se inseriam na vida quotidiana da sociedade.

O tema compliance digital no contexto da administração pública, decorrente do direito digital, estabelece possibilidades para que estas tecnologias sejam utilizadas com ética, eficiência e respeito aos direitos fundamentais. A sociedade de vigilância, na qual estamos inseridos, é capaz de monitorar nossas preferências e desejos com apensas um “click” nas plataformas das redes sociais que estão por todos os lados e à disposição de qualquer indivíduo.

Se as grandes empresas coletam dados, o Estado também o faz. A todo instante, um sem número de dados trafegam pelos bancos de dados da administração pública e são utilizados, armazenados e compartilhados para os mais diversos fins. Entretanto, a sociedade está cada vez mais atenta ao que ocorre com estes dados e com a sua utilização, gerando certa desconfiança que, por sinal, é confirmada toda vez que as mídias divulgam vazamentos de dados pessoais ou utilização indevida, causando transtorno ao polo mais fraco desta relação: o indivíduo.

O Estado democrático de direito possibilita que vários órgãos atuem conjuntamente, ou não, para a proteção dos direitos fundamentais. Não se pode negar que, no atual estágio da sociedade, a proteção de dados é tema amplamente debatido pelo no mercado e na administração pública. Para tanto, a LGPD criou a ANPD e o ordenamento jurídico pátrio o TCU para possam atuar em conformidade com as suas competências na política de proteção de dados brasileira.

Com fundamento em tais condições é que esta pesquisa se utilizou da expertise destes dois órgãos para analisar a proteção de dados na PMDF à luz do acórdão n° 1.384/2022 e da fiscalização sofrida pela Secretaria de Estado de Educação do GDF.

O objetivo foi alcançado no instante em que se definiu que a PMDF se encontra no nível "inicial" de adequação à proteção de dados, uma vez que no momento devido não houve resposta à auditoria do TCU/2021, juntando-se, em tese, ao rol das 225 entidades que obtiveram a mesma qualificação.

Ressalta-se que este nível obtido está aquém do que seria normalmente esperado, pois a auditoria ocorreu no ano de 2021, com acórdão publicado em 2022, o que sugeriria que medidas administrativas fossem tomadas a fim de compreender as necessidades e fortalecer a Política de Proteção de Dados da PMDF.

Para corroborar com esta afirmativa, serão descritas as dimensões cuja pesquisa detectou valores inferiores à média obtida pelo TCU.

Na dimensão do "contexto organizacional", a PMDF indicou "0,33" sendo que a média obtida foi de "0,42". Na dimensão da "capacitação", a PMDF indicou "0,00" sendo que a média obtida foi de "0,27". Na dimensão da "conformidade de tratamento", a PMDF indicou "0,20" sendo que a média obtida foi de "0,24". Na dimensão da "violação de dados pessoais", a PMDF indicou "0,10" sendo que a média obtida foi de "0,23". E por fim na dimensão de "medidas de proteção", a PMDF indicou "0,20" sendo que a média obtida foi de "0,32".

Diante dos dados apresentados na pesquisa, o que pode ser extraído é que apesar da auditoria do TCU, no ano de 2021, a PMDF não se esforçou para compreender o problema e buscar os ajustes necessários para uma adequação mais efetiva. Ademais, como tratado,

a Portaria de Proteção de Dados somente foi publicada em 2022 e, apesar de descrever algumas medidas, nada foi realizado naquele momento.

A preocupação se mantém quando foram solicitados os artefatos produzidos pelo Subcomitê Executivo e nenhum deles se destinava a procedimentos ou orientações quanto ao tema, reforçando que mesmo após a Política ser criada não houve efetividade.

Na parte final do trabalho, com suporte na doutrina e nos entendimentos dos órgãos de fiscalização, este pesquisador sugeriu algumas medidas para melhor adequar a proteção de dados na PMDF, sendo que algumas são voltadas para o Alto Comando, ou Alta Gestão, e outras para o Subcomitê Executivo de Proteção de Dados na PMDF.

Como primeira sugestão, e diante dos dados apresentados na pesquisa, sugere-se voltar às atenções para o engajamento da Alta Cúpula, com conceitos sobre liderança, motivação e a conscientização de que a inércia no compliance gera responsabilização dos seus integrantes.

A segunda se destina à revisão do planejamento estratégico da PMDF para tornar mais robusta as diretrizes inerentes à proteção de dados, uma vez que, nem mesmo a 2ª edição, realizada no final do ano de 2024, contemplou o que foi tratado pelo TCU.

Como outra sugestão, tem-se que existe a necessidade de formalizar a Política dando-se integrantes que possam agregar conhecimento, de forma estável e contínua. Sabe-se que a rotatividade de funções gera insegurança e ineficiência, principalmente no tocante ao aprendizado.

Ultrapassadas as sugestões para o Alto Comando, voltam-se os olhares para o nível tático-operacional, ou seja, para o Subcomitê Executivo. De início, com base o que se observou na pesquisa, nota-se que não existe um conhecimento suficiente sobre o tema na PMDF.

Desta forma, sugere-se que seja aplicado questionário a fim de desvendar quais funções precisam de mais conhecimento e quais devem passar por cursos mais básicos de proteção de dados. A partir deste questionário é que se poderá passar para a capacitação do efetivo.

Também, sugeriu-se a criação de plano de capacitação a fim de que a adequação pudesse ser alavancada, pois não se produz aquilo que não se conhece. Se não for disponibilizado conhecimento para a elaboração de artefatos não será colhida nenhuma resposta efetiva. Existem vários cursos, inclusive proporcionados pela Escola de Governo – GDF e pela ENAP, que podem suprir esta deficiência sem qualquer custo para a PMDF. Assim, com um cronograma de capacitação, sob a coordenação do Subcomitê Executivo, seria possível estabelecer prioridades e atender às expectativas da LGPD.

Outra sugestão foi a alteração da página oficial da PMDF a fim de que possa atender aos anseios da LGPD. Como apresentado, a política de proteção de dados deve seguir o exemplo de outros órgãos, tais como o TCDF e o CBMDF proporcionando a visualização rápida e uma transparência efetiva.

De igual forma, foi sugerido um fluxo para a comunicação de incidente em proteção de dados. Tendo conhecimento da organização, e com o suporte com estudos comparados, faz-se necessário que o Subcomitê Executivo promova esta comunicação, sob pena de sanções administrativas por parte da ANPD.

Por fim, tratou-se de sugerir uma efetiva comunicação com os titulares de dados pessoais, pois os dados apresentados não permitiram concluir que existem ou se é eficiente. A LGPD expressamente determina que exista uma comunicação efetiva com o titular dos dados, transmitindo, dentre outras, a finalidade, a adequação, necessidade. A pesquisa concluiu que não existe esta comunicação, nem qualquer artefato que oriente o interessado ou que trate de um fluxo comunicacional.

Em sede de conclusão, esta pesquisa possibilitará, além de outros trabalhos, uma melhor adequação à LGPD por parte da PMDF. Ademais, espera-se que possa ser utilizado como objeto de estudos ou comparativos no âmbito do GDF para que outras instituições possam investigar e promover a boa governança em proteção de dados pessoais na administração pública.

# REFERÊNCIAS

REFERÊNCIAS

## REFERÊNCIAS


ALCANTARA, Douglas Siviotti; JÚNIOR, Ednaldo Lúcio dos Santos. Mapeamento dos tratamentos de dados pessoais. *In*: **Governança em privacidade e proteção de dados: uma visão integrada aos negócios empresariais**. Curitiba-PR, Editora Casa Editorial, 2022.

ALMEIDA, Ursula Ribeiro de. **A proteção de dados pessoais na Constituição: o impacto da EC 115**. Disponível em: https://www.conjur.com.br/2022-fev-27/almeida-protecao-dados-pessoais-constituicao-ec-115/. Acessado em: 05 de maio de 2024.

ARTESE, Gustavo. Compliance digital e privacidade. *In*: **Manual de compliance**. Rio de Janeiro, Editora Forense, 2020.

ASSI, Marcos. **Compliance: como implementar**. São Paulo, editora Trevisan, 2018.

BARROSO, Luis Roberto. Neoconstitucionalismo e constitucionalização do Direito / Neoconstitutionalism and constitutionalization of the Law. **REVISTA QUAESTIO IURIS**, *[S. l.]*, v. 2, n. 1, p. 1–48, 2014. Disponível em: https://www.e-publicacoes.uerj.br/quaestioiuris/article/view/11641. Acesso em: 10 jun. 2024.

BARROSO, Luís Roberto. Judicialização, Ativismo Judicial e Legitimidade Democrática. **(SYN)THESIS**, *[S. l.]*, v. 5, n. 1, p. 23–32, 2012. Disponível em: https://www.e-publicacoes.uerj.br/synthesis/article/view/7433. Acesso em: 7 jun. 2024.

BENJAMIN, Antônio; MARQUES, Claudia; BESSA, Leonardo. **Manual de direito do consumidor**. 3ª ed. Editora revista dos Tribunais, São Paulo, 2010.

BERTOCCELLI, Rodrigo de Pinho. Compliance. *In*: **Manual de Compliance**. 2ª edição, Rio de Janeiro, Editora Forense, 2020.

BOBBIO, Norberto. **A era dos direitos**. Rio de Janeiro, editora Elsevier, 2004.

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

BRASIL. Guia de boas práticas. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf.

BRASIL. Acórdão n° 1384/2022, processo TC- TCU 039.606/2020-1. Disponível em: https://portal.tcu.gov.br/data/files/B4/25/78/27/D9C818102DFE0FF7F18818A8/038.172-2019-4-AN%20-%20auditoria_Lei%20Geral%20de%20Protecao%20de%20Dados.pdf. Acessado em 15 de setembro de 2023.

CALSING, Renata de Assis. Proteção de dados pessoais e autoridade de controle: perspectivas e desafios para o Brasil sob a ótica do direito comparado. Programa de pós-doutoramento em Direito. Disponível em https://repositorio.cgu.gov.br/handle/1/66225. Acessado em 18 de junho de 2024.

CASTELLS, Manuel. A sociedade em rede. Editora Paz&Terra, volume 1, 24ª Edição, Rio de Janeiro – RJ, 2022.

CAVALCANTE, Pedro. Transformações contemporâneas no estado brasileiro: macrorreformas ou inovações incrementais na era da governança. *In*: **Reformas do Estado no Brasil: trajetórias, inovações e desafios**. Editora Cepal, Rio de Janeiro, 2020.

DELEUZE, Gilles. Post-Scriptum sobre as sociedades de controle. *In*: L'Autre Journal, n° 1, 1990. Disponível em: https://historiacultural.mpbnet.com.br/pos-modernismo/Post-Scriptum_sobre_as_Sociedades_de_Controle.pdf.

DISTRITO FEDERAL. Decreto n° 42.036 de 27 de abril de 2021. Disponível em: https://www.sinj.df.gov.br/sinj/Norma/551e54f29493499ca4201ef5e6f7ab35/Decreto_42036_27_04_2021.html.

DISTRITO FEDERAL. Portaria PMDF n° 1279, de 23 de junho de 2022. Disponível em: https://intranet.pmdf.df.gov.br/controleLegislacao2/PDF/3749.pdf.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais [livro eletrônico]: elementos da formação da Lei Geral de Proteção de Dados, 2ª edição, São Paulo: Thomson Reuters Brasil, 2020.

DUARTE, Daniel Edler. Estudo de vigilância. *In*: **Coleção Panorama**, 2023. Disponível em: https://drive.google.com/file/d/1HUsoSQcbqkk91J48zKNMNAsE6ezDo1Wn/view. Acesso no dia: 17 de julho de 2024.

FACHIN, Zulmar. DESAFIOS DA REGULAÇÃO DO CIBERESPAÇO E A PROTEÇÃO DOS DIREITOS DA PERSONALIDADE. **Revista Jurídica (FURB)**, *[S. l.]*, v. 25, n. 56, p. e10081, Disponível em: https://ojsrevista.furb.br/ojs/index.php/juridica/article/view/10081. Acesso em: 15 jul. 2024.

FERNANDES, Bernardo Gonçalves. **Curso de direito constitucional**. 5ª edição, editora juspodium, Salvador, 2013.

FILHO, Eduardo Tomasevicius. *In:* **Estudos avançados**. Marco Civil da Internet. Uma lei sem conteúdo normativo. Disponível em: https://www.scielo.br/j/ea/a/n87YsBGnphdHHBSMpCK7zSN/?format=pdf&lang=pt#:~:text=O%20texto%20do%20Marco%20Civil,e%20que%20colabora%C3%A7%C3%A3o%20se%20pretende. Acesso em: 10 de julho de 2024.

FONTOURA, Antônio Bazzanella; RODRIGUES, Rosemberg Augusto Pereira. Direitos do titular: estabelecendo uma comunicação efetiva com o titular de dados pessoais. In: Governança em privacidade e proteção de dados: uma visão integrada aos negócios empresariais. Curitiba, editorial Casa, 2022.

FRANÇA, Ana Cristina Limongi. Comportamento organizacional: conceitos e práticas. São Paulo, editora Saraiva, 2006.

GARBACCIO, G. L.; VADELL, L.-M. B.; TORCHIA, B. Principais disposições da governança em privacidade à luz da Lei Geral de Proteção de Dados no Brasil. **Revista Justiça do Direito**, *[S. l.]*, v. 36, n. 1, p. 204-230, 2022. DOI: 10.5335/rjd. v36i1.13379. Disponível em: https://seer.upf.br/index.php/rjd/article/view/13379. Acesso em: 10 jun. 2024.

GARCIA, Fernanda; LIMA, Isabela de M. Bragança; KIYOHARA, Jefferson. Indicadores para avaliação do programa de compliance. In: Guia prático de compliance. 1ª edição, Rio de Janeiro, editora Forense, 2020.

GONÇALVES, Vitor Hugo Pereira. **Marco Civil da Internet comentado**. 1ª edição, Atlas, São Paulo, 2017.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 5ª ed. São Paulo, Atlas, 2008. Pdf.

GRIN, Eduardo José. A atuação do TCU no police making da administração pública federal: modernização gerencial ou expansão dos papéis do controle externo?. *In*: **Reformas do estado no Brasil: trajetórias, inovações e desafios**. Editora Cepal, Rio de Janeiro, 2020.

HARARI, Yuval Noah. **Uma breve história da humanidade sapiens**. Porto Alegre, editora L&PM, 2020.

HARARI, Yuval Noah. **21 lições para o século 21**. São Paulo, editora Companhia das letras, 2018.

AKATOS, E. M., MARCONI, M. A. **Fundamentos de metodologia científica.** 7ed. São Paulo: Atlas, 2010.

LEAL, Rogério Gesta. Controle de Integridade e Administração Pública: Sinergias Necessárias. In: Sequência, n° 86, p. 148-169, dez.2020. Disponível em: https://www.scielo.br/j/seq/a/Pjw5xbscsJh5n5x7YcK5z6P/.

LEMES, Mariana Carolina. Governança (disciplinar) algorítmica. Revista de Direito Governança e Novas Tecnologias; 2021. Disponível em https://www.researchgate.net/publication/354050689_GOVERNANCA_DISCIPLINAR_ALGORITMICA. Acessado em 16 de julho de 2024.

LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de. Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. *In*: **Revista de direito**, 2020. Disponível em: file:///C:/Users/user/Downloads/admin1,+15%20(4).pdf.

MARTINS, Humberto Falcão; MARINI, Caio. Governança Pública Contemporânea: uma tentativa de dissecação conceitual. **Revista do TCU**, Brasília, n. 130, p. p. 42–53, 2014. Disponível em: https://revista.tcu.gov.br/ojs/index.php/RTCU/article/view/40. Acesso em: 15 jun. 2025.

MATIAS-PEREIRA, José. **Manual de gestão pública contemporânea**. 6ª edição, São Paulo, editora Atlas, 2020.

MATHIAS, Maria Isabel da Cunha. OCDE e governança pública: o Brasil está apto para integrar a organização?. *In*: **Boletim de economia e política internacional**; n° 28, 2020. Disponível em: https://repositorio.ipea.gov.br/bitstream/11058/10544/1/bepi_28_ocde.pdf.

MAGACHO, Bruna Toledo Piza; TRENTO, Melissa. LGPD e compliance na Administração Pública: o Brasil está preparado para um cenário em transformação contínua dando segurança aos dados da população? É possível mensurar os impactos das adequações necessárias no setor público? Quais mudanças culturais promover para a manutenção da boa governança?. *In*: **Revista brasileira de pesquisas jurídicas**. 2021.

MEDEIROS, Jeanine Lykawka. A atuação do Tribunal de Contas e as políticas públicas de saúde. *In*: **Revista Caderno Virtual**. Disponível em: file:///C:/Users/pericles.araujo/Downloads/7040-Texto%20do%20Artigo-22191-24124-10-20230514%20(1).pdf. Acessado em: 20 de agosto de 2024.

MEIRELES, Adriana Veloso. Privacidade no século 21: proteção de dados, democracia e modelos regulatórios. In: revista brasileira de ciências políticas, 2023. Disponível em: https://doi.org/10.1590/0103-3352.2023.41.265909.

MELLO, Breno Cesar de Souza. Inteligência artificial e a não neutralidade dos algoritmos sobre os "corpos dóceis". Revista das Faculdades Integradas Vianna Júnior. V. 12, 2021. Disponível em:file:///C:/Users/user/Downloads/776-Texto%20do%20artigo-1891-2565-10-20210901.pdf.

MENDES, Gilmar; COELHO, Inocêncio; BRANCO, Paulo. **Curso de Direito Constitucional**. 5ª edição, São Paulo, editora Saraiva, 2010.

MORAES, Alexandre de. **Direitos Humanos fundamentais**. 8ª edição, editora Atlas, São Paulo, 2007.

NEWSTROM, Jonh W. **Comportamento organizacional: o comportamento humano no trabalho**. São Paulo, Mcgraw-Hill, 2008.

NUNES, Pablo. Um Rio de olhos seletivos: uso de reconhecimento facial pela polícia fluminense. Rio de Janeiro, CESesc, 2022. Disponível em: https://drive.google.com/file/d/1Yn0mSEs6AeqaDZDuSjBdJO_WbuLuIEzn/view.

OCDE (2019), *O caminho para se tornar um setor público orientado por dados*, Estudos de governo digital da OCDE, OECD Publishing, Paris, https://doi.org/10.1787/059814a7-en

PARISER, Eli. O filtro invisível: o que a internet está escondendo de você. Editora Zahar, Rio de Janeiro, 2012.

PESCARMONA, Ana Carolina F. Iapichini; Crespo, Liana Irani A. Cunha; ALCANTARA, Eunice; PEREIRA, C. Carneiro. A importância do tone at

the top e os seus desafios na prática. *In*: **Guia Prático de Compliance**. Editora Forense, Rio de Janeiro, 2020.

PESSOA, João Pedro Seefeldt. **O efeito Orwell na sociedade em rede: cibersegurança, regime global de vigilância social e direito à privacidade no século XXI**. Porto Alegre, editora Fi, 2020.

PINHEIRO, Patrícia Peck. **Direito Digital**. 5ª edição, São Paulo, 2012.

PINHEIRO. Patrícia Peck. Proteção de dados pessoais: comentários à lei n° 13.709/2018. São Paulo, Saraiva, 2018.

ROS, Luciano da. Accountability legal e Corrupção. In: Revista CGU2595-668x; ano 2019. disponível em https://repositorio.cgu.gov.br/bitstream/1/44356/14/V11.n19_Accountability.pdf. Acessado em 10 de maio de 2025.

ROSA, Glaucio Monteiro. Privacidade e proteção de dados: uma abordagem histórica e evolucionista. *In*: **Governança em privacidade e proteção de dados: uma visão integrada aos negócios empresariais**. 1ª edição. Curitiba, Editora Casa, 2022.

SAAD-DINIZ, Eduardo. **Ética negocial e compliance: entre a educação executiva e a interpretação judicial**. São Paulo, editora Thomson Reuters, 2019.

SALAMA, Bruno Meyerhof. **Estudos em direito & economia: micro, macro e desenvolvimento**, 1ª edição, Curitiba, editora Virtual Gratuita, 2017.

SOUZA, Nadialice Francischini. Limites da intervenção do Estado nas relações de consumo. In: Seara jurídica, v.1, n.5, 2011. Disponível em: https://web.unijorge.edu.br/sites/searajuridica/pdf/anteriores/2011/1/searajuridica_2011_1_pag1.pdf. Acessado em 10 de junho de 2024.

SOARES PINTO, C. P. . Fatores Institucionais Para A Implementação Do Decreto De Governança (Decreto N° 9203/2017) Nas Entidades Da Administração Pública Federal Indireta. **Revista Debates em Administração Pública – REDAP**, *[S. l.]*, v. 4, n. 5, 2023. Disponível em: https://www.portaldeperiodicos.idp.edu.br/redap/article/view/7655. Acesso em: 17 mar. 2025.

SOUZA MELLO, B. C. de. Inteligência artificial e a não neutralidade dos algoritmos sobre os “corpos dóceis”. **Revista Vianna Sapiens**, *[S. l.]*, v. 12, n. 2, p. 24, 2021. DOI: 10.31994/rvs.v12i2.776. Disponível em:

https://www.viannasapiens.com.br/revista/article/view/776. Acesso em: 16 jul. 2024.

TAJRA, Sanmya Feitosa. Gestão estratégica na saúde: reflexões e práticas para uma administração voltada para a excelência. 3ª edição. Editora Iátria, São Paulo, 2009.

TEIXEIRA, Graziela Dias; SENA, Lucas; SILVA, Suylan de Almeida Midlej e. Governança pública e democracia: o papel da Controladoria Geral da União na promoção da Accountability Social. **Tempo Social**, São Paulo, Brasil, v. 36, n. 2, p. 171–202, 2024. DOI: 10.11606/0103-2070.ts.2024.216403. Disponível em: https://revistas.usp.br/ts/article/view/216403.. Acesso em: 13 maio. 2025.

VAINZOF, Rony. **Lei Geral de Proteção de Dados comentada**. 2ª edição, editora Revista dos Tribunais, São Paulo, 2019.

VIEIRA, Carolina Belli; BOAS, Ana Alice Vilas; ANDRADE, Rui Otávio Bernardes de; OLIVEIRA, Elias Rodrigues de. Motivação na Administração Pública: considerações teóricas sobre a aplicabilidade dos pressupostos das teorias motivacionais na esfera pública. *In*: **Revista ADMpg Gestão Estratégica**; v.4, n.1, 2011. Disponível em: https://www.admpg.com.br/revista2011/artigos/12.pdf.

# APÊNDICES

APÊNDICES

# APÊNDICES

## APÊNDICE I



POLÍCIA MILITAR
DISTRITO FEDERAL

Governo do Distrito Federal
Polícia Militar do Distrito Federal
Gabinete do Comandante-Geral
Chefia da Assessoria Jurídico-Legislativa

Despacho – PMDF/GCG/AJL/CH

Brasília, 21 de novembro de 2024.

Ao Chefe de Gabinete do GCG

Assunto: Solicitação de informações para pesquisa acadêmica de Mestrado.

1. Ao tempo em que o cumprimento, solicito o encaminhamento do presente processo para o DEC/PMDF a fim de que seja analisado o formulário de pesquisa que o acompanha e, caso conveniente, direcionado ao Subcomitê Executivo de Proteção de Dados Pessoais da PMDF (Auditor da PMDF).

2. Trata-se de pesquisa institucional que fará parte da dissertação de mestrado (IDP) com o título "**ANÁLISE DO ÍNDICE DE ADEQUAÇÃO À PROTEÇÃO DE DADOS PELA POLÍCIA MILITAR DO DISTRITO FEDERAL À LUZ DO ACÓRDÃO N° 1.384/2022 DO TRIBUNAL DE CONTAS DA UNIÃO**" e que terá o escopo de investigar a adequação da Corporação à LGPD.

3. A pesquisa é composta por perguntas fechadas, e que foram aplicadas pelo TCU, mas que não foram respondidas pela PMDF naquele momento. Ademais, tendo em vista que o objetivo é de apenas coletar informações (sim/parcialmente/não) as opções de inclusão de documentos foram retiradas.

4. Neste sentido a pesquisa encontra-se no documento PDF (156684759) e, com a análise da área técnica de ensino, poderá seguir para aquele Subcomitê, para ser acessado pelo link (https://docs.google.com/forms/d/1NE9tcLKHg-tlB3zd1Kvpw-x09ivwNJwtkCfCtkbzOJo/edit).

5. No mais, quaisquer dúvidas podem ser solucionadas pelo telefone (whatsapp): (61) 981026920 - TC Péricles.

PÉRICLES QUEIROZ ARAÚJO - TC QOPM

Chefe da AJL/GCG e pesquisador (mestrando)

Documento assinado eletronicamente por **PERICLES QUEIROZ ARAUJO - TC QOPM, Matr.0050669-9, Chefe da Assessoria Jurídico-Legislativa**, em 21/11/2024, às 18:48, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

# ANEXO I

POLÍCIA MILITAR
DISTRITO FEDERAL

Governo do Distrito Federal
Polícia Militar do Distrito Federal
Divisão de Apoio Educacional e Pesquisa
Seção de Pesquisa

Parecer Técnico n.º 35/2024 - PMDF/DEC/DAEP/SP

1. Trata de solicitação para pesquisa Acadêmica de Mestrado do TC QOPM PÉRICLES QUEIROZ ARAÚJO, Chefe da AJL/GCG e pesquisador (mestrando), através do Despacho– PMDF/GCG/AJL/CH (156683111), no qual é solicitado a análise do formulário de pesquisa e seu posterior encaminhamento ao Subcomitê Executivo de Proteção de Dados Pessoais da PMDF (Auditoria da PMDF).

2. Tal formulário é parte da pesquisa institucional intitulada "ANÁLISE DO ÍNDICE DE ADEQUAÇÃO À PROTEÇÃO DE DADOS PELA POLÍCIA MILITAR DO DISTRITO FEDERAL À LUZ DO ACÓRDÃO N° 1.384/2022 DO TRIBUNAL DE CONTAS DA UNIÃO" fará parte de sua dissertação de mestrado (IDP), com escopo na adequação da PMDF à LGPD. **Importante salientar que esta pesquisa foi iniciada em 2021 pelo Tribunal de Contas da União/TCU e, naquela época, não foi respondida na sua totalidade pela PMDF, por isso as menções às datas nele expressas devem ser desconsideradas.**

3. Os questionamentos da pesquisa estão disponíveis neste processo no hiperlink 156684759 (Formulário), mas também estão disponíveis no Google Forms (**CLICAR AQUI**) para futura resposta do Subcomitê Executivo de Proteção de Dados Pessoais da PMDF.

4. Tal solicitação alinha-se ao disposto no Art. 413 da Portaria PMDF N° 1.109, DE 31 DE DEZEMBRO DE 2019, que Estabelece o Regulamento Geral de Educação (RGE) da Polícia Militar do Distrito Federal, *in verbis:*

> Art. 413 Admite-se, em prol do desenvolvimento científico, a realização de atos de pesquisa de outras instituições no âmbito da Corporação, desde que não afetem os valores institucionais, em especial a hierarquia e disciplina, segundo avaliação do órgão do DEC em cujas atribuições se encontre a responsabilidade pelo acompanhamento ou controle de pesquisas.
>
> § 1º A avaliação referida no caput será realizada por meio da análise do projeto e instrumentos de pesquisa.
>
> § 2º Somente será admitida a realização de pesquisa de caráter científico com integrantes da Corporação se o projeto de pesquisa tiver sido avaliado e aprovado por comitê de ética.
>
> § 3º A responsabilidade por conduzir a aplicação da pesquisa de outra instituição, devidamente aprovada, é do próprio pesquisador, sob orientação e articulação de órgão do DEC.
>
> § 4º Havendo relação próxima entre objeto de pesquisa e as atividades desenvolvidas na Corporação, a realização de atos de pesquisa externa será autorizada mediante **declaração do pesquisador de que cederá formalmente uma cópia de inteiro teor do trabalho final ao mesmo órgão que autorizou a**

5. Não foi verificada a necessidade de submissão a Comitê de Ética em Pesquisa, uma vez que o questionário demanda apenas dados secundários.

6. Quanto ao mérito da temática, ela se apresenta como de grande relevância para a PMDF e não afeta os valores institucionais.

7. Considerando os pontos acima mencionados, esta chefia é de **PARECER FAVORÁVEL** à realização da pesquisa. Cabe ressaltar ao pesquisador, que o mesmo deverá anexar ao processo **declaração do pesquisador de que cederá formalmente uma cópia de inteiro teor da dissertação de mestrado, quando finalizada, ao DEC.**



8. É o parecer.

## ANEXO II

POLÍCIA MILITAR
DISTRITO FEDERAL

Governo do Distrito Federal
Polícia Militar do Distrito Federal
Auditoria
Chefia da Auditoria Financeira

Despacho – PMDF/DCC/AUD/SAF/CH

Brasília, 03 de dezembro de 2024.

Assunto: Solicitação de informações para pesquisa acadêmica de Mestrado.

1. Ciente do Despacho–PMDF/GCG/AJL/CH (157614628);

2. Ao Major Igor e ao 2º Ten Wanderilo para responderem o questionário (156684759) solicitado em conformidade com o Doc. SEI/GDF nº 157543306.

Documento assinado eletronicamente por **JUCILENE GARCEZ PIRES - CEL QOPM, Matr.0050455-6, Auditor(a)**, em 03/12/2024, às 17:01, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

## ANEXO III QUESTIONÁRIO DO TCU

**2.1 A organização conduziu iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD?**

(sim/não/parcialmente)

**2.2 A organização elaborou plano de ação, plano de projeto ou documento similar para direcionar a iniciativa de adequação à LGPD?**

(sim/não)

**3.1 A organização conduziu iniciativa para identificar outros normativos, além da LGPD, que abrangem comandos relacionados à proteção de dados pessoais e que também devem ser respeitados?**

(sim/não)

**3.2 A organização identificou as categorias de titulares de dados pessoais com os quais se relaciona?**

(sim/não/parcialmente)

**3.3 A organização conduziu iniciativa para identificar os operadores que realizam tratamento de dados pessoais em seu nome?**

Sim (a iniciativa foi concluída e todos os operadores foram identificados) / Sim (a iniciativa foi concluída e a organização constatou que não há operadores que realizam tratamentos de dados pessoais em seu nome) / Parcialmente (a iniciativa ainda está em andamento) / Não (ainda não foi conduzida iniciativa para identificar os operadores)

**3.3.1 A organização adequou os contratos firmados com os operadores identificados de forma a estabelecer suas**

**responsabilidades e papéis com relação à proteção de dados pessoais?**

Sim (A organização adequou todos os contratos firmados com os operadores que foram identificados) / Parcialmente (A organização adequou os contratos firmados com alguns operadores que foram identificados) / Não (A organização não adequou os contratos firmados com os operadores que foram identificados).

**3.4 A organização avaliou se há tratamento de dados que envolva controlador conjunto?**

(sim/não)

**3.4.1 Caso exista controlador conjunto, os papéis e responsabilidades de cada um dos controladores estão definidos em contrato, acordo de cooperação ou instrumento similar?**

Sim (os papéis e responsabilidades de cada um dos controladores estão definidos em contrato, acordo de cooperação ou instrumento similar) / Parcialmente (há acordo de cooperação ou instrumento similar firmado, mas nem todos os papéis e responsabilidades de cada um dos controladores estão definidos) / Não se aplica (não há relação da organização com controlador conjunto) / Não (os papéis e responsabilidades de cada um dos controladores não estão definidos em contrato, acordo de cooperação ou instrumento similar)

**3.5 A organização identificou os processos de negócio que realizam tratamento de dados pessoais?**

Sim (todos os processos de negócio que realizam tratamento de dados pessoais foram identificados) / Parcialmente (alguns processos de negócio que realizam tratamento de dados pessoais foram identificados) / Não (ainda não foi conduzida iniciativa para identificar os processos de negócio que realizam tratamento de dados pessoais)

**3.5.1 A organização identificou quem são os responsáveis pelos processos de negócio que realizam tratamento de dados pessoais e que já foram identificados?**

Sim (a organização identificou os responsáveis por todos os processos de negócio que realizam tratamento de dados pessoais e que já foram identificados) / Parcialmente (a organização identificou os responsáveis por alguns dos processos de negócio que realizam tratamento de dados pessoais e que já foram identificados) / Não (a organização não identificou os responsáveis pelos processos de negócio que realizam tratamento de dados pessoais e que já foram identificados).

**3.6 A organização identificou quais são os dados pessoais tratados por ela?**

Sim (todos os dados pessoais tratados pela organização foram identificados) / Parcialmente (alguns dados pessoais tratados pela organização foram identificados) / Não (a organização não identificou os dados pessoais que são tratados por ela).

**3.6.1 A organização identificou os locais onde os dados pessoais identificados são armazenados?**

Sim (a organização identificou os locais onde são armazenados todos os dados pessoais que já foram identificados).

**3.7 A organização avaliou os riscos dos processos de tratamento de dados pessoais que foram identificados?**

(sim/não)

**4.1 A organização possui Política de Segurança da Informação ou instrumento similar?**

(sim/não)

**4.2 A organização possui Política de Classificação da Informação ou instrumento similar?**

(sim/não)

**4.2.1 A Política de Classificação da Informação** (ou instrumento similar) abrange diretrizes para a classificação de dados pessoais?

(sim/não)

**4.2.1.1 A Política de Classificação da Informação abrange diretrizes para identificar dados pessoais sensíveis e relacionados a crianças e adolescentes?**

(sim/não)

**4.3 A organização possui Política de Proteção de Dados Pessoais?**

(sim/não)

**4.4 A organização nomeou o encarregado pelo tratamento de dados pessoais?**

(sim/não)

**4.4.1 A nomeação do encarregado foi publicada em veículo de comunicação oficial?**

(sim/não)

**4.4.3 A identidade e as informações de contato do encarregado foram divulgadas na internet?**

(sim/não)

**4.4.2 Em qual setor da organização está lotado o encarregado?**

Auditoria / Controle Interno (compliance) / Jurídico / Outros / Ouvidoria Tecnologia da Informação

**5.1 A organização possui Plano de Capacitação que abrange treinamento e conscientização dos seus colaboradores em proteção de dados pessoais?**

(sim/não)

**5.1.1 O Plano de Capacitação considera que pessoas que exercem funções com responsabilidades essenciais relacionadas à proteção de dados pessoais devem receber treinamento diferenciado?**

(sim/não)

**5.2 Colaboradores da organização que estão diretamente envolvidos em atividades que realizam tratamento de dados pessoais receberam treinamentos relacionados ao tema?**

Sim (todos os colaboradores da organização que estão diretamente envolvidos em atividades que realizam tratamento de dados pessoais receberam treinamentos relacionados ao tema) / Parcialmente (alguns colaboradores da organização que estão diretamente envolvidos em atividades que realizam tratamento de dados pessoais receberam treinamentos relacionados ao tema) / Não (nenhum dos colaboradores da organização que estão diretamente envolvidos em atividades que realizam tratamento de dados pessoais receberam treinamentos relacionados ao tema).

**6.1 A organização identificou e documentou as finalidades das atividades de tratamento de dados pessoais?**

Sim (todas as finalidades das atividades de tratamento de dados pessoais foram identificadas e documentadas) / Parcialmente (algumas finalidades das atividades de tratamento de dados pessoais foram identificadas e documentadas) / Não (as finalidades das atividades de tratamento de dados pessoais ainda não foram identificadas e documentadas).

**6.1.1 A organização avaliou se coleta apenas os dados estritamente necessários para cumprir com as finalidades de tratamento de dados pessoais que foram identificadas?**

(sim/não)

**6.1.2 A organização avaliou se os dados pessoais são retidos (armazenados) durante o tempo estritamente necessário para cumprir com as finalidades de tratamento de dados pessoais que foram identificadas?**

(sim/não)

**6.2 A organização identificou e documentou as bases legais que fundamentam as atividades de tratamento de dados pessoais?**

Sim (as bases legais que fundamentam todas as atividades de tratamento de dados pessoais da organização foram definidas e documentadas) / Parcialmente (as bases legais que fundamentam algumas das atividades de tratamento de dados pessoais da organização foram definidas e documentadas) / Não (nenhuma base legal que fundamenta as atividades de tratamento de dados pessoais da organização foi definida e documentada)

**6.3 Há um registro (e.g.: inventário) instituído para consolidar informações relacionadas às características das atividades de tratamento de dados pessoais?**

(sim/não)

**6.4 A organização elaborou Relatório de Impacto à Proteção de Dados Pessoais?**

Sim (a organização elaborou Relatório de Impacto à Proteção de Dados Pessoais que abrange TODOS os processos de tratamento de dados pessoais que podem gerar riscos aos titulares) / Sim (a organização elaborou Relatório de Impacto à Proteção de Dados

Pessoais que abrange ALGUNS processos de tratamento de dados pessoais que podem gerar riscos aos titulares) / Não / Não se aplica (a organização não executa processo de tratamento de dados pessoais que pode gerar riscos às liberdades civis e aos direitos fundamentais dos titulares).

**6.4.1 A organização implementou controles para mitigar os riscos identificados por meio da elaboração do Relatório de Impacto de Proteção de Dados Pessoais?**

Sim (a organização implementou controles para mitigar todos os riscos identificados por meio da elaboração do Relatório de Impacto de Proteção de Dados Pessoais) / Parcialmente (a organização implementou controles para mitigar alguns riscos identificados por meio da elaboração do Relatório de Impacto de Proteção de Dados Pessoais) / Não (a organização não implementou controles para mitigar os riscos identificados por meio da elaboração do Relatório de Impacto de Proteção de Dados Pessoais).

**7.1 A organização possui Política de Privacidade?**

(sim/não)

**7.1.1 A Política de Privacidade está publicada na internet?**

(sim/não)

**7.2 Foram implementados mecanismos para atender os direitos dos titulares elencados no art. 18 da LGPD e aplicáveis à organização?**

Sim (foram implementados mecanismos para atender todos os direitos dos titulares elencados no art. 18 da LGPD e aplicáveis à organização) / Parcialmente (foram implementados mecanismos para atender alguns direitos dos titulares elencados no art. 18 da LGPD e aplicáveis à organização) / Não (não foram implementados

mecanismos para atender os direitos dos titulares elencados no art. 18 da LGPD)

**8.1 A organização identificou os dados pessoais são compartilhados com terceiros?**

Sim (os dados pessoais que são compartilhados com terceiros foram identificados) / Parcialmente (alguns dados pessoais que são compartilhados com terceiros foram identificados) / Não se aplica (a organização não realiza compartilhamento de dados pessoais com terceiros) / Não (não houve iniciativa para identificar dados pessoais que são compartilhados com terceiros)

**8.1.1 Os compartilhamentos de dados pessoais identificados estão em conformidade com os critérios estabelecidos na LGPD?**

Sim (os compartilhamentos de dados pessoais estão em conformidade com os critérios estabelecidos na LGPD) / Parcialmente (alguns compartilhamentos de dados pessoais estão em conformidade com os critérios estabelecidos na LGPD).

**8.1.2 A organização registra eventos relacionados à transferência dos dados pessoais que são compartilhados com terceiros e que foram identificados?**

Sim (a organização registra eventos relacionados à transferência de todos os dados pessoais que são compartilhados com terceiros e que foram identificados) / Parcialmente (a organização registra eventos relacionados à transferência de alguns dados pessoais que são compartilhados com terceiros e que foram identificados).

**8.1.3 Algum caso de compartilhamento envolve transferência internacional de dados pessoais?**

(sim/não)

**8.1.3.1 As transferências internacionais de dados pessoais estão de acordo com os casos previstos na LGPD?**

(sim/não)

**9.1 A organização possui Plano de Resposta a Incidentes que abrange o tratamento de incidentes que envolvem violação de dados pessoais?**

(sim/não)

**9.2 A organização possui sistema para o registro de incidentes de segurança da informação que envolvem violação de dados pessoais?**

(sim/não)

**9.3 A organização possui sistema para registro das ações adotadas para solucionar incidentes de segurança da informação que envolvem violação de dados pessoais?**

(sim/não)

**9.4 A organização monitora proativamente a ocorrência de eventos que podem ser associados à violação de dados pessoais?**

(sim/não)

**9.5 A organização estabeleceu procedimentos para comunicar à ANPD e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares?**

(sim/não)

**10.1 A organização é capaz de comprovar que adotou medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais?**

(sim/não)

**10.2 A organização implementou processo para registro, cancelamento e provisionamento de usuários em sistemas que realizam tratamento de dados pessoais?**

Sim (a organização implementou processo formal para registro, cancelamento e provisionamento de usuários em todos os sistemas que realizam tratamento de dados pessoais) / Parcialmente (a organização implementou processo formal para registro, cancelamento e provisionamento de usuários em alguns sistemas que realizam tratamento de dados pessoais) / Não (a organização não implementou processo formal para registro, cancelamento e provisionamento de usuários em sistemas que realizam tratamento de dados pessoais).

**10.3 A organização registra eventos das atividades de tratamento de dados pessoais?**

Sim (a organização registra os eventos de todas as atividades de tratamento de dados pessoais) / Parcialmente (a organização registra os eventos de algumas atividades de tratamento de dados pessoais) / Não (a organização não registra os eventos de atividades de tratamento de dados pessoais).

**10.4 A organização utiliza criptografia para proteger os dados pessoais?**

Sim (a organização utiliza criptografia para proteger todos os dados pessoais) / Parcialmente (a organização utiliza criptografia para proteger alguns dados pessoais) / Não (a organização não utiliza criptografia para proteger os dados pessoais)

**10.5 A organização adotou medidas para assegurar que processos e sistemas sejam projetados, desde a concepção, em conformidade com a LGPD (Privacy by Design e Privacy by Default)?**

(sim/não)

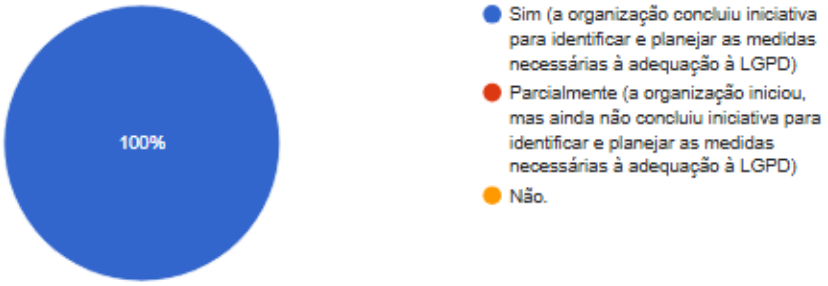
# ANEXO IV QUESTIONÁRIO TCU RESPONDIDO PELA PMDF

## 2. Preparação

2.1 A organização conduziu iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD?

Copiar gráfico

2 respostas




2.2 A organização elaborou plano de ação, plano de projeto ou documento similar para direcionar a iniciativa de adequação à LGPD?

Copiar gráfico

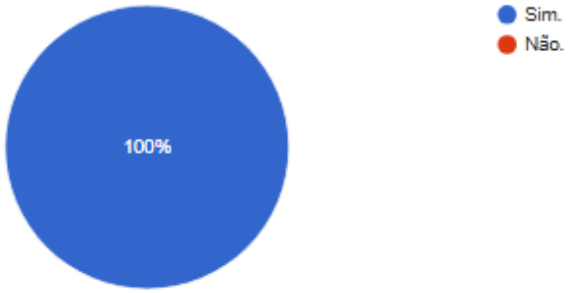
2 respostas

## 3. Contexto organizacional

3.1 A organização conduziu iniciativa para identificar outros normativos (e.g.: leis, regulamentos e instruções normativas), além da LGPD, que abrangem comandos relacionados à proteção de dados pessoais e que também devem ser respeitados?

Copiar gráfico

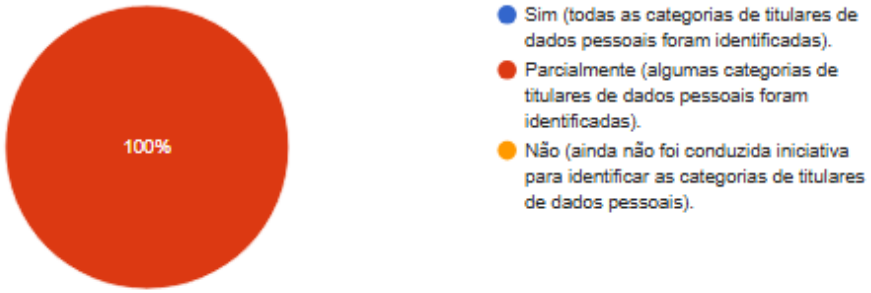
2 respostas




3.2 A organização identificou as categorias de titulares de dados pessoais com os quais se relaciona?

Copiar gráfico

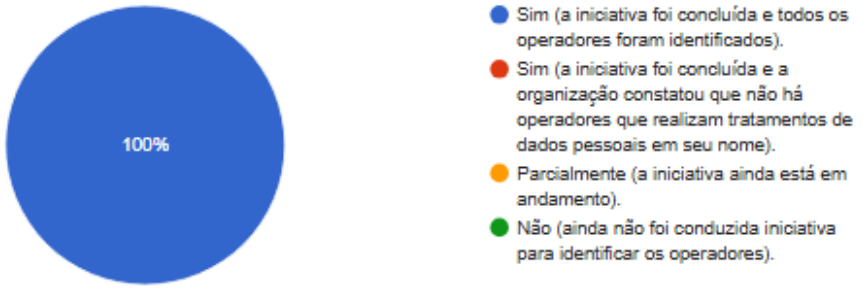
2 respostas



3.3 A organização conduziu iniciativa para identificar os operadores que realizam tratamento de dados pessoais em seu nome?

Copiar gráfico

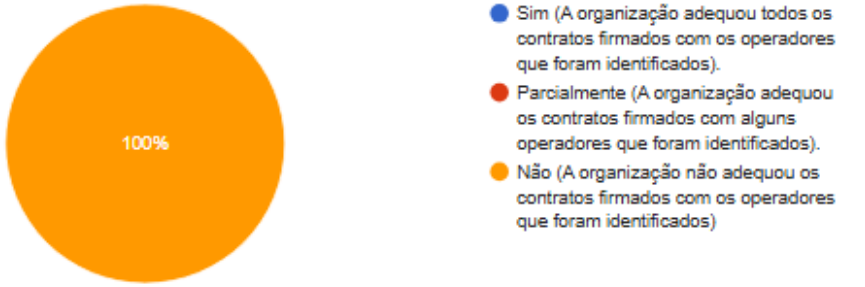
2 respostas




3.3.1 A organização adequou os contratos firmados com os operadores identificados de forma a estabelecer suas responsabilidades e papéis com relação à proteção de dados pessoais?

Copiar gráfico

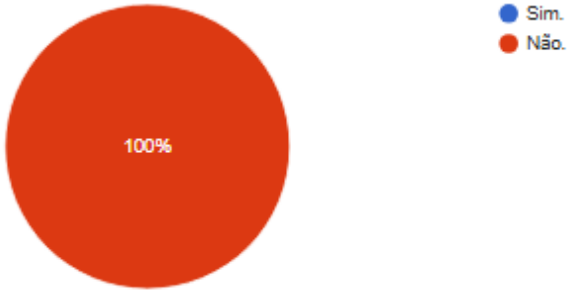
2 respostas



3.4 A organização avaliou se há tratamento de dados que envolva controlador conjunto?

Copiar gráfico

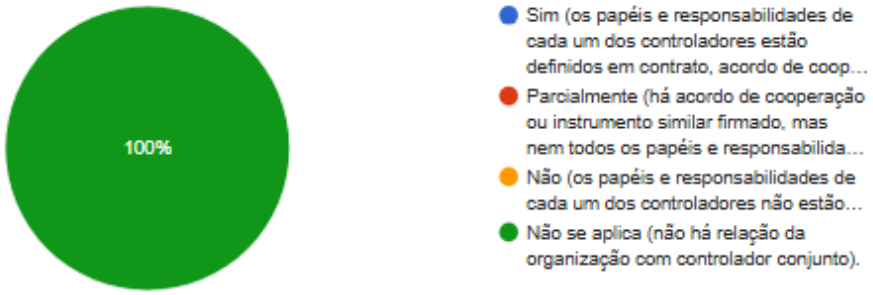
2 respostas




3.4.1 Caso exista controlador conjunto, os papéis e responsabilidades de cada um dos controladores estão definidos em contrato, acordo de cooperação ou instrumento similar?

Copiar gráfico

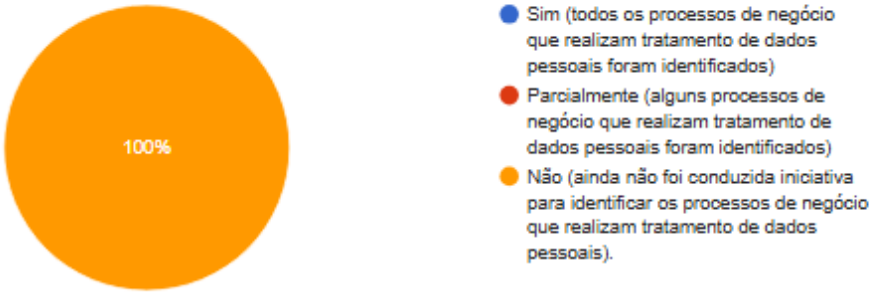
2 respostas



3.5 A organização identificou os processos de negócio que realizam tratamento de dados pessoais?

Copiar gráfico

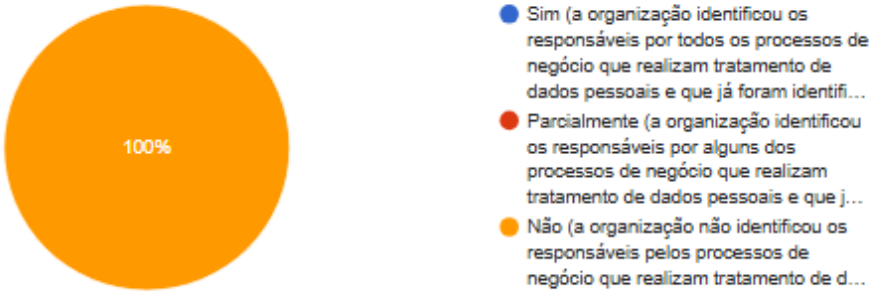
2 respostas




3.5.1 A organização identificou quem são os responsáveis pelos processos de negócio que realizam tratamento de dados pessoais e que já foram identificados?

Copiar gráfico

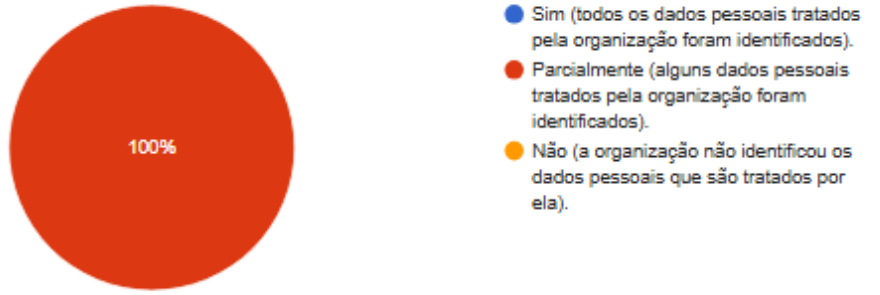
2 respostas



3.6 A organização identificou quais são os dados pessoais tratados por ela?

Copiar gráfico

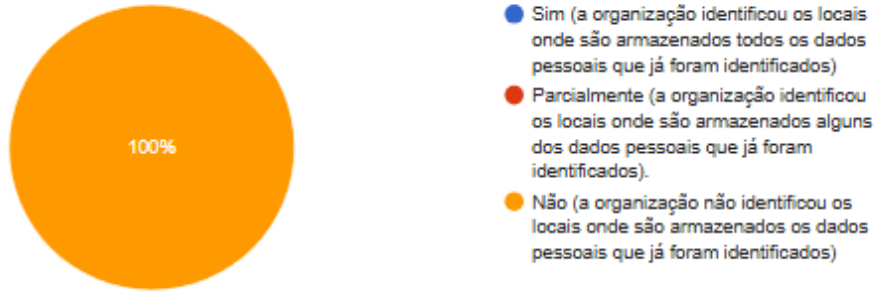
2 respostas




3.6.1 A organização identificou os locais onde os dados pessoais identificados são armazenados?

Copiar gráfico

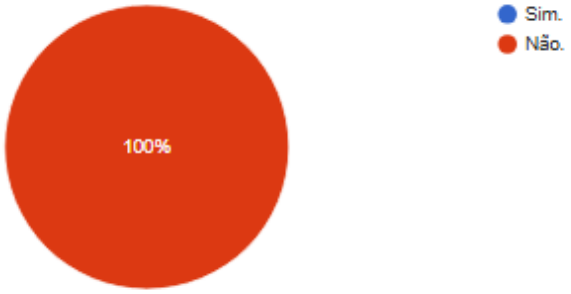
2 respostas



3.7 A organização avaliou os riscos dos processos de tratamento de dados pessoais que foram identificados?

Copiar gráfico

2 respostas

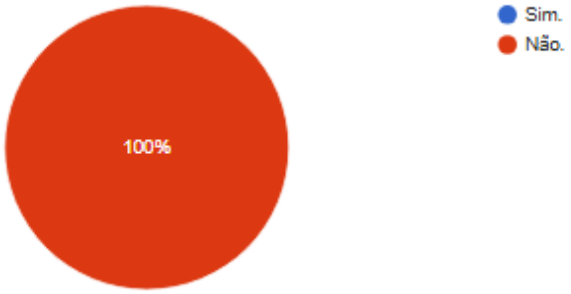



## 4. Liderança

4.1 A organização possui Política de Segurança da Informação ou instrumento similar?

Copiar gráfico

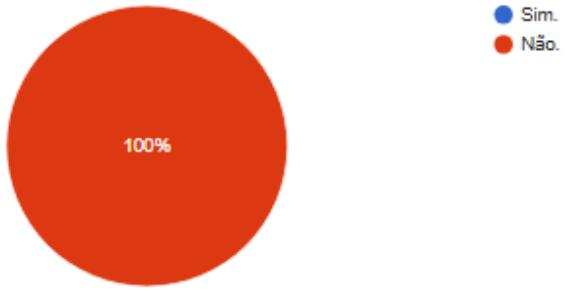
2 respostas



4.2 A organização possui Política de Classificação da Informação ou instrumento similar?

Copiar gráfico

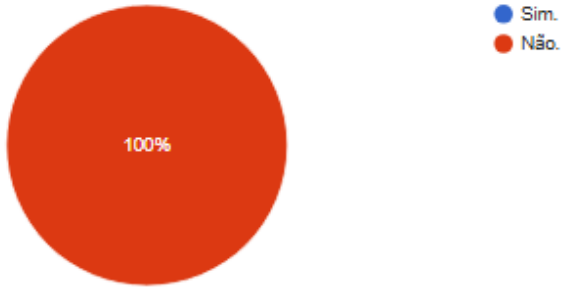
2 respostas




4.2.1 A Política de Classificação da Informação (ou instrumento similar) abrange diretrizes para a classificação de dados pessoais?

Copiar gráfico

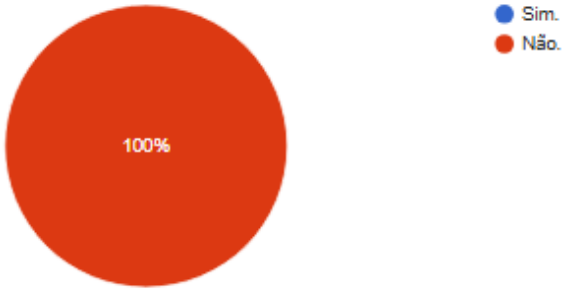
2 respostas



4.2.1.1 A Política de Classificação da Informação (ou instrumento similar) abrange diretrizes para identificar dados pessoais sensíveis e relacionados a crianças e adolescentes?

Copiar gráfico

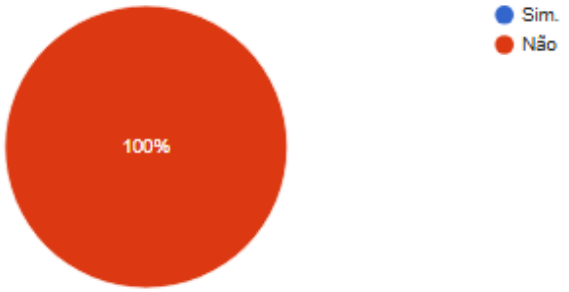
2 respostas




4.2.1.2 A Política de Classificação da Informação (ou instrumento similar) abrange diretrizes para identificar dados pessoais de crianças e de adolescentes?

Copiar gráfico

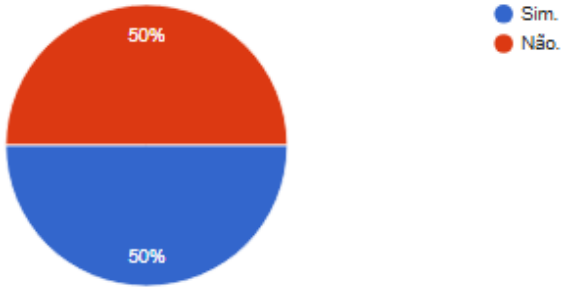
2 respostas



4.3 A organização possui Política de Proteção de Dados Pessoais (ou instrumento similar)?

Copiar gráfico

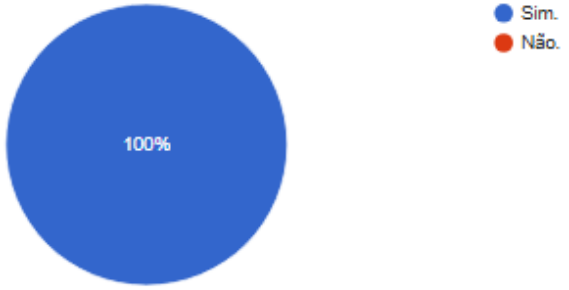
2 respostas




4.4 A organização nomeou o encarregado pelo tratamento de dados pessoais?

Copiar gráfico

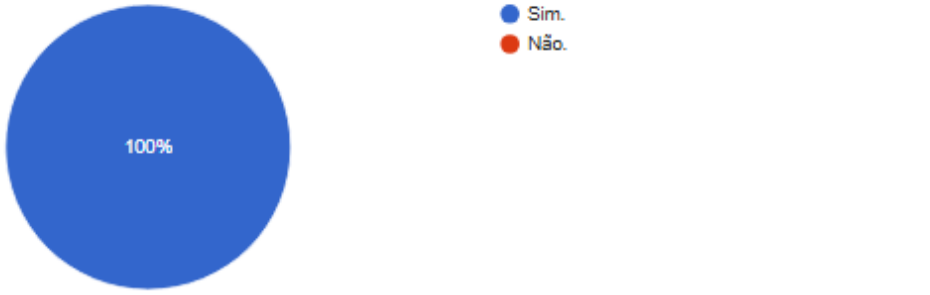
2 respostas



4.4.1 A nomeação do encarregado foi publicada em veículo de comunicação oficial?

Copiar gráfico

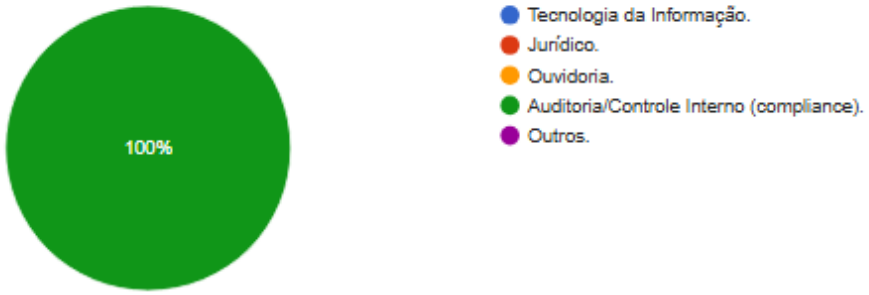
2 respostas




4.4.2 Em qual setor da organização está lotado o encarregado?

Copiar gráfico

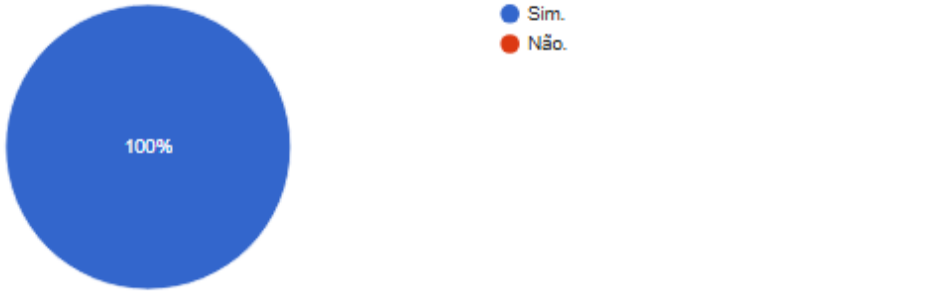
2 respostas




4.4.3 A identidade e as informações de contato do encarregado foram divulgadas na internet?

Copiar gráfico

2 respostas

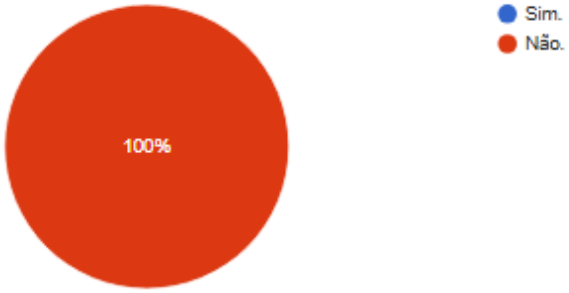


## 5. Capacitação

5.1 A organização possui Plano de Capacitação (ou instrumento similar) que abrange treinamento e conscientização dos seus colaboradores em proteção de dados pessoais?

Copiar gráfico

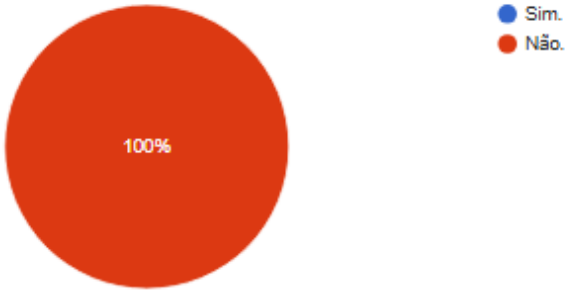
2 respostas




5.1.1 O Plano de Capacitação (ou instrumento similar) considera que pessoas que exercem funções com responsabilidades essenciais relacionadas à proteção de dados pessoais devem receber treinamento diferenciado?

Copiar gráfico

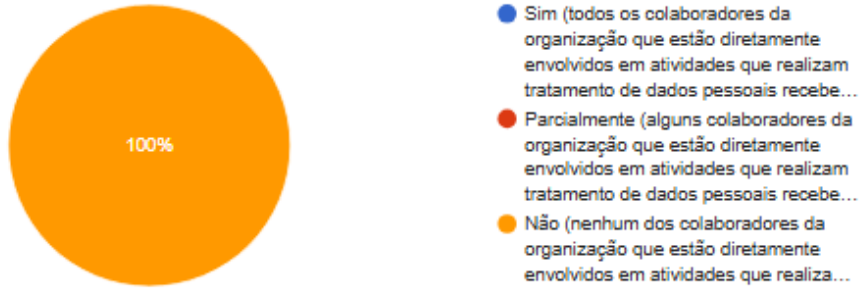
2 respostas



5.2. Colaboradores da organização que estão diretamente envolvidos em atividades que realizam tratamento de dados pessoais receberam treinamentos relacionados ao tema?

Copiar gráfico

2 respostas

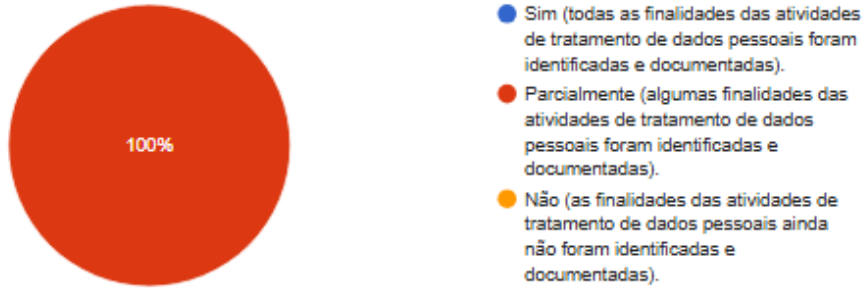



## 6. Conformidade do tratamento

6.1 A organização identificou e documentou as finalidades das atividades de tratamento de dados pessoais?

Copiar gráfico

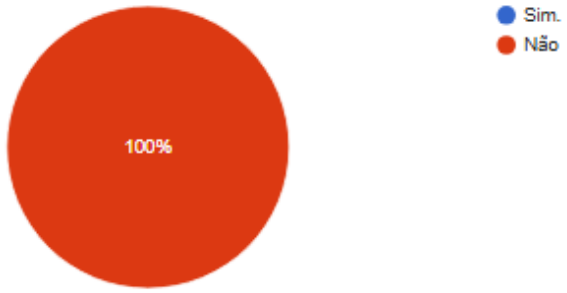
2 respostas



6.1.1 A organização avaliou se coleta apenas os dados estritamente necessários para cumprir com as finalidades de tratamento de dados pessoais que foram identificadas?

Copiar gráfico

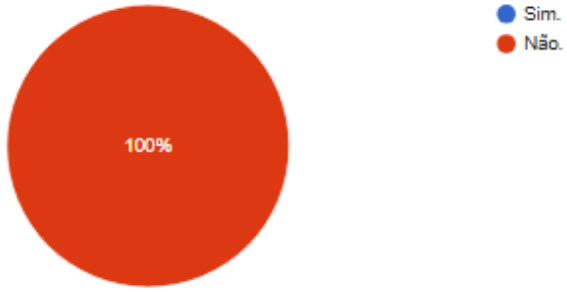
2 respostas




6.1.2 A organização avaliou se os dados pessoais são retidos (armazenados) durante o tempo estritamente necessário para cumprir com as finalidades de tratamento de dados pessoais que foram identificadas?

Copiar gráfico

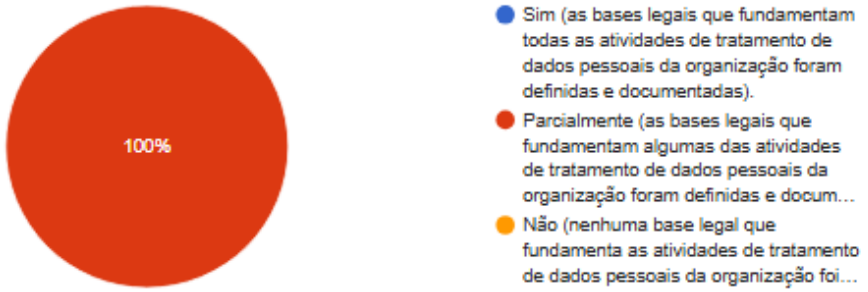
2 respostas



6.2 A organização identificou e documentou as bases legais que fundamentam as atividades de tratamento de dados pessoais?

Copiar gráfico

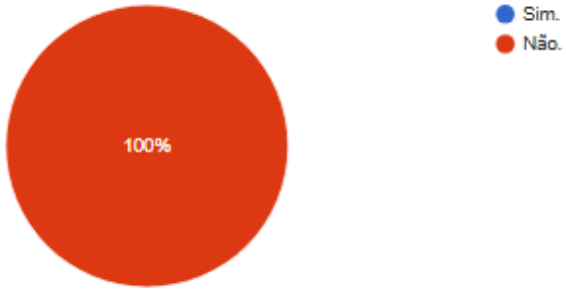
2 respostas




6.3 Há um registro (e.g.: inventário) instituído para consolidar informações relacionadas às características das atividades de tratamento de dados pessoais?

Copiar gráfico

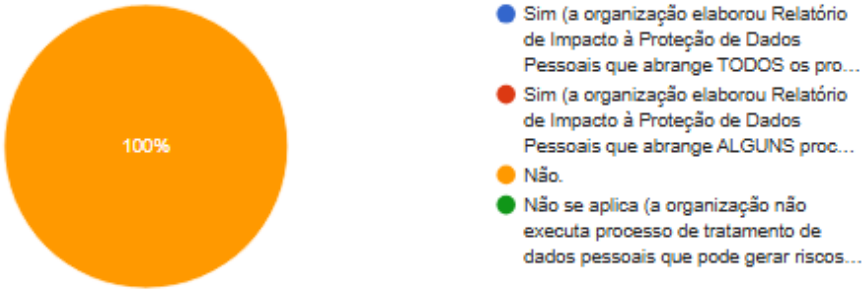
2 respostas



6.4 A organização elaborou Relatório de Impacto à Proteção de Dados Pessoais?

Copiar gráfico

2 respostas




6.4.1 A organização implementou controles para mitigar os riscos identificados por meio da elaboração do Relatório de Impacto de Proteção de Dados Pessoais?

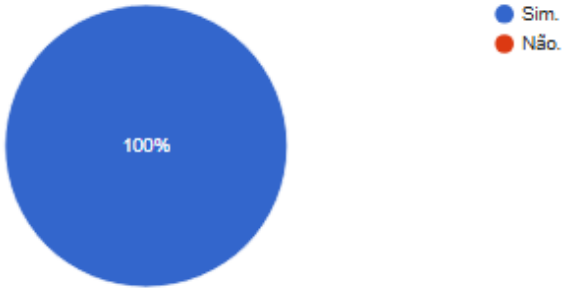
Copiar gráfico

2 respostas

## 7. Direitos do titular

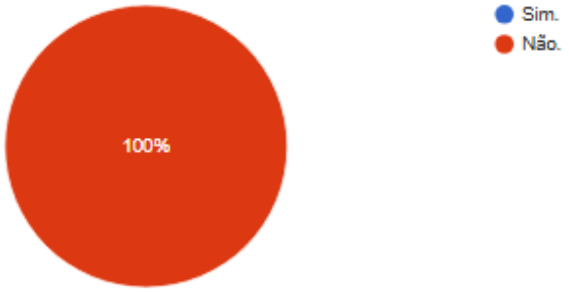
7.1 A organização possui Política de Privacidade (ou instrumento similar)? Copiar gráfico

2 respostas




7.1.1 A Política de Privacidade (ou instrumento similar) está publicada na internet? Copiar gráfico

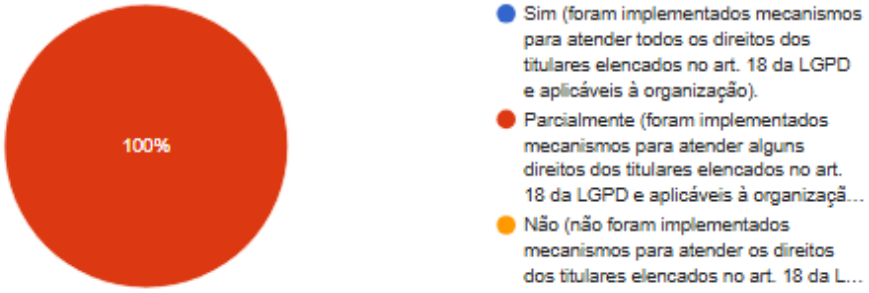
2 respostas



7.2 Foram implementados mecanismos para atender os direitos dos titulares elencados no art. 18 da LGPD e aplicáveis à organização?

Copiar gráfico

2 respostas

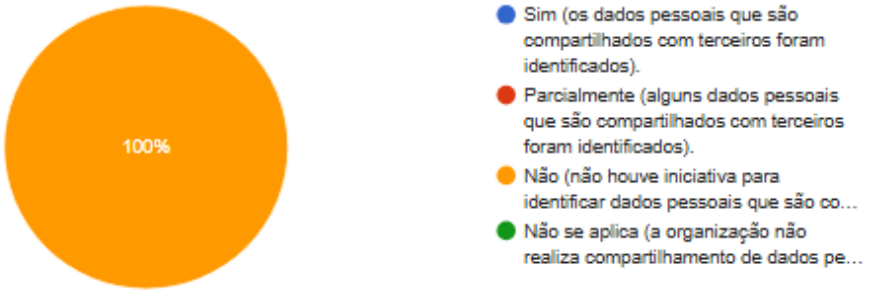



## 8. Compartilhamento de dados pessoais

8.1 A organização identificou os dados pessoais são compartilhados com terceiros?

Copiar gráfico

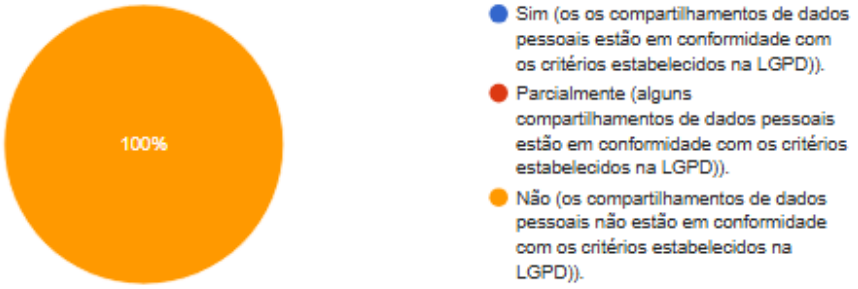
2 respostas



8.1.1 Os compartilhamentos de dados pessoais identificados estão em conformidade com os critérios estabelecidos na LGPD?

Copiar gráfico

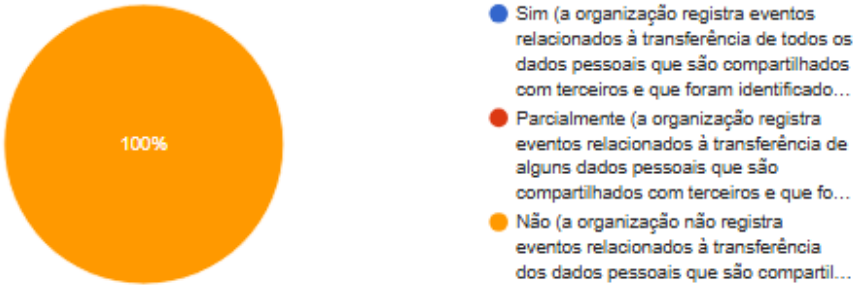
1 resposta




8.1.2 A organização registra eventos relacionados à transferência dos dados pessoais que são compartilhados com terceiros e que foram identificados?

Copiar gráfico

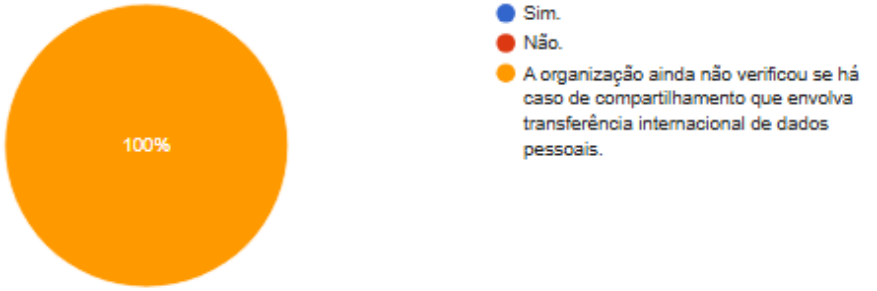
2 respostas



8.1.3 Algum caso de compartilhamento envolve transferência internacional de dados pessoais?

Copiar gráfico

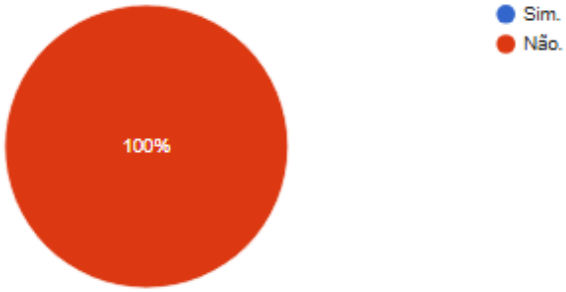
2 respostas




8.1.3.1 As transferências internacionais de dados pessoais estão de acordo com os casos previstos na LGPD?

Copiar gráfico

2 respostas

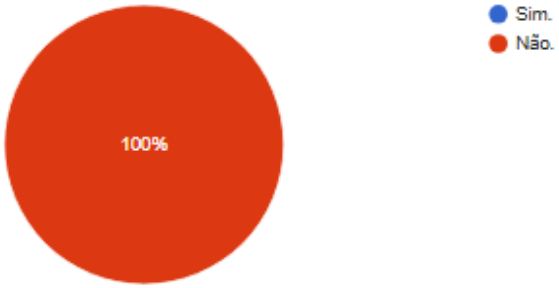


## 9. Violação de dados pessoais

9.1 A organização possui Plano de Resposta a Incidentes (ou documento similar) que abrange o tratamento de incidentes que envolvem violação de dados pessoais?

Copiar gráfico

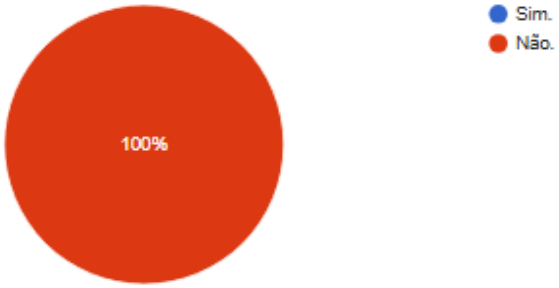
2 respostas




9.2 A organização possui sistema para o registro de incidentes de segurança da informação que envolvem violação de dados pessoais?

Copiar gráfico

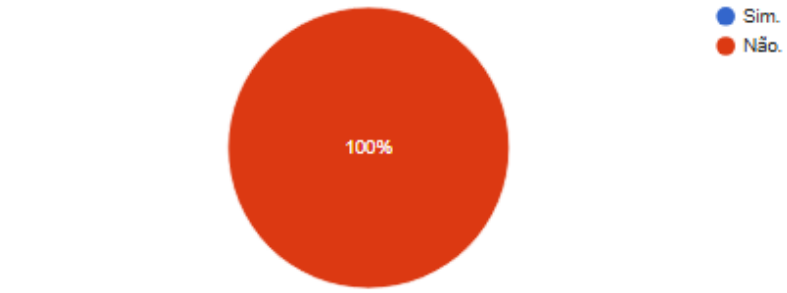
2 respostas



9.3 A organização possui sistema para registro das ações adotadas para solucionar incidentes de segurança da informação que envolvem violação de dados pessoais?

Copiar gráfico

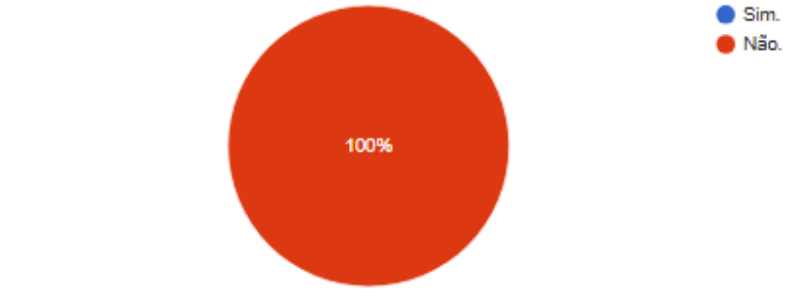
2 respostas




9.4 A organização monitora proativamente a ocorrência de eventos que podem ser associados à violação de dados pessoais?

Copiar gráfico

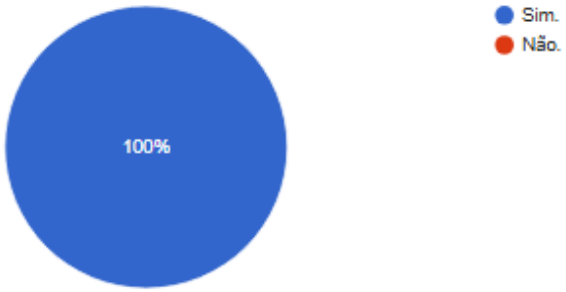
2 respostas



9.5 A organização estabeleceu procedimentos para comunicar à Autoridade Nacional de Proteção de Dados e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares?

Copiar gráfico

2 respostas

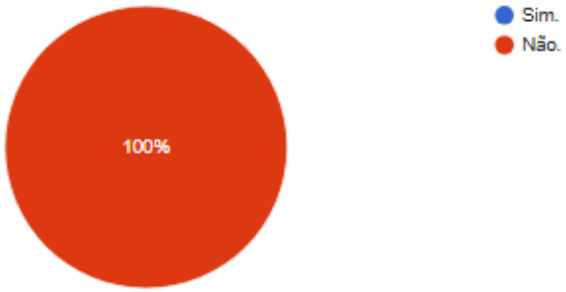



## 10. Medidas de proteção

10.1 A organização é capaz de comprovar que adotou medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais?

Copiar gráfico

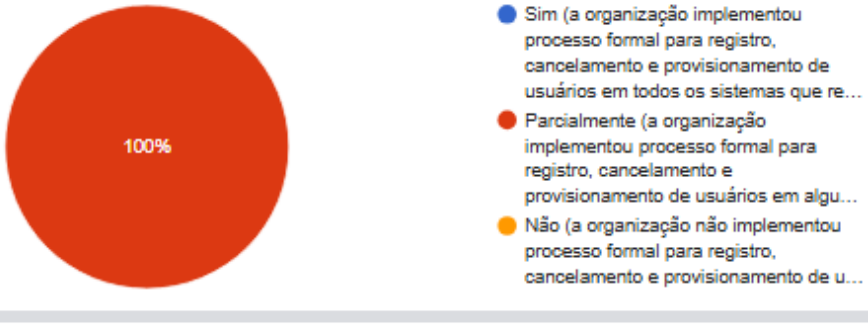
2 respostas



10.2 A organização implementou processo para registro, cancelamento e provisionamento de usuários em sistemas que realizam tratamento de dados pessoais?

Copiar gráfico

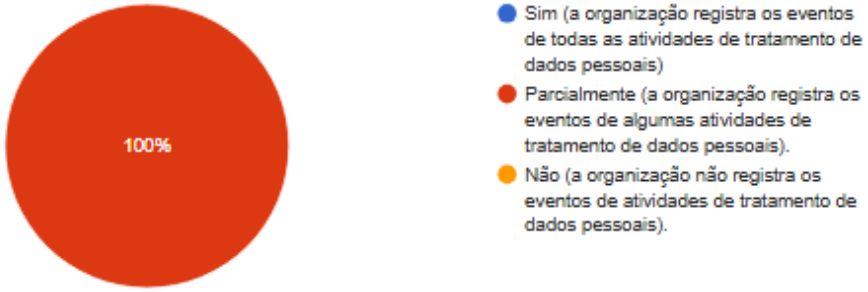
2 respostas




10.3 A organização registra eventos das atividades de tratamento de dados pessoais?

Copiar gráfico

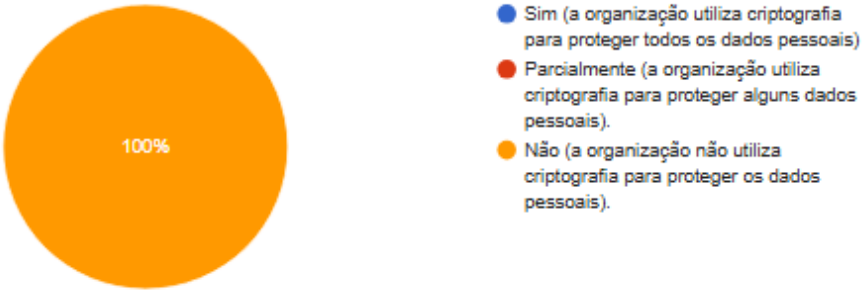
2 respostas



10.4 A organização utiliza criptografia para proteger os dados pessoais?

Copiar gráfico

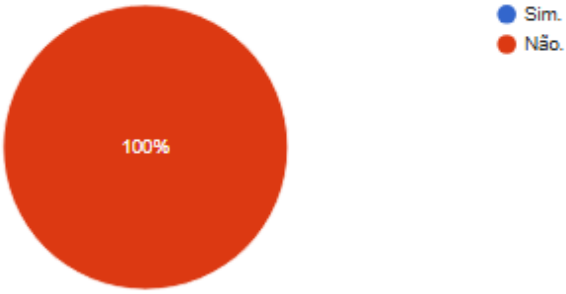
2 respostas




10.5 A organização adotou medidas para assegurar que processos e sistemas sejam projetados, desde a concepção, em conformidade com a LGPD (Privacy by Design e Privacy by Default)?

Copiar gráfico

2 respostas



## ANEXO V PORTARIA PMDF Nº 1279/2022

# PORTARIA Nº 1279/2022

**GOVERNO DO DISTRITO FEDERAL**

**POLÍCIA MILITAR DO DISTRITO FEDERAL**

**ESTADO-MAIOR**

*Aprova a Política de Proteção de Dados Pessoais – PPDP no âmbito do Polícia Militar do Distrito Federal e estabelece a aplicação dos preceitos da Lei federal nº 13.709, de 14 de agosto de 2018, concernente à Lei Geral de Proteção de Dados Pessoais e dá outras providências.*

**O COMANDANTE-GERAL DA POLÍCIA MILITAR DO DISTRITO FEDERAL,** no uso da competência, prevista no art. 4º da Lei Federal nº 6.450, de 14 de outubro de 1977, combinado com o inciso III do art. 8º do Decreto federal nº 10.443, de 28 de julho de 2020; tendo em vista o contido no art. 28 do Decreto distrital nº 42.036, de 27 de abril de 2021, que dispõe sobre a aplicação da Lei federal nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais; e

**Considerando** teor dos atos e documentos constantes do Processo SEI-GDF nº 00054-00058593/2020-66.

**RESOLVE:**

## CAPÍTULO I
## DA FINALIDADE

**Art. 1º** Aprovar a Política de Proteção de Dados Pessoais – PPDP, no âmbito da Polícia Militar do Distrito Federal – PMDF, em observância ao art. 28 do Decreto Distrital nº 42.036, de 27 de abril de 2021, que dispõe sobre a aplicação da Lei Federal nº 13.709, de 2018 – Lei Geral de Proteção de Dados Pessoais.

**Parágrafo único:** A PPDP estabelece princípios e regras que devem nortear o tratamento de dados pessoais, físicos e digitais na PMDF, a fim de garantir a proteção dos dados de seus titulares, define atribuições e diretrizes iniciais para a obtenção da gradual conformidade da PMDF ao previsto na Lei nº 13.709/2018 e no Decreto Distrital nº 42.036/2021, bem como cria e estabelece as diretrizes para a atuação do Comitê Gestor de Proteção de Dados Pessoais – CGPDP e do Subcomitê Executivo de Proteção de Dados Pessoais – SEPDP.

## CAPÍTULO II
## DOS CONCEITOS

**Art. 2º** Para o disposto nesta Portaria, considera-se:
**I –** política: definição de determinado objetivo da instituição e dos meios para atingi-lo;





**II –** programa: conjunto de mecanismos e procedimentos administrados de forma integrada, reunidos em documento único, no qual são previstas ações articuladas e dinâmicas para atingir determinado objetivo;
**III –** público interno: policiais militares, assemelhados, servidores civis e colaboradores, assim compreendidos os estagiários e os terceirizados;
**IV –** público externo: usuários dos serviços do PMDF e todos os que, de alguma forma, estabeleçam relações com a corporação;
**V –** privacidade: esfera íntima ou particular do indivíduo;
**VI –** pessoa física: pessoa natural;
**VII –** titular: pessoa física a quem se referem os dados pessoais objeto de tratamento;
**VIII –** dado pessoal: informação relativa à pessoa física identificada ou identificável;
**IX –** dado pessoal sensível: informação biométrica ou sobre origem racial ou étnica, saúde, vida sexual, convicção religiosa, opinião política, filiação a sindicato ou a organização religiosa, filosófica ou política;
**X –** dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
**XI –** banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
**XII –** tratamento dos dados: qualquer atividade pertencente ao ciclo de vida dos dados pessoais;
**XIII –** ciclo de vida dos dados: todas as etapas de manuseio dos dados, desde o surgimento destes na instituição até o respectivo descarte ou o arquivamento;
**XIV –** consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
**XV –** anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
**XVI –** transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;
**XVII –** Autoridade Nacional de Proteção de Dados Pessoais – ANPD: órgão vinculado à

Presidência da República, ao qual caberá, dentre outras atribuições, fiscalizar a aplicação da LGPD nas entidades do poder público e aplicar sanções em caso de descumprimento de suas determinações;
**XVIII –** controlador: pessoa jurídica de direito público a quem compete definir todas as ações relativas ao tratamento dos dados pessoais;
**XIX –** unidade gestora: ambiente sob o qual o controlador tem competência de atuação;
**XX –** representante do controlador: autoridade máxima titular de cada órgão ou entidade do Distrito Federal que atua como representante do seu respectivo Controlador perante os órgãos de controle;
**XXI –** operador: pessoa física que realiza o tratamento em nome do controlador, em todas as instâncias da instituição ou no âmbito de contratos ou instrumentos congêneres firmados com ele;
**XXII –** operadores internos: chefes das unidades de tecnologia da informação e comunicação ou unidades equivalentes responsáveis por bancos de dados, tecnologia da informação e sistemas de cada unidade gestora;
**XXIII –** operadores externos: pessoas físicas ou jurídicas prestadores de serviço de banco de dados, tecnologia da informação e sistemas que atuam fora da estrutura organizacional da unidade gestora;
**XXIV –** agentes de tratamento: o controlador e os operadores;
**XXV –** encarregado governamental: pessoa física, lotada na Casa Civil do Distrito





Federal, que atua como canal de comunicação entre os Encarregados Setoriais, os Controladores e a Autoridade Nacional de Proteção de Dados;
**XXVI –** encarregado setorial: pessoa física que atua como canal de comunicação entre o Controlador, os titulares dos dados e o Encarregado Governamental dentro da unidade gestora;
**XXVII –** sub-operador: a pessoa física que, no âmbito da PMDF, operacionaliza o tratamento de dados conforme estabelecido pelo Operador, nos limites de sua competência.

## CAPÍTULO III

## DOS PRINCÍPIOS

**Art. 3º** Deverão ser considerados os seguintes princípios no tratamento de dados pessoais e em todas as ações relativas a ele:
**I –** boa-fé: convicção de agir com correção e em conformidade com o Direito;
**II –** finalidade: o tratamento dos dados deve possuir propósitos legítimos, específicos, explícitos e informados;
**III –** adequação: o tratamento dos dados deve ser compatível com a finalidade pela qual são
tratados;
**IV –** necessidade: limitação do tratamento ao mínimo necessário para o alcance da finalidade,
considerados apenas os dados pertinentes, proporcionais e não excessivos;
**V –** livre acesso: garantia aos titulares de consulta facilitada e gratuita sobre a forma e a duração do tratamento de seus dados pessoais bem como sobre a integralidade deles;
**VI –** qualidade dos dados: garantia aos titulares de exatidão, clareza, relevância e atualização dos dados de acordo com a necessidade e para o cumprimento da finalidade do respectivo tratamento;
**VII –** transparência: garantia aos titulares de informações claras, precisas e acessíveis sobre o
tratamento de seus dados pessoais e sobre os agentes de tratamento;
**VIII –** segurança e prevenção: utilização de medidas técnicas e administrativas que garantam a
proteção dos dados pessoais contra acessos não autorizados e a prevenção contra situações
acidentais ou ilícitas que gerem destruição, perda, alteração, comunicação ou difusão desses dados;
**IX –** não discriminação: vedação de realizar o tratamento de dados pessoais para fins discriminatórios, ilícitos ou abusivos;
**X –** responsabilização e prestação de contas: demonstração de que os agentes de tratamento da instituição são responsáveis por este e adotam medidas eficazes para o cumprimento das normas de proteção dos dados pessoais.

# CAPÍTULO IV
# DOS AGENTES DE TRATAMENTO, DO ENCARREGADO SETORIAL E DOS COLEGIADOS



## Seção I
## Dos Agentes de Tratamento

**Art. 4º** Para os fins da presente portaria, consideram-se Agentes de Tratamento o Controlador e os Operadores.
**Art. 5º** Os agentes de tratamento ficam sujeitos às sanções previstas na Lei nº 13.709/2018, aplicáveis pela autoridade nacional.
**Parágrafo único.** Os agentes que não se enquadrarem como agentes de tratamento de dados poderão ser responsabilizados cível, penal e administrativamente.
**Art. 6º** Para todos os efeitos previstos na Lei Geral de Proteção de Dados, no âmbito da PMDF, o Representante do Controlador é o Comandante-Geral.
**Parágrafo único.** O Subcomandante-Geral é o Representante Adjunto do Controlador, que responderá nos afastamentos legais e impedimentos do Representante do Controlador.
**Art. 7º** Compete ao Representante do Controlador:
**I –** controlar e gerir a atividade de tratamento de dados;
**II –** fornecer as instruções para a política de proteção de dados pessoais e respectivos programas;
**III –** determinar a capacitação dos Operadores, para que atuem com responsabilidade, critério e ética;
**IV –** fiscalizar a observância pelos Operadores das instruções e das normas sobre a matéria;
**V –** nomear o Encarregado Setorial titular e suplente e informar ao Encarregado Governamental seus nomes e informações de contato;
**VI –** obter o consentimento específico do titular, quando necessário;
**VII –** instrumentalizar a portabilidade dos dados;
**VIII –** garantir a transparência no tratamento de dados;
**IX –** manter o registro das operações de tratamento de dados pessoais;
**X –** comunicar ao Encarregado Governamental, à Autoridade Nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, nos termos do art.48 da Lei nº 13.709/2018;
**XI –** incentivar a disseminação da cultura da privacidade de dados pessoais na corporação;
**XII –** determinar a contínua atualização desta Política e o desenvolvimento dos respectivos programas.

**Art. 8º** Para os fins a que se destina a presente portaria, são considerados os Operadores Interno e Externos da PMDF:
**I –** Operadores Internos: o Diretor da Diretoria de Telemática, o Chefe do Centro de Inteligência e o Corregedor-Geral;
**II –** Operadores Externos: pessoas físicas ou jurídicas que exerçam atividade de tratamento de dados pessoais na Corporação, bem como os terceiros com vínculos materializados por contratos administrativos e instrumentos congêneres firmados com a PMDF.
**Art. 9º** Compete aos Operadores (interno e externo):
**I –** realizar o tratamento de dados pessoais segundo as instruções fornecidas pelo Representante do Controlador e pelo Encarregado Setorial cujas competências encontram-se nesta portaria;
**II –** manter os dados pessoais protegidos de acesso não autorizado, divulgação, destruição, perda acidental ou qualquer tipo de violação de dados pessoais;
**III –** manter registros das operações de tratamentos de dados pessoais que realizar;





**IV –** observar as boas práticas e padrões de Governança previstos na LGPD;
**V –** comunicar ao Encarregado Setorial a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, nos termos da LGPD;
**VI –** quando autorizado pelo Representante do Controlador ou pelo Encarregado Setorial, e no pleno exercício de sua capacidade técnica, decidir sobre:
**a)** sistema, método ou ferramentas utilizadas para coletar os dados pessoais;
**b)** meios utilizados para transferir os dados pessoais de uma organização para outra;
**c)** métodos utilizados para recuperar dados pessoais de determinados indivíduos;
**d)** maneira de garantir que o método por trás do cronograma de retenção seja respeitado;
**e)** meio de garantir a segurança dos dados;
**f)** método de armazenamento de dados pessoais;
**VII –** capacitarem-se para exercer as atividades que envolvam dados pessoais com eficiência, ética, critério e responsabilidade.

## Seção II

## Do Encarregado Setorial

**Art. 10°** O Encarregado Setorial será o Auditor da PMDF, que se reportará ao Representante do Controlador e ao Encarregado Governamental, quando necessário.
**Parágrafo único.** O Encarregado Setorial Suplente será o Corregedor Adjunto da PMDF, competindo-lhe substituir o titular em seus afastamentos legais e impedimentos.
**Art. 11°** Compete ao Encarregado Setorial:
**I –** orientar os Operadores internos e externos a respeito das boas práticas e padrões de Governança de dados e segurança da informação, a serem tomadas em relação à proteção de dados pessoais, conforme disposto nas legislações correlatas;
**II –** realizar o atendimento dos titulares de dados pessoais internos e externos à Corporação;
**III –** aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
**IV –** deter amplo e sólido conhecimento sobre a legislação de proteção de dados pessoais e normas correlatas;
**V –** elaborar e manter atualizado o Relatório de Impacto à Proteção de Dados Pessoais – RIPD;
**VI –** atentar-se às demais atribuições determinadas pelo Representante do Controlador;
**VII –** receber as comunicações do Encarregado Governamental e adotar providências;
**VIII –** reportar-se ao Encarregado Governamental, que o orientará e supervisionará em caso de comunicação com a ANPD;
**IX –** apoiar a implementação e a manutenção de práticas de conformidade da PMDF à legislação sobre o tratamento de dados pessoais;
**X –** propor campanhas educativas na Corporação sobre o tratamento de dados pessoais;
**XI –** responder aos incidentes no tratamento de dados pessoais;
**XII –** fiscalizar a observância da presente portaria no âmbito da Corporação e buscar a responsabilização de eventuais transgressões.

## Seção III
## Dos colegiados
## Comitê Gestor de Proteção de Dados Pessoais – CGPDP



**Art. 12°** Para os fins previstos nesta Portaria, as funções do Comitê Gestor de Proteção de Dados Pessoais – CGPDP será exercido pelo Alto Comando da Corporação cujas atribuições estão descritas nas legislações específicas da PMDF, bem como outras que se fizerem necessárias para o cumprimento da presente Política de Proteção de Dados Pessoais.

**Art. 13°** O presidente do Comitê Gestor de Proteção de Dados Pessoais – CGPDP será o Comandante-Geral que, na função de Representante do Controlador, ou seu substituto legal, será assessorado, em suas decisões, pelos membros que compõem o Alto Comando da PMDF.

**Parágrafo único.** Diante da Complexidade da matéria é possível que sejam convocadas ou convidadas equipes técnicas e multidisciplinares para esclarecerem dúvidas dos membros do Comitê, bem como para auxiliar o Representante do Controlador na tomada de decisão.

**Art. 14°** Nas reuniões do Comitê Gestor de Proteção de Dados Pessoais – CGPDP sempre estará presente o Encarregado Setorial (Auditor da PMDF), principalmente quando forem por ele solicitadas, momento em que apresentará o(s) tema(s) constantes em pauta, bem como responderá aos questionamentos realizados pelos membros do Comitê.

**Parágrafo único.** O Encarregado Setorial não integra o Comitê Gestor de Proteção de Dados Pessoais – CGPDP, motivo pelo qual sua manifestação não será consignada como voto efetivo como os dos demais membros.

**Art. 15°** São atribuições do Comitê Gestor de Proteção de Dados Pessoais – CGPDP, dentre outras:

**I –** analisar a implementação da Lei Geral de Proteção de Dados (LGPD), no âmbito da PMDF, e fomentar medidas que torne mais eficiente o processo de adaptação e conformidade em face da LGPD;

**II –** propor medidas ao Governo do Distrito Federal, por intermédio do Comitê Intersecretarial de Análise de Aplicação da LGPD, para a implementação da Lei Especial no âmbito do Distrito Federal, que auxiliem na Proteção de Dados na PMDF;

**III –** analisar, debater e decidir as questões provenientes do Subcomitê Executivo de Proteção de Dados Pessoais – SEPDP;

**IV –** elaborar relatórios ou outros documentos que sirvam para a melhoria da Política de Proteção de Dados na PMDF;

**V –** convocar ou convidar, policiais militares e pessoas físicas ou jurídicas, respectivamente, para auxiliar na tomada de decisão sobre questões de alta complexidade ou de extrema relevância para a
PMDF e que estejam relacionadas às boas práticas da proteção de dados.

**Art. 16°** O Comitê Gestor de Proteção de Dados Pessoais – CGPDP reunir-se-á bimestralmente em caráter ordinário, e, extraordinariamente, sempre que necessário, podendo a reunião extraordinária ser solicitada por quaisquer de seus membros ou pelo Encarregado Setorial.

**Parágrafo único.** O secretariado do Comitê Gestor de Proteção de Dados Pessoais – CGPDP será realizado com a mesma logística da reunião de Alto Comando.

## Seção IV

## Dos colegiados Subcomitê Executivo de Proteção de Dados Pessoais – SEPDP





**Art. 17°** Fica instituído, no âmbito da Polícia Militar do Distrito Federal, o Subcomitê Executivo de Proteção de Dados Pessoais – SEPDP, bem como aprovada a organização mínima de seu Regimento Interno.

**Art. 18°** O Subcomitê Executivo de Proteção de Dados Pessoais – SEPDP é órgão consultivo dentro da estrutura organizacional, de atuação permanente, e tem como finalidade auxiliar o estabelecimento de Políticas e Diretrizes para a implementação e aperfeiçoamento de Proteção de Dados.

**Art. 19°** O Presidente do Subcomitê Executivo de Proteção de Dados Pessoais – SEPDP será o Auditor da PMDF e terá como substituto o Corregedor-Adjunto, nos casos de afastamentos legais e impedimentos.

**Parágrafo Único.** Para os efeitos legais, quando encontrar-se na função prevista nesta portaria, o Auditor da PMDF será o Encarregado Setorial e o Corregedor-Adjunto o seu suplente, tendo como atribuições, dentre outras:

**I –** orientar Operadores internos e externos e sub-Operadores a respeito das boas práticas e padrões de Governança de dados, a serem tomadas em relação à proteção de dados pessoais, conforme disposto na Lei nº 13.709/2018;

**II –** aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

**III –** executar as demais atribuições determinadas pelo Controlador ou estabelecidas em normas complementares.

**IV –** receber as comunicações do Encarregado Governamental e adotar providências, dentre elas a de comunicar, imediatamente, o Representante do Controlador sobre a demanda;

**V –** reportar-se ao Encarregado Governamental;

**VI –** convocar e presidir as reuniões do Subcomitê;

**VII –** coordenar, orientar e supervisionar as atividades do Subcomitê;

**VIII –** convocar, abrir, presidir, suspender, prorrogar e encerrar as reuniões ordinárias e extraordinárias;

**IX –** submeter ao debate e à votação as matérias a serem deliberadas, apurando os votos e proclamando os resultados;
**X –** requisitar informações e diligências necessárias à execução das atividades do Subcomitê;
**XI –** indicar, dentre os membros do Subcomitê, relatores para matérias que necessitarem de apreciação;
**XII –** indicar representantes do Subcomitê para participar de fóruns de debates com instituições que desenvolvam projetos de pesquisa ou estudos sobre o tema;
**XIII –** proferir, além do voto ordinário, voto de desempate em processo decisório;
**Art. 20°** A competência, a organização e o funcionamento do Subcomitê Executivo, além das disposições previstas nesta portaria, serão descritas em Regimento Interno que será apresentado, mediante proposta, para ser devidamente aprovada pelo Comitê Gestor de Proteção de Dados
Pessoais – CGPDP, dentro do prazo estabelecido nas Disposições Finais e Transitórias.
**Art. 21°** O Subcomitê Executivo de Proteção de Dados Pessoais – SEPDP é composto, minimamente, pelo:
**I –** Conselho Deliberativo;
**II –** Consultoria Técnica;
**III –** Secretaria.
**Art. 22°** O Conselho Deliberativo será presidido pelo Encarregado Setorial (Auditor da PMDF) e composto pelos seguintes membros:
**I –** Subdiretor da DITEL/PMDF;
**II –** Subchefe do CCS/PMDF;





**III –** Subchefe do Centro de Inteligência/PMDF;
**III –** Oficial indicado pelo Departamento de Logística e Finanças.
**IV –** Oficial indicado pelo Departamento de Gestão de Pessoal;
**VI –** Oficial indicado pelo Departamento de Educação e Cultura;
**VI –** Oficial indicado pelo Departamento de Saúde e Assistência ao Pessoal;
**VII –** Oficial indicado pelo Departamento Operacional;
**VIII –** Oficial indicado pelo Departamento de Controle e Correição.
**Parágrafo único.** Os membros titulares poderão ser eventualmente substituídos, por ocasião de seus afastamentos e impedimentos legais, por representantes transitórios indicados pelo dirigente da área temática a qual aquele é afeto.
**Art. 23°** A Consultoria Técnica será formada por membros efetivos da Polícia Militar do Distrito Federal ou por pessoa cuja qualificação seja compatível com as matérias afetas a serem discutidas.
**Parágrafo único.** Os membros da Consultoria Técnica, que não terão direito a voto, serão definidos e previamente indicados pelo Conselho Deliberativo, de forma que todas as áreas que possuam pertinência com a temática a ser deliberada sejam contempladas.

**Art. 24°** A Secretaria do Subcomitê Executivo de Proteção de Dados Pessoais – SEPDP, a quem compete o assessoramento administrativo e apoio logístico do Colegiado, será exercida por uma das Seções da Auditoria da PMDF, previamente definida pelo Encarregado Setorial, que fará constar no
Regimento Interno.

**Parágrafo único.** A função de Secretário do Subcomitê será exercida pelo Chefe da PM-2 do Estado-Maior ou pelo seu Assessor.

**Art. 25°** Compete ao Subcomitê Executivo de Proteção de Dados Pessoais – SEPDP, dentre outras:

**I –** elaborar proposta de Regimento Interno que será apresentada ao Comitê Gestor de Proteção de Dados Pessoais – CGPDP;

**II –** elaborar propostas de Políticas e Diretrizes para Proteção de Dados para a PMDF, alinhadas aos objetivos estratégicos;

**III –** propor as prioridades para execução e monitoramento das atividades voltadas a Proteção de Dados na PMDF;

**IV –** sugerir demandas e projetos de capacitação e treinamento de pessoal para desenvolvimento das competências necessárias para a operacionalização e gestão dos serviços para a Proteção de Dados;

**V –** revisar anualmente o seu Regimento Interno, e ainda, a qualquer tempo, propor revisões da legislação interna da PMDF visando aprimorar a Governança de Proteção de Dados;

**VI –** propor a divulgação das informações relativas às atividades e deliberações adotadas no âmbito do Subcomitê, desde que devidamente aprovadas pelo Comitê;

**VII –** elaborar políticas e diretrizes, a serem submetidas a apreciação do Comitê, para minimização dos riscos e do aumento no nível de segurança da Proteção de Dados;

**VIII –** submeter ao Comitê Gestor proposta à ser encaminhada ao EM visando a criação de Grupos de Trabalho, Grupos Temáticos e Comissões, com a finalidade de examinar e propor soluções para temas específicos;

**IX –** elaborar e submeter ao Comitê Gestor o Relatório de Impacto à Proteção de Dados Pessoais – RIPD.

**Parágrafo único.** As decisões do Conselho Deliberativo são tomadas por maioria simples e têm a natureza de recomendação técnica ao Comitê Gestor de Proteção de Dados Pessoais – CGPDP, a
quem cabe a homologação dos temas deliberados

## CAPÍTULO V
## DO TRATAMENTO DE DADOS PESSOAIS NA PMDF

**Art. 26°** O tratamento de dados pessoais pela PMDF é realizado para o atendimento de sua
finalidade institucional, na persecução do interesse público, com o objetivo de executar suas
competências legais e de cumprir as atribuições legais.
**Parágrafo único.** A PMDF zelará para que o titular do dado pessoal tenha assegurados os direitos previstos nos Arts. 18 e 19 da LGPD.
**Art. 27°** O tratamento de dados pessoais pela PMDF será realizado nas seguintes hipóteses:
**I –** mediante o consentimento pelo titular;
**II –** para o cumprimento de obrigação legal ou regulatória pelo Controlador;
**III –** para o uso compartilhado de dados necessários à execução de políticas públicas previstas em legislação específica ou respaldadas em contratos, convênios ou instrumentos congêneres,observadas as disposições do Capítulo IV da LGPD;
**IV –** para a realização de estudos, garantida, sempre que possível, a anonimização dos dados pessoais;
**V –** quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
**VI –** para o exercício regular de direitos em processo judicial, administrativo ou arbitral, este último nos termos da Lei de Arbitragem – a Lei nº 9.307, de 23 de setembro de 1996;
**VII –** para a proteção da vida ou da incolumidade física do titular ou de terceiros;
**VIII –** para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
**IX –** para atender, quando necessário, a seus interesses legítimos ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
**X –** para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.
*§ 1º* Em observância a suas atribuições constitucionais e legais, a PMDF poderá, no estrito limite de suas atividades de segurança pública, com fulcro no art. 4º, III, "a", da LGPD, tratar dados pessoais com dispensa de obtenção de consentimento pelos respectivos titulares.
*§ 2º* Eventuais atividades que transcendam o escopo da função de segurança pública estarão sujeitas à obtenção de consentimento dos interessados, previsto no inciso I do caput deste artigo, que será obtido por escrito ou por outro meio que demonstre a manifestação da vontade do titular, nos termos do art. 8º da Lei nº 13.709/2018.
*§ 3º* O consentimento do titular poderá ser revogado a qualquer momento mediante sua manifestação expressa, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de
eliminação.
§ 4º Também é dispensada a exigência do consentimento previsto no inciso I do caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos na LGPD.

§ 5º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade,





a boa-fé e o interesse público que justificaram sua disponibilização.

**Art. 28°** Os contratos com terceiros, para o fornecimento de produtos ou para a prestação de serviços necessários para a atividade da Corporação, poderão, conforme o caso, necessitar de disciplina própria de proteção de dados pessoais, a qual deverá estar disponível para ser consultada
pelos interessados, bem como para a fiscalização pela PMDF nos termos das legislações específicas.

**Art. 29°** A PMDF publicará, de modo claro e atualizado, e em lugar de fácil acesso e visualização no site institucional, destinado à divulgação de informações sobre a privacidade de dados pessoais:

**I –** a previsão legal, a finalidade e os procedimentos que fundamentam a realização do tratamento de dados pessoais na Instituição, conforme previsto nesta portaria;
**II –** a identificação do representante do Controlador e o seu contato;
**III –** as identificações dos Encarregados Setoriais, titular e suplente, e os seus contatos;
**IV –** as responsabilidades dos Operadores envolvidos no tratamento e os direitos do titular, com menção expressa ao art. 18 da LGPD.

**Art. 30°** O tratamento dos dados pessoais deverá ser realizado até que ocorra o descarte ou arquivamento na Instituição, abrangendo:

**I –** o acesso;
**II –** a coleta;
**III –** a avaliação;
**IV –** a classificação;
**V –** o armazenamento;
**VI –** o controle;
**VII –** a extração;
**VIII –** a comunicação;
**IX –** a distribuição;
**X –** a difusão;
**XI –** a eliminação;
**XII –** a modificação;
**XIII –** o processamento;
**XIV –** a produção;
**XV –** a recepção;
**XVI –** a reprodução;
**XVII –** a transferência;
**XVIII –** a transmissão;
**XIX –** a utilização.

## CAPÍTULO VIII
## DAS DIRETRIZES

**Art. 31°** Para conformar os processos e os procedimentos da Corporação à LGPD, deverão ser consideradas as seguintes diretrizes pelos setores envolvidos, dentre outras:
**I –** levantamento dos dados pessoais tratados na PMDF;
**II –** mapeamento dos fluxos de dados pessoais na PMDF;
**III –** verificação da conformidade do tratamento com o previsto na LGPD;
**IV –** definição e publicação de programa de gerenciamento de riscos do tratamento de dados pessoais na PMDF;



**V –** revisão e atualização da política e dos programas de segurança da informação;
**VI –** definição de procedimentos e processos que garantam a disponibilidade, a integridade e a confidencialidade dos dados pessoais durante seu ciclo de vida;
**VII –** definição do modo de prestar as informações sobre o tratamento de dados pessoais;
**VIII –** revisão e adequação à LGPD dos contratos firmados no âmbito da PMDF;
**IX –** revisão e adequação à LGPD dos processos e procedimentos relacionados à área de saúde da corporação;
**X –** definição do ciclo de vida das informações pessoais e da necessidade de consentimento para utilização de dados pessoais na parte administrativa e operacional da PMDF.

## CAPÍTULO IX
## DA SEGURANÇA E DAS BOAS PRÁTICAS DE GOVERNANÇA

**Art. 32°** Serão adotadas boas práticas de Governança capazes de inspirar comportamentos
adequados e de mitigar os riscos de comprometimento de dados pessoais.
Parágrafo único. As boas práticas adotadas de proteção de dados pessoais e a Governança
implantada deverão ser objeto de campanhas informativas, na esfera interna da Corporação e em seu site eletrônico, visando a disseminação da cultura protetiva, com a conscientização e a
sensibilização dos interessados.
**Art. 33°** Os dados pessoais tratados pela PMDF devem:
**I –** ser protegidos por procedimentos internos, com trilhas de auditoria para registrar autorizações, utilização, impactos e violações;
**II –** ser mantidos disponíveis, exatos, adequados, pertinentes e atualizados, sendo retificado ou
eliminado o dado pessoal mediante informação ou constatação de impropriedade respectiva ou face a solicitação de remoção, devendo a neutralização ou descarte do dado observar as condições e períodos da tabela de prazos de retenção de dados;
**III –** ser compartilhados somente para o exercício das atividades voltadas ao estrito exercício de suas competências legais e constitucionais, ou para atendimento de políticas públicas aplicáveis;
**IV –** ser revistos em periodicidade mínima anual, sendo de imediato eliminados aqueles que já não forem necessários, por terem cumprido sua finalidade ou por ter se encerrado o seu prazo de retenção.
**Art. 34°** A informação sobre o tratamento de dados pessoais sensíveis ou referentes a crianças ou adolescentes estará disponível em linguagem clara, simples, concisa, transparente, inteligível e acessível, na forma da lei.

## CAPÍTULO X
## DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

**Art. 35°** A PMDF, como órgão de Segurança Pública, poderá realizar transferências internacionais de dados pessoais, sendo que, em tais casos, deverá ser observado o previsto nos Arts. 33 a 36 da LGPD.



**Parágrafo único.** Na hipótese do caput, os casos não abrangidos pelo § 1º, do **Art. 27°**, desta Portaria, implicarão em prévia e formal autorização, na forma do § 2º do referido artigo, ou por anonimização do dado pessoal para fins exclusivamente estatísticos.

**Art. 36°.** Toda correspondência oficial por e-mail deverá ser realizada utilizando-se o correio eletrônico institucional da PMDF.

**Art. 37°** As informações protegidas por sigilo continuam resguardadas pelos atos normativos a elas relacionados.

**Art. 38°** O Encarregado Setorial deverá, utilizando-se dos trabalhos do Subcomitê Executivo, estabelecer um canal de comunicação direta, na internet da Corporação, para aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências, dentro do prazo de 60 (sessenta) dias, à contar da data da publicação desta portaria.

**Parágrafo único.** Na impossibilidade do cumprimento do prazo estabelecido no caput, deverá, mediante justificativa fundamentada, solicitar mais prazo para a realização da medida.

**Art. 39°** O Encarregado Setorial deverá, utilizando-se dos trabalhos do Subcomitê Executivo, propor ao Comitê de Gestão um modelo de "Manual Explicativo" que possibilite a sua utilização pelos integrantes da Corporação e que, também, possa ser disponibilizado na internet para os titulares de
dados.

**Art. 40°** O Estado-Maior deverá elaborar palestra para ser ministrada aos membros do Comitê de Gestão e outros policiais militares cujas funções estejam diretamente ligadas à matéria de LGPD.

**Art. 41°** O Departamento de Educação e Cultura – DEC/PMDF deverá, no prazo de 60 (sessenta) dias, contados da publicação desta portaria, elaborar e encaminhar ao Encarregado Setorial um estudo contendo as informações necessárias para que os cursos de carreira da Corporação tenham
acesso ao conteúdo referente à LGPD, mediante inclusão na grande curricular.

**Art. 42°** O Subcomitê Executivo, no prazo de 30 (trinta) dias, contados da publicação desta portaria, apresentará proposta de ferramenta de Tecnologia da Informação, ao Comitê de Gestão, para que seja possível solicitar ao usuário/titular dos dados, ao acessar o site da Corporação, uma forma de
"aceite" de que os seus dados pessoais serão utilizados pela Corporação para o exercício das suas finalidades Institucionais.

**Parágrafo único.** Na impossibilidade do cumprimento do prazo estabelecido no caput, deverá, mediante justificativa fundamentada, solicitar mais prazo para a realização da medida.

**Art. 43°** Visando o início do período de adequação da PMDF às normas previstas na LGDP, o Subcomitê Executivo deverá encaminhar ao Comitê de Gestão, dentro do prazo de 90 (noventa) dias, contados da data de publicação desta portaria, proposta de Relatório de Impacto à Proteção de
Dados Pessoais – RIPD para aprovação e novos direcionamentos quanto as medidas à serem tomadas.
**Parágrafo único.** Na impossibilidade do cumprimento do prazo estabelecido no caput, deverá, mediante justificativa fundamentada, solicitar mais prazo para a realização da medida.
**Art. 44°** Tendo em vista o cumprimento das Diretrizes previstas nesta portaria, fica estabelecido o prazo de até 100 (cem) dias, contados da data da publicação da presente portaria, para que o Subcomitê Executivo encaminhe estudo sobre as prioridades que devem ser enfrentadas no âmbito da PMDF, principalmente aquelas relacionadas ao Departamento de Assistência à Saúde e Pessoal –





DSAP/PMDF e Departamento Operacional – DOP/PMDF.
**Parágrafo único.** Neste estudo deverá constar, necessariamente, as informações que possam subsidiar o Comitê de Gestão na decisão sobre a resolução dos problemas, os custos necessários e riscos para o caso de não realização das medidas apresentadas.
**Art. 45°** Após a publicação da presente portaria, o Subcomitê Executivo terá o prazo de até 30 (trinta) dias para propor a íntegra do seu Regimento Interno ao Comitê de Gestão, dispondo sobre as competências e demais atividades inerentes ao Colegiado, para aprovação e publicação.
**Art. 46°** A Política de proteção de dados, prevista nesta portaria, deverá, mediante proposta do Subcomitê Executivo ao Comitê de Gestão, ser revisada e aperfeiçoada permanentemente, conforme sejam implementadas as respectivas diretrizes e constatada necessidade de novas previsões para conformidade da PMDF à LGPD e suas legislações correlatas.
**Art. 47°** Os casos omissos serão resolvidos pela legislação afeta a LGDP, principalmente pelo Decreto Distrital nº 42.036/2021 e pela da Lei Federal nº 13.709/2018, bem como pelas orientações exaradas pelo Encarregado Governamental, mas sempre mediante deliberação do Comitê Gestor de
Proteção de Dados Pessoais – CGPDP.
**Art. 48°** Esta Portaria entra em vigor na data de sua publicação.

**FÁBIO AUGUSTO VIEIRA – CEL QOPM**
Comandante-Geral

# ANEXO VI FORMULÁRIO DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS - ANPD

ANPD Autoridade Nacional de Proteção de Dados

**Formulário de Comunicação de Incidente de Segurança com Dados Pessoais**

| Dados do Controlador | | | |
|---|---|---|---|
| Razão Social / Nome: | | | |
| CNPJ/CPF: | | | |
| Endereço: | | | |
| Cidade: | | Estado: | |
| CEP: | | | |
| Telefone: | | E-mail: | |
| Declara ser Microempresa ou Empresa de Pequeno Porte: | | ☐ Sim | ☐ Não |
| Declara ser Agente de Tratamento de Pequeno Porte[1]: | | ☐ Sim | ☐ Não |
| Informe o número aproximado de titulares cujos dados são tratados por sua organização: | | | |
| **Dados do Encarregado** | | | |
| Possui um encarregado pela proteção de dados pessoais? | | ☐ Sim | ☐ Não |
| Nome: | | | |
| CNPJ/CPF: | | | |
| Telefone: | | E-mail: | |

| Dados do Notificante / Representante Legal | |
|---|---|
| ☐ O próprio encarregado pela proteção de dados. | |
| ☐ Outros (especifique): | |
| Nome: | |
| CNPJ/CPF: | |
| Telefone: | |
| E-mail: | |

A documentação comprobatória da legitimidade para representação do controlador junto à ANPD deve ser protocolada em conjunto com o formulário de comunicação de incidente.

- *Encarregado*: ato de designação/nomeação/procuração.
- *Representante*: contrato social e procuração, se cabível.

[1] Nos termos do REGULAMENTO DE APLICAÇÃO DA LEI Nº 13.709, DE 14 DE AGOSTO DE 2018, aprovado pela RESOLUÇÃO CD/ANPD Nº 2, DE 27 DE JANEIRO DE 2022. (https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019)

| Tipo de Comunicação | |
|---|---|
| ☐ Completa | *Todas as informações a respeito do incidente estão disponíveis e* ***a comunicação aos titulares já foi realizada****.* |
| ☐ Preliminar | *Nem todas as informações sobre o incidente estão disponíveis, justificadamente, ou a* ***comunicação aos titulares ainda não foi realizada****.*<br>*A complementação deverá ser encaminhada no prazo de* ***20 dias úteis*** *a contar da data da comunicação* – Art. 6º § 3º do Regulamento de Comunicação de Incidentes. |
| ☐ Complementar | *Complementação de informações prestadas em comunicação preliminar.* |
| **A comunicação complementar deve ser protocolada no mesmo processo que a comunicação preliminar.** | |

➢ A comunicação preliminar é insuficiente para o cumprimento da obrigação estabelecida pelo art. 48 da LGPD e deve ser complementada pelo controlador no prazo estabelecido.

| Avaliação do Risco do Incidente |
|---|
| ☐ O incidente de segurança pode acarretar risco ou dano relevante aos titulares. |
| ☐ O incidente não acarretou risco ou dano relevante aos titulares. **(Comunicação Complementar)** |
| ☐ O risco do incidente aos titulares ainda está sendo apurado. **(Comunicação Preliminar)** |
| **Justifique, se cabível, a avaliação do risco do incidente:** |

| Da Ciência da Ocorrência do Incidente | | |
|---|---|---|
| **Por qual meio se tomou conhecimento do incidente?** | | |
| ☐ Identificado pelo próprio controlador. | ☐ Notificação do operador de dados. | ☐ Denúncia de titulares/terceiros. |
| ☐ Notícias ou redes sociais. | ☐ Notificação da ANPD. | ☐ Outros. (especifique) |
| **Descreva, resumidamente, de que forma a ocorrência do incidente foi conhecida:** | | |
| | | |
| **Caso o incidente tenha sido comunicado ao controlador por um operador, informe:** | | |
| **Dados do Operador** | | |
| Razão Social / Nome: | | |
| CNPJ/CPF: | | |
| E-mail: | | |
| Cabe ao controlador solicitar ao operador as informações necessárias à comunicação do incidente. | | |

| Da Tempestividade da Comunicação do Incidente | |
|---|---|
| **Informe as seguintes datas, sobre o incidente:** | |
| Quando ocorreu | |
| Quando tomou ciência | |
| Quando comunicou à ANPD | |
| Quando comunicou aos titulares | |
| **Justifique, se cabível, a não realização da comunicação à ANPD e aos titulares de dados afetados no prazo de 3 (três) dias úteis conforme prevê o Art. 6º da Resolução CD/ANPD nº 15, de 24 de abril de 2024 que aprova o Regulamento de Comunicação de Incidente de Segurança.** | |
| | |
| **Se cabível, informe quando e a quais outras autoridades o incidente foi comunicado:** | |
| | |

| Da Comunicação do Incidente aos Titulares dos Dados | |
|---|---|
| **Os titulares dos dados afetados foram comunicados sobre o incidente?** | |
| ☐ Sim. | ☐ Não, por não haver risco ou dano relevante a eles. |
| ☐ Não, mas o processo de comunicação está em andamento. | ☐ Não, vez que o risco do incidente ainda está sendo apurado. (**comunicação preliminar**) |
| **Se cabível, quando os titulares serão comunicados sobre o incidente?** | |
| | |

| **De que forma a ocorrência do incidente foi comunicada aos titulares?** | |
|---|---|
| ☐ Comunicado individual por escrito. *(mensagem eletrônica / carta / e-mail / etc.)* | ☐ Anúncio público no sítio eletrônico, mídias sociais ou aplicativos do controlador. |
| ☐ Comunicado individual por escrito com confirmação de recebimento. *(mensagem eletrônica / carta / e-mail / etc.)* | ☐ Ampla divulgação do fato em meios de comunicação, por iniciativa do controlador. (*especifique abaixo*) |
| ☐ Outros. (*especifique abaixo*) | ☐ Não se aplica. |
| **Descreva como ocorreu a comunicação:** | |
| | |
| **Quantos titulares foram comunicados individualmente sobre o incidente?** | |
| | |
| **Justifique, se cabível, o que motivou a não realização da comunicação individual aos titulares:** | |
| | |

**O comunicado aos titulares deve utilizar linguagem clara e conter, ao menos, as seguintes informações:**

1. resumo e data de ocorrência do incidente;
2. descrição dos dados pessoais afetados;
3. riscos e consequências aos titulares de dados;
4. medidas tomadas e recomendadas par mitigar seus efeitos, se cabíveis;
5. dados de contato do controlador para obtenção de informações adicionais sobre o incidente.

| **O comunicado aos titulares atendeu os requisitos acima?** | |
|---|---|
| ☐ Sim | ☐ Não |

- Se não atendidos os requisitos, o comunicado aos titulares deverá ser devidamente retificado.
- Poderá ser solicitada pela ANPD, a qualquer tempo, cópia do comunicado aos titulares para fins de fiscalização.

| **Descrição do Incidente** | |
|---|---|
| **Qual o tipo de incidente? (Informe o tipo mais específico)** | |
| ☐ Sequestro de Dados (*ransomware*) sem transferência de informações. | ☐ Sequestro de dados (*ransomware*) com transferência e/ou publicação de informações. |
| ☐ Exploração de vulnerabilidade em sistemas de informação. | ☐ Vírus de Computador / *Malware*. |
| ☐ Roubo de credenciais / Engenharia Social. | ☐ Violação de credencial por força bruta. |
| ☐ Publicação não intencional de dados pessoais. | ☐ Divulgação indevida de dados pessoais. |
| ☐ Envio de dados a destinatário incorreto. | ☐ Acesso não autorizado a sistemas de informação. |
| ☐ Negação de Serviço (DoS). | ☐ Alteração/exclusão não autorizada de dados. |
| ☐ Perda/roubo de documentos ou dispositivos eletrônicos. | ☐ Descarte incorreto de documentos ou dispositivos eletrônicos. |
| ☐ Falha em equipamento (hardware). | ☐ Falha em sistema de informação (*software*). |
| ☐ Outro tipo de incidente cibernético. (especifique abaixo) | ☐ Outro tipo de incidente não cibernético. (especifique abaixo) |
| **Descreva, resumidamente, como ocorreu o incidente:** | |

| Explique, resumidamente, por que o incidente ocorreu (identifique a causa raiz, se conhecida): |
|---|
| |
| |
| |
| |
| Que medidas foram adotadas para corrigir as causas do incidente? |
| |

| Impactos do Incidente Sobre os Dados Pessoais | |
|---|---|
| **De que forma o incidente afetou os dados pessoais (admite mais de uma marcação):** | |
| ☐ Confidencialidade | Houve acesso não autorizado aos dados, violando seu sigilo. |
| ☐ Integridade | Houve alteração ou destruição de dados de maneira não autorizada ou acidental. |
| ☐ Disponibilidade | Houve perda ou dificuldade de acesso aos dados por período significativo. |

| Se aplicável, quais os tipos de dados pessoais sensíveis foram violados? (admite mais de uma marcação) | | |
|---|---|---|
| ☐Origem racial ou étnica. | ☐Convicção religiosa. | ☐Opinião política. |
| ☐Referente à saúde. | ☐Biométrico. | ☐Genético. |
| ☐Referente à vida sexual. | ☐Filiação a organização sindical, religiosa, filosófica ou política. | |
| **Se aplicável, descreva os tipos de dados pessoais sensíveis violados:** | | |
| | | |

| Quais os demais tipos de dados pessoais violados? (admite mais de uma marcação) | | |
|---|---|---|
| ☐ Dados básicos de identificação *(ex: nome, sobrenome, data de nascimento, matrícula)* | ☐ Número de documentos de identificação oficial. *(ex: RG, CPF, CNH, passaporte)* | ☐ Dados de contato. *(ex: telefone, endereço, e-mail)* |
| ☐ Dados de meios de pagamento. *(ex: cartão de crédito/débito)* | ☐ Cópias de documentos de identificação oficial. | ☐ Dados protegidos por sigilo profissional/legal. |
| ☐ Dado financeiro ou econômico. | ☐ Nomes de usuário de sistemas de informação. | ☐ Dado de autenticação de sistema. *(ex: senhas, PIN ou tokens)* |
| ☐ Imagens / Áudio / Vídeo | ☐ Dado de geolocalização. *(ex: coordenadas geográficas)* | ☐ Outros (especifique abaixo) |
| **Descreva os tipos de dados pessoais não sensíveis violados:** | | |

| Riscos e Consequências aos Titulares dos Dados | |
|---|---|
| **Foi elaborado um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) das atividades de tratamento afetadas pelo incidente?** | |
| ☐ Sim | ☐ Não |

| Qual o número total de titulares cujos dados são tratados nas atividades afetadas pelo incidente? | |
|---|---|
| | |
| **Qual a quantidade aproximada de titulares afetados[2] pelo incidente?** | |
| Total de titulares afetados | |
| Crianças e/ou adolescentes | |
| Outros titulares vulneráveis | |
| **Se aplicável, descreva as categorias de titulares vulneráveis afetados:** | |
| | |

| Quais a categorias de titulares foram afetadas pelo incidente? (admite mais de uma marcação) | | |
|---|---|---|
| ☐ Funcionários. | ☐Prestadores de serviços. | ☐ Estudantes/Alunos. |
| ☐ Clientes/Cidadãos. | ☐ Usuários. | ☐ Inscritos/Filiados. |
| ☐ Pacientes de serviço de saúde. | ☐Ainda não identificadas. | ☐ Outros. (especifique abaixo) |
| **Informe o quantitativo de titulares afetados, por categoria:** | | |

| Quais as prováveis consequências do incidente para os titulares? (admite mais de uma marcação) | | |
|---|---|---|
| ☐ Danos morais. | ☐ Danos materiais. | ☐ Violação à integridade física |
| ☐ Discriminação social. | ☐ Danos reputacionais. | ☐ Roubo de identidade. |
| ☐ Engenharia social / Fraudes. | ☐ Limitação de acesso a um serviço. | ☐ Exposição de dados protegidos por sigilo profissional/legal. |
| ☐ Restrições de direitos. | ☐ Perda de acesso a dados pessoais. | ☐ Outros (especifique abaixo). |

**Se cabível, descreva as prováveis consequências do incidente para cada grupo de titulares:**

**Qual o provável impacto do incidente sobre os titulares? (admite só uma marcação)**

☐ Podem não sofrer danos, sofrer danos negligenciáveis ou superáveis sem dificuldade.

☐ Podem sofrer danos, superáveis com certa dificuldade.

☐ Podem sofrer danos importantes, superáveis com muita dificuldade.

☐ Podem sofrer lesão ou ofensa a direitos ou interesses difusos, coletivos ou individuais, que, dadas as circunstâncias, ocasionam ou tem potencial para ocasionar dano significativo ou irreversível.

[2] Titular afetado é aquele cujos dados podem ter tido a confidencialidade, integridade ou disponibilidade violadas e que ficará exposto a novos riscos relevantes em razão do incidente.

**Se cabível, quais medidas foram adotadas para mitigação dos riscos causados pelo incidente aos titulares?**

## Medidas de Segurança Técnicas e Administrativas para a Proteção dos Dados Pessoais

**Os dados violados estavam protegidos de forma a impossibilitar a identificação de seus titulares?**

| | | |
|---|---|---|
| ☐ Sim, integralmente protegidos por criptografia / pseudonimização. | ☐ Sim, parcialmente protegidos por criptografia / pseudonimização. | ☐ Não. |

**Descreva os meios utilizados para proteger a identidade dos titulares, e a quais tipos dados foram aplicados:**

| **Antes do incidente, quais das seguintes medidas de segurança eram adotadas? (admite mais de uma marcação)** | | |
|---|---|---|
| ☐ Políticas de segurança da informação e privacidade. | ☐ Processo de Gestão de Riscos. | ☐ Registro de incidentes. |
| ☐ Controle de acesso físico. | ☐ Controle de acesso lógico. | ☐ Segregação de rede. |
| ☐ Criptografia/Anonimização. | ☐ Cópias de segurança. (*backups*) | ☐ Gestão de ativos. |
| ☐ Antivírus. | ☐ Firewall. | ☐ Atualização de Sistemas. |
| ☐ Registros de acesso (logs). | ☐ Monitoramento de uso de rede e sistemas. | ☐ Múltiplos fatores de autenticação. |
| ☐ Testes de invasão. | ☐ Plano de resposta a incidentes. | ☐ Outras (especifique). |
| **Descreva as demais medidas de segurança técnicas e administrativas adotadas antes do incidente:** | | |

| **Após o incidente, foi adotada alguma nova medida de segurança? (admite mais de uma marcação)** | | |
|---|---|---|
| ☐ Políticas de segurança da informação e privacidade. | ☐ Processo de Gestão de Riscos. | ☐ Registro de incidentes. |
| ☐ Controle de acesso físico. | ☐ Controle de acesso lógico. | ☐ Segregação de rede. |
| ☐ Criptografia/Anonimização. | ☐ Cópias de segurança. (*backups*) | ☐ Gestão de ativos. |
| ☐ Antivírus. | ☐ Firewall. | ☐ Atualização de Sistemas. |
| ☐ Registros de acesso (logs). | ☐ Monitoramento de uso de rede e sistemas. | ☐ Múltiplos fatores de autenticação. |
| ☐ Testes de invasão. | ☐ Plano de resposta a incidentes. | ☐ Outras (especifique). |
| **Se cabível, descreva as medidas de segurança adicionais adotadas após o incidente:** | | |
| **As atividades de tratamento de dados afetadas estão submetidas a regulações de segurança setoriais?** | | |
| ☐ Sim | ☐ Não | |
| **Se cabível, indique as regulamentações setoriais de segurança aplicáveis às atividades de tratamento de dados afetadas pelo incidente:** | | |

## ANEXO VII - DIAGNÓSTICO – CULTURA ORGANIZACIONAL LGPD – CGE/PR

### DIAGNÓSTICO - CULTURA ORGANIZACIONAL – LGPD

Este diagnóstico inicial procura identificar o conhecimento de todos os servidores, sobre a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018.
São 10 (dez) perguntas e não há identificação das pessoas.
Prazo para resposta:
*Obrigatório

1. Insira sua unidade/setor: *

2. Você já participou de capacitação sobre a Lei Geral de Proteção de Dados dentro ou fora do órgão? *

- ○ Palestra
- ○ Seminário
- ○ Curso (Presencial ou EaD)
- ○ Leitura de textos e documentos
- ○ Não possuo capacitação no assunto
- ○ Outro:

3. Você sabe o que são dados pessoais? *

- ○ Sim
- ○ Não

4. Em seu trabalho no órgão, você realiza alguma atividade que envolve dados pessoais? *

- ○ Sim
- ○ Não
- ○ Não sei

5. Por quais meios você trabalha com dados pessoais? *

- ○ Sistemas
- ○ Planilhas Eletrônicas
- ○ Documentos Eletrônicos
- ○ Documentos Físicos
- ○ Não sei dizer se trabalho com dados pessoais no dia a dia
- ○ Outro:

6. Dos fluxos que fazem parte do seu trabalho no órgão, em quais você faz uso de dados pessoais? *

- ○ Distribuição
- ○ Requisição de informações
- ○ Análise jurídica
- ○ Requerimentos diversos
- ○ Solicitação de cumprimento de decisões
- ○ Não sei informar
- ○ Outro:

7. Por quais meios você recebe as solicitações para trabalhar com dados pessoais no órgão? *

- ○ E-mail
- ○ Físico
- ○ Telefone
- ○ Não sei responder
- ○ Outro:

8. Há alguma orientação a respeito do tratamento dos dados pessoais que instruem as solicitações ou requerimentos? *

- ○ Sim
- ○ Não
- ○ Não é necessária orientação, pois o uso da informação é institucional
- ○ Outro:

9. Somente os dados pessoais estritamente necessários são acessados? *

- ○ Sim
- ○ Não
- ○ Não sei informar

10. Deseja fazer alguma consideração sobre o assunto Proteção de Dados?

- ○ Sim
- ○ Não

Se sim, descreva.


idp
A ESCOLHA QUE
TRANSFORMA
O SEU CONHECIMENTO