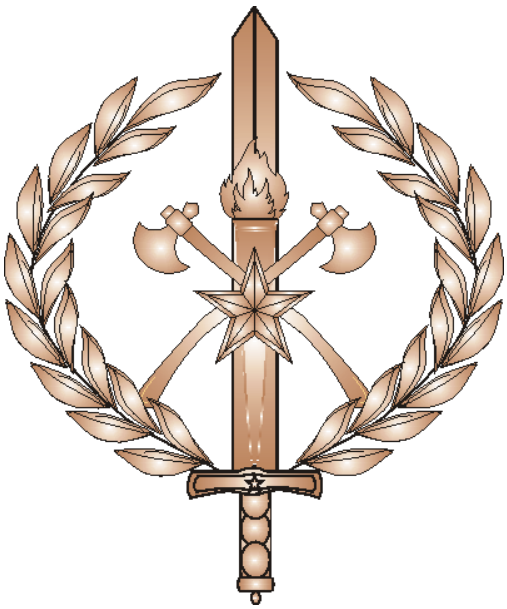
CORPO DE BOMBEIROS MILITAR DO DISTRITO FEDERAL
DEPARTAMENTO DE ENSINO, PESQUISA, CIÊNCIA E TECNOLOGIA
DIRETORIA DE ENSINO
CENTRO DE ESTUDOS DE POLÍTICA, ESTRATÉGIA E DOUTRINA
CURSO DE ALTOS ESTUDOS PARA OFICIAIS

MAJ. QOBM/Compl. **ARNALDO** ALVES DE ALVARENGA



O CORPO DE BOMBEIROS MILITAR DO DISTRITO FEDERAL FRENTE À LEI GERAL DE PROTEÇÃO DE DADOS: DIAGNÓSTICO DE CONFORMIDADE E PROPOSTA DE PLANO DE ADEQUAÇÃO

BRASÍLIA
2025

MAJ. QOBM/Compl. **ARNALDO** ALVES DE ALVARENGA

O CORPO DE BOMBEIROS MILITAR DO DISTRITO FEDERAL FRENTE À LEI GERAL DE PROTEÇÃO DE DADOS: DIAGNÓSTICO DE CONFORMIDADE E PROPOSTA DE PLANO DE ADEQUAÇÃO

Artigo científico apresentado ao Centro de Estudos de Política, Estratégia e Doutrina como requisito para conclusão do Curso de Altos Estudos para Oficiais do Corpo de Bombeiros Militar do Distrito Federal.

Orientador: Ten-Cel. RRm. **BENUR** WANDERLEY MIRANDA DA SILVA

BRASÍLIA
2025

MAJ. QOBM/Compl. **ARNALDO** ALVES DE ALVARENGA

O CORPO DE BOMBEIROS MILITAR DO DISTRITO FEDERAL FRENTE À LEI GERAL DE PROTEÇÃO DE DADOS: DIAGNÓSTICO DE CONFORMIDADE E PROPOSTA DE PLANO DE ADEQUAÇÃO

Artigo científico apresentado ao Centro de Estudos de Política, Estratégia e Doutrina como requisito para conclusão do Curso de Altos Estudos para Oficiais do Corpo de Bombeiros Militar do Distrito Federal.

Aprovado em: _____/_____/_____.

BANCA EXAMINADORA

_____
André Telles Campos – Cel QOBM/Comb.
Presidente

_____
Robson Coelho de Oliveira –Cel. QOBM/Comb.
Membro

_____
Luís Cláudio da Fonseca Franco – Ten-Cel RRm. QOBM/Comb.
Membro

_____
Benur Wanderley **Miranda** da Silva – Ten-Cel RRm.QOBM/Comb.
Orientador

TERMO DE AUTORIZAÇÃO PARA PUBLICAÇÃO

AUTOR: Maj. QOBM/Compl. ARNALDO ALVES DE ALVARENGA

TÍTULO: O CORPO DE BOMBEIROS MILITAR DO DISTRITO FEDERAL FRENTE À LEI GERAL DE PROTEÇÃO DE DADOS: DIAGNÓSTICO DE CONFORMIDADE E PROPOSTA DE PLANO DE ADEQUAÇÃO

DATA DE DEFESA: 00/00/2025.

Acesso ao documento		
(x) Texto completo	( ) Texto parcial	( ) Apenas metadados
Em caso de autorização parcial, especificar a(s) parte(s) que deverá(ão) ser disponibilizadas:		

Licença
DECLARAÇÃO DE DISTRIBUIÇÃO NÃO EXCLUSIVA O referido autor: a) Declara que o documento entregue é seu trabalho original, e que detém o direito de conceder os direitos contidos nesta licença. Declara também que a entrega do documento não infringe, tanto quanto lhe é possível saber, os direitos de qualquer outra pessoa ou entidade. b) Se o documento entregue contém material do qual não detém os direitos de autor, declara que obteve autorização do detentor dos direitos de autor para conceder ao CBMDF os direitos requeridos por esta licença, e que esse material cujos direitos são de terceiros está claramente identificado e reconhecido no texto ou conteúdo do documento entregue. Se o documento entregue é baseado em trabalho financiado ou apoiado por outra instituição que não o CBMDF, declara que cumpriram quaisquer obrigações exigidas pelo respectivo contrato ou acordo. LICENÇA DE DIREITO AUTORAL Na qualidade de titular dos direitos de autor da publicação, autorizo a Biblioteca da Academia de Bombeiro Militar disponibilizar meu trabalho por meio da Biblioteca Digital do CBMDF, com as seguintes condições: disponível sob Licença Creative Commons 4.0 International, que permite copiar, distribuir e transmitir o trabalho, desde que seja citado o autor e licenciante. Não permite o uso para fins comerciais nem a adaptação desta. A obra continua protegida por Direito Autoral e/ou por outras leis aplicáveis. Qualquer uso da obra que não o autorizado sob esta licença ou pela legislação autoral é proibido.

_____

ARNALDO ALVES DE ALVARENGA
MAJ. QOBM/Compl.

RESUMO

Este artigo diagnostica a conformidade do Corpo de Bombeiros Militar do Distrito Federal (CBMDF) com a Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018), focalizando as áreas administrativas, áreas-meio, da Corporação. Utilizando metodologia mista e parâmetros do Acórdão nº 1384/2022 do Tribunal de Contas da União (TCU), combina análise documental com pesquisa empírica via *Control Self-Assessment (CSA)* junto a 40 gestores militares. A análise documental avaliou normativos internos e sua aderência legal, enquanto questionários estruturados geraram dados estatísticos para classificar o grau de conformidade em diferentes dimensões institucionais. Os resultados revelam adequação normativa parcial coexistindo com percepções de baixa conformidade entre gestores - evidenciando hiato crítico entre política formal e prática organizacional. Principais achados incluem: lacunas em governança de dados, ausência de políticas estruturadas de segurança da informação, capacitação insuficiente e desconhecimento sobre obrigações específicas como nomeação de Encarregado pelo Tratamento de Dados Pessoais (EPD) e comunicação de incidentes à Agência Nacional de Proteção de Dados (ANPD). A conformidade documental, presente parcialmente, não se reflete na cultura institucional, sendo insuficiente para garantir efetividade no cumprimento da LGPD. Como contribuição prática, propõe-se plano de adequação focado em governança, segurança e capacitação, orientado pela metodologia TCU. O plano visa reduzir riscos jurídicos e operacionais do tratamento inadequado de dados pessoais, consolidando cultura organizacional voltada à proteção da privacidade, integridade pública e conformidade legal no setor de segurança pública. Este estudo supre lacunas na literatura científica ao explorar desafios da implementação da LGPD em instituições militares de segurança pública, servindo como modelo replicável para diagnósticos similares em outras corporações e esferas governamentais.

Palavras-chave: Conformidade. Governança de dados. LGPD. Proteção de dados pessoais. Segurança pública.

ABSTRACT

This article diagnoses the compliance of the Federal District Military Fire Department (CBMDF) with the General Personal Data Protection Law (LGPD - Law No. 13,709/2018), focusing on the administrative and support areas of the Corporation. Employing a mixed methodology and parameters from Federal Court of Accounts (TCU) Ruling No. 1384/2022, it combines documentary analysis with empirical research via Control Self-Assessment (CSA) among 40 military managers. The documentary analysis evaluated internal regulations and their legal adherence, while structured questionnaires generated statistical data to classify the degree of compliance across different institutional dimensions. The results reveal partial normative adequacy coexisting with perceptions of low compliance among managers—evidencing a critical gap between formal policy and organizational practice. Key findings include: gaps in data governance, absence of structured information security policies, insufficient training, and lack of awareness regarding specific obligations such as the appointment of a Personal Data Processing Officer (EPD) and incident reporting to the National Data Protection Authority (ANPD). Documentary compliance, while partially present, is not reflected in institutional culture and proves insufficient to ensure effective LGPD compliance. As a practical contribution, a strategic adequacy plan is proposed, focused on governance, security, and training, guided by TCU methodology. The plan aims to reduce legal and operational risks from inadequate personal data processing while consolidating an organizational culture oriented toward privacy protection, public integrity, and legal compliance in the public security sector. This study addresses gaps in the scientific literature by exploring challenges in LGPD implementation within military public security institutions, serving as a replicable model for similar diagnostics in other corporations and governmental spheres.

Keywords: Compliance. Data governance. LGPD. Personal data protection. Public security.

1 INTRODUÇÃO

A intensificação da transformação digital na administração pública brasileira tem ampliado exponencialmente o volume de dados pessoais tratados por órgãos estatais, convertendo a governança da informação em uma prioridade estratégica (DONEDA, 2019; BIONI, 2019). A promulgação da Lei nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais (LGPD) — estabeleceu um marco legal imprescindível para regular o tratamento de dados no território nacional. Essa obrigação estatal foi reforçada pela Emenda Constitucional nº 115/2022, que alçou a proteção de dados ao *status* de direito fundamental, conferindo-lhe natureza de cláusula pétrea (BRASIL, 2022).

A *cibercriminalidade* cresce internacionalmente, e o Brasil já chegou a ocupar o segundo lugar no mundo em tentativas de ataques de *ransomware*[1], segundo a CISO Advisor (2023). Esses ataques geralmente criptografam os dados das vítimas e exigem pagamento para liberar as informações. Exemplos como *WannaCry e Ryuk* demonstram sua complexidade e periculosidade, reforçando a necessidade urgente de adotar medidas preventivas.

Em 2023, 83% das organizações brasileiras que enfrentaram ataques *hackers* relataram ter pagado resgates, com prejuízos médios que passaram de R$ 6 milhões por incidente (SUTTO, 2024). Um caso notório foi o ataque às Lojas Renner em 2021, que resultou em perdas superiores a R$ 20 milhões, evidenciando como os controles internos de várias empresas ainda podem estar vulneráveis diante dessas ameaças.

No Distrito Federal, a ameaça deixou de ser algo teórico e passou a ser uma preocupação real. Em março de 2023, um ataque cibernético atingiu dados da Secretaria de Educação e do Corpo de Bombeiros Militar do DF (METRÓPOLES, 2024). Além disso, em 2024, a vulnerabilidade ficou ainda mais evidente com mais de dezesseis incidentes formais registrados pela Controladoria do CBMDF (anexo I), através do “Formulário de Comunicação de Incidente de Segurança com Dados Pessoais”, disponível no Sistema INOVA. Casos como o vazamento de informações de alunos do Colégio Militar Dom Pedro II e a exposição de dados sigilosos de um

[1] *Ransomware*: software malicioso que criptografa dados do usuário e exige pagamento de resgate para liberação do acesso aos arquivos. Constitui ameaça significativa à segurança da informação segundo ABNT NBR ISO/IEC 27001:2013.

militar da reserva (Processos n.º 00053-00020630/2025-04 e 00053-00032925/2025-15) mostram claramente o impacto dessas falhas na prática. Essas ocorrências envolveram a utilização do Guia Orientativo de Respostas a Incidentes de Segurança com Dados Pessoais, publicado no Boletim Geral nº 212/2023, que estabeleceu procedimentos padronizados para contenção, investigação e comunicação desses eventos.

No âmbito do CBMDF, a situação fica ainda mais delicada devido ao volume e à sensibilidade dos dados que são manejados. A corporação lida com informações pessoais e confidenciais de bombeiros militares, servidores civis, pensionistas, dependentes e cidadãos atendidos em áreas essenciais, como saúde, educação, finanças, perícias de incêndio e assistência social (CBMDF, 2025). Embora existam alguns esforços para melhorar essa questão — como o Boletim Geral nº 073/2023, que criou a Comissão de Adequação do CBMDF à LGPD, cujos trabalhos estão parados mesmo após várias prorrogações — ainda há problemas importantes. Entre eles, a ausência de uma política pública de privacidade bem definida, documentos internos desatualizados e falta de capacitação adequada para quem trabalha com esses dados.

No âmbito sancionador, a ANPD instaura processos e aplica penalidades. A Resolução CD/ANPD nº 4/2023 aprovou o Regulamento de Dosimetria e Aplicação de Sanções Administrativas, definindo critérios e prevendo sanções não pecuniárias para órgãos públicos (advertência e publicização da infração) e medidas corretivas (ANPD, 2023).

No CBMDF, agentes públicos envolvidos no tratamento de dados sujeitam-se às sanções disciplinares do Regulamento Disciplinar do Exército e responsabilização por improbidade administrativa quando violarem deveres de proteção e governança de dados (BRASIL, 2002; BRASIL, 1992). A ANPD esclareceu, em 2021, o início da aplicação das sanções administrativas da LGPD (ANPD, 2021).

Apesar do avanço na regulamentação, ainda não existem estudos práticos que avaliem de forma sistemática o quanto os corpos de bombeiros militares estão em conformidade com a LGPD. Essa questão é destacada por autores como Pironti (2021) e por auditorias recentes do Tribunal de Contas da União (TCU, 2022), que

apontam a falta de mecanismos efetivos para verificar essa conformidade no dia a dia da gestão pública.

Com base nisso, este artigo científico tem como ponto de partida a seguinte pergunta: Como adaptar as práticas do CBMDF para garantir a proteção real dos dados pessoais de bombeiros militares, dependentes, pensionistas e cidadãos civis atendidos pela corporação?

Para respondê-la, definiu-se como objetivo geral: Elaborar um plano institucional de adequação do CBMDF à LGPD.

Já os objetivos específicos incluem:

a) Diagnosticar o nível de conformidade do CBMDF à LGPD;

b) Avaliar a percepção dos gestores da área administrativa (área-meio), que mais tratam dados pessoais, quanto ao grau de conformidade com a LGPD;

c) Realizar análise documental das normas institucionais e dos documentos elaborados pela Comissão de Adequação do CBMDF à LGPD;

d) Propor recomendações para adequar as práticas administrativas do CBMDF à LGPD.

Este estudo é importante não só porque visa reduzir riscos jurídicos e operacionais, mas também para fortalecer a maturidade institucional do CBMDF diante das demandas legais e sociais de hoje. Manter conforme à LGPD não é apenas uma obrigação legal, mas também um compromisso ético de proteger a dignidade de todas as pessoas, bem como preservar a imagem institucional. Além disso, pode servir como modelo de governança de dados para outros órgãos de segurança pública.

Por fim, o artigo está organizado em seis partes: Introdução; Revisão de literatura; Metodologia; Resultados; Discussão e Diagnóstico Crítico; e Proposta de Plano de Adequação.

2 DESENVOLVIMENTO

2.1 Revisão de literatura

Para avaliar se o CBMDF está conforme a LGPD, é fundamental contar com uma base teórica e jurídica sólida. Assim, esse tema está organizado em cinco pontos principais: primeiro, a importância de reconhecer a proteção de dados e sua regulamentação; segundo, o consentimento do titular dos dados; terceiro, a publicidade e transparência e a proteção de dados pessoais; quarto, destacar o Acórdão nº 1.384/2022 do TCU como um parâmetro técnico importante na avaliação; e, por fim, destacar o papel das cortes superiores na consolidação das decisões e da jurisprudência sobre esse tema.

2.1.1 A proteção de dados como direito fundamental e sua regulamentação

A proteção de dados pessoais, que surgiu a partir do direito à privacidade, ganhou um *status* de direito fundamental independente no ordenamento brasileiro com a Emenda Constitucional nº 115/2022. Essa mudança foi resultado do acréscimo do inciso LXXIX ao artigo 5º da Constituição Federal, que diz: “é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais”. Tal alteração representa um marco importante, pois garante ao titular o controle sobre suas informações, promovendo a chamada autodeterminação informativa (Doneda, 2019).

No âmbito infraconstitucional, a LGPD estabeleceu princípios essenciais como finalidade, adequação, necessidade e responsabilização (art. 6º). Ela exige que as instituições públicas adotem padrões elevados de transparência e segurança na gestão dos dados. O modelo brasileiro de proteção se inspira bastante no Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR), especialmente na definição de conceitos, deveres do controlador e medidas de proteção técnica.

2.1.2 O consentimento do titular dos dados pessoais

O consentimento (art. 7º, I da LGPD) não é adequado para uso indiscriminado no setor público, principalmente devido à desigualdade de poder entre o Estado e o cidadão (Bioni, 2019). O artigo 23 da LGPD deixa claro que o tratamento de dados

por órgãos públicos deve se basear em uma obrigação legal ou regulatória, afastando a necessidade de consentimento em situações relacionadas a políticas públicas, execução de competências legais ou proteção de interesses públicos.

Nesse cenário, o consentimento não deve ser visto como uma autorização absoluta, mas sim como um mecanismo subsidiário. A atuação do Estado precisa estar fundamentada em política institucionais, bem definidas, que assegurem proporcionalidade, finalidade clara e a minimização dos dados coletados. A ausência desses princípios pode gerar riscos jurídicos e institucionais, podendo até levar à responsabilização objetiva, conforme o artigo 42 da LGPD.

2.1.3 Publicidade *versus* proteção de dados pessoais

A LGPD traz uma nova abordagem, baseada na transparência aliada à responsabilidade. No setor público, é fundamental equilibrar o princípio constitucional da publicidade (artigo 37, *caput* da Constituição Federal) com a necessidade de proteger os dados pessoais. Isso ajuda a evitar violações indevidas à privacidade, à honra e à imagem dos titulares dessas informações (Blum; López, 2020).

Para isso, é preciso reformular os processos de gestão da informação nas instituições públicas. Isso inclui criar regras sobre como classificar os dados, limitar o acesso conforme o perfil funcional de cada pessoa e manter registros que possam responsabilizar quem manipula essas informações. Acocella (2020) reforça que esse equilíbrio é especialmente importante em áreas como segurança pública, saúde e recursos humanos — setores em que o CBMDF atua diretamente — porque lidam com uma abundância de dados sensíveis, tornando indispensável a implementação de controles normativos e tecnológicos adequados.

2.1.4. Os Acórdãos TCU nº 1.384/2022 e o nº 1372/2025 (junho de 2025)

Para avaliar o quanto a Administração Pública Federal está adequada à LGPD, o TCU criou, por meio do Acórdão nº 1.384/2022 (Plenário), uma matriz diagnóstica que contempla nove critérios técnicos de controle institucional. O relator, Ministro Augusto Nardes, identificou fragilidades estruturais em 382 instituições federais auditadas e sugeriu diretrizes claras para medir o nível de maturidade organizacional no tratamento de dados pessoais (TCU, 2022).

Os nove parâmetros estabelecidos foram os seguintes:

1) Existência de cláusulas contratuais específicas de proteção de dados;

2) Política de classificação da informação institucionalizada;

3) Política formal de proteção de dados pessoais (PPDP);

4) Programa contínuo de capacitação em LGPD;

5) Política de privacidade clara, pública e acessível;

6) Mecanismos formais para atendimento aos direitos dos titulares;

7) Plano institucional de resposta a incidentes de segurança;

8) Controles de acesso baseados em perfil funcional;

9) Utilização de criptografia ou soluções tecnológicas equivalentes.

Neste estudo, esses critérios foram operacionalizados por meio da elaboração de um Checklist de Conformidade à LGPD (CC-LGPD). A aplicação foi feita usando a técnica de autoavaliação estruturada CSA, o que permitiu uma avaliação objetiva do grau de conformidade do CBMDF com os padrões técnicos estabelecidos.

Em junho de 2025, o TCU publicou um novo relatório de auditoria (Acórdão nº 1372/2025 - Plenário) que reforça o uso do mesmo modelo de autoavaliação de controles, conhecido como CSA, aplicado inicialmente no Acórdão nº 1.384/2022. Nessa fiscalização, foram avaliadas 387 organizações públicas federais, incluindo CBMDF, por ser mantido pela União, visando acompanhar a evolução na implementação da LGPD. A metodologia permaneceu baseada em um questionário eletrônico estruturado, respondido pelos gestores, que gerou o indicador de conformidade com a LGPD (iLGPD), inclusive pelo CBMDF.

Essa abordagem permitiu uma comparação da maturidade organizacional ao longo do tempo. Os resultados mostraram uma melhora discreta no cenário nacional de conformidade, com uma diminuição dos níveis considerados “inexpressivo” e “inicial”, além de um aumento nos níveis “intermediário” e “aprimorado”. Essa nova avaliação reforça a atualidade e a confiabilidade do método CSA, fortalecendo

também a validade prática deste estudo, que utilizou essa mesma abordagem técnico-normativa para verificar a conformidade institucional com a LGPD.

2.1.4.1 Fundamentação normativa dos parâmetros utilizados pelo TCU

A análise da conformidade do CBMDF com a LGPD (Lei nº 13.709/2018) utiliza como base os critérios técnicos estabelecidos pelo Acórdão nº 1.384/2022 do TCU. Esses critérios refletem uma governança institucional sólida na proteção de dados pessoais. Além de serem respaldados pela legislação brasileira, eles também estão alinhados com normas internacionais de referência, como a ISO/IEC 27001:2013 (gestão de segurança da informação), a ISO/IEC 27002:2013 (controles de segurança) e a ISO/IEC 27701:2019 (privacidade da informação).

Nesse contexto, o Acórdão nº 1.384/2022 se destaca como um importante instrumento técnico e normativo de avaliação, ao mostrar que 76,7% das entidades auditadas àquela oportunidade estavam em estágio “Inexpressivo” ou “Inicial” de conformidade.

A seguir, apresenta-se a fundamentação legal e técnica de cada parâmetro utilizando os dados do aludido acórdão de 2022 e da LGPD:

1. Cláusulas contratuais com operadores

A ausência de cláusulas contratuais específicas, que obriguem as contratadas a protegerem dados pessoais, compromete a responsabilização conjunta e a rastreabilidade das obrigações entre controlador e operador. Segundo o art. 5º, VI da LGPD, controlador é quem toma decisões sobre o tratamento de dados pessoais, enquanto operadores (art. 5º, VII) são pessoas físicas ou jurídicas que processam esses dados em seu nome. O CBMDF atua como operador ao tratar dados por determinação legal e, simultaneamente, contrata terceiros — principalmente na área da saúde — que, ao manusearem dados pessoais em seu nome, assumem automaticamente essa condição operacional.

2. Política de classificação da informação

Classificar informações por nível de sensibilidade (dados pessoais ou sensíveis) é fundamental para aplicar o princípio da minimização (arts. 6º, VII) e

estabelecer controles de acesso eficazes (art. 46 da LGPD). O TCU constatou que 65% dos órgãos analisados não possuíam política definida. Essa política organiza os dados pela sensibilidade, determinando proteção e acesso adequados conforme o risco envolvido, sendo essencial para a segurança da informação.

3. Política de Proteção de Dados Pessoais (PPDP)

A PPDP organiza o programa de governança em privacidade e orienta os controles internos (artigo 50 da LGPD). O TCU constatou que 82% dos órgãos públicos ainda não formalizaram essa política. A PPDP estabelece diretrizes, princípios, responsabilidades e práticas para o tratamento adequado dos dados pessoais, promovendo gestão transparente e segura.

4. Programa de capacitação continuada em proteção de dados pessoais

A capacitação contínua dos agentes de tratamento — pessoas autorizadas pelo controlador ou operador a executar o tratamento de dados (art. 5º, VIII, LGPD) — é fundamental para garantir conformidade legal e prevenir violações. Contudo, apenas 10% das instituições promovem treinamentos regulares sobre LGPD.

5. Política de privacidade institucional

A Política de Privacidade Institucional — documento que explicita quais dados pessoais são coletados, como são utilizados, com quem compartilhados e os direitos dos titulares — garante acesso a informações claras sobre o tratamento de dados. Tal política materializa o princípio da transparência (art. 6º, LGPD) e atende às exigências informativas do art. 9º. Contudo, 75% das entidades carecem dessa política, configurando grave violação do dever de transparência conforme jurisprudência consolidada.

6. Mecanismos de atendimento aos titulares dos dados pessoais

Os canais de comunicação e processos internos devem viabilizar o exercício célere e eficiente dos direitos dos titulares — como acesso, correção, eliminação e portabilidade de dados (arts. 18 e 19, LGPD). Contudo, apenas 14% das organizações demonstraram capacidade operacional completa para atender essas requisições, conforme jurisprudência consolidada.

7. Plano de resposta a incidentes com dados pessoais

O Plano de Resposta a Incidentes — documento que define ações para identificar, conter e comunicar vazamentos de dados pessoais — materializa a obrigação do controlador de notificar incidentes à ANPD e aos titulares afetados, além de adotar medidas mitigatórias de riscos (art. 48, LGPD). Entretanto, 84% das instituições públicas auditadas carecem desse instrumento.

8. Controles de acesso baseados em perfil funcional

A segmentação do acesso por necessidade funcional — princípio que restringe o tratamento de dados ao mínimo necessário para cada função específica — constitui exigência expressa das medidas de segurança (arts. 46 a 49, LGPD). Contudo, apenas 16% das entidades implementaram esse controle de forma abrangente

9. Uso de criptografia ou solução equivalente

A criptografia, embora facultativa, constitui técnica eficaz de mitigação de riscos conforme art. 48, §3º da LGPD. Contudo, 43% dos órgãos auditados não empregavam qualquer forma de ofuscação ou anonimização de dados, segundo acórdão do TCU.

A análise desses critérios evidencia que o cumprimento da LGPD demanda abordagem integrada: normas internas, práticas robustas de segurança da informação, capacitação de agentes públicos e canais eficientes de comunicação com titulares. Documentos formais sem implementação prática são insuficientes para atender ao padrão de responsabilidade legal.

Para o CBMDF, essa fundamentação, acima exposta, possibilita diagnóstico preciso da maturidade institucional, identificando pontos críticos e oportunidades de melhoria. Ao correlacionar essa avaliação às melhores práticas internacionais e orientações do TCU, o estudo fundamenta um plano que alinha ações às exigências legais, técnicas e sociais da proteção de dados no setor público.

2.1.5 Jurisprudência das Cortes Superiores: STF e STJ sobre LGPD

A jurisprudência do Supremo Tribunal Federal tem consolidado o direito à proteção de dados como garantia constitucional. No julgamento conjunto da ADI 6649 e ADPF 695 (2022), a Corte reafirmou que compartilhamento de dados entre órgãos públicos deve respeitar princípios da necessidade, finalidade e transparência, conforme arts. 7º e 23 da LGPD. Declarou inconstitucional o art. 22 do Decreto nº 10.046/2019, exigindo reestruturação do Comitê Central de Governança de Dados, e confirmou competência exclusiva da União para legislar sobre proteção de dados (ADI 6561).

No mesmo sentido, o Superior Tribunal de Justiça, no REsp 2.147.374-SP (Info STJ 838/2024), consolidou que responsabilidade civil por vazamentos de dados é objetiva, inclusive em ataques cibernéticos. A ausência de comprovação de fatores externos ou medidas técnicas atualizadas pode responsabilizar o controlador, conforme arts. 42 a 46 da LGPD.

Esses entendimentos esclarecem que incidentes de segurança não eximem órgãos públicos do dever de diligência. Reforçam a necessidade de *accountability*, exigindo demonstração de políticas eficazes, controles adequados e respostas rápidas à violação de dados.

Nesse contexto, o setor público — especialmente instituições militares como o CBMDF — deve evoluir de postura reativa para governança preventiva, pautada por critérios objetivos de conformidade e mitigação de riscos. Esse arcabouço jurídico-jurisprudencial sustenta o modelo avaliativo desta pesquisa e orienta as recomendações do Plano de Adequação.

2.2 Metodologia

2.2.1 Estrutura Metodológica Geral

Esta pesquisa é classificada como aplicada, pois busca oferecer soluções práticas e concretas para o desafio do CBMDF se adequar à LGPD. Optou-se por um método exploratório-descritivo, com foco em entender melhor o funcionamento organizacional e identificar o nível de conformidade tanto na documentação quanto nas operações, segundo a legislação vigente.

Foi utilizada uma abordagem mista, que combina técnicas qualitativas — voltadas para interpretar documentos e percepções dos gestores — e quantitativas, que mensuram o Índice Global de Conformidade à LGPD (iG-LGPD) com base em critérios técnicos específicos.

Ademais, os dados foram coletados através de análise documental oficial e questionário de autoavaliação estruturado, aplicado nos meses de maio e junho de 2025 via Google *Forms*. O instrumento foi encaminhado pelo processo SEI nº 00053-00054379/2025-73 aos diretores e comandantes de centros, policlínicas e colégios, bem como ao chefe dos projetos sociais, seguindo os parâmetros do Acórdão nº 1.384/2022 do TCU. A combinação de fontes normativas, evidências institucionais e percepções dos gestores conferiu rigor à análise.

2.2.2 Pesquisa Bibliográfica

A fundamentação teórica desta pesquisa foi construída com base em livros de renomados doutrinadores no Brasil, como Pironti (2021), Doneda (2019), e Bioni (2019), bem como em artigos científicos, normas técnicas e jurisprudência especializada. Essas fontes serviram tanto para embasar o referencial teórico quanto para orientar a elaboração dos instrumentos de coleta e análise dos dados. Essa base conceitual apoiou a abordagem sobre proteção de dados, governança pública e conformidade com a LGPD, levando em consideração os critérios técnicos do Acórdão TCU n.º 1.384/2022 e guiando toda a lógica avaliativa adotada ao longo do estudo.

2.2.3 Pesquisa Documental

A análise documental seguiu os princípios do art. 6º da LGPD, que orientam a interpretação normativa e atuação dos agentes públicos no tratamento de dados: finalidade (uso com propósito legítimo), necessidade (tratamento limitado ao essencial), segurança (proteção por medidas técnicas e administrativas), transparência (clareza sobre o tratamento), qualidade dos dados (exatidão e atualização) e acesso livre (garantia de acesso à informação pública). Esses princípios transcendem exigências formais, demandando base normativa sólida sustentada por políticas efetivas de governança e proteção de dados.

Complementarmente, a análise seguiu diretrizes técnicas das normas ISO/IEC 27701:2019, 27001:2013 e 27002:2013, referências mundiais para gestão da privacidade e segurança da informação. A ISO/IEC 27001 estabelece requisitos para Sistema de Gestão de Segurança da Informação (SGSI), a 27002 apresenta controles e boas práticas para implementação, e a ISO/IEC 27701 amplia essas orientações focando especificamente na proteção de dados pessoais, alinhando-se aos princípios da LGPD.

A combinação dos conceitos da LGPD com os controles das normas ISO proporciona abordagem integrada e robusta, permitindo avaliar não apenas a existência de documentos institucionais, mas sua conformidade às boas práticas de governança, exigências legais e eficácia na mitigação de riscos. Essa metodologia híbrida confere maior confiabilidade e credibilidade técnico-jurídica aos resultados.

2.2.4 Pesquisa de Campo: Autoavaliação de Controles (CSA)

A coleta de informações foi feita usando a técnica de Autoavaliação de Controles Internos (*Control Self-Assessment – CSA*), através do *Checklist* de Conformidade à LGPD (CC-LGPD), que aparece no Apêndice A. Esse instrumento foi direcionado aos gestores das áreas mais envolvidas e sensíveis no tratamento de dados pessoais no CBMDF, segundo o mapeamento de dados institucional. As OBMs selecionadas foram: Recursos Humanos, Finanças, Ouvidoria, Ensino, Compras, Contratos, Ajudância-Geral, Projetos Sociais, e Colégios Militares, por meio de processo SEI 00053-00054379/2025-73.

O CC-LGPD foi criado com base nos nove critérios técnicos do Acórdão TCU nº 1.384/2022, divididos em 21 perguntas práticas. Assim, foi possível avaliar de forma clara e objetiva o nível de conformidade de cada instituição com a lei.

2.2.5 População, Amostra e Critérios de Exclusão

Na pesquisa, foram convidados gestores das unidades administrativas mencionadas, sendo diretor e subdiretor nas diretorias, e um representante nos demais órgãos, perfazendo cerca de 40 gestores. Optou-se por amostragem não probabilística por conveniência, obtendo-se 38 respostas válidas, o que representa 95% do universo de gestores identificados.

Consoante o artigo 4º, inciso III, da LGPD, foram excluídos os setores operacionais que atuam diretamente na segurança pública, defesa nacional ou repressão penal. Essas áreas devem possuir regras específicas para a proteção de dados pessoais.

2.2.6 Instrumentos e Parâmetros de Avaliação

O CC-LGPD contou com 21 perguntas objetivas, organizadas em nove áreas, conforme explicado no item 2.1.4 acima. Além disso, o Acórdão TCU nº 1.384/2022 foi utilizado como referência técnica para avaliar o diagnóstico institucional.

As respostas foram avaliadas usando escalas dicotômicas (0 ou 1) ou trinárias (0, 1 ou 2), com uma pontuação máxima de 40 pontos. O desempenho geral foi resumido no Índice Global de Conformidade à LGPD (iG-LGPD), que foi classificado assim:

a) Baixa conformidade: IG ≤ 39%

b) Conformidade parcial: 40% ≤ IG ≤ 74%

c) Conformidade satisfatória: IG ≥ 75%

2.2.7 Procedimentos de Coleta e Análise de Dados

Os dados foram coletados em duas fases:

a) análise de documentos internos;

b) aplicação do CSA aos gestores.

Para tratar os dados quantitativos, usou-se técnicas descritivas simples, como frequências e percentuais, com o auxílio do Microsoft Excel®.

Ao combinar informações documentais e relatos dos gestores, garantiu-se maior confiança nos resultados e validação das conclusões. Essa abordagem permitiu análise ampla, integrando conformidade documental com percepção dos gestores, seguindo o modelo do TCU.

2.2.8 Limitações da Pesquisa

Entre as limitações identificadas, destaca-se a resistência de alguns setores à participação, lacunas na formalização das normas, a falta de um controle documental sistemático e o uso de práticas informais no tratamento de dados. Para enfrentar esses desafios, foram asseguradas condições éticas básicas, como a confidencialidade e a obtenção da autorização do Encarregado pelo Tratamento de Dados Pessoais institucional.

Como consequência, recomenda-se que essa metodologia seja aplicada em outras organizações do setor público de segurança, como uma ferramenta de avaliação diagnóstica padronizada e de monitoramento contínuo do cumprimento da LGPD.

2.3 Resultados e discussão

2.3.1 Análise documental

A análise documental teve como objetivo revisar, de forma técnica e organizada, a existência, o conteúdo e a efetividade dos instrumentos normativos e administrativos essenciais para garantir a conformidade com a LGPD. Foram avaliados os principais atos internos, documentos operacionais e contratos, considerando a LGPD, os critérios estabelecidos no Acórdão TCU nº 1.384/2022 e as orientações da NBR ISO/IEC 27701:2019. Além disso, a fundamentação de cada achado possui embasamento legal e jurisprudencial explicados na seção “Revisão de Literatura” deste artigo. Veja os pontos principais:

a) Instrução Normativa nº 4/2024 – DERHU

Essa norma regula o tratamento e o acesso a dados pessoais presentes em processos administrativos envolvendo sigilo profissional, especialmente na área da saúde institucional. Apesar de avançar ao limitar acessos indevidos e responsabilizar os servidores, sua abrangência ainda é limitada. Ela não cobre aspectos relacionados aos direitos dos titulares, cláusulas contratuais padrão, política geral de dados, planos de capacitação ou de resposta a incidentes.

b) Portaria nº 2/2022 – Política de Proteção de Dados Pessoais (PPDP/CBMDF)

Este documento é o principal marco normativo do CBMDF na área de proteção de dados. Define princípios, direitos dos titulares, ciclo de vida das informações, obrigações internas, governança, contratos e transparência. No entanto, apresenta algumas lacunas relevantes: não há uma política de privacidade específica, política de classificação das informações, procedimentos claros para atendimento aos titulares, planos de capacitação ou controle de acessos. Além disso, faltam planos técnicos para resposta a incidentes e cláusulas padronizadas de proteção nos contratos. Assim, apesar de ser uma estrutura importante, ainda precisa ser consolidada na prática e na técnica.

c) Portaria nº 25/2023 – Unidade Gestora da LGPD (UGLGPD/CBMDF)

Essa portaria cria formalmente a unidade responsável pela gestão da LGPD na instituição e define quem são os responsáveis internos. Contudo, ela não estabelece procedimentos operacionais, planos de capacitação ou protocolos específicos para atendimento aos titulares, ou segurança da informação. A ausência dessas orientações compromete a efetividade da unidade como órgão de governança de dados.

d) Portaria nº 40/2022 – Plano de Dados Abertos (PDA/CBMDF)

Ela regulamenta a disponibilização de dados públicos com foco na transparência ativa. No entanto, não prevê mecanismos para separar dados públicos de informações pessoais protegidas nem aborda aspectos como classificação dos dados, consentimento, privacidade, capacitação ou resposta a incidentes. Por isso, embora importante para promover a transparência, essa portaria não atende completamente aos requisitos da LGPD e precisa estar alinhada com as políticas de proteção de dados pessoais.

e) Guia Orientativo de Respostas a Incidentes com Dados Pessoais (2023)

Este documento técnico operacional define os procedimentos internos para responder a incidentes relacionados à segurança da informação, seguindo as orientações da LGPD e da ANPD. É uma das iniciativas mais completas do CBMDF nesse tema, abordando ações de mitigação, registros e notificações. No entanto, ele não inclui diretrizes específicas sobre privacidade, classificação dos dados ou

mecanismos para atendimento aos titulares. Além disso, falta estabelecer controles de acesso e cláusulas contratuais específicas — pontos que limitam sua atuação isoladamente.

f) Análise dos editais de licitações e contratos (CBMDF/2025)

Os contratos e editais foram selecionados via consulta ao portal de transparência do CBMDF (https://www.cbm.df.gov.br/lai/), aba "Licitações e Contratos", em 15 de julho de 2025, analisando-se todos os instrumentos contratuais disponíveis.

Assim, destaco os contratos ARMOR PRINT LTDA e TRIEL-HT S/A, bem como o Edital de Credenciamento nº 01/2025 para serviços médicos e contratos de credenciamento diversos) carecem de cláusulas específicas de proteção de dados pessoais, contrariando os arts. 39 e 42 da LGPD. O Edital PE nº 90059/2025, embora inclua cláusulas sobre proteção de dados, confidencialidade e treinamento, omite orientações sobre notificação de incidentes e descarte seguro dos dados. A análise indica que os contratos administrativos não estão totalmente alinhados com a LGPD, fragilizando o controle sobre operadores e terceiros.

g) Portaria nº 31/2012 – Manual de Redação Oficial do CBMDF

O objetivo dessa portaria foi padronizar a elaboração de documentos institucionais como memorandos, ofícios, relatórios e portarias. No entanto, a versão atual apresenta sérios descompassos com a LGPD (Lei nº 13.709/2018), refletindo normativa desatualizada.

Verificou-se que o Manual de Redação Oficial foi elaborado antes da adoção do Sistema Eletrônico de Informações (SEI), hoje responsável pela tramitação oficial de documentos na administração pública federal. O SEI foi criado para fortalecer segurança, rastreabilidade, transparência e economicidade no manuseio de informações. No entanto, a ausência de alinhamento entre o manual e os fluxos do SEI compromete a conformidade institucional com práticas modernas de segurança da informação e governança documental.

Além disso, alguns modelos promovem coleta excessiva de dados pessoais — como nome completo, RG, CPF, endereço e estado civil —, violando princípios da

LGPD como necessidade, finalidade e minimização (coletar apenas o indispensável para finalidade clara e legal).

O documento também falha ao não abordar mecanismos cruciais, como anonimização, consentimento, tratamento de dados sensíveis, restrição de acesso por perfis e direitos dos titulares. A ausência desses elementos compromete não só conformidade com a LGPD, mas também segurança jurídica das comunicações institucionais, sobretudo quando lidam com dados sigilosos.

A forma como o BG do CBMDF publica informações pessoais, como divórcios, casamentos — inclusive homoafetivos—, expõe indevidamente a intimidade dos militares. A divulgação irrestrita desses dados fere princípios da LGPD, gerando riscos à privacidade e integridade dos envolvidos.

Diante disso, a atualização desse manual torna-se urgente. Essa revisão deve incorporar os princípios da LGPD, recomendações do Acórdão TCU nº 1.384/2022 e normas técnicas da ABNT, como a NBR ISO/IEC 27701:2019, garantindo maior proteção de dados e respeito à privacidade.

h) A Portaria nº 11, de 1º de abril de 2025, do CBMDF

Trata do sigilo institucional, mas não supre os critérios exigidos pela LGPD para classificação de dados pessoais, como sensibilidade ou minimização (arts. 6º e 46). Também não segue práticas das normas ISO/IEC 27001 e 27002 sobre proteção e controle de acesso a dados pessoais.

i) A Portaria nº 19/2025, que alterou o Regimento Interno do CBMDF

Criou a Seção de Governança de Dados (SEGOD) no Gabinete do Comandante-Geral, institucionalizando a gestão de dados como uma função fixa. A medida reforça o compromisso do CBMDF com a LGPD ao centralizar políticas, integrar ações de segurança da informação e apoiar decisões estratégicas.

Ademais, diante da análise documental, a instituição encontra-se em fase de adequação, com marcos importantes estabelecidos, mas ainda apresentando lacunas estruturais críticas sobre proteção de dados pessoais. A ausência de instrumentos essenciais — política de privacidade, classificação da informação pessoal, cláusulas

contratuais padrão e programas de capacitação — prejudica a maturidade da governança de dados pessoais. Contudo, iniciativas como a Portaria nº 2/2022 e o Guia de Incidentes representam avanços concretos.

O quadro abaixo oferece uma visão geral clara e objetiva sobre a situação dos documentos do CBMDF relacionados à conformidade com a LGPD. Nele, destaca-se os principais instrumentos considerados essenciais para a adequação da instituição, baseando-se nos critérios estabelecidos pela ANPD, nas normas técnicas da ABNT (como as NBR ISO/IEC 27701:2019, 27001:2013 e 27002:2013), além do Acórdão nº 1.384/2022 do TCU.

Este quadro organiza o *status* de implementação de cada documento dentro do CBMDF, classificando-os como "possui", "não possui", "em execução" ou "parcialmente implementado". Também apresenta detalhes das evidências documentais consultadas no SEI. Essa abordagem facilita a compreensão dos avanços feitos pela instituição e evidencia as lacunas normativas que ainda precisam ser preenchidas para que a corporação esteja totalmente conforme a LGPD.

Figura 1 – Quadro da Conformidade da adequação do CBMDF à LGPD

Documento / Instrumento Essencial	Status no CBMDF	Evidência Documental
Política de Proteção de Dados Pessoais (PPDP)	Regulamentação existente, mas não substitui política normativa	Portaria nº 2/2022; SEI 158980485
Nomeação do Encarregado (DPO)	Possui	Boletins Gerais; Relatório (SEI 158980485)
Política de Privacidade de Dados Pessoais	Não Possui	SEI 149019971; SEI 158980485
Política de Segurança da Informação (dados pessoais)	Não Possui	SEI 149019971
Política de Cookies[1]	Não Possui	Não identificada
Plano de Resposta a Incidentes	Possui	Guia de Incidentes (2023); SEI 152929061
Inventário de Dados (Data Mapping)	Possui	Plano de Trabalho (SEI 152521744)
Relatório de Impacto à Proteção de Dados (RIPD)	Não Possui	SEI 158980485
Cláusulas Contratuais Padronizadas	Parcialmente Implementadas	SEI 164540305
Acordos de Compartilhamento de Dados	Não Possui	SEI 158980485

Fonte: O autor.

A análise subsequente examina os principais documentos produzidos pela Comissão de Adequação do CBMDF à LGPD e suas subcomissões, conforme registros do SEI. Cada instrumento foi avaliado quanto à finalidade, conteúdo normativo e alinhamento às exigências legais e técnicas, particularmente à LGPD e ao Acórdão TCU nº 1.384/2022. A seguir, inicia-se pelo:

a) Relatório de Auditoria nº 1/2024 – CBMDF/CTROL/COMISSOES/AGTIC - (SEI nº 130859289 | Processo nº 00053-00131264/2023-48)

Este relatório apresenta uma análise detalhada sobre o nível de maturidade do CBMDF em termos de segurança da informação. Ele revelou várias lacunas importantes na estrutura de governança de dados, como a ausência da Norma de Segurança da Informação e Comunicação (NoSIC), a falta de uma política de retenção de dados, uma gestão inadequada do consentimento dos usuários e controles insuficientes sobre os registros de acesso (logs). Além disso, identificou falhas na realização de testes de vulnerabilidade e a ausência total de aplicação dos princípios

de *"Privacy by Design*" (Privacidade desde a Concepção) e "*Privacy by Default" (*Privacidade por Padrão). Isso demonstra que, até o momento, a postura do órgão ainda é mais reativa do que proativa na proteção dos dados pessoais.

b) Relatório Final da Subcomissão de Observância ao Acórdão TCU nº 1.384/2022 - (SEI nº 158980485 | Processo nº 00053-00034524/2024-19)

Este relatório apresenta uma avaliação detalhada da conformidade do CBMDF com os nove parâmetros técnicos estabelecidos pelo TCU. Entre as principais questões identificadas, estão a ausência de cláusulas contratuais específicas para proteção de dados, fragilidades nos mecanismos de atendimento aos titulares e a falta de fluxos formais para o tratamento dessas informações. Para melhorar essa situação, o documento recomenda ações concretas, como a assinatura de acordos de compartilhamento, a criação de políticas específicas e a atualização do manual de redação oficial. Dessa forma, o relatório ajuda a transformar as orientações do Acórdão em obrigações práticas e administrativas.

c) Relatório nº 10/2024 da Subcomissão de Adequação dos Sistemas de TI (SEI nº 149019971 | Processo nº 00053-00140974/2023-69)

Focado na infraestrutura digital, o relatório identificou sistemas operando fora do escopo da Diretoria de Tecnologia da Informação e Comunicação (DITIC), fenômeno denominado "*Shadow IT*". Constatou-se ausência de Relatórios de Impacto à Proteção de Dados (RIPD) e políticas de privacidade definidas. Observou-se que alguns sistemas não utilizam criptografia padrão e carecem de inventários sistematizados. Sistemas críticos como SIPROS e WEBMED operam sem governança formal, elevando riscos de violações de dados pessoais.

d) Plano de Trabalho do CBMDF/CTROL/COMISSÕES/LGPD - (SEI nº 152521744 | Processo nº 00053-00163122/2023-40)

Este documento estratégico define as etapas para a adaptação institucional às exigências da LGPD. Ele inclui ações como o mapeamento de fluxos de dados, revisão de documentos, capacitações e atualização das normas internas. Apesar do avanço na gestão do processo, a implementação completa do plano depende de medidas estruturais importantes, como a padronização das normas, a

institucionalização de políticas específicas e a adoção de indicadores que acompanhem a conformidade.

e) Memorando nº 60/2024 – CBMDF/DICOA/SECON/SUCOV - (SEI nº 140008803)

Este documento trata da padronização de cláusulas contratuais relacionadas à LGPD. Embora apresente uma minuta de cláusula de proteção de dados, o memorando revela que, até então, na maioria dos contratos vigentes, essas cláusulas eram inexistentes ou estavam apenas começando a ser implementadas. A falta de uma previsão contratual adequada prejudica a responsabilização de terceiros e enfraquece o papel do CBMDF como controlador de dados.

f) Memorando nº 29/2025 – CBMDF/DICOA - (SEI nº 164540305)

Este memorando consolida o posicionamento da Diretoria de Contratações e Aquisição sobre a adequação dos instrumentos contratuais à LGPD. Apesar de destacar avanços e do apoio da Procuradoria-Geral do DF, o documento também reconhece limitações operacionais para fiscalizar o cumprimento das obrigações previstas. Essa dificuldade na fiscalização pode comprometer a eficácia das cláusulas e representa uma vulnerabilidade jurídica para o CBMDF.

g) Memorando nº 32/2025 – CBMDF/DITIC/SESIS - (SEI nº 163346466)

Este documento aborda a existência de sistemas legados e externos à estrutura institucional, como SIPROS, WEBMED e Moodle EAD, que operam com dados sensíveis sem controle direto da DITIC. A própria Seção de Sistemas reconhece que não possui conhecimento técnico suficiente sobre as medidas de segurança para dados pessoais adotadas nesses sistemas, o que configura uma violação ao art. 46 da LGPD e aumenta o risco de incidentes de segurança.

h) Planilha Modelo de Mapeamento de Dados Pessoais – modelo CGDF

Ferramenta técnica criada para identificar o ciclo de vida dos dados pessoais nas diferentes áreas da Corporação. Embora seja um recurso importante para a metodologia de trabalho, os relatórios da subcomissão indicam que seu uso ainda é limitado e pouco sistematizado. A falta de atualizações constantes compromete a construção de um Registro das Operações de Tratamento (RoPA), exigido pelo art. 37 da LGPD.

i) Relatório Preliminar de Avaliação de Conformidade à LGPD

Este relatório apresenta uma análise resumida usando uma metodologia de pontuação baseada nos parâmetros do Acórdão TCU nº 1.384/2022. O índice geral de conformidade do CBMDF foi avaliado em 55,6%, classificando a instituição como "Conformidade Parcial". O documento reconhece avanços importantes, como a criação da Política de Proteção de Dados Pessoais (PPDP) e o Guia de Incidentes, mas destaca a necessidade urgente de formalizar políticas complementares, atualizar contratos e estruturar canais eficientes para atendimento aos titulares dos dados.

Portanto, a análise documental não apenas mostrou o estado atual de conformidade do órgão com as normas, mas também serviu como base para criar o *checklist* de avaliação e para desenvolver recomendações estratégicas, que serão discutidas nos próximos tópicos.

2.3.2 Análise das Percepções dos Gestores (método CSA/TCU)

Os dados indicam que há várias barreiras institucionais que dificultam a implementação adequada da LGPD no CBMDF. A principal dificuldade apontada pelos gestores está relacionada à falta de capacitação dos servidores em proteção de dados, mencionada por 86,8% dos respondentes (n=33). Isso revela uma necessidade urgente de melhorar a formação técnica das equipes. Outras dificuldades frequentes incluem o desconhecimento dos direitos dos titulares (55,3%), a sobrecarga de trabalho dos gestores (55,3%) e a falta de uma infraestrutura tecnológica adequada (52,6%).

Além dessas questões, também foram identificados obstáculos culturais e normativos, como a resistência às mudanças na organização (52,6%), a ausência de protocolos formais para o descarte seguro de dados (47,4%) e a fragilidade nos mecanismos de resposta a incidentes de segurança (36,8%). Esses resultados mostram que os desafios para atingir a conformidade vão além da ausência de regras: eles envolvem aspectos operacionais, culturais e estruturais que precisam de ações integradas de governança, treinamento e revisão de processos internos. Enquanto, essas questões não são resolvidas, elas comprometem a transparência do órgão e o cumprimento da obrigação legal de proteger os dados pessoais, conforme determina o artigo 6º da LGPD.

A Tabela 1 mostra os resultados das respostas dos gestores do CBMDF ao usar o CSA. O questionário teve 21 perguntas objetivas, organizadas segundo os eixos que o TCU definiu para avaliar a conformidade da instituição com a LGPD.

Cada pergunta foi respondida em uma escala que indica o nível de conformidade: ausente, parcialmente implementado ou totalmente implementado. Com essas respostas, foi possível calcular o Índice Global de Conformidade (iGLGPD). Ao consolidar os dados, identificamos os níveis médios de aderência em cada categoria, o que ajudou a classificar a instituição como estando em "Conformidade Parcial", conforme os critérios do próprio instrumento.

Esses resultados refletem a percepção geral da instituição sobre o estágio atual da implementação da LGPD no CBMDF. Eles mostram avanços importantes, como a nomeação do encarregado e a existência de uma política geral de proteção, todavia apontam fragilidades relevantes, como a ausência de uma política de privacidade, mecanismos operacionais para responder a incidentes e controles técnicos sistematizados.

A coluna "Categoria" apresenta os temas mais frequentes apontados pelos participantes. Já a coluna “n” indica o número de gestores, em um total de 38, que marcaram cada uma dessas barreiras em suas unidades administrativas. A coluna “%” mostra a porcentagem que esse número representa em relação ao total de respondentes. O dado mais comum foi a "falta de capacitação dos servidores", apontada por 33 gestores, o que corresponde a 86,8%. Em seguida, aparecem o “desconhecimento dos direitos dos titulares” e a “sobrecarga de atribuições dos gestores”, ambos com 55,3%. Essas informações refletem a percepção do próprio setor sobre os principais obstáculos para a implementação prática da LGPD.

Tabela 1 – Barreiras à Adequação à LGPD segundo a Percepção dos Gestores

Categoria	Nº	%
Falta de capacitação dos servidores sobre a LGPD	33	86,8 %
Desconhecimento dos direitos dos titulares por parte dos servidores	21	55,3 %
Sobrecarga de atribuições dos gestores para acompanhar a LGPD	21	55,3 %
Recursos tecnológicos insuficientes (sistemas, segurança, suporte)	20	52,6 %
Resistência cultural à mudança e à implantação de boas práticas	20	52,6 %
Ausência de protocolos padronizados para descarte seguro de dados	18	47,4 %
Fragilidade nos mecanismos de resposta a incidentes de segurança	13	34,2 %
Armazenamento inadequado de documentos físicos com dados pessoais	12	31,6 %
Ausência de política institucional formalizada de proteção de dados	11	28,9 %
Normativas internas desatualizadas ou em desacordo com a LGPD	7	18,4 %
Ausência de controle de acesso a sistemas com dados pessoais	7	18,4 %

Fonte: O autor.

O resultado geral dessa análise revelou que a mediana do Índice Global de Conformidade (iG-LGPD) entre os respondentes foi de apenas 27,5%. Segundo a escala de classificação adotada, isso indica que a corporação está na faixa de baixa conformidade prática. Ou seja, na percepção dos responsáveis pelas unidades administrativas, os princípios, direitos, deveres e protocolos previstos na LGPD ainda não estão totalmente integrados à rotina institucional.

A Tabela 2 – Nível de Conformidade Prática Percebido pelos Gestores (IG-LGPD) resume a autoavaliação de 38 gestores das áreas administrativas do CBMDF sobre as práticas diárias de proteção de dados. O resultado mostra que a maioria: 31 gestores (81,6%) se posicionaram na faixa de baixa conformidade (iG-LGPD ≤ 39%). Apenas 7 gestores (18,4%) atingiram uma conformidade parcial (entre 40% e 74%), e nenhum deles declarou estar em um nível satisfatório (acima de 75%). Em resumo, mais de quatro em cada cinco líderes reconhecem que os controles existentes ainda são insuficientes em relação às exigências da LGPD.

Essa distribuição reforça a ideia de que há uma diferença significativa entre o que está previsto nas normas da corporação e o que realmente acontece na prática diária. Embora existam portarias e políticas que indicam uma intenção de adequação “no papel”, a percepção dos gestores mostra fragilidades graves em capacitação, tecnologia e cultura organizacional. Esses resultados também apontam onde é mais importante concentrar esforços — principalmente em treinamentos e no fortalecimento

dos mecanismos de controle — para melhorar o índice de conformidade e alcançar níveis mais aceitáveis.

Tabela 2 – Nível de Conformidade Prática Percebido pelos Gestores (IG-LGPD)

Faixa de Conformidade	Critério (%)	Nº de Gestores	Percentual (%)
Baixa Conformidade	≤ 39%	31	81,6%
Conformidade Parcial	40% – 74%	7	18,4%
Conformidade Satisfatória	≥ 75%	0	0%
Total	—	38	100%

Fonte: O autor.

Dessa forma, com base na análise dos documentos, constatou-se que o CBMDF está em um estágio de conformidade parcial com a LGPD. Houve alguns avanços, mas ainda há lacunas nas normativas. Já a percepção dos gestores, avaliada por meio de uma ferramenta estruturada de autoavaliação (CSA), mostrou um cenário de baixa conformidade na prática, com uma média de apenas 27,5%. Esses resultados indicam que a adaptação institucional continua no começo, com pouca integração entre as normas, as práticas e a cultura organizacional. Por isso, é importante realizar uma pesquisa mais aprofundada e propor ações concretas para que as práticas institucionais possam proteger os dados pessoais de forma eficaz, por meio de um plano bem estruturado.

2.4 Plano de Adequação do CBMDF à LGPD

Para atingir o objetivo desta pesquisa e evoluir de uma conformidade parcial para uma postura institucional sólida, o Plano de Adequação do CBMDF à LGPD foi elaborado a partir de um diagnóstico técnico baseado na autoavaliação documental e do CSA. O foco é responder às lacunas identificadas.

A proteção e o tratamento ético das informações institucionais sustentam o Objetivo Estratégico 10 do Plano Estratégico 2025–2030 do CBMDF — "Intensificar o uso dos sistemas de informação na tomada de decisão qualificada". A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) integra-se à estrutura de Governança de Dados, assegurando que toda coleta, armazenamento, compartilhamento e descarte de informações pessoais ocorra de forma lícita, transparente e segura. Essa adequação transcende a mera conformidade legal:

reforça a confiança social e dos servidores na integridade informacional da corporação, promovendo ambiente digital responsável alinhado aos princípios de *accountability* e eficiência pública (art. 37, CF/88).

A implementação da Governança de Dados deve observar a ABNT NBR ISO/IEC 27001:2022, que estabelece o Sistema de Gestão da Segurança da Informação (SGSI), orientando controles que garantam confidencialidade, integridade e disponibilidade das informações, além da gestão de riscos e incidentes de segurança. A convergência entre princípios da LGPD e práticas da ABNT viabiliza políticas robustas de proteção de dados, monitoramento contínuo dos sistemas e padronização de auditorias internas. Assim, a governança digital consolida-se sobre base normativa sólida, permitindo transformação tecnológica segura, sustentável e conforme padrões internacionais de gestão da informação.

Entre as principais ações estratégicas para a conformidade institucional com a LGPD, destaca-se a necessidade de institucionalização de políticas formais e integradas, cuja ausência ou implementação parcial foi constatada na análise documental do CBMDF (Brasil, 2018; Brasil, 2024).

Tais instrumentos incluem a Política de Proteção de Dados Pessoais (art. 50, *caput* e §2º, LGPD), a Política de Privacidade Institucional (arts. 6º, VI e IX; e 9º, LGPD), a Política de Segurança da Informação (arts. 46 a 49, LGPD), a Política de Classificação da Informação (art. 6º, VII; art. 46, LGPD), o Plano de Resposta a Incidentes com Dados Pessoais (art. 48, LGPD), o Plano de Capacitação dos Agentes Públicos (art. 50, §2º, II e art. 41, §2º, III, LGPD), e a Política de Retenção e Eliminação de Dados Pessoais (arts. 15 e 6º, III e IX, LGPD). Esses instrumentos são considerados pilares para uma governança efetiva da privacidade e da proteção de dados, sendo exigidos tanto pela legislação quanto por boas práticas consolidadas em auditorias públicas.

Além da criação de normativos, o plano também prevê a implementação de governança de dados. Essa estrutura terá funções bem definidas entre o Comitê de Governança, a Unidade Gestora da LGPD (UGLGPD) e o EPD, seguindo as orientações da Lei Geral de Proteção de Dados e das diretrizes da norma ISO/IEC 27701:2019 (ABNT, 2019).

Essa organização será responsável por operacionalizar o programa de conformidade, incluindo ações como o mapeamento de dados pessoais (Data Mapping), elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) e a criação de canais acessíveis aos titulares para dúvidas ou solicitações. Essas medidas são essenciais para preencher lacunas críticas, como a ausência de protocolos operacionais e mecanismos técnicos sistematizados, identificadas nas respostas dos gestores (Brasil, 2025).

Outro ponto central do plano é o investimento contínuo na capacitação dos bombeiros. Sugere-se que sejam realizados treinamentos em três níveis: sensibilização geral, capacitação gerencial e formação técnica especializada. Essa estratégia busca superar um dos principais obstáculos à adequação à LGPD apontado pelos gestores — a falta de preparo do efetivo, mencionada por 86,8% dos respondentes (Brasil, 2025).

Além disso, o plano inclui ações para promover uma mudança cultural na instituição, como simulações de incidentes de segurança, auditorias nos perfis de acesso e revisões contratuais com cláusulas específicas para proteção de dados. Assim, toda essa abordagem visa garantir uma resposta estruturada e integrada às exigências legais e técnicas, promovendo uma evolução significativa na maturidade institucional do CBMDF em matéria de proteção de dados pessoais (ABNT, 2022; TCU, 2025).

Ademais, o detalhamento completo do Plano de Adequação do CBMDF à LGPD — incluindo cronograma, indicadores-chave de desempenho e instrumentos de conformidade — está disponível no Apêndice B deste artigo. Esse anexo foi elaborado seguindo as diretrizes metodológicas adotadas nesta pesquisa e visa oferecer aos gestores públicos, profissionais da área e interessados uma referência prática e replicável para o planejamento estratégico de conformidade com a LGPD.

Ainda, em 04 de agosto de 2025, o CBMDF recebeu, através do Ofício nº 24121/2025-TCU/SEPROC referente ao Acórdão nº 1372/2025-Plenário (Processo nº 00053-00082213/2025-47), determinações específicas do TCU para adequação à LGPD. O ofício decorre de auditoria de conformidade para diagnosticar controles de organizações públicas federais quanto à proteção de dados pessoais.

Por fim, as recomendações ao CBMDF incluem: elaboração de plano de capacitação sobre proteção de dados com treinamento diferenciado para funções essenciais, harmonizando LGPD e Lei de Acesso à Informação; criação e divulgação de Política de Privacidade no sítio institucional; envolvimento do Alto Comando na liderança do processo conforme art. 17 do Decreto 9.203/2017; e integração das unidades de controle interno no processo, incluindo avaliação e monitoramento de riscos de privacidade em planejamentos, focando pontos críticos das peças técnicas do TCU e avaliação periódica da efetividade das medidas implementadas.

3 CONSIDERAÇÕES FINAIS

Este estudo objetivou como adaptar as práticas do CBMDF para garantir a proteção real dos dados pessoais de bombeiros militares, dependentes, pensionistas e cidadãos civis atendidos pela corporação. A ideia foi fornecer subsídios para a elaboração de um plano de adequação que seja sólido e alinhado com a realidade da instituição, que está pronto e pode ser apresentado ao Comitê Interno de Governança Pública institucional para aprovação e implementação. Para isso, foi realizada uma análise que comparou a conformidade normativa com a prática operacional, e o resultado foi claro: existe uma grande diferença entre o que a política formal diz e o que acontece no dia a dia.

Embora os documentos oficiais da Corporação mostrem uma conformidade parcial, a percepção dos gestores envolvidos na operação revela que essa implementação continua no início. Há uma espécie de “síndrome da política de papel”, onde as normas existem, mas não são realmente incorporadas à cultura organizacional ou aos processos internos.

As principais razões para essa desconexão incluem a falta de um programa estruturado e contínuo de capacitação, a visão da LGPD como uma carga extra de tarefas — e não como uma orientação estratégica — além de uma resistência cultural que ainda não reconhece a proteção de dados como um valor institucional importante. Portanto, conclui-se que o processo de adequação do CBMDF à LGPD vai além do cumprimento das regras ou do uso de tecnologia: demanda uma mudança cultural profunda e um compromisso de governança que seja liderado pela alta direção e permeie todas as camadas da corporação.

A contribuição desta pesquisa se manifesta em três pontos principais. Primeiro, fornece ao CBMDF um diagnóstico baseado em evidências, que aponta os pontos fracos e revela suas causas estruturais. Segundo, apresenta um plano e prático para a adequação, com ações concretas, prazos definidos e indicadores de desempenho, permitindo que a corporação avance de maneira sustentável. Por último, ao analisar a aplicação da LGPD em uma instituição militar de segurança pública, o estudo ocupa um espaço ainda pouco explorado na literatura científica e oferece um modelo analítico e operacional que pode ser adaptado por outras organizações de segurança pública enfrentando desafios semelhantes.

Para pesquisas futuras, recomenda-se realizar estudos longitudinais para acompanhar a eficácia do plano proposto ao longo do tempo, observando como evoluem os níveis de conformidade. Além disso, análises comparativas entre diferentes corpos de bombeiros ou forças de segurança estaduais e federais podem identificar boas práticas e vulnerabilidades comuns. Também será importante investigar, no futuro, os impactos da legislação específica sobre proteção de dados voltada para segurança pública e investigação criminal, preparando o CBMDF para os ajustes necessários em suas atividades essenciais e concluindo o ciclo completo de governança dos dados pessoais na instituição.

REFERÊNCIAS

ACOCELLA, J. **Impactos da LGPD sobre a atuação da administração pública: alguns desafios e sua efetividade**. In: DAL POZZO, A. N.; MARTINS, R. M. (org.). **LGPD & administração pública: uma análise ampla dos impactos**. São Paulo: Revista dos Tribunais, 2020. p. 359–376.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001:2022 — Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos**. Rio de Janeiro: ABNT, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27701:2019 — Tecnologia da informação — Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes**. Rio de Janeiro: ABNT, 2019.

BARDIN, L. **Análise de conteúdo**. São Paulo: Edições 70, 2016.
BARDIN, L. **Análise de conteúdo**. [PDF]. Disponível em: https://madmunifacs.files.wordpress.com/2016/08/analise-de-conteudo-bardin.pdf. Acesso em: 21 jul. 2025.

BIONI, B. R. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.

BLUM, R. O.; LÓPEZ, N. **Lei Geral de Proteção de Dados no setor público: transparência e fortalecimento do Estado Democrático de Direito**. Cadernos Jurídicos, São Paulo, v. 21, n. 53, p. 171–177, jan./mar. 2020.

BRASIL. **Constituição da República Federativa do Brasil** (1988). Brasília, DF: Senado Federal, 1988.

BRASIL. **Lei n.º 13.709, de 14 ago. 2018 — Lei Geral de Proteção de Dados Pessoais (LGPD)**. Diário Oficial da União, Brasília, DF, 15 ago. 2018.

BRASIL. **Emenda Constitucional n.º 115, de 10 fev. 2022**. Diário Oficial da União, Brasília, DF, 11 fev. 2022a.

BRASIL. Tribunal de Contas da União. **Acórdão n.º 1384/2022 — Plenário**. Rel. Min. Augusto Nardes. Brasília, DF, 1 jun. 2022b. Disponível em: https://pesquisa.apps.tcu.gov.br/resultado/acordao-completo/1384/2022. Acesso em: 21 jul. 2025.

BRASIL. Tribunal de Contas da União. **Acórdão n.º 1372/2025 — Plenário**. Rel. Min. Walton Alencar Rodrigues. Proc. TC 009.980/2024-5. Brasília, DF, 25 jun. 2025. Disponível em: https://www.tcu.gov.br. Acesso em: 21 jul. 2025.

BRASIL. Tribunal de Contas da União. **Risco alto à privacidade de dados pessoais coletados pelo governo**. Portal TCU, 2024. Disponível em: https://portal.tcu.gov.br/imprensa/noticias/tcu-verifica-risco-alto-a-privacidade-de-

dados-pessoais-coletados-pelo-governo.htm. Acesso em: 21 jul. 2025.

CBMDF. **Portaria n.º 2/2022 — Política de Proteção de Dados Pessoais (PPDP/CBMDF)**. Brasília, DF: CBMDF, 2022a.

CBMDF. **Portaria n.º 31/2012 — Manual de Redação Oficial do CBMDF**. Brasília, DF: CBMDF, 2012b.

CBMDF. **Portaria n.º 40/2022 — Plano de Dados Abertos (PDA/CBMDF)**. Brasília, DF: CBMDF, 2022d.

CBMDF. **Controladoria (CTROL). Comissões. LGPD. Plano de Trabalho do CBMDF/CTROL/COMISSÕES/LGPD**. Brasília, DF: CBMDF, 2023a. SEI n.º 152521744; Processo n.º 00053-00163122/2023-40.

CBMDF. **Guia Orientativo de Respostas a Incidentes com Dados Pessoais**. Brasília, DF: CBMDF, 2023. Publicado no Boletim Geral n.º 212/2023b.

CBMDF. **Controladoria (CTROL). Comissões. Agência de Tecnologia da Informação e Comunicação (AGTIC). Relatório de Auditoria n.º 1/2024**. Brasília, DF: CBMDF, 2024a. SEI n.º 130859289; Processo n.º 00053-00131264/2023-48.

CBMDF. **Departamento de Recursos Humanos (DERHU). Instrução Normativa n.º 4/2024**. Brasília, DF: CBMDF, 2024b.

CBMDF. **Subcomissão de Adequação dos Sistemas de TI. Relatório n.º 10/2024**. Brasília, DF: CBMDF, 2024c. SEI n.º 149019971; Processo n.º 00053-00140974/2023-69.

CBMDF. **Relatório Preliminar de Avaliação de Conformidade à LGPD**. Brasília, DF: CBMDF, CBMDF, 2024d.

CBMDF. **Diretoria de Contratações e Aquisição (DICOA). Seção de Contratação (SECON). Subseção de Convênios (SUCOV). Memorando n.º 60/2024**. Brasília, DF: CBMDF, 2024e. SEI n.º 140008803.

CBMDF. **Subcomissão de Observância ao Acórdão TCU n.º 1.384/2022. Relatório Final**. Brasília, DF: CBMDF, 2024f. SEI n.º 158980485; Processo n.º 00053-00034524/2024-19.

CBMDF. **Contrato com ARMOR PRINT LTDA**. Brasília, DF: CBMDF, 2025a.

CBMDF. **Contrato com TRIEL-HT S/A**. Brasília, DF: CBMDF, 2025b.

CBMDF. **Diretoria de Contratações e Aquisição (DICOA). Memorando n.º 29/2025**. Brasília, DF: CBMDF, 2025c. SEI n.º 164540305.

CBMDF. **Diretoria de Tecnologia da Informação e Comunicação (DITIC). Seção de Sistemas (SESIS). Memorando n.º 32/2025**. Brasília, DF: CBMDF, 2025d. SEI n.º 163346466.

CBMDF. **Edital de Credenciamento n.º 01/2025 para serviços médicos**. Brasília, DF: CBMDF, 2025e.

CBMDF. **Edital PE n.º 90059/2025**. Brasília, DF: CBMDF, 2025f.

CBMDF. **LGPD Informa!** Brasília, DF: Portal institucional, 2025g. Disponível em: https://www.cbm.df.gov.br/lgpd-informa/. Acesso em: 21 jul. 2025.

CBMDF**. Plano Estratégico do Corpo de Bombeiros Militar do Distrito Federal 2025–2030.** Aprovado pela Portaria nº 13, de 13 de janeiro de 2025, publicada no Boletim Geral nº 004/2025. Brasília, DF: CBMDF, 2025. 78 p.

CBMDF. **Portaria n.º 11, de 1.º de abril de 2025 — Dispõe sobre o sigilo institucional**. Brasília, DF: CBMDF, 2025h.

CBMDF. **Portaria n.º 19/2025 — Altera o Regimento Interno do CBMDF e cria a Seção de Governança de Dados (SEGOD)**. Brasília, DF: CBMDF, 2025i.

CBMDF. **Relatório de análise de conformidade à LGPD no CBMDF com base na metodologia do TCU**. Brasília, DF: CBMDF, 2025j.

CISO ADVISOR. **Brasil já ocupa o 2.º lugar no ranking mundial de *ransomware***. 20 maio 2023. Disponível em: https://cisoadvisor.com.br/brasil-ranking-ransomware. Acesso em: 21 jul. 2025.

DONEDA, D. **Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

FOLHA DE S.PAULO. SANTANA, J. **Brasil lidera em vazamento de dados na internet**. 18 abr. 2024. Disponível em: https://www1.folha.uol.com.br. Acesso em: 21 jul. 2025.

INFORCHANNEL. **Custo médio global de uma violação de dados foi de US$ 4,88 mi, revela IBM**. 30 jul. 2024. Disponível em: https://inforchannel.com.br/2024/07/30/custo-medio-global-de-uma-violacao-de-dados-foi-de-us-488-mi-revela-ibm/. Acesso em: 21 jul. 2025.

LE MONDE DIPLOMATIQUE BRASIL. **LGPD em vigor, ANPD militarizada**. 2024. Disponível em: https://diplomatique.org.br/lei-geral-de-protecao-de-dados-em-vigor-anpd-militarizada/. Acesso em: 21 jul. 2025.

METRÓPOLES. **Hackers invadem sistemas do GDF de olho em dados da educação e dos bombeiros**. Coluna Grande Angular, 30 jun. 2024. Disponível em: https://www.metropoles.com/colunas/grande-angular/hackers-invadem-sistemas-do-gdf. Acesso em: 21 jul. 2025.

MINUTO DA SEGURANÇA. **Qual o custo da violação de dados?** 2024. Disponível em: https://minutodaseguranca.blog.br/qual-o-custo-da-violacao-de-dados/. Acesso em: 21 jul. 2025.

NORMAS.LEG.BR. **Emenda Constitucional n.º 115/2022**. Disponível em:

https://normas.leg.br/?urn=urn:lex:br:federal:emenda.constitucional:2022-02-10;115. Acesso em: 21 jul. 2025.

PIRONTI, R. (coord.). **Lei Geral de Proteção de Dados no setor público**. Belo Horizonte: Fórum, 2021.

PRODANOV, C. C.; FREITAS, E. C. **Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico**. 2. ed. Novo Hamburgo: Feevale, 2013.

QMS BRASIL. **ISO 27001:2013 e ISO 27701:2020 — guia compacto**. 2021. Disponível em: https://qmsbrasil.com.br/wp-content/uploads/2021/06/iso-27001-iso-27701-compactado.pdf. Acesso em: 21 jul. 2025.

SERPRO. **Sete anos do GDPR: impactos na LGPD e o uso de dados para prevenção a fraudes**. 2025. Disponível em: https://www.serpro.gov.br/menu/noticias/noticias-2025/sete-anos-do-gdpr. Acesso em: 21 jul. 2025.

SOFTEXPERT BLOG. **5 critical factors for an effective Control Self-Assessment (CSA)**. 2024. Disponível em: https://blog.softexpert.com/en/5-critical-factors-control-self-assessment-csa/. Acesso em: 21 jul. 2025.

TCU. **Acórdão 1384/2022 — PDF integral**. Disponível em: https://www.trt7.jus.br/files/acesso_informacao/transparencia/acoes_de_controle/TCU/Acordao_1384-2022-TCU-Plenario.pdf. Acesso em: 21 jul. 2025.

TRT4. **Bibliografia sobre a Lei Geral de Proteção de Dados (LGPD)**. ago. 2021. Disponível em: https://www.trt4.jus.br/portais/media/606207/Bibliografia%20atualizada%20LGPD%20-%20agosto%202021.pdf. Acesso em: 21 jul. 2025.

TRT15. **Lei Geral de Proteção de Dados Pessoais — LGPD**. Disponível em: https://trt15.jus.br/legislacao/lei-geral-de-protecao-de-dados-pessoais. Acesso em: 21 jul. 2025.

APÊNDICE A

Questionário de Autoavaliação de Controles (*Control Self-Assessment – CSA*)

Prezado(a) Senhor(a) Oficial,

Este questionário integrará uma pesquisa acadêmica conduzida no âmbito do Curso de Altos Estudos para Oficiais do Corpo de Bombeiros Militar do Distrito Federal (CBMDF) sob o objetivo de realizar um diagnóstico institucional sobre a adequação do CBMDF à Lei Federal nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD) e propor um plano de adequação para a Corporação. Para tanto este questionário está lastreado em diretrizes de adequação de organizações públicas e privadas à LGPD, segundo a Norma Técnica ABNT ISO/IEC 27701:2019, capitaneada por vários parâmetros topicalizados ao Acórdão nº 1.384/2022-TCU - Plenário.

As respostas são confidenciais e serão utilizadas exclusivamente para fins acadêmicos e institucionais. Solicitamos a colaboração de Vossa Senhoria para responder com base na realidade de atuação de sua área de gestão.

Bloco 1 - Capacitação em Proteção de Dados (mencionado Acórdão do TCU)

1. Vossa Senhoria já recebeu capacitação específica sobre a LGPD ou acerca da proteção de dados pessoais no âmbito do CBMDF?

Marcar apenas uma oval.

- o Sim
- o Não

2. Em sua OBM da gestão, existem treinamentos periódicos sobre proteção de dados pessoais ou são ofertados?

Marcar apenas uma oval.

- o Sim, de forma regular
- o Sim, de forma eventual

- Não são realizados treinamentos

Bloco 2 - Normativas Internas Atualizadas (mencionado Acórdão do TCU)

(se as normas estão adequadas à LGPD)

3. As normativas internas da sua OBM estão atualizadas segundo os dispositivos normativos da LGPD?

Marcar apenas uma oval.

- Sim, são abrangentes e atualizadas
- Sim, são abrangentes, mas necessitam de atualização
- Não, esta área de atuação da gestão não dispõe de normativas específicas sobre a LGPD

4. Saberia informar se o CBMDF possui uma Política de Proteção de Dados Pessoais?

Marcar apenas uma oval.

- Sim
- Não

5. A Política de Proteção de Dados Pessoais do CBMDF tem sido devidamente disseminada junto aos militares e civis de sua OBM?

Marcar apenas uma oval.

- Sim
- Não
- Foi pouco disseminada

6. Sua OBM possui política formal de classificação de informações que categorize os dados por nível de sensibilidade (ex: público, restrito)?

Marcar apenas uma oval.

- Sim
- Não

Bloco 3 - Contratos com operadores de dados pessoais

"operador" é a pessoa ou empresa que faz o tratamento dos dados pessoais em nome de outra o chamado "controlador"

Exemplos práticos:

Um hospital (controlador) contrata uma empresa de TI para gerenciar seus sistemas com dados de pacientes. Essa empresa é o operador.

Uma escola pública (controladora) contrata um sistema terceirizado para gerenciar notas e presenças dos alunos. O operador é quem desenvolve e opera esse sistema.

7. Os contratos firmados por OBM com empresas terceirizadas ou prestadores de serviço que tratam dados pessoais contêm cláusulas específicas sobre a LGPD?

Marcar apenas uma oval.

- Sim, em todos os contratos
- Em alguns contratos
- Não há cláusulas sobre LGPD
- Não se aplica à minha área

8. Sua OBM realiza algum tipo de controle ou auditoria sobre o cumprimento dessas cláusulas pelos operadores de dados?

Marcar apenas uma oval.

- Sim
- Não

- Não se aplica

Bloco 3 Controle de Acesso e Segurança dos Sistemas de Informações utilizados (mencionado Acórdão do TCU)

9. Os sistemas de Informação utilizados por sua OBM possuem controle de acesso individualizado (login e senha pessoal) que não tenham sofrido qualquer ataque cibernético?

Marcar apenas uma oval.

- Sim
- Não
- Parcialmente
- Não sei informar

10. Saberia informar se nos Sistemas de Informação de OBM, há aplicação de criptografia ou tecnologias equivalentes para proteção dos dados pessoais sensíveis?

Marcar apenas uma oval.

- Sim, de forma integral
- Sim, parcialmente
- Não sei informar

Bloco 4: Segurança técnica - Criptografia e autenticação

A criptografia é uma técnica usada para proteger informações

Autenticação é o processo de confirmar a identidade de quem está tentando acessar um sistema ou informação.

11. Quais medidas técnicas de segurança são adotadas na OBM para proteger os dados pessoais tratados?

Marque todas que se aplicam.

- Uso de senhas fortes e atualizadas periodicamente
- Criptografia de dados sensíveis
- Níveis de acessos aos sistemas
- Nenhuma dessas opções
- Não sei informar

Bloco 4 - Armazenamento, Descarte e Compartilhamento de Dados (mencionado no Acórdão do TCU)

12. Existem procedimentos formalizados para o armazenamento seguro de documentos físicos e digitais contendo dados pessoais em sua OBM?

Marcar apenas uma oval.

- Sim
- Não
- Parcialmente

13. Existem diretrizes específicas para o descarte seguro de documentos contendo dados pessoais em sua OBM?

Marcar apenas uma oval.

- Sim, formalizadas por normativa
- Sim, baseadas apenas em práticas operacionais
- Não existem diretrizes claras
- Não sei

14. Existe "Política de Privacidade Institucional" aplicável ao compartilhamento de dados pessoais em sua OBM?

Marcar apenas uma oval.

- Sim
- Não
- Não sei informar

Bloco 5 Atendimento aos Direitos dos Titulares (mencionado no Acórdão do TCU)

15. Há procedimentos definidos em OBM para atendimento de solicitações dos titulares de dados pessoais (como acesso, retificação ou eliminação)?

Marcar apenas uma oval.

- Sim, formalizado
- Sim, mas não formalizado
- Não há procedimento definido

Bloco 6 Governança e Nomeação de Encarregado Setorial pela Proteção de Dados Pessoais - (mencionado no Acórdão do TCU)

16. Vossa Senhoria tem conhecimento da existência em OBM de um Encarregado Setorial pela Proteção de Dados Pessoais (Data Protection Officer - DPO) formalmente designado pela Alta Gestão do CBMDF?

Marcar apenas uma oval.

- Sim
- Não
- Não sei informar

17. Caso saiba quem é o DPO, marque as opções que melhor descrevem sua percepção: (DPO é a sigla em inglês para Data Protection Officer,, chamado no Brasil de: Encarregado pelo Tratamento de Dados Pessoais)

Marcar apenas uma oval.

- Sei como contatar o DPO

- Nunca tive contato com o DPO

18. Existem mecanismos internos para comunicação de incidentes de segurança envolvendo dados pessoais na OBM?

Marcar apenas uma oval.

- Sim
- Não
- Não sei informar

Bloco 7 As principais dificuldades ou desafios enfrentados para a plena adequação da sua área às diretrizes da LGPD

19. Quais são, na sua opinião, as principais dificuldades ou desafios enfrentados para a plena adequação da sua área às diretrizes da LGPD? (Marque todas as opções que se aplicarem)

Marque todas que se aplicam.

- Falta de capacitação dos servidores sobre a LGPD
- Ausência de política institucional formalizada de proteção de dados
- Normativas internas desatualizadas ou em desacordo com a LGPD
- Armazenamento inadequado de documentos físicos com dados pessoais
- Ausência de controle de acesso a sistemas com dados pessoais
- Fragilidade nos mecanismos de resposta a incidentes de segurança
- Desconhecimento dos direitos dos titulares por parte dos servidores
- Ausência de protocolos padronizados para descarte seguro de dados
- Recursos tecnológicos insuficientes (sistemas, segurança, suporte)
- Resistência cultural à mudança e à implantação de boas práticas

- Sobrecarga de atribuições dos gestores para acompanhar a LGPD
- Não há dificuldades significativas no momento

Bloco 8 Retenção e descarte de dados pessoais

20. Na sua área, há regras claras sobre por quanto tempo manter dados pessoais armazenados?

Marcar apenas uma oval.

- Sim, há política institucional
- Não há regras definidas

21. Existe um procedimento formalizado para o descarte seguro de documentos (físicos ou digitais) que contenham dados pessoais?

Marcar apenas uma oval.

- Sim
- Não
- Não sei informar

APÊNDICE B

Plano de Adequação do Corpo De Bombeiros Militar do Distrito Federal (CBMDF) à Lei Geral De Proteção de Dados Pessoais (LGPD)

Versão 1.0
Brasília-DF
2025

Minuta para Aprovação

SUMÁRIO

1. APRESENTAÇÃO
2. OBJETIVOS
1. Objetivo Geral
2. Objetivos Específicos
3. ARCABOUÇO NORMATIVO E TÉCNICO
4. ESTRUTURA DE GOVERNANÇA DE DADOS: COORDENAÇÃO MULTISSETORIAL
1. Comitê de Governança de Dados
2. Encarregado pela Proteção de Dados (EPD)
3. Unidade Gestora da LGPD (UGLGPD)
4. Gestores das Áreas-Meio
5. PROGRAMA DE CONFORMIDADE: EIXOS ESTRATÉGICOS E ARTEFATOS
1. Eixo 1: Governança e Normatização
2. Eixo 2: Tecnologia e Segurança da Informação
3. Eixo 3: Capacitação e Cultura
6. DETALHAMENTO DOS ARTEFATOS DO PROGRAMA DE CONFORMIDADE
1. TERMOS E AVISOS
2. CONTRATOS
3. NORMATIVOS
4. MANUAIS E PLANOS
5. SEI (SISTEMA ELETRÔNICO DE INFORMAÇÕES)
6. FERRAMENTAS
7. TREINAMENTOS
7. ROTEIRO DE IMPLEMENTAÇÃO (CRONOGRAMA E KPIs)
8. DISPOSIÇÕES FINAIS
9. REFERÊNCIAS

1. APRESENTAÇÃO

O presente Plano de Adequação é o documento norteador para a implementação e a manutenção da conformidade do Corpo de Bombeiros Militar do Distrito Federal (CBMDF) com a Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD). Sua elaboração fundamenta-se em um diagnóstico institucional aprofundado, que revelou um significativo hiato entre o arcabouço normativo existente na Corporação e a sua efetiva aplicação nas rotinas operacionais das áreas-meio (conformidade prática percebida pelos gestores de 27,5%) (ALVARENGA, 2025).

Este documento, portanto, não se limita a ser um checklist de conformidade. Trata-se de um roteiro estratégico, prático e objetivo, que visa traduzir as exigências legais em processos, controles e uma cultura organizacional de proteção de dados, em alinhamento com as melhores práticas de governança, as normas da ABNT (série NBR ISO/IEC 27000) e as diretrizes do Acórdão nº 1384/2022 do Tribunal de Contas da União (TCU).

2. OBJETIVOS

2.1. Objetivo Geral

Instituir um programa de conformidade contínua à LGPD nas áreas-meio do CBMDF, estabelecendo uma estrutura de governança de dados robusta, implementando controles técnicos e administrativos eficazes e promovendo uma cultura de privacidade e segurança da informação em todos os níveis da Corporação (ALVARENGA, 2025).

2.2. Objetivos Específicos

- Formalizar e fortalecer a estrutura de governança de dados, definindo papéis e responsabilidades.

- Revisar e adequar os normativos internos, contratos e processos para garantir o alinhamento com a LGPD.

- Implementar medidas de segurança da informação para proteger os dados pessoais contra acessos não autorizados e incidentes.

- Estruturar canais e procedimentos claros para garantir o exercício dos direitos dos titulares de dados.

- Desenvolver e executar um programa de capacitação contínua para todo o efetivo envolvido no tratamento de dados pessoais.

- Estabelecer um ciclo de monitoramento e melhoria contínua do programa de conformidade (ALVARENGA, 2025).

3. ARCABOUÇO NORMATIVO E TÉCNICO

Este plano está alinhado ao seguinte conjunto de normas e referenciais técnicos:

- **Lei Federal nº 13.709/2018 (LGPD):** Principal marco legal que rege o tratamento de dados pessoais (BRASIL, 2018).

- **Emenda Constitucional nº 115/2022:** Eleva a proteção de dados pessoais à categoria de direito fundamental (BRASIL, 2022).

- **Decreto Distrital nº 45.771/2024:** Regulamenta a aplicação da LGPD na Administração Pública do Distrito Federal (BRASIL, 2024).

- **Acórdão nº 1384/2022 – TCU:** Estabelece os nove parâmetros de avaliação de conformidade que nortearam o diagnóstico e as ações deste plano (TRIBUNAL DE CONTAS DA UNIÃO, 2022).

- **Acórdão nº 1372/2025 (junho de 2025) – TCU:** O TCU consolidou auditoria de 387 órgãos federais revelando que apenas 42% estão adequados à LGPD, evidenciando descumprimento sistemático da norma e riscos generalizados à proteção de dados pessoais dos cidadãos.

- **ABNT NBR ISO/IEC 27000:** Conjunto de normas técnicas para a gestão da segurança da informação (ISO/IEC 27001) e da privacidade (ISO/IEC 27701), que servem como referencial de melhores práticas (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2019; 2022).

- **Framework COSO (Internal Control – Integrated Framework):** Modelo de

referência para a estruturação dos controles internos e da governança de riscos (COSO, 2013).

4. ESTRUTURA DE GOVERNANÇA DE DADOS: COORDENAÇÃO

Para garantir a eficácia e a sustentabilidade do programa de conformidade, propõe-se a seguinte estrutura de governança, com papéis e responsabilidades claramente definidos:

- **Comitê de Governança de Dados:** Órgão estratégico de alto nível, presidido por um membro do alto comando, com a função de aprovar políticas, alocar recursos e monitorar os indicadores de conformidade do plano.

- **Encarregado pela Proteção de Dados, Oficial de Proteção de Dados (EPD):** Agente central do programa, com autonomia garantida, responsável por atuar como canal de comunicação com os titulares e a ANPD, orientar as áreas internas e supervisionar a execução das políticas de proteção de dados.

- **Unidade Gestora da LGPD (UGLGPD):** Equipe multidisciplinar (composta por membros da Controladoria, Jurídico, DITIC, DERHU, etc.) que atua como o braço operacional do DPO, responsável por executar as ações do plano, elaborar pareceres técnicos e conduzir o mapeamento de dados.

- **Gestores das Áreas-Meio:** Responsáveis diretos pela implementação dos controles de proteção de dados em seus respectivos processos e por garantir que suas equipes estejam devidamente capacitadas.

5. PROGRAMA DE CONFORMIDADE: EIXOS ESTRATÉGICOS E ARTEFATOS

O plano de adequação é estruturado em três eixos complementares, que resultarão na produção de um conjunto de artefatos e ferramentas essenciais para a governança de dados no CBMDF. Vide quadro 1 abaixo:

Eixo Estratégico	**Foco Principal**	**Artefatos / Entregáveis Gerados**
Eixo 1 – Governança e Normatização	Estruturação normativa, política e	TERMOS E AVISOS: Política de Privacidade pública.

	organizacional.	CONTRATOS: Cláusulas-padrão de LGPD para editais e contratos. NORMATIVOS: Revisão de portarias e do Manual de Redação Oficial. COORDENAÇÃO MULTISSETORIAL: Instituição do Comitê de Governança de Dados e fortalecimento da UGLGPD.
Eixo 2 – Tecnologia e Segurança da Informação	Controles técnicos, sistemas e práticas de segurança.	PLANO DE RESPOSTA A INCIDENTES: Operacionalização do guia existente com simulações e definição de equipes. FERRAMENTAS: Implementação de inventário de dados (ROPA), análise de riscos e ferramentas de monitoramento (SIEM). SEI: Desenvolvimento de orientações específicas para o tratamento de dados no SEI.
Eixo 3 – Capacitação e Cultura de Proteção de Dados	Educação institucional e engajamento do efetivo.	TREINAMENTOS: Programa de capacitação contínuo e multinível (básico, gerencial, especialista). MANUAIS E PLANOS: Produção de guias práticos e materiais educativos para apoiar a implementação da LGPD.

Fonte: O autor.

6. DETALHAMENTO DOS ARTEFATOS DO PROGRAMA DE CONFORMIDADE

Esta seção detalha os principais documentos, ferramentas e estruturas a serem desenvolvidos e implementados como parte deste plano.

- **TERMOS E AVISOS:** Reúne os avisos de privacidade e termos de uso que orientam de forma clara e transparente os titulares sobre como seus dados pessoais são tratados pelo CBMDF. O principal entregável é a **Política de Privacidade Institucional**, a ser publicada no site oficial.

- **CONTRATOS:** Disponibiliza modelos e cláusulas contratuais que asseguram o cumprimento da LGPD nas relações com terceiros. O principal entregável é o **Adendo de Proteção de Dados Pessoais**, de inclusão obrigatória em todos os contratos e credenciamentos.

- **NORMATIVOS:** Repositório de normas internas, instruções e orientações que regulamentam o tratamento de dados. Inclui a revisão de portarias existentes e a atualização do **Manual de Redação Oficial**.

- **MANUAIS E PLANOS:** Guias práticos e documentos estratégicos que apoiam a implementação da LGPD. Inclui o **Plano de Resposta a Incidentes** e guias operacionais para os servidores.

- **SEI (EM BREVE):** Orientações específicas para garantir o tratamento adequado de dados pessoais nos processos e solicitações monitoradas no Sistema Eletrônico de Informações (SEI), considerando a criação do ambiente UG-LGPD – Unidade Gestora da LGPD.

- **FERRAMENTAS:** Recursos técnicos e operacionais como planilhas para Inventário de Dados (ROPA - Registro das Operações de Tratamento), matrizes para Análise de Riscos e *templates* para elaboração de Relatório de Impacto à Proteção de Dados (RIPD).

- **TREINAMENTOS:** Materiais educativos, vídeos, oficinas e cursos dirigidos aos bombeiros militares sobre os princípios e práticas de proteção de dados, compondo o Programa de Capacitação Continuada, inclusive via redes sociais e canais de informação.

- **COORDENAÇÃO MULTISSETORIAL DE IMPLEMENTAÇÃO:** Estrutura colegiada responsável pela condução integrada das ações. Apresenta os integrantes do Comitê de Governança de Dados, do DPO e da UGLGPD, com suas funções e modelo de atuação.

- **PLANO DE RESPOSTA A INCIDENTES:** Documento orientador que descreve as ações a serem seguidas em situações de incidente de segurança, desde a detecção e tratamento até o encerramento e a comunicação à ANPD e aos titulares.

- Desta maneira observe o quadro 2 abaixo:

7. ROTEIRO DE IMPLEMENTAÇÃO (CRONOGRAMA E KPIs)

Ação Recomendada	Eixo Estratégico	Setor Responsável (Sugestão)	Prazo	Indicador de Sucesso (KPI)
1.1. Publicar a Política de Privacidade institucional.	Governança	Controladoria / DPO / Comunicação Social	Curto (<6 meses)	Política de Privacidade publicada e acessível publicamente.
1.2. Desenvolver e implementar cláusulas-padrão de LGPD.	Governança	Assessoria Jurídica / Diretoria de Contratações	Curto (<6 meses)	100% dos novos contratos e credenciamentos contêm a cláusula-padrão.
1.3. Estruturar o canal oficial de atendimento aos titulares.	Governança	Controladoria / DPO / Ouvidoria	Curto (<6 meses)	Canal implementado; Tempo médio de resposta < 15 dias.
2.1. Desenvolver e implementar o Programa de Capacitação (Nível Básico).	Capacitação	Diretoria de Ensino (DERHU) / DPO	Curto (<6 meses)	80% do efetivo conclui o módulo básico no primeiro ano.
3.1. Realizar auditoria de perfis de acesso nos sistemas.	Tecnologia	Diretoria de Tecnologia da Informação (DITIC)	Médio (6-12 meses)	Relatório de auditoria concluído e plano de correção implementado.
3.2. Operacionalizar o Plano de Resposta a Incidentes com	Tecnologia	DITIC / UGLGPD	Médio (6-12 meses)	Relatório de pós-ação da simulação com lições aprendidas.

simulações.				
4.1. Instituir formalmente o Comitê de Governança de Dados.	Governança	Comando-Geral / DPO	Médio (6-12 meses)	Comitê instituído por portaria, com reuniões periódicas registradas.
4.2. Incluir o tema "Proteção de Dados" nos cursos de formação.	Capacitação	Diretoria de Ensino (DERHU)	Longo (>12 meses)	Matrizes curriculares dos principais cursos atualizadas.
4.3. Implementar o ciclo de monitoramento via CSA semestral.	Governança	Controladoria / DPO	Longo (>12 meses)	Mediana do IG-LGPD com aumento de 15% em relação ao diagnóstico inicial.

Fonte: O autor.

8. DISPOSIÇÕES FINAIS

Este Plano de Adequação é um documento dinâmico e deverá ser revisado ser revisado pelo Encarregado de Dados do CBMDF, Estado-Maior Geral e Comitê de Governança de Dados, ou sempre que ocorrerem mudanças significativas na legislação, estrutura organizacional ou processos de tratamento de dados institucionais, e servirá com uma resposta aos cidadãos, bem como a TCU conforme o Acórdão nº 1372/2025 (junho de 2025).

REFERÊNCIAS

ALVARENGA, Arnaldo Alves de. **O Corpo de Bombeiros Militar do Distrito Federal está adequado à LGPD?** Brasília: CBMDF, 2025. Artigo (Curso de Altos Estudos para Oficiais) – Centro de Estudos de Política, Estratégia e Doutrina, Corpo de Bombeiros Militar do Distrito Federal, Brasília, 2025.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001:2022**. Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos. Rio de Janeiro: ABNT, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27701:2019**. Tecnologia da informação — Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes. Rio de Janeiro: ABNT, 2019.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BRASIL. **Decreto nº 45.771, de 08 de maio de 2024**. Dispõe sobre a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais - LGPD, [...] no âmbito da Administração Pública Direta e Indireta do Distrito Federal. Diário Oficial do Distrito Federal, Brasília, DF, 9 maio 2024.

BRASIL. [Constituição (1988)]. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais [...]. Brasília, DF: Presidência da República, 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018.

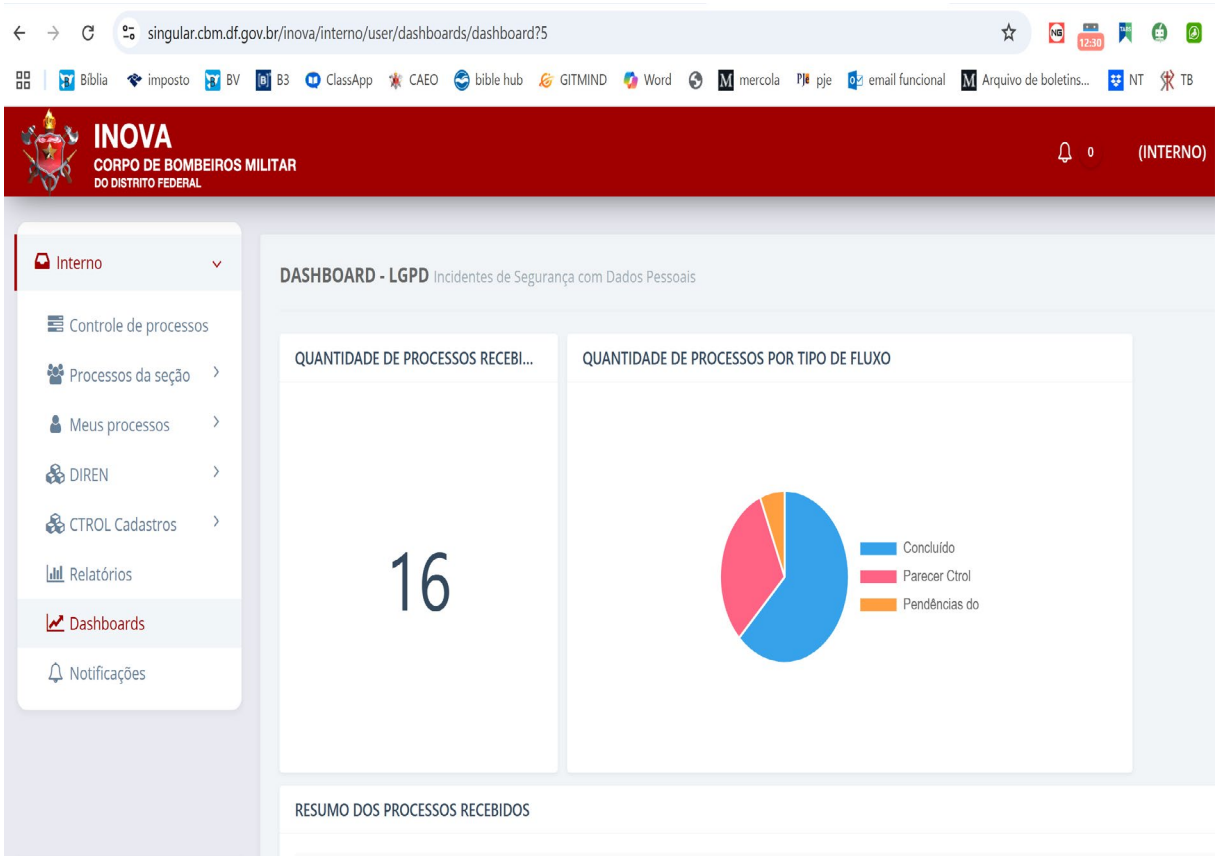
CBMDF**. Plano Estratégico do Corpo de Bombeiros Militar do Distrito Federal 2025–2030.** Aprovado pela **Portaria nº 13, de 13 de janeiro de 2025**, publicada no Boletim Geral nº 004/2025. Brasília, DF: CBMDF, 2025. 78 p.

COSO. **Internal Control – Integrated Framework**. Committee of Sponsoring Organizations of the Treadway Commission, 2013.

TRIBUNAL DE CONTAS DA UNIÃO. **Acórdão nº 1.384/2022 – Plenário**. Relator: Ministro Augusto Nardes. Sessão de 15/06/2022. Diário Oficial da União, Brasília, DF, 20 jun. 2022.

ANEXO A

Dashboard – LGPD – Número de incidentes com dados pessoais até julho de 2025



Declaração de uso de ferramenta de Inteligência Artificial

Durante a elaboração deste trabalho, o autor recorreu à ferramenta ChatGPT (OpenAI) com o objetivo de auxiliar na organização de ideias, obtenção de insights, análise de dados e reformulação de trechos textuais. Após a utilização da ferramenta, o autor procedeu à revisão crítica, sobretudo de seu orientador do TCC, responsabilizando-se integralmente pela originalidade, precisão e qualidade acadêmica do trabalho apresentado.