A CONSTRUÇÃO DO DIAGNÓSTICO DE MATURIDADE EM PROTEÇÃO DE DADOS PESSOAIS

Fábio Fernandes Libonati[1]
Thiago Ryuichi Hirata[2]

Resumo: *O trabalho tem como objetivo discutir a criação do Diagnóstico de Maturidade em Proteção de Dados Pessoais como ferramenta de controle interno para avaliar o processo de adequação da Prefeitura de São Paulo à Lei Geral de Proteção de Dados Pessoais. Trata-se de uma metodologia personalizada, fundamentada em uma abordagem baseada em riscos, com a sistematização de controles em temas e fases para se nortear ações de adaptação às exigências legais e melhores práticas. A partir da experiência na construção da referida ferramenta, serão apresentados os benefícios esperados, as limitações enfrentadas e aspectos-chave na construção do projeto.*

Palavras-chave: *Metodologia. Maturidade. Dados Pessoais. Controle interno.*

INTRODUÇÃO

A Lei Geral de Proteção de Dados Pessoais (LGPD) disciplinou o tratamento de dados pessoais em âmbito nacional e estabeleceu contornos para tal atividade. Em que pese a extensão do normativo, a lei não trouxe um caminho a ser trilhado para sua implementação. Em outras palavras, referido diploma trouxe uma série de obrigações para os agentes de tratamento, bem como direitos aos titulares dos dados pessoais, mas não apresentou formas claras para sua operacionalização, mesmo considerando as regulamentações emitidas pela Agência Nacional de Proteção de Dados (ANPD) até o momento.

O presente artigo tem como objetivo discutir a solução desenvolvida pela Controladoria Geral do Município (CGM) para auxiliar a Prefeitura do Município de São Paulo a enfrentar este desafio. Para tanto, o artigo adotará o seguinte percurso: (i) apresentação do contexto normativo e da necessidade de avaliação do nível de adequação à LGPD; (ii) explanação do desenvolvimento de metodologia personalizada para auxiliar os gestores públicos nessa tarefa; (iii) discussão do planejamento para implementação do projeto; e (iv) análise sobre a construção da ferramenta.

1 Auditor Municipal de Controle Interno e Advogado. Possui graduação em Direito (2012) e mestrado em Direito do Estado pela Universidade de São Paulo (2020).

2 Auditor Municipal de Controle Interno. Possui graduação em Engenharia de Produção (2013) e em Direito (2021) pela Universidade de São Paulo e pós-graduação em Direito 4.0: Direito Digital, Proteção de Dados e Cibersegurança pela Pontifícia Universidade Católica do Paraná (2025).

1. A NECESSIDADE E A RELEVÂNCIA DA MENSURAÇÃO DO NÍVEL DE ADEQUAÇÃO À LGPD

Sem prejuízo de outros marcos normativos anteriores a respeito da proteção de dados pessoais, foi com o advento da LGPD que o tema começou a ser tratado de forma sistemática no país. Com a sua promulgação, o Brasil passou a compor o grupo de 79% dos países no mundo que possuem legislação sobre privacidade e proteção de dados pessoais. Esse percentual demonstra o crescente interesse global por uma tutela jurídica voltada a *"harmonizar o desenvolvimento da tecnologia e a preservação dos direitos de personalidade e de privacidade dos titulares de dados"* (BRITTO; RIBEIRO, 2018).

A importância do assunto no país se ampliou com a recente inclusão da proteção de dados pessoais como direito fundamental no rol previsto no Art. 5º da Constituição Federal com a promulgação da Emenda Constitucional nº 115/2022. A constitucionalização desse direito se mostra de indiscutível importância para a Administração Pública, uma vez que norteia a conduta dos seus agentes e permeia toda a sua atuação.

Nota-se que, mesmo que a LGPD já esteja em vigor, ainda há uma série de dispositivos previstos na lei que serão objeto de normatização futura pela ANPD. Nesse contexto, é importante que a Administração Pública esteja em conformidade com as exigências da legislação, mas que também esteja preparada para se adaptar às evoluções tecnológicas e regulatórias sobre o tema no país.

No município de São Paulo, coube ao Decreto nº 59.767/2020 regulamentar a aplicação da LGPD. Dois pontos merecem destaque do referido normativo: (i) a atuação da CGM, por meio de seu dirigente, designado como Encarregado da Administração Pública Municipal Direta e, como consequência, a criação da Coordenadoria de Proteção de Dados Pessoais (CPD) no âmbito do órgão de controle, por meio do Decreto nº 62.809/2023; e (ii) a previsão de elaboração de um conjunto de regras de boas práticas e de governança de dados pessoais, em linha com o disposto no Art. 50 da LGPD.

Para cumprimento do ponto (ii), foi editada a Instrução Normativa CGM nº 01/2022, que estabeleceu disposições referentes ao tratamento de dados pessoais no âmbito da Administração Pública Municipal. Embora o normativo já apresentasse diversas orientações, foi identificada, em virtude da complexidade e ineditismo do tema, a necessidade de elaboração de um conjunto de diretrizes de ordem mais prática para guiar os agentes públicos nesse desafiador processo de adaptação.

Nesse momento, a Prefeitura de São Paulo apresentava órgãos de diferentes características e em estágios variados na implementação de medidas de adequação à LGPD. Para se assegurar que todo o processo de adaptação fosse conduzido de maneira padronizada, progressiva, e envolvesse todas as uni-

dades, tornou-se imprescindível se mapear o cenário de cada uma delas. Essa mensuração se mostrava também fundamental para se garantir a efetividade das medidas adotadas, conforme Art. 50, §2º, II, da LGPD.

Ocorre que, até a elaboração deste artigo, não havia no país metodologia consolidada para se realizar a mensuração do nível de maturidade ou adequação à LGPD. Evidência disto, inclusive, é a manifestação da ANPD de que não reconhece qualquer entidade que forneça selo ou atestado de conformidade à LGPD.

Nesse contexto, nota-se que diferentes instituições promoveram iniciativas próprias para mensuração do nível de maturidade ou adequação à LGPD no setor público nos últimos anos, a exemplo dos trabalhos do Conselho Nacional de Controle Interno (CONACI), da Secretaria da Controladoria do Estado de Pernambuco (SCGE), do Tribunal de Contas da União (TCU) e da Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (SGD/MGI).

Observa-se que essas iniciativas apresentaram diferenças relevantes entre si, como variações nos procedimentos, critérios e forma de apresentação dos resultados. Entende-se que isso é reflexo das características das instituições que as desenvolveram, que atuam tanto com a gestão, como com o controle interno e o externo, e que, portanto, possuem diferentes objetivos.

Considerando o contexto de adaptação à cultura da privacidade e da proteção de dados pessoais no país, a CGM desenvolveu metodologia personalizada para se aferir o estágio de adequação à LGPD da Administração Pública Municipal Direta, que foi formalizada por meio da Instrução Normativa CGM nº 02/2024.

2. A METODOLOGIA PARA O DESENVOLVIMENTO DO DIAGNÓSTICO DE MATURIDADE

O *"Diagnóstico de Maturidade em Proteção de Dados Pessoais"* foi concebido como uma ferramenta estratégica destinada a oferecer aos gestores públicos um panorama sobre as suas unidades a respeito do estágio de adequação à LGPD, e, assim, impulsionar a adoção de medidas concretas nesse processo.

Na delimitação do escopo para o desenvolvimento da ferramenta, definiu-se o foco em todos os órgãos, tendo em vista que o Controlador Geral do Município havia sido designado como Encarregado da Administração Pública Municipal Direta. Ademais, optou-se por não se restringir o escopo à critérios de conformidade, abrangendo também aspectos de governança, boas práticas e melhoria contínua.

O Diagnóstico de Maturidade foi elaborado por meio de uma abordagem baseada em riscos[3] voltada à privacidade[4] e utilizou como principal referência o *NIST Privacy Framework*. A metodologia se mostra alinhada institucionalmente ao modelo de gestão de riscos adotado pela CGM e às principais normas técnicas sobre o assunto. O desenvolvimento da ferramenta seguiu as quatro etapas clássicas da gestão de riscos[5]: (i) identificação; (ii) análise; (iii) avaliação; e (iv) tratamento.

O trabalho também teve inspiração nas quatro referências de modelo de mensuração para o setor público citadas no capítulo anterior, além do Modelo de Capacidade de Auditoria Interna (IA-CM) do Instituto dos Auditores Internos (IIA), adotado como referência institucional da CGM.

2.1. DEFINIÇÃO DOS TEMAS E IDENTIFICAÇÃO DOS RISCOS ASSOCIADOS

O desenvolvimento da ferramenta teve início com o mapeamento dos macroprocessos-chave relacionados à privacidade no âmbito dos órgãos municipais[6].

Para isso, foi realizada análise comparativa dos tópicos dos modelos de mensuração utilizados como referência. Como resultado, foram selecionados oito macroprocessos-chave, que foram denominados como "*temas*": estrutura organizacional; governança; tratamento de dados pessoais; direitos dos titulares; resposta a incidentes; transparência; segurança da informação; e gestão de terceiros.

A organização em temas mostrou-se relevante por facilitar a estruturação da ferramenta a partir de elementos essenciais à proteção de dados pessoais. A partir dos temas definidos, foram identificados os principais riscos de privacidade associados[7], por meio do qual se estabeleceu a base para as etapas seguintes do desenvolvimento do Diagnóstico de Maturidade.

A identificação dos riscos foi realizada por meio de um exame das fontes de risco e de cenários potenciais, adotando-se uma abordagem baseada em

3 A definição de risco relaciona-se ao "efeito da incerteza nos objetivos". (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). Gestão de riscos — Diretrizes. NBR ISO 31000:2018. Rio de Janeiro: ABNT, 2018. p. 1)

4 É importante considerar as particularidades do campo da privacidade na gestão de riscos. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). Segurança da informação, segurança cibernética e proteção da privacidade — Aplicação da ABNT NBR ISO 31000:2018 para gestão de riscos de privacidade organizacional. NBR ISO/IEC 27557:2023. Rio de Janeiro: ABNT, 2023. p. vi).

5 Gestão de riscos se refere a "atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos" (ABNT, ref. 21, p. 1).

6 "Para aumentar a eficiência e efetividade da gestão de riscos, é essencial selecionar os processos-chave com base nas atividades operacionais, táticas e estratégicas". (SÃO PAULO (Cidade), ref. 24, p. 16 e 17).

7 "O propósito da identificação de riscos é encontrar, reconhecer e descrever riscos que possam ajudar ou impedir que uma organização alcance seus objetivos". (ABNT, ref. 21. p. 12).

eventos[8]. Essa etapa da metodologia foi finalizada com o detalhamento de cada risco identificado, incluindo a análise de suas principais causas e respectivas consequências.

2.2. ANÁLISE DOS RISCOS E CÁLCULO DO RISCO INERENTE

A segunda etapa da elaboração da ferramenta consistiu na análise dos riscos[9], com a avaliação de parâmetros de probabilidade e impacto de cada risco, atribuindo-se notas em uma escala de cinco faixas para cada parâmetro[10].

No contexto da privacidade, é importante destacar que a avaliação do impacto apresenta uma dimensão dupla[11]: considera tanto os efeitos da concretização do risco para a organização quanto para os indivíduos. Para os indivíduos, os impactos se relacionam com a perda de dignidade, a discriminação, a perda econômico-financeira, a perda da autodeterminação, entre outros. Ressalta-se que impactos sofridos pelos titulares de dados pessoais podem, indiretamente, repercutir sobre a própria organização, ocasionando, por exemplo, a aplicação de multas, o comprometimento da imagem institucional e a perda de oportunidades[12].

Para a atribuição das notas aos parâmetros de probabilidade e impacto, adotou-se uma abordagem qualitativa[13], com base na experiência no tema e no julgamento profissional da equipe[14]. A combinação dos parâmetros de probabilidade e impacto permitiu o cálculo do risco inerente[15], que foi classificado em uma escala de quatro faixas, por meio do seu posicionamento em uma matriz de risco[16].

8 "Uma abordagem baseada em eventos para identificar riscos é um exame de alto nível das fontes de riscos e dos cenários potenciais que podem ocorrer com base nessas fontes de riscos". (ABNT, ref. 22, p. 7).

9 "O propósito da análise de riscos é compreender a natureza do risco e suas características, incluindo o nível de risco, onde apropriado". (ABNT, ref. 21, p. 13).

10 Mesmas faixas utilizadas institucionalmente pela CGM. (SÃO PAULO (Cidade), ref. 24, p. 26 e 27).

11 "As consequências para a organização diferem necessariamente dos impactos de privacidade para os indivíduos". (ABNT, ref. 22, p. 9).

12 "Como resultado dos problemas que as pessoas enfrentam, uma organização pode sofrer impactos, por exemplo, custos decorrentes de não estar em conformidade, perda de receita decorrente do abandono de produtos e serviços pelo cliente, ou danos à sua reputação de marca externa ou cultura interna". (NIST, ref. 23, p. 4).

13 "As técnicas de análise podem ser qualitativas, quantitativas ou uma combinação destas, dependendo das circunstâncias e do uso pretendido". (ABNT, ref. 21, p. 13).

14 "A avaliação dos riscos é antes uma questão de julgamento profissional que uma questão passível de mensuração precisa". (CONSELHO FEDERAL DE CONTABILIDADE (CFC). NBC TA 200 (R1): Objetivos Gerais do Auditor Independente e a Condução da Auditoria em Conformidade com Normas de Auditoria. Brasília, DF: CFC, 19 ago. 2016. Disponível em: https://www1.cfc.org.br/sisweb/SRE/docs/NBCTA200(R1).pdf. Acesso em: 25 ago. 2025 p.14)

15 Refere-se ao "nível de risco ao qual uma organização está exposta antes de qualquer ação de mitigação ou qualquer controle preexistente ter sido levado em conta". (SÃO PAULO (Cidade), ref. 24, p. 43).

16 Mesma matriz de riscos utilizada institucionalmente pela CGM. (SÃO PAULO (Cidade), ref. 24. p. 28 e 29).

2.3. AVALIAÇÃO DOS RISCOS E DEFINIÇÃO DOS REQUISITOS DE PRIVACIDADE

A terceira etapa do desenvolvimento do Diagnóstico de Maturidade foi a avaliação dos riscos[17], momento no qual foram priorizados aqueles que demandavam a implementação de medidas de tratamento. Observa-se que este procedimento envolve tomadas de decisão que dependem do apetite[18] e da tolerância [19]ao risco do gestor, visando mantê-los dentro de níveis aceitáveis, sendo possível adotar diferentes estratégias.

Entre as respostas ao risco consideradas como premissa para o trabalho, incluíram-se: *"mitigar", "transferir", "evitar" e "aceitar"*. Nesse momento, foram selecionados, para continuidade da avaliação, apenas os riscos classificados como *"extremos"* ou *"altos"* (totalizando catorze), em razão de sua relevância. Para eles, adotou-se como resposta padrão a mitigação, enquanto os demais riscos foram classificados como aceitos.

Essa etapa da metodologia foi concluída com a identificação dos requisitos de privacidade, definidos a partir da avaliação de riscos realizada[20]. Assim, para cada risco remanescente, foi associado um requisito correspondente, acompanhado das referências à legislação aplicável, a normas técnicas e a boas práticas reconhecidas pela ANPD e outras instituições.

2.4. TRATAMENTO DOS RISCOS E CÁLCULO DO RISCO RESIDUAL

Após a seleção dos principais riscos e seus respectivos requisitos de privacidade, iniciou-se a quarta etapa do desenvolvimento do Diagnóstico de Maturidade, correspondente à definição das medidas de tratamento[21]. No escopo da ferramenta, essas medidas foram denominadas *"controles"*[22].

A escolha dos controles baseou-se nas referências já citadas e nos Controles CIS Versão 8, que contém exemplos de controles aplicáveis ao contexto da privacidade. Com base nessas fontes, foram selecionados setenta controles para compor a ferramenta, com o objetivo de verificar a implementação dos requisitos de privacidade e mitigar os riscos associados.

17 "O propósito da avaliação de riscos é apoiar decisões". (ABNT, ref. 21, p. 13).

18 Refere-se à "quantidade e os tipos de riscos que a organização está disposta a aceitar para atingir os seus objetivos". (SÃO PAULO (Cidade), ref. 24, p. 43).

19 Refere-se ao "nível de variação aceitável quanto à realização de um objetivo, podendo ser para mais ou para menos". (SÃO PAULO (Cidade), ref. 24, p. 43).

20 "Os requisitos de privacidade especificam a maneira em que um sistema, produto ou serviço precisa funcionar para satisfazer os resultados de privacidade desejados pelas partes interessadas [...]. Para definir os requisitos de privacidade, considere os requisitos de privacidade em nível organizacional [...] e as saídas de uma avaliação de risco de privacidade". (NIST, ref. 23, p. 39).

21 "O propósito do tratamento de riscos é selecionar e implementar opções para abordar riscos". (ABNT, ref. 21, p. 14).

22 Refere-se a "medida que mantém e/ou modifica o risco". (ABNT, ref. 21, p. 2).

Após a definição dos controles foi conduzida uma avaliação sobre a sua efetividade esperada[23], por meio de uma abordagem qualitativa, com base na experiência no tema e no julgamento profissional da equipe. Para isso, atribuiu-se uma nota a cada um deles, simulando-se o efeito previsto sobre os riscos, em uma escala de cinco faixas[24].

Essa avaliação, combinada com o risco inerente, permitiu o cálculo do risco residual[25]. A classificação do risco residual utilizou as mesmas faixas aplicadas aos riscos inerentes, sendo determinada pelo seu posicionamento na mesma matriz de risco previamente referenciada. Ao final, todos os riscos residuais foram enquadrados na categoria "médio". Vide exemplo da aplicação da metodologia na Tabela 01.

***Tabela 01**. Exemplo da aplicação da metodologia*

Seção	Tópico	Aplicação
2.1. Definição de temas e identificação de riscos	Tema	Estrutura Organizacional
	Risco	Lentidão no processo ou não adequação do órgão à LGPD
	Causa	Ausência de encarregado
	Consequência	Titulares: direitos não atendidos; Órgãos: sanções da ANPD
2.2. Análise de riscos	Impacto	Muito Alto
	Probabilidade	Alto
	Risco Inerente	Alto
2.3. Avaliação de riscos	Resposta ao risco	Mitigar
	Requisito de privacidade	Art. 23, III, LGPD
2.4. Tratamento de riscos	Controle	Nomeação do encarregado
	Efetividade do controle	Mediano
	Risco residual	Médio

***Fonte:** autores, adaptado de SÃO PAULO (Cidade), ref. 18*

3. O PLANEJAMENTO PARA A EXECUÇÃO DO DIAGNÓSTICO DE MATURIDADE

Terminada a etapa de desenho do Diagnóstico de Maturidade, o projeto também demonstrou preocupação com o planejamento da sua implementação, tendo em vista a necessidade de se institucionalizar os procedimentos e se mensurar o avanço ao longo do tempo. O projeto da implementação da ferramenta

23 "Após a implementação, uma organização avalia iterativamente os controles quanto à sua eficácia no cumprimento dos requisitos de privacidade e no gerenciamento do risco de privacidade". (NIST, ref. 23, p. 41).

24 Mesmas faixas utilizadas institucionalmente pela CGM. (SÃO PAULO (Cidade), ref. 24, p. 32).

25 Refere-se ao "nível de risco ao qual uma organização está exposta mesmo depois de serem consideradas as ações de mitigação e os controles preexistentes". (SÃO PAULO (Cidade), ref. 24, p. 43).

contemplou: (i) o estabelecimento de fases de implementação; (ii) a definição de competências e procedimentos; e (iii) a formalização e aprovação dos procedimentos criados.

3.1. DEFINIÇÃO DAS FASES

Considerando-se a elevada quantidade de controles selecionados, foi estabelecida progressão de sua implementação com base em critérios de priorização. No âmbito do Diagnóstico de Maturidade, esse ordenamento foi estruturado em cinco *"fases"*: preparatório, básico, intermediário, avançado e institucionalização.

De modo geral, a implementação dos controles se baseou na sua respectiva complexidade. Assim, controles complexos foram posicionados em fases posteriores, uma vez que poderiam exigir a implementação prévia de controles mais simples. Isso possibilita maior foco e agilidade nas fases iniciais, enquanto permite maior profundidade na implementação dos controles mais avançados. Essa estruturação se mostra importante para orientar o gestor público na alocação eficiente de esforços e recursos limitados.

3.2. DEFINIÇÃO DE COMPETÊNCIAS E PROCEDIMENTOS

Com relação às competências e procedimentos dos órgãos, foi estabelecido um ciclo anual, no qual cada unidade deve: (i) preencher uma autoavaliação sobre os controles correspondentes à fase em que se encontra no Diagnóstico de Maturidade; (ii) realizar análise de lacunas sobre os controles ainda não implementados; (iii) planejar as ações para o próximo período; e (iv) implementar os controles conforme o planejamento. Observa-se que o desenho desse procedimento segue o ciclo PDCA (*Plan-Do-Check-Act*[26]).

Dentre os procedimentos atribuídos aos órgãos, destaca-se a autoavaliação de controles (do inglês CSA – *Control Self Assessment*[27]). Em atenção ao princípio da responsabilização e da prestação de contas, todo o procedimento de autoavaliação deve ser documentado pelos gestores, indicando a existência ou não de cada controle, ou a sua não aplicabilidade, sempre de forma justificada. Os órgãos só avançam para a avaliação da fase seguinte após concluírem a implementação de todos os controles da fase anterior ou apresentarem justificativa para sua não aplicabilidade.

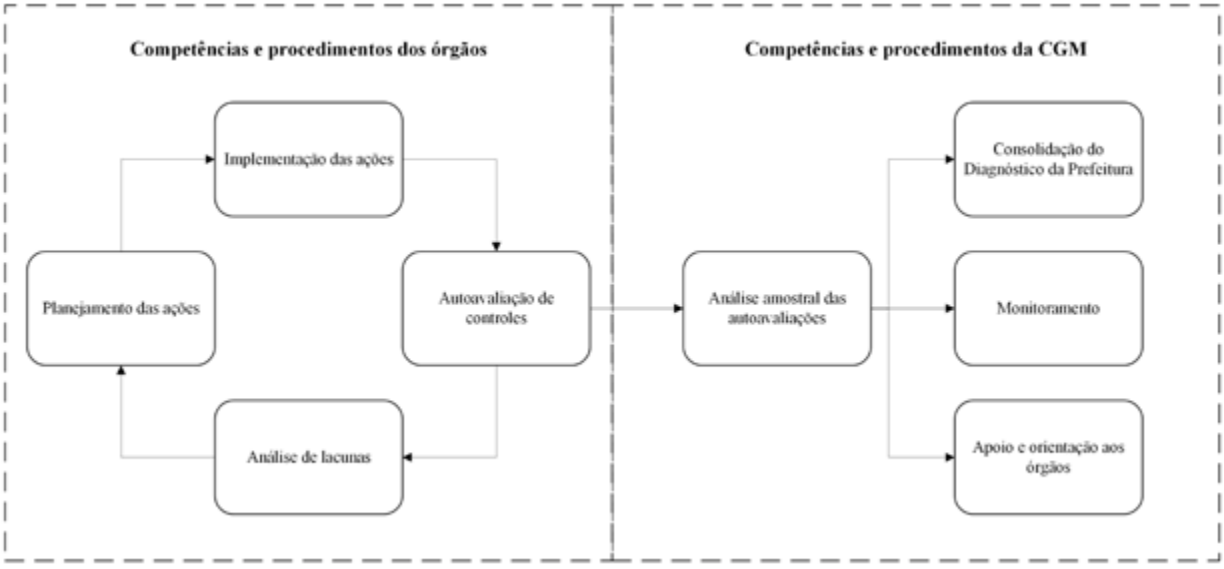
26 Planejar, executar, verificar e agir (tradução livre). (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). Sistemas de gestão da qualidade — Requisitos. NBR ISO 9001:2015. Rio de Janeiro: ABNT, 2015. p. Ix).

27 Tradução livre. Trata-se de um mecanismo no qual o gestor público avalia seu próprio sistema de controle interno, ampliando seu conhecimento sobre as operações e permitindo a atuação para melhoria contínua. (INSTITUTE OF INTERNAL AUDITORS (IIA). A perspective on control self-assessment. Professional Practice Pamphlet 98-2. Altamonte Springs, FL: IIA, 1998. Disponível em: https://www.iiajapan.com/pdf/data/csa/pp98-2.pdf. Acesso em: 19 ago. 2025. p. 4).

Quanto às competências e procedimentos da CGM, foram definidas quatro atividades principais: (i) análise amostral das autoavaliações dos órgãos; (ii) consolidação das autoavaliações para a elaboração do diagnóstico amplo de toda a Prefeitura; (iii) monitoramento periódico de controles e fases previamente concluídas; e (iv) fornecimento de apoio e orientação aos órgãos ao longo de todo o processo.

Em relação aos procedimentos executados pela CGM, merece destaque a análise amostral das autoavaliações. A CPD ficou responsável por essa atividade, limitando-se a verificar a existência de evidências da implementação dos controles ou justificativas para a sua não aplicabilidade, sem se aprofundar em aspectos de mérito das decisões dos gestores públicos ou da efetividade dos controles[28]. Vide na Figura 01 resumo dos procedimentos e competências:

Figura 01. Competências e procedimentos



Fonte: autores, adaptado de SÃO PAULO (Cidade), ref. 18.

3.3. FORMALIZAÇÃO E APROVAÇÃO

A metodologia e o procedimento do Diagnóstico de Maturidade foram formalizados em proposta de instrução normativa pelo Controlador Geral do Município. Considerando-se o alcance do normativo a todos os órgãos, a sua aprovação contou com a particularidade de passar por deliberação da Comissão Municipal de Acesso à Informação (CMAI).

A CMAI caracteriza-se como colegiado composto por integrantes da alta administração municipal, com competências relacionadas ao monitoramento

28 Isso não implica em prejuízo à realização de auditorias, permitindo que a CGM atue de forma estratégica, especialmente diante de situações que possam configurar irregularidade.

do cumprimento da Lei de Acesso à Informação. A partir do advento do Decreto nº 59.767/2020, a CMAI passou a ter competência para deliberar sobre assuntos relacionados à aplicação da LGPD. Tal procedimento foi relevante para se conferir legitimidade às decisões tomadas no âmbito da metodologia de gestão de riscos[29]. Por fim, o projeto também foi institucionalizado com o alinhamento ao planejamento estratégico da CGM.

4. ANÁLISES SOBRE A CONSTRUÇÃO DO DIAGNÓSTICO DE MATURIDADE

Após detalhar o processo de construção da ferramenta, torna-se relevante apresentar uma análise sobre os benefícios esperados, os desafios e limitações enfrentados e os aspectos-chave para a condução do projeto.

4.1. BENEFÍCIOS ESPERADOS

Desde a sua concepção, o Diagnóstico de Maturidade já se configura como um instrumento de orientação, pois aponta aos gestores públicos as principais medidas de governança e conformidade que devem ser adotadas em suas unidades. Esse direcionamento contribui para a priorização de ações, estabelece maior urgência para temas críticos e apoia a tomada de decisão baseada em critérios objetivos.

Além de permitir a análise individualizada de cada órgão, a ferramenta possibilita a obtenção de um panorama consolidado de todos os órgãos. Essa visão integrada é fundamental para embasar decisões estratégicas e orientar a formulação de políticas públicas. Ademais, nota-se que a visão em fases facilita a comunicação rápida do estágio de adequação de cada órgão, conferindo-se também transparência e melhor compreensão do assunto pelos munícipes.

A sistematização das informações facilita a identificação de boas práticas e casos de sucesso, que podem servir de referência e ser replicados em outros órgãos. Ao mesmo tempo, evidencia vulnerabilidades e pontos de atenção, permitindo direcionar esforços e recursos para apoiar unidades que enfrentam maiores desafios na adequação à LGPD. Isso colabora para que a implementação de medidas pelos órgãos ocorra de maneira mais ágil e padronizada.

Entende-se que o Diagnóstico de Maturidade contribui tanto para a Administração Pública quanto para a sociedade. De um lado, esperam-se avanços na gestão e no fortalecimento da cultura de proteção de dados pessoais aos agentes públicos. Por outro, o atendimento às demandas dos cidadãos também

29 "[...] o compromisso explícito e genuíno de agentes da alta direção da organização é essencial para conferir credibilidade ao programa e influenciar a tomada de decisões dos agentes membros da organização em suas atividades diárias de forma positiva". (MARQUES DE CARVALHO, Vinicius; MATTIUZO, Marcela; PONCE, Paula Pedigoni. Boas Práticas e Governança na LGPD. In: Doneda, Danilo; et. al. (Coord.). Tratado de Proteção de Dados pessoais. Rio de Janeiro: Forense, 2021, p. 370).

é aprimorado, fortalecendo-se a confiança nas instituições públicas, com a geração de benefícios para toda a municipalidade.

4.2. DESAFIOS E LIMITAÇÕES

O Diagnóstico de Maturidade configura-se como uma ferramenta de apoio à gestão no processo de adequação à LGPD. Seu desenvolvimento teve como pressuposto o princípio da boa-fé, buscando-se garantir a veracidade, a fidedignidade e a exatidão da autoavaliação realizada pelos gestores. Destaca-se que o objetivo da ferramenta, portanto, não é exercer controle corretivo, mas atuar de forma preventiva, sem eximir os órgãos de suas responsabilidades.

Nesse sentido, destaca-se ainda a utilização da nomenclatura *"maturidade"*, que indica um estágio de evolução da unidade, e não exclusivamente a sua conformidade. De fato, o instrumento considera critérios amplos, que envolvem também governança, boas práticas e melhoria contínua. A ferramenta ainda está sujeita a revisões constantes, em função de novas orientações da ANPD, do surgimento de tecnologias emergentes e de outras mudanças no cenário regulatório, inviabilizando-se a ideia de garantia permanente e estática de adequação.

Observa-se que o principal desafio na construção da ferramenta esteve relacionado com as competências e as diferenças existentes entre os órgãos municipais. Nesse sentido, a CGM adotou distintas estratégias para lidar com as dificuldades encontradas (i) na definição dos temas, (ii) na classificação dos riscos e (iii) na seleção dos controles.

Na definição dos temas, foi necessário lidar com assuntos em que há intersecção com a competência de outros órgãos, tais como segurança da informação e matérias jurídicas. Para endereçar essa questão, a ferramenta abordou aspectos dessas áreas correlatas, mas permaneceu focada na privacidade. Dessa forma, entende-se que esses temas devem ser trabalhados a partir de uma visão integrada, considerando-se também as orientações dos órgãos que possuem competências relacionadas.

Na classificação dos riscos, o desenho da ferramenta teve que lidar com as diferenças entre os órgãos e seus contextos, que apresentam níveis de risco distintos. Para tratar esse entrave, permitiu-se maior flexibilidade ao se considerar o apetite e a tolerância ao risco do gestor, a quem foi dada autonomia para propor, justificadamente, variações na aplicação da metodologia.

Na seleção dos controles, a ferramenta considerou critérios de relevância, de modo que não foi contemplada a totalidade de exigências previstas em normativos e boas práticas. É fundamental que os gestores considerem essa limitação para adaptar o Diagnóstico de Maturidade a outros requisitos de privacidade aplicáveis aos seus respectivos contextos.

Por fim, analisando-se o planejamento da implementação da ferramenta, observa-se o desafio advindo da grande quantidade de controles selecionados. Por isso, o Diagnóstico de Maturidade previu também a orientação da implementação dos controles por meio da sua divisão em fases, reconhecendo-se que o processo de adequação à LGPD é contínuo e não ocorre de forma imediata.

4.3. ASPECTOS-CHAVE PARA A CONDUÇÃO DO PROJETO

Ao se analisar o processo de construção do Diagnóstico de Maturidade, observam-se diversos fatores que contribuíram diretamente para o desenvolvimento do trabalho. A identificação desses fatores se mostra importante para documentar lições aprendidas e auxiliar outros entes públicos que eventualmente optem por implementar políticas semelhantes.

Na análise do planejamento do projeto, considera-se que um dos fatores determinantes para o desenvolvimento da ferramenta foi o comprometimento institucional da CGM com a pauta da privacidade, materializado com a criação da CPD por meio do Decreto nº 62.809/2023. Nesse sentido, a formação de uma equipe técnica multidisciplinar, dotada de autonomia técnica e dedicada a apoiar a adequação da Administração Pública Municipal à LGPD representa um marco inicial e um dos principais impulsionadores do processo de transformação.

Na análise da construção da ferramenta, observa-se que a posição da CGM como órgão central de controle interno foi um fato que contribuiu para o desenvolvimento da ferramenta. Primeiramente, porque a centralidade da sua atuação mostra-se um diferencial para se lidar com a transversalidade do tema por todos os órgãos. Ademais, destaca-se a expertise da CGM em gestão de riscos, auditoria, governança e conformidade, competências que contribuíram diretamente para a aplicação da metodologia baseada em riscos na elaboração da ferramenta.

Na análise do projeto operacional, entende-se que a presença de um corpo técnico efetivo na CGM, incluindo Auditores Municipais de Controle Interno, constituiu um fator importante para a continuidade do projeto. Considera-se que a existência de equipe qualificada e estável representa um diferencial, especialmente em um ambiente novo em que se regula o direito à privacidade, muitas vezes desconhecido pelos agentes públicos e marcado por mudanças frequentes.

Na análise da formalização do projeto, nota-se que o comprometimento da alta administração constituiu elemento fundamental para a sua aprovação. Da perspectiva da gestão de riscos, ressalta-se a relevância e o simbolismo da ratificação do projeto pela CMAI, que se mostrou indispensável, dado que representa o firmamento da tolerância e do apetite ao risco pelo gestor. Tal postura reflete uma mudança cultural que requer engajamento da estratégia à operação,

salientando-se também a importância da institucionalização do projeto com o alinhamento ao planejamento estratégico da CGM.

5. CONCLUSÃO

Considerando a necessidade de adequação da Administração Pública à LGPD, bem como da ausência de instruções claras em como operacionalizar a implementação do referido diploma, foi elaborada metodologia personalizada pela CGM de forma a contemplar as peculiaridades do ente municipal. Referida metodologia foi construída a partir de um processo de gestão de riscos em privacidade e sistematização de controles aptos a tratá-los.

Espera-se que a ferramenta contribua com o fortalecimento da cultura de proteção de dados pessoais, subsidiando a tomada de decisão dos gestores públicos. Elaborar uma metodologia que possa ser adaptada aos diferentes contextos dos órgãos representou um dos maiores desafios desse projeto. Além disso, como limitação, imprescindível o registro que a metodologia não representa um ateste de conformidade, mas uma classificação a partir do conceito de maturidade.

Como fatores que contribuíram para o desenvolvimento do projeto, tem-se o comprometimento da alta administração, evidenciado pela criação de uma coordenadoria vocacionada ao tema no âmago da CGM, órgão central de controle interno com atuação transversal, e pela aprovação da metodologia por parte da CMAI. No aspecto operacional, a presença de um corpo técnico, com integrantes da carreira de Auditor Municipal de Controle Interno, foi fundamental, considerando que experiência e julgamento profissional, elementos basilares para a melhor técnica de trabalhos de auditoria, foram determinantes no processo de gestão de riscos e atribuição de medidas potencialmente mitigadoras.

O Diagnóstico de Maturidade ilustra o potencial de uma ferramenta de controle interno como forma de auxiliar o gestor no processo de adequação de seus processos e atividades às balizas postas pela LGPD, com a finalidade de se alcançar um cenário em que o tratamento de dados pessoais pelo ente público ocorra de forma segura e legítima.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). Gestão de riscos — Diretrizes. NBR ISO 31000:2018. Rio de Janeiro: ABNT, 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). Segurança da informação, segurança cibernética e proteção da privacidade — Aplicação da ABNT

NBR ISO 31000:2018 para gestão de riscos de privacidade organizacional. NBR ISO/IEC 27557:2023. Rio de Janeiro: ABNT, 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). Segurança da informação, segurança cibernética e proteção à privacidade – Controles de segurança da informação. NBR ISO/IEC nº 27002:2022. Rio de Janeiro: ABNT, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). Segurança da informação, segurança cibernética e proteção à privacidade – Sistemas de gestão da segurança da informação – Requisitos. NBR ISO/IEC nº 27001:2022. Rio de Janeiro: ABNT, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). Sistemas de gestão da qualidade — Requisitos. NBR ISO 9001:2015. Rio de Janeiro: ABNT, 2015.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). 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. NBR ISO/IEC nº 27701:2020. Rio de Janeiro: ABNT, 2020.

BRASIL. Agência Nacional de Proteção de Dados (ANPD). ANPD esclarece dúvidas sobre a atuação do Encarregado e a emissão de selos de conformidade com a LGPD. Brasília, DF: ANPD, 31 mar. 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-esclarece-duvidas-sobre-a-atuacao-do-encarregado-e-a-emissao-de-selos-de-conformidade-com-a-lgpd. Acesso em: 18 ago. 2025.

BRASIL. Agência Nacional de Proteção de Dados (ANPD). Guia Orientativo: Tratamento de dados pessoais pelo Poder Público. Versão 2.0. Brasília, DF: ANPD, jun. 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 18 ago. 2025.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República. [2024]. Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 22 ago. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da República Federativa do Brasil, Brasília, DF, 15 ago. 2018. [2022]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 18 ago. 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos (MGI). Guia do Framework de Privacidade e Segurança da Informação, versão 1.1.2. Brasília, DF: MGI, set. 2023. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf. Acesso em: 22 ago. 2025.

BRASIL. Tribunal de Contas da União (TCU). ACÓRDÃO nº 1.384/2022. Plenário. Brasília, DF: TCU, 2022. Disponível em: https://pesquisa.apps.tcu.gov.br/redireciona/acordao-completo/ACORDAO-COMPLETO-2521877. Acesso em: 22 ago. 2025.

BRITTO, Nara Pinheiro Reis Ayres de; RIBEIRO, Alanna Muniz. Soft Law e Hard Law como Caminho para Afirmação do Direito à Proteção de Dados: Uma Análise da Experiência Internacional de Brasileira. In: FERNANDES, Ricardo Vieira de Carvalho; CARVALHO. Angelo Gamba Prata de (Coord.). Tecnologia jurídica & direito digital: II Congresso Internacional de Direito, Governo e Tecnologia – 2018: Belo Horizonte: Fórum, 2018.

CENTER FOR INTERNET SECURITY (CIS). Controles CIS – Versão 8. East Greenbush, NY: CIS, 2021. Disponível em: https://www.cisecurity.org/controls/v8. Acesso em: 20 ago. 2025.

CONSELHO FEDERAL DE CONTABILIDADE (CFC). NBC TA 200 (R1): Objetivos Gerais do Auditor Independente e a Condução da Auditoria em Conformidade com Normas de Auditoria. Brasília, DF: CFC, 19 ago. 2016. Disponível em: https://www1.cfc.org.br/sisweb/SRE/docs/NBCTA200(R1).pdf. Acesso em: 25 ago. 2025.

CONSELHO NACIONAL DE CONTROLE INTERNO (CONACI). Diagnóstico de Adequação à LGPD: Pesquisa 01/2022. Brasília, DF: CONACI, 2022. Disponível em: https://conaci.org.br/wp-content/uploads/2023/08/Diagnostico-de-adequacao.pdf. Acesso em: 22 ago. 2025.

INSTITUTO DOS AUDITORES INTERNOS (IIA). Modelo de Capacidade de Auditoria Interna para o Setor Público (IA-CM). 2. ed. São Paulo: IIA Brasil, 2017. Disponível em: https://iiabrasil.org.br/IA-CM.pdf. Acesso em: 19 ago. 2025.

INSTITUTE OF INTERNAL AUDITORS (IIA). A perspective on control self-assessment. Professional Practice Pamphlet 98-2. Altamonte Springs, FL: IIA, 1998. Disponível em: https://www.iiajapan.com/pdf/data/csa/pp98-2.pdf. Acesso em: 19 ago. 2025.

MARQUES DE CARVALHO, Vinicius; MATTIUZO, Marcela; PONCE, Paula Pedigoni. Boas Práticas e Governança na LGPD. In: Doneda, Danilo; et. al. (Coord.). Tratado de Proteção de Dados pessoais. Rio de Janeiro: Forense, 2021.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). NIST Privacy Framework: a tool for improving privacy through enterprise risk management (ERM). Version 1.0. Gaithersburg: NIST, 2020. Disponível em: https://doi.org/10.6028/NIST.CSWP.01162020pt. Acesso em: 19 ago. 2025.

PERNAMBUCO. Secretaria da Controladoria Geral do Estado (SCGE). LGPD Pernambuco. Recife: SCGE, 2025 Disponível em: https://www.scge.pe.gov.br/lgpd-rede-de-encarregados/. Acesso em: 22 ago. 2025.

SÃO PAULO (Cidade). Decreto nº 59.767, de 15 de setembro de 2020. Regulamenta a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei de Proteção de Dados Pessoais (LGPD) – no âmbito da Administração Municipal direta e indireta. Diário Oficial da Cidade, São Paulo, SP, 16 set. 2020. Disponível em: https://legislacao.prefeitura.sp.gov.br/leis/decreto-59767-de-15-de-setembro-de-2020. Acesso em: 18 ago. 2025.

SÃO PAULO (Cidade). Decreto nº 62.809, de 3 de outubro de 2023. Dispõe sobre a reorganização da Controladoria Geral do Município – CGM [...]. Diário Oficial da Cidade, São Paulo, SP, 04 out. 2023. Disponível em: https://legislacao.prefeitura.sp.gov.br/leis/decreto-62809-de-3-de-outubro-de-2023. Acesso em: 18 ago. 2025.

SÃO PAULO (Cidade). Controladoria Geral do Município (CGM). Instrução Normativa CGM nº 01, de 21 de julho de 2022. Estabelece disposições referentes ao tratamento de dados pessoais no âmbito da Administração Pública Municipal de São Paulo. Diário Oficial da Cidade, São Paulo, SP: CGM, 22 jul. 2022. [2025].

SÃO PAULO (Cidade). Controladoria Geral do Município (CGM). Instrução Normativa CGM/SP nº 02, de 23 de dezembro de 2024. Aprova a Metodologia de Diagnóstico de Maturidade em Proteção de Dados Pessoais e disciplina o procedimento de autoavaliação por parte dos órgãos da Administração Pública Municipal. Diário Oficial da Cidade, São Paulo, SP: CGM, 27 dez. 2024.

SÃO PAULO (Cidade). Controladoria Geral do Município (CGM). Manual de Gestão de Riscos. Versão 01/2023. São Paulo, SP: CGM, 2024. Disponível em: https://www.prefeitura.sp.gov.br/cidade/secretarias/upload/controladoria_geral/Manual_Gestao_Riscos_versao01_2023_publicacao_03_01_2024.pdf. Acesso em: 19 ago. 2025.

SÃO PAULO (Cidade). Controladoria Geral do Município (CGM). Planejamento Estratégico – Ciclo 2024–2026. São Paulo, SP: CGM, 2024. Disponível em: https://www.prefeitura.sp.gov.br/cidade/secretarias/upload/controladoria_geral/PlanejamentoEstrategicovf_publicacao_10_06_2024.pdf. Acesso em: 19 ago. 2025.

SÃO PAULO (Cidade). Controladoria Geral do Município (CGM). Relatório - Justificativa Técnica Diagnóstico de Maturidade. São Paulo, SP: CGM, 2024. Disponível em: Documento SEI 105381368. Acesso em: 29 ago. 2025.

SÃO PAULO (Cidade). Secretaria Municipal de Inovação e Tecnologia (SMIT). Orientações Técnicas de Segurança da Informação. São Paulo, SP: SMIT, 2023. Disponível em: https://tecnologia.prefeitura.sp.gov.br/?page_id=1155. Acesso em: 20 ago. 2025.

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT (UNCTAD). Data Protection and Privacy Legislation Worldwide. Geneva: UNCTAD, 02 jul. 2025. Disponível em: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide. Acesso em: 18 ago. 2025.

PREFEITURA DE
SÃO PAULO