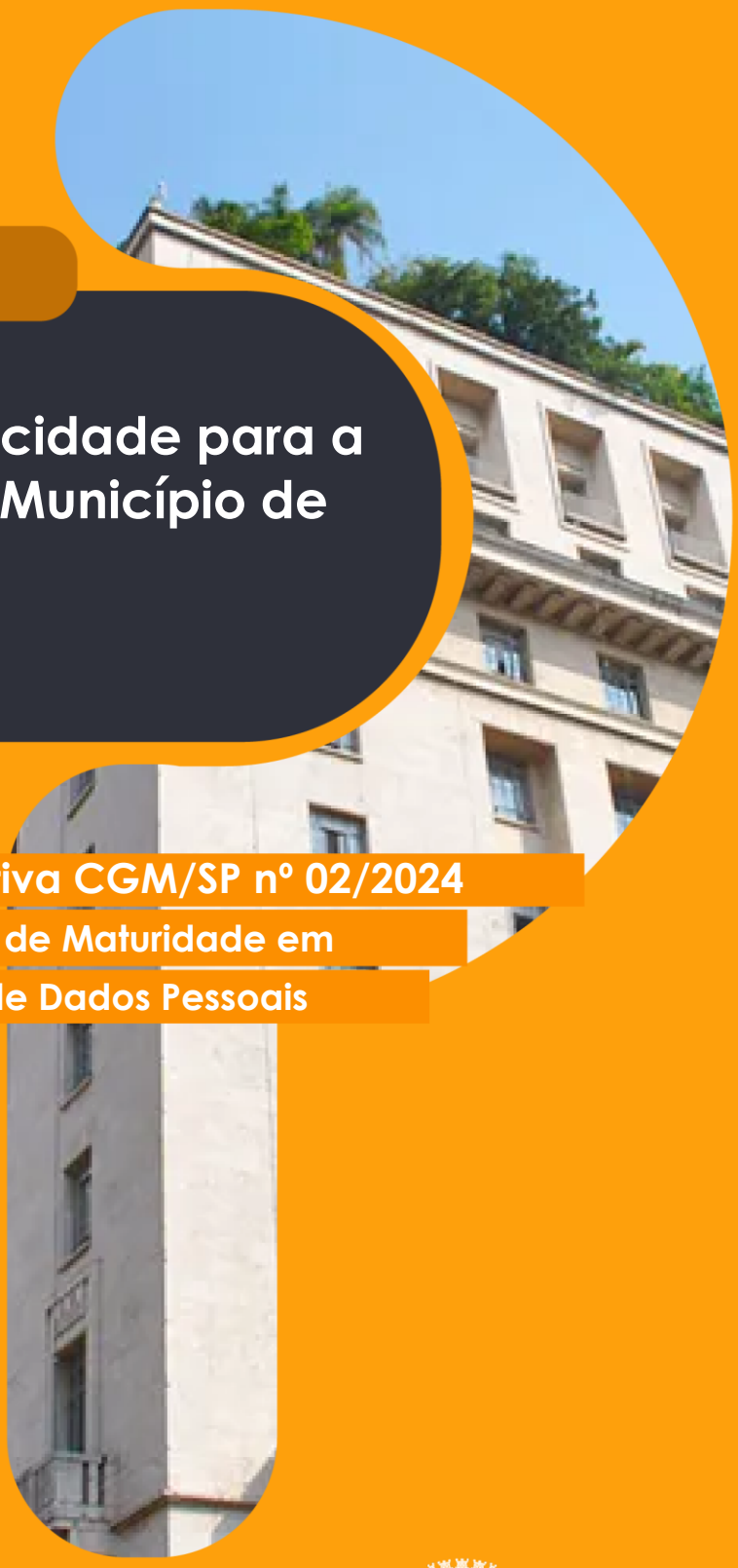
MANUAL

Gestão de Riscos em Privacidade para a Administração Pública do Município de São Paulo (Controle 18)



Instrução Normativa CGM/SP nº 02/2024

Diagnóstico de Maturidade em Proteção de Dados Pessoais

PREFEITURA DE SÃO PAULO

FICHA TÉCNICA

Prefeitura do Município de São Paulo

Prefeito

Ricardo Nunes

Controladoria Geral do Município

Controlador Geral do Município

Daniel Falcão

Chefe de Gabinete

Thalita Abdala Aris

Equipe da Coordenadoria de Proteção de Dados Pessoais

Coordenador

Marcus Vinicius Marins

Elaboração

Fábio Fernandes Libonati

Thiago Ryuichi Hirata

Revisão

Maria Victoria Teodoro Raimundo

Arte e Diagramação

Marília Miquelin de Oliveira

Versão 01

Dezembro de 2025

Este manual foi elaborado em cumprimento aos termos do Decreto Municipal nº 59.767, de 15 de setembro de 2020, que regulamenta a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018, no âmbito do Poder Executivo do Município de São Paulo.

Controlador Geral do Município

Daniel Falcão

VERSÃO

Versão	Descrição	Data
1.0	Versão inicial	12/2025

Sumário

1. Apresentação

Este manual foi elaborado com o objetivo de auxiliar os agentes públicos responsáveis por implementar os controles previstos na Instrução Normativa CGM/SP nº 02/2024, que 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. O foco deste manual é a implementação do "*Controle 18 – Plano de Gestão de Riscos*".

Os órgãos e entidades possuem autonomia técnica e devem considerar o contexto, o volume e o risco dos tratamentos de dados pessoais realizados na implementação deste controle. Assim, o modelo apresentado neste manual não é de uso obrigatório, possui natureza orientativa e poderá ser adaptado para diferentes realidades, desde que justificado.

2. Metodologia

A Controladoria Geral do Município de São Paulo desenvolveu metodologia que objetiva auxiliar os órgãos da PMSP a implementar parte dos controles do Diagnóstico de Maturidade em Proteção de Dados Pessoais. A utilização do modelo proposto traz diversos benefícios, como, por exemplo:

- orientar e solucionar dúvidas na implementação dos controles;
- acelerar a implementação por órgãos que se encontram em estágios iniciais de maturidade; e
- padronizar a execução dos procedimentos.

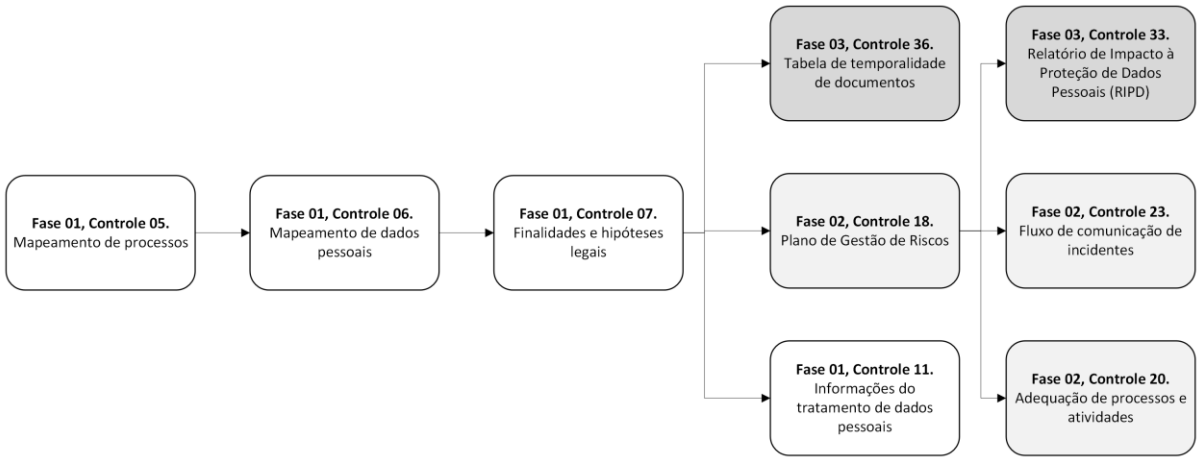
A metodologia desenvolvida se baseia na implementação estruturada e organizada dos seguintes controles do diagnóstico (note-se que são controles que constam em diferentes fases):

Fase 01, Controle 05 – Mapeamento de processos;
Fase 01, Controle 06 – Mapeamento de dados pessoais;
Fase 01, Controle 07 – Finalidades e hipóteses legais;
Fase 01, Controle 11 - Informações do tratamento de dados pessoais;
Fase 02, Controle 18 – Plano de gestão de riscos;
Fase 02, Controle 20 - Adequação de processos e atividades;
Fase 02, Controle 23 – Fluxo de comunicação de incidentes;
Fase 03, Controle 33 - Relatório de Impacto à Proteção de Dados Pessoais;
Fase 03, Controle 36 – Tabela de temporalidade de documentos.

A implementação destes controles foi pensada para ocorrer de maneira sequencial, de modo que a implementação do controle anterior será pré-requisito para a implementação do próximo, uma vez que os controles anteriores irão consolidar informações fundamentais para a sequência de implementação. Trata-se de uma "*trilha*" de implementação.

Para auxiliar os gestores públicos na aplicação da metodologia, foi desenvolvida uma ferramenta em Planilha no formato Excel, cujo objetivo é detalhar e orientar o passo-a-passo de como implementar os controles, de maneira didática e amigável. Espera-se que a estrutura seja útil para simplificar e facilitar a implementação dos controles. A figura a seguir ilustra a estrutura sequencial da implementação dos controles selecionados:

Figura 01: Trilha de implementação de controles selecionados



Fonte: CGM/CPD

O foco deste manual é a implementação do controle "*Fase 02, Controle 18 – Plano de Gestão de Riscos*".

3. Conceitos iniciais

Inicialmente, é importante esclarecer que o objetivo deste manual não é explicar ou interpretar conceitos teóricos relacionados à proteção de dados pessoais. Trata-se de um manual de aplicação prática, que busca sistematizar as orientações e o conhecimento já produzido pela Agência Nacional de Proteção de Dados (ANPD) e outras instituições de referência, visando auxiliar os gestores públicos da Prefeitura de São Paulo na aplicação dos conceitos às suas diferentes realidades.

O presente manual tomou como principal referência os documentos listados a seguir, que devem ser consultados pelos gestores públicos para maiores informações.

- ABNT NBR ISO/IEC nº 27001:2022. Segurança da informação, segurança cibernética e proteção à privacidade – Sistemas de gestão da segurança da informação – Requisitos.

- ABNT NBR ISO/IEC nº 27002:2022. Segurança da informação, segurança cibernética e proteção à privacidade – Controles de segurança da informação.

- ABNT NBR ISO/IEC nº 27557:2023. Segurança da Informação, segurança cibernética e proteção da privacidade – Aplicação da ABNT NBR ISO 31000:2018 para gestão de riscos de privacidade organizacional.

- ABNT NBR ISO/IEC nº 27701:2020. 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.

- ABNT NBR ISO nº 31000:2018. Gestão de riscos – Diretrizes.

- Controles CIS, Versão 8, 2021.

- Guia Orientativo sobre a Instrução Normativa CGM/SP nº 01/2022 para a Administração Pública do Município de São Paulo, versão 01, 2023.

- Guia Orientativo sobre a Privacidade e a Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo, versão 01, 2023.

- Manual de Gestão de Riscos da CGM, Versão 1, 2023.

- Metodologia de Governança de Processos da ANPD, Versão 1.0, 2024.

- NIST Privacy Framework: a Tool for Improving Privacy Through Enterprise Risk Management, Versão 1.0, 2020.

Conforme a metodologia da trilha de implementação dos controles selecionados pela CGM-SP, verifica-se que a implementação do presente controle, relacionado à gestão de riscos em privacidade, depende da implementação prévia dos controles:

- "*mapeamento de processos*" (Fase 01, Controle 05);
- "*mapeamento de dados pessoais*" (Fase 01, Controle 06); e
- "*finalidades e hipóteses legais*" (Fase 01, Controle 07).

Ademais, considera-se necessária a implementação prévia do Controle 19 - "*Política de Gestão de Riscos em Privacidade*". Isto porque estas etapas irão fornecer elementos que serão a base da implementação do presente controle.

3.1. Gestão de riscos

De acordo com o Manual de Gestão de Riscos da CGM, "*risco é definido como a possibilidade de que um evento ocorra e afete, positivamente (risco positivo) ou negativamente (risco negativo), os objetivos pretendidos.*" Para a ABNT NBR ISO nº 31000:2018, a definição de risco relaciona-se ao "*efeito da incerteza nos objetivos".*

Observa-se que os riscos estão presentes na rotina das organizações e, da análise das duas definições apresentadas, envolvem a existência de incertezas sobre o atingimento de seus objetivos. Dessa forma, a gestão dos riscos acaba por ganhar especial importância no contexto das organizações, principalmente para a sua alta direção.

A ABNT NBR ISO 31000:2018 descreve o conceito de "*gestão de riscos*" como "*atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos*". A norma destaca ainda que *"gerenciar riscos é iterativo e auxilia as organizações no estabelecimento de estratégias, no alcance de objetivos e na tomada de decisões fundamentadas".* Trata-se, portanto, de uma maneira de reduzir as incertezas a níveis aceitáveis, a fim de que a organização tenha maior segurança sobre o atingimento de seus objetivos.

Para mais informações sobre gestão de riscos, recomenda-se a leitura dos seguintes documentos:

- Manual de Gestão de Riscos da CGM, Versão 1, 2023.

- ABNT NBR ISO nº 31000:2018. Gestão de riscos – Diretrizes.

3.2. Gestão de riscos em privacidade

A gestão de riscos pode envolver áreas diferentes como a segurança da informação, a segurança cibernética e a privacidade. Embora interligadas, essas áreas possuem escopos distintos. A segurança da informação visa proteger qualquer tipo de informação (sendo física ou digital), assegurando a sua confidencialidade, integridade e disponibilidade. Já a segurança cibernética pode ser entendida como um subconjunto da segurança da informação, tendo foco na proteção de sistemas, redes e dados no ambiente digital. Por sua vez, a privacidade possui foco específico na proteção de dados pessoais.

O presente manual possui como escopo a gestão de riscos de privacidade, ou seja, trata-se de um contexto particular em que se aplica a gestão de riscos.

A ABNT NBR ISO/IEC 27557:2023 aponta as diferenças entre a gestão de riscos da segurança da informação e a gestão de riscos de privacidade para organizações que tratam dados pessoais.

Por um lado, a norma comenta que a gestão de riscos de segurança da informação tradicionalmente se concentra no conceito clássico de risco, com foco na organização como um todo, utilizando-se da fórmula amplamente aceita de risco = impacto x probabilidade.

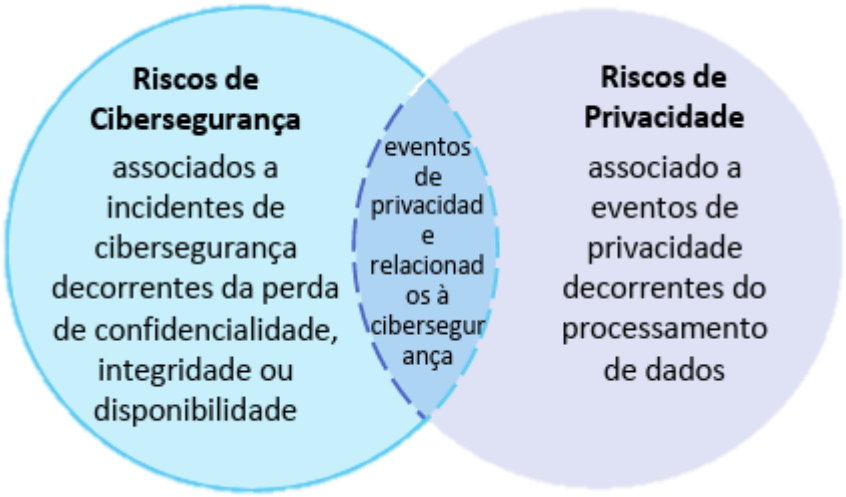
Por outro lado, a norma destaca que a gestão de riscos de privacidade possui a peculiaridade de considerar o impacto da privacidade dos indivíduos como um componente do risco organizacional global. Nesse sentido, ressalta que, apesar de as avaliações de privacidade terem foco no impacto sobre os indivíduos, é necessário considerar como esse impacto contribui para o risco organizacional global. Observa-se que eventos de privacidade podem ter consequências negativas para a organização, como impacto na reputação, na confiança de parceiros e clientes, nos resultados e nas perspectivas de crescimento.

Figura 02: Relação entre risco de privacidade e risco organizacional

Fonte: NIST Privacy Framework

O NIST Privacy Framework, por sua vez, realiza comparação entre riscos de cibersegurança e os riscos de privacidade. Nesse sentido, destaca que, apesar de distintos, há uma intersecção entre eles: "*mesmo sabendo que o gerenciamento do risco de segurança cibernética contribui para o gerenciamento do risco de privacidade, isso não é suficiente, pois os riscos de privacidade também podem surgir de fontes não relacionadas aos incidentes de cibersegurança*".

Figura 03: Relação entre risco de segurança cibernética e risco de privacidade



Fonte: NIST Privacy Framework

Em resumo, observa-se que a gestão de riscos pode envolver áreas diferentes como a segurança da informação, a segurança cibernética e a privacidade, que, embora interligadas, possuem escopos distintos. Especificamente quanto à gestão de riscos de privacidade, verifica-se que a disciplina se torna relevante pois incentiva que a organização estude o impacto da privacidade dos indivíduos e o considere no seu modelo de gestão de riscos global. Além disso, conforme explicado, em muitas situações a gestão dos riscos de privacidade será indissociável da gestão de riscos de segurança da informação e de segurança cibernética, uma vez que são campos interrelacionados. Nota-se, portanto, que a gestão de riscos de privacidade contribuirá na geração de valor para os indivíduos e para a organização, em uma atuação interdisciplinar que poderá envolver diversas áreas.

Para mais informações sobre gestão de riscos de privacidade, recomenda-se a leitura dos seguintes documentos:

- ABNT NBR ISO/IEC nº 27557:2023. Segurança da Informação, segurança cibernética e proteção da privacidade – Aplicação da ABNT NBR ISO 31000:2018 para gestão de riscos de privacidade organizacional.

- Guia Orientativo sobre a Privacidade e a Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo, versão 01, 2023.

- NIST Privacy Framework: a Tool for Improving Privacy Through Enterprise Risk Management, Versão 1.0, 2020.

3.3. Estrutura de gestão de riscos

A ABNT NBR ISO 31000:2018 apresenta um conceito de estrutura da gestão de riscos, personalizável de acordo com as necessidades da organização, formado por seis componentes:

- **Liderança e comprometimento**: relaciona-se com a importância da alta direção para a gestão de riscos, devendo incentivá-la e promovê-la em toda a organização.

- **Integração**: as organizações possuem estruturas e contextos diferentes, de modo que a gestão de riscos deve ocorrer em todas as suas partes de forma integrada, ou seja, não separada da governança, da liderança, dos objetivos organizacionais e das operações, incluindo aspectos de privacidade.

- **Concepção**: deve-se conceber uma estrutura para gestão de riscos de forma personalizada ao contexto externo e interno da organização, articulando-se a liderança e o comprometimento da alta direção através de uma política, por exemplo. É importante definir papéis e responsabilidades na gestão de riscos, além de alocar os recursos apropriados para garantir a sua continuidade e de estabelecer canais de comunicação eficazes com toda a organização.

- **Implementação**: a implementação da gestão de riscos exige o engajamento e a conscientização das partes interessadas.

- **Avaliação**: é importante mensurar periodicamente o desempenho da estrutura de gestão de riscos, avaliando se ela permanece adequada aos objetivos da organização.

- **Melhoria**: deve-se monitorar e adaptar continuamente a estrutura da gestão de riscos de acordo com mudanças internas e externas à organização.

Figura 04: Estrutura de gestão de riscos da ABNT NBR ISO 31000:2018

Fonte: Manual de Gestão de Riscos da CGM e ABNT NBR ISO 31000:2018

Por sua vez, o Manual de Gestão de Riscos da CGM apresenta a estrutura de gestão de riscos das unidades da Prefeitura de São Paulo, com base no Modelo de Três Linhas desenvolvido pelo Instituto de Auditoria Interna (IIA). Nessa estrutura esquematizada da Prefeitura de São Paulo, destacam-se quatro instâncias principais:

- **Gestores de risco (1ª Linha, na Gestão)**: representa os gestores imediatos dos servidores que executam as atividades relacionadas aos riscos.

- **Núcleo especializado de gestão de riscos (2ª Linha, na Gestão)**: representa os agentes públicos responsáveis pela coordenação da gestão de riscos, devendo ser liderados pelo Responsável pelo Controle Interno (RCI) do órgão.

- **Comitê de gestão de riscos (Órgão de Governança)**: representa a alta administração do órgão, responsável por seu planejamento estratégico e definição de objetivos.

- **Auditoria Interna (3ª Linha, Avaliação Independente)**: representa a avaliação independente e objetiva sobre questões relacionadas ao atingimento dos objetivos.

Figura 05: Modelo de Três Linhas do IIA

Fonte: IIA Brasil e Manual de Gestão de Riscos da CGM

Figura 06: Modelo de Três Linhas do IIA

Fonte: Manual de Gestão de Riscos da CGM

4. Metodologia para gestão de riscos em privacidade

A metodologia proposta para a gestão de riscos em privacidade foi dividida em 5 etapas, com base na metodologia da ABNT NBR ISO 31000:2018 e do Manual de Gestão de Riscos da CGM. Cada uma das etapas possui objetivos diferentes conforme se observa no quadro a seguir.

Tabela 01: Etapas da Gestão de Riscos em Privacidade

Etapa	Objetivo
01. Definição de escopo	Definir o escopo de análise com base na priorização dos processos conforme relevância
02. Identificação de riscos	Identificar os principais riscos em privacidade associados a cada processo, assim como suas causas e consequências
03. Análise de riscos	Analisar os riscos identificados, quanto à sua probabilidade e impacto, obtendo-se o risco inerente
04. Avaliação de riscos	Avaliar o tipo de resposta ao risco, comparando-se os resultados da análise de riscos com os critérios de risco estabelecidos
05. Tratamento de riscos	Avaliar os controles existentes e sua efetividade, obtendo-se o risco residual

Fonte: CGM/CPD

Nota-se que o presente manual não contemplou as etapas de "*Comunicação e Consulta*", "*Monitoramento e Análise Crítica*" e "*Registro e Relato*", que estão presentes na metodologia da ABNT NBR ISO 31000:2018 e do Manual de Gestão de Riscos da CGM. Para informações a respeito dessas etapas, sugere-se a leitura das respectivas referências citadas.

Caso o órgão já possua um processo estruturado de gestão de riscos, em nível organizacional, recomenda-se que a gestão de riscos de privacidade seja incorporada a esse processo, não sendo necessário executá-la em separado.

Adiante, serão detalhadas cada uma das etapas da metodologia proposta.

4.1. Etapa 01: Definição de escopo da gestão de riscos em privacidade

De acordo com a ABNT NBR ISO 31000:2018, é importante que a organização estabeleça escopo, contexto e critérios da gestão de riscos, conforme se explica a seguir.

- **Escopo**: o processo de gestão de riscos pode ser aplicado em diferentes níveis (como exemplo, cita-se o nível estratégico, tático, operacional, um programa, um projeto ou outras atividades). Dessa forma, torna-se relevante definir previamente o escopo em consideração na gestão de riscos. No contexto do presente manual, focam-se os processos que realizam tratamento de dados pessoais.

- **Contexto**: a análise dos contextos externo e interno, por sua vez, mostra-se necessária para personalizar a gestão de riscos ao ambiente da organização. No contexto do presente manual, a análise de contexto permite observar aspectos externos, como novas orientações da ANPD aplicáveis a determinados setores ou tecnologias, e aspectos internos, como a criticidade no tratamento de dados pessoais.

- **Critérios**: a definição de critérios é importante para que a alta direção realize a tomada de decisão de forma fundamentada sobre a quantidade e o tipo de risco que aceita assumir em relação ao atingimento dos objetivos organizacionais. Os critérios devem refletir os valores, objetivos e recursos da organização, estando previstos em políticas e declarações sobre a gestão de riscos. Nota-se que os critérios são dinâmicos, podendo ser revistos periodicamente. No contexto do presente manual, deve-se incluir a análise de privacidade dos indivíduos e seu impacto sobre a organização como um todo, conforme dispõe a ABNT NBR ISO/IEC 27557:2023. Sobre o tema, maior detalhamento será apresentado na "*Etapa 04. Avaliação de riscos*".

Na Etapa 01 do presente manual, será dado foco à análise do contexto e à definição do escopo da gestão de riscos de privacidade.

A partir da lista de processos elaborada na implementação do Controle 05 *("mapeamento de processos"*), será realizada uma priorização dos processos para análise mais detalhada. O

objetivo dessa priorização é focar os esforços nos processos que tenham maior criticidade no tratamento de dados pessoais.

Considerando que o presente manual tem foco em privacidade e proteção de dados pessoais, é interessante apresentar um critério para priorização dos processos nesse contexto.

Nesse sentido, sugere-se que seja utilizado como critério para priorização o **"*Resultado do alto risco*"**, que foi calculado na implementação do Controle 06 – Parte II *("Classificação das Operações de Tratamento*"). Para cada processo, a metodologia anteriormente aplicada indicou como "*Resultado do alto risco*":

- ***"Sim"***: considera-se que o processo envolve o tratamento de dados pessoais de alto risco, ou seja, entende-se que há criticidade no tratamento de dados pessoais. Recomenda-se que os processos com essa classificação sejam priorizados para análise detalhada.

- **"*Não*"**: considera-se que o processo não envolve o tratamento de dados pessoais de alto risco, de modo que a recomendação é de não priorizar estes processos para análise detalhada.

- **"*Avaliar*"**: neste caso, cabe ao gestor avaliar se deve priorizar ou não o processo, utilizando-se de outras informações de que disponha para a tomada de decisão.

O critério sugerido é passível de adaptação pelo gestor público, desde que possua fundamento para essa decisão. Nesse sentido, o gestor pode definir que um processo que não possui tratamento de dados pessoais de alto risco deve ser priorizado para análise detalhada. Da mesma forma, o gestor também pode optar pela não priorização de um processo que possui tratamento de alto risco.

É importante ponderar que o critério utilizado pela CGM-SP ("*Resultado do alto risco*") tem foco no contexto da privacidade e proteção de dados pessoais. Nos Apêndices I e II estão exemplificadas outras ferramentas de análise que podem ser utilizadas para a priorização dos processos, conforme descrito pelo Manual de Gestão de Riscos da CGM-SP e pela Metodologia

de Governança de Processos da ANPD. Ressalta-se que os critérios utilizados por essas outras ferramentas têm foco no gerenciamento de processos desses órgãos, possuindo utilidade para diversos outros fins.

4.2. Etapa 02: Identificação de riscos em privacidade

De acordo com a ABNT NBR ISO 31000:2018, o *"propósito da identificação de riscos é encontrar, reconhecer e descrever riscos que possam ajudar ou impedir que uma organização alcance seus objetivos"*. A identificação dos riscos pode ser feita através da aplicação de diferentes técnicas, devendo-se considerar fontes que estão sob controle da organização ou não.

O normativo recomenda considerar os seguintes fatores na identificação dos riscos: "*fontes tangíveis e intangíveis de risco; causas e eventos; ameaças e oportunidades; vulnerabilidades e capacidades; mudanças nos contextos externo e interno; indicadores de riscos emergentes; natureza e valor dos ativos e recursos; consequências e seus impactos nos objetivos; limitações de conhecimento e de confiabilidade da informação; fatores temporais; vieses, hipóteses e crenças dos envolvidos"*. Para mais informações, consulte o Anexo I.

A ABNT NBR ISO/IEC 27557:2023, por sua vez, descreve duas abordagens para identificar riscos em uma organização: baseada em eventos e baseada em ativos.

- **Baseada em eventos:** "*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*". Trata-se de uma análise sobre possíveis eventos de privacidade que podem ocorrer, com foco na avaliação de cenários e de fontes de riscos, que pode ser feita através de entrevistas e análise dedutiva.

- **Baseada em ativos**: *"Uma abordagem baseada em ativos para a identificação de riscos envolve olhar atentamente para os ativos organizacionais e identificar as ameaças e as vulnerabilidades que podem afetar esses ativos".* Trata-se de uma análise que parte dos ativos da organização, construindo cenários de riscos a partir de sistemas, *hardwares*, ambientes físicos, entre outros.

A metodologia do presente manual recomenda que a identificação dos riscos seja feita **por processo, baseada em eventos.** Isto significa partir da lista de processos priorizados na etapa anterior, realizando-se um exame de alto nível de fontes de risco e cenários potenciais.

O Manual de Gestão de Riscos da CGM sugere que a identificação dos riscos seja feita em fases, passando de uma visão geral para a específica. Nesse sentido, busca-se identificar os principais riscos associados aos processos priorizados (estratégicos e críticos), para, em um segundo momento, identificar riscos secundários, incluindo os riscos associados aos processos não priorizados.

Com relação a ferramentas para a identificação de riscos recomenda-se a leitura dos seguintes documentos:

- **Manual de Gestão de Riscos da CGM**: recomenda a utilização de dados históricos, análises teóricas, opiniões de especialistas, e outras técnicas de coleta de informação, tais como: *brainstorming*, análise SWOT, análise da causa-raiz e entrevistas.

- **Guia Orientativo sobre a Instrução Normativa CGM/SP nº 01/2022**: recomenda a realização de entrevistas com executores dos processos, apresentando modelo de entrevista e de questionário sobre a percepção de riscos.

Para cada um dos riscos identificados, espera-se que seja elaborada a sua descrição, assim como a listagem de suas possíveis causas e consequências. Para o estudo de causas e consequências, o Manual de Gestão de Riscos da CGM sugere a utilização das seguintes ferramentas: diagramas de causa e efeito, fluxogramas, diagramas de influência, diagrama *bow tie*. Para consultar exemplos de riscos de privacidade, consulte o Anexo II.

4.3. Etapa 03: Análise de riscos em privacidade

De acordo com a ABNT NBR ISO 31000:2018, o *"propósito da análise de riscos é compreender a natureza do risco e suas características, incluindo o nível de risco, onde apropriado"*. Para isso, podem ser utilizadas diversas técnicas de análise qualitativa ou quantitativa, buscando-se maior clareza para a tomada de decisões.

O normativo recomenda considerar os seguintes fatores na análise dos riscos: "*a probabilidade de eventos e consequências; a natureza e magnitude das consequências; complexidade e conectividade; fatores temporais e volatilidade; a eficácia dos controles existentes; sensibilidade e níveis de confiança*".

Por sua vez, o Manual de Gestão de Riscos da CGM esclarece que é neste momento em que se analisa o risco sob os parâmetros de **probabilidade e impacto**:

- **Probabilidade**: relaciona-se às chances de o risco ocorrer, podendo estar fundamentada em análise quantitativa (estatística ou histórica) ou qualitativa (opiniões de especialistas, informações teóricas etc.). O Manual de Gestão de Riscos da CGM sugere classificar a probabilidade estimada de acordo com as seguintes faixas:

    - **Muito baixo**: ocorrência improvável, com frequência menor que 20%. "*Evento nunca ocorreu e em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade"*

    - **Baixo**: ocorrência rara, com frequência entre 20 e 40%. *"Evento nunca ocorreu, mas de forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade"*

    - **Médio**: ocorrência possível, com frequência entre 40 e 60%. *"Evento já ocorreu no passado e de alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade"*

    - **Alto**: ocorrência provável, com frequência entre 60 e 80%. *"Evento já ocorreu no passado e de forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade"*

    - **Muito alto**: ocorrência praticamente certa, com frequência maior que 80%. *"De forma inequívoca, o evento está ocorrendo ou já ocorreu e as circunstâncias indicam claramente que poderá ser recorrente em um curto espaço de tempo"*

- **Impacto**: relaciona-se às repercussões da ocorrência do risco, podendo ser financeiras, orçamentárias, operacionais, de imagem, sociais, de integridade, de conformidade, dentre outras. Pode estar fundamentada também em análise quantitativa (impacto financeiro, orçamentário etc.) ou qualitativa (opiniões de especialistas, benchmarking etc.). Sobre o impacto, destacam-se dois pontos:

    - **Classificação**: sugere-se classificar o impacto estimado de acordo com as seguintes faixas: muito baixo, baixo, médio, alto e muito alto. Na análise, deve-se considerar aspectos como a gravidade e a reversibilidade dos danos nas diversas perspectivas citadas.

    - **Impactado**: conforme a ABNT NBR ISO/IEC 27557:2023, o impacto na gestão de riscos de privacidade tem um aspecto duplo: deve-se avaliar o impacto sobre os indivíduos, assim como as consequências para a organização. De acordo com o normativo, *"as consequências para a organização diferem necessariamente dos impactos de privacidade para os indivíduos"*.

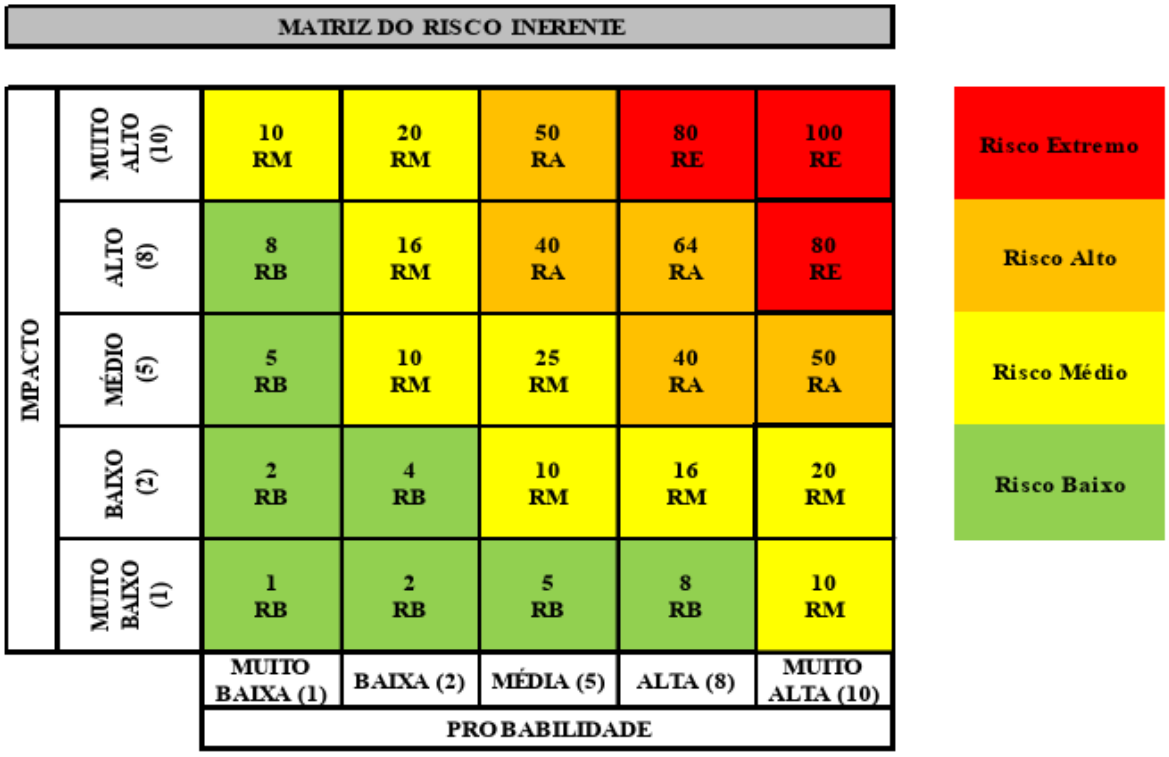
        - **Indivíduos**: para a ABNT NBR ISO/IEC 27557:2023, "*os impactos de privacidade sobre os indivíduos são uma externalidade para a organização. Portanto, pode ser difícil para a organização estimar exatamente o impacto sobre cada indivíduo*". Entre os possíveis impactos aos indivíduos, destacam-se a perda de dignidade, discriminação, perda econômica, perda da autodeterminação e a perda da confiança, entre outros.

        - **Organização**: conforme a ABNT NBR ISO/IEC 27557:2023, os impactos sobre a organização envolvem multas (e outros custos de não conformidade), comprometimento da imagem (danos à reputação), perda de ativos físicos, oportunidades perdidas, diminuição de vendas (custos diretos de negócio), dano à cultura organizacional, perda de tempo, retrabalho, entre outros.

O resultado da multiplicação entre os parâmetros de Probabilidade e Impacto irá resultar no **Risco Inerente**. Trata-se do nível de risco existente antes da aplicação de qualquer controle ou medida de tratamento. Para a classificação do risco inerente, utiliza-se a Matriz de Riscos, que resultará na classificação em: Baixo, Médio, Alto e Extremo.

Risco Inerente = Probabilidade x Impacto

Figura 07: Classificação do Risco Inerente



Fonte: Manual de Gestão de Riscos da CGM

4.4. Etapa 04: Avaliação de riscos em privacidade

De acordo com a ABNT NBR ISO 31000:2018, o *"propósito da avaliação de riscos é apoiar decisões"*. Trata-se da comparação dos resultados da análise de riscos com os critérios de risco estabelecidos pela alta direção, conforme se explicou na Etapa 01, durante a definição de escopo, contexto e critérios.

A definição dos critérios pela alta direção relaciona-se com o apetite ao risco ao qual está disposta a tomar. Nota-se que o apetite ao risco irá depender do contexto da organização - há

setores e momentos em que se aceitam naturalmente riscos maiores, associados também a retornos mais elevados, como por exemplo o setor financeiro, empresas de tecnologia ou startups inovadoras. Por sua vez, há setores como o da saúde, defesa ou infraestrutura que tendem a operar com baixa tolerância ao risco, pois qualquer falha poderia resultar em gravíssimas e irreparáveis consequências. Portanto, a definição do critério de risco dependerá da cultura organizacional, do contexto, do momento ao qual a organização está inserida e de obrigações legais de cada setor.

Neste momento, a comparação com os critérios irá contribuir para a tomada de decisão sobre as ações que devem ser tomadas sobre os riscos. As decisões podem se referir a:

- **Aceitar**: o risco encontra-se em nível aceitável pelo gestor. Nesse caso, opta-se por não tomar nenhuma ação adicional, assumindo-se as possíveis consequências da concretização do risco.

- **Mitigar**: o risco encontra-se em nível superior ao aceitável pelo gestor. Nesse caso, opta-se por ações de tratamento, que podem reduzir a probabilidade de ocorrência e/ou o impacto do risco.

- **Evitar**: o risco encontra-se em nível superior ao aceitável pelo gestor. Nesse caso, opta-se por ações de tratamento, que podem envolver a eliminação da causa do risco ou a não realização da atividade associada a ele. Trata-se de estratégia útil quando o risco é muito alto e inaceitável e não há medidas eficazes de mitigação.

- **Transferir**: o risco encontra-se em nível superior ao aceitável pelo gestor. Nesse caso, opta-se por ações de tratamento, que podem realocar a responsabilidade ou o impacto do risco para terceiros, reduzindo a exposição da organização. Isto pode ser realizado através de contratos, seguros, parcerias, entre outros.

No contexto do presente manual, espera-se que estejam definidos critérios que considerem tanto o impacto na privacidade dos indivíduos como as consequências para a organização. A definição desses critérios irá contribuir para a tomada de decisão no tratamento dos riscos

identificados, levando-se em consideração uma ótica dual, que busca dar atenção aos objetivos da organização ao mesmo tempo em que se preocupa com os indivíduos.

O resultado da avaliação de riscos será considerado para a última etapa, referente ao tratamento dos riscos.

4.5. Etapa 05: Tratamento de riscos em privacidade

De acordo com a ABNT NBR ISO 31000:2018, o *"propósito do tratamento de riscos é selecionar e implementar opções para abordar riscos".* Trata-se de um processo iterativo, no qual selecionam-se controles para manter os riscos em níveis adequados aos critérios de risco estabelecidos pela alta direção.

Por sua vez, a ABNT NBR ISO/IEC 27557:2023 destaca que a seleção de opções de tratamento de risco deve considerar não somente o contexto da própria organização, mas também a privacidade dos indivíduos.

Inicialmente, deve-se realizar a **identificação dos controles** existentes relacionados a cada risco. De acordo com a ABNT NBR ISO 31000:2018, a definição de "*controle*" relaciona-se com "*medida que mantém e/ou modifica o risco*". Como exemplo, citam-se *checklists*, políticas, capacitação, manuais, indicadores de desempenho, entre outros.

A identificação dos controles pode tomar como base o mapeamento de processos realizado previamente, assim como a realização de entrevistas direcionadas para esse fim. Destaca-se que cada risco pode ter mais de um controle, assim como um mesmo controle pode tratar diferentes riscos.

O próximo passo será realizar a **avaliação dos controles**, conforme os critérios listados a seguir pelo Manual de Gestão de Riscos da CGM:

- **Inexistente***: "Os controles são inexistentes, mal desenhados ou mal implementados, isto é, não funcionais".*

- **Fraco**: *"Os controles existentes têm abordagens ad hoc, ou seja, tendem a ser aplicados caso a caso, e a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas".*

- **Mediano**: *"Os controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas".*

- **Satisfatório**: *"Os controles implementados são sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente".*

- **Forte**: *"Os controles implementados podem ser considerados a "melhor prática", mitigando todos os aspectos relevantes do risco".*

O resultado da avaliação da Efetividade dos Controles, multiplicado pelo Risco Inerente, irá resultar no **Risco Residual**. Trata-se do nível de risco existente após a aplicação de controles ou medidas de tratamento. Para a classificação do risco residual, utiliza-se a Matriz de Riscos, que resultará na classificação em: Baixo, Médio, Alto e Extremo.

Risco Residual = Risco Inerente x Efetividade dos Controles

A fim de se aprofundar o conhecimento a respeito de controles aplicáveis ao contexto da privacidade e da proteção de dados pessoais, recomenda-se a leitura do Anexo III e das seguintes referências:

- ABNT NBR ISO/IEC nº 27001:2022. Segurança da informação, segurança cibernética e proteção à privacidade – Sistemas de gestão da segurança da informação – Requisitos.

- ABNT NBR ISO/IEC nº 27002:2022. Segurança da informação, segurança cibernética e proteção à privacidade – Controles de segurança da informação.

- ABNT NBR ISO/IEC nº 27701:2020. 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.

- Controles CIS, Versão 8, 2021.

- Guia Orientativo sobre a Instrução Normativa CGM/SP nº 01/2022 para a Administração Pública do Município de São Paulo, versão 01, 2023.

- Guia Orientativo sobre a Privacidade e a Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo, versão 01, 2023.

- NIST Privacy Framework: a Tool for Improving Privacy Through Enterprise Risk Management, Versão 1.0, 2020.

4.6. Competências e responsabilidades

Para fins de implementação do controle, são identificados dois tipos de atores principais:

(i) gestor do processo; e
(ii) coordenador da implementação do controle.

Ao gestor do processo, cabe a identificação dos pontos de melhoria e suas respectivas propostas de soluções, com relação aos processos sob sua gestão. O gestor do processo se situa em nível tático, tendo a responsabilidade de coordenar o processo sob sua gestão, de buscar alinhamento ao nível estratégico e, ao mesmo tempo, orientar o nível operacional sobre a execução do processo.

Por sua vez, o coordenador da implementação do controle deve orientar, distribuir e coordenar o trabalho de todos os gestores de processos do respectivo órgão. Espera-se que, ao final do trabalho, ele possa consolidar o trabalho de todas as áreas envolvidas em um banco de dados único do órgão.

4.7. Formalização e aprovação

Para a finalização do trabalho, sugere-se que seja realizada reunião de encerramento entre o coordenador da implementação do controle e os gestores de processos, a fim de se demonstrar o resultado alcançado. É importante que haja formalização do trabalho feito e que o documento seja validado pelos gestores.

5. Ferramenta da Planilha no formato Excel

A Controladoria Geral do Município de São Paulo desenvolveu uma ferramenta em Planilha no formato Excel para auxiliar os órgãos na implementação dos controles selecionados na presente metodologia.

Para a etapa de adequação de processos, o órgão deverá preencher as abas denominadas "*18. Gestão de Riscos – Parte 1*" e "*18. Gestão de Riscos – Parte 2*". Conforme explicado anteriormente, o coordenador da implementação do controle pode distribuir a planilha para os diferentes gestores de processo do órgão, que deverão realizar o preenchimento destas abas. Caberá ao coordenador consolidar os dados de todas as abas preenchidas pelos gestores ao final do trabalho.

5.1. Parte 1: Definição de escopo

A aba "*18. Gestão de Riscos – Parte 1*" traz uma visão consolidada de informações relevantes de todos os processos do órgão, a partir das quais será possível realizar a **priorização dos processos** para análise detalhada. Nesta aba, será necessário preencher apenas a coluna sobre a priorização final dos processos, ou seja, o parecer do gestor após as análises realizadas. As demais colunas serão preenchidas automaticamente com informações de outras abas. A priorização dos processos pode ser feita utilizando-se os filtros da planilha em colunas auxiliares, com base nos campos sugeridos neste manual:

- **Tratamento de dados pessoais**: possui como resposta "*Sim*" ou "*Não*", conforme preenchido na Aba "*5. Map Processos*". Sugere-se que sejam filtrados os processos com resposta "*Sim*".

- **Resultado do Alto Risco**: possui como resposta "*Sim*", "*Não*" ou "*Avaliar*", conforme preenchido na Aba "*6. Classificação Operações*". Sugere-se que sejam filtrados os processos com resposta "*Sim*" e "*Avaliar*".

5.1.1. Preenchimento das linhas

Cada linha da planilha se refere a um "*processo*" diferente. Deve-se preencher a coluna "*Priorização Final*" com "*Sim*" ou "*Não*".

5.1.2. Preenchimento das colunas

As colunas seguem os elementos conforme explicado anteriormente neste manual, estando preenchidas com a informação:

- ***"Área", "Processo" e "Principais Atividades":*** preenchimento automático conforme a aba "*5. Map Processos*". Traz informação relevante para identificação do processo e seu contexto;

- ***"Tratamento de dados pessoais"***: preenchimento automático conforme a aba "*5. Map Processos*". Traz informação relevante para a priorização dos processos, com a aplicação de filtro nesta coluna;

- ***"Resultado do alto risco"***: preenchimento automático conforme a aba "*6. Classificação Operações*". Traz informação relevante para a priorização dos processos, com a aplicação de filtro nesta coluna;

- ***"Priorização Final"***: preenchimento manual, a partir de opções de uma lista, com "*Sim*" ou "*Não*". Busca informar o parecer do gestor sobre a seleção do processo para o escopo de análise. Embora a priorização do processo esteja no âmbito da tolerância ao risco do gestor, recomenda-se que que todos os processos que tenham sido classificados como de alto risco ("*Sim*" na coluna "*Resultado do alto risco*") sejam classificados como "*Sim*" na coluna "*Priorização Final*";

- ***"Extremo", "Alto", "Médio", "Baixo" e "Total de Riscos"***: preenchimento automático conforme a aba "*18. Gestão de Riscos – Parte 2*", que será preenchida adiante. Contém informação relevante para a gestão de riscos por processo, referente à quantidade riscos relacionados ao processo (informação total e por nível de risco).

A tabela a seguir traz exemplo de como a planilha estará preenchida.

Tabela 02: Preenchimento das colunas da aba 18. Gestão de Riscos – Parte 1

Coluna da planilha	Descrição	Tipo de resposta	Exemplo
Área	Identificação da área ou setor do gestor do processo	Campo automático - não preencher	*Controladoria Geral do Município de São Paulo / Assessoria de Comunicação*
Processo	Identificação do nome do processo	Campo automático - não preencher	*Publicação de Relatórios da Auditoria Geral do Município, Notas Técnicas e Notas de Monitoramento*
Principais Atividades	Identificação das principais atividades do processo	Campo automático - não preencher	*1. Recebimento do documento para publicização; 2. Revisão do documento; 3. Publicação do documento.*
Tratamento de Dados Pessoais	Identificação se há ou não tratamento de dados pessoais no processo	Campo automático - não preencher	*Sim*
Resultado do Alto Risco	Resultado da avaliação de alto risco	Campo automático - não preencher	*Sim*
Priorização Final	Parecer do gestor sobre a seleção do processo para o escopo de análise	Lista – escolher opção da lista	*Sim*
Extremo	Compilação da quantidade total de riscos extremos identificados	Campo automático - não preencher	*1*
Alto	Compilação da quantidade total de riscos altos identificados	Campo automático - não preencher	*1*
Médio	Compilação da quantidade total de riscos médios identificados	Campo automático - não preencher	*1*
Baixo	Compilação da quantidade total de riscos baixos identificados	Campo automático - não preencher	*1*
Total de Riscos	Compilação da quantidade total de riscos identificados	Campo automático - não preencher	*4*

Fonte: CGM/CPD

5.2. Parte 2: Identificação, análise, avaliação e tratamento de riscos em privacidade

A aba "*18. Gestão de Riscos – Parte 2*" tem a finalidade de realizar a **identificação, análise, avaliação e tratamento de riscos em privacidade**. Para isso, está estruturada conforme a Matriz de Gestão de Riscos apresentada neste manual, trazendo uma visão detalhada sobre os processos. Nesse ponto, sugere-se que sejam contemplados apenas os riscos relacionados aos processos priorizados na aba anterior.

5.2.1. Preenchimento das linhas

Diferentemente das demais abas da ferramenta, cada linha da planilha **não** se refere a um "*processo*", mas sim a um "*risco*". Dessa forma, diferentes linhas podem se referir a diferentes riscos de um mesmo processo. Ao mesmo tempo, é possível que um processo não esteja referenciado em nenhuma das linhas, caso ele não tenha sido priorizado para análise.

5.2.2. Preenchimento das colunas

O preenchimento das colunas segue os elementos explicados anteriormente neste manual. Algumas colunas deverão ser preenchidas manualmente, enquanto outras são automaticamente preenchidas para facilitar a análise dos processos:

- **"*Área*" e "*Processo*"**: preenchimento manual, a partir de opções de uma lista, conforme a aba "*5. Map Processos*". Busca situar o contexto, ou seja, o processo em que o risco foi identificado;

- ***"Principais Atividades", "Fluxo dos dados pessoais"* e *"Dados pessoais"*:** preenchimento automático, conforme as abas "*5. Map Processos*" e "*6. Map Dados Pessoais*". Busca trazer informações úteis para facilitar a análise do processo;

- **"*Finalidade*"**: preenchimento automático, conforme a aba "*7. Finalidades e Hipóteses*". Busca trazer informações úteis para facilitar a análise do processo;

- **"*Descrição do Risco*", *"Causa"* e *"Consequência"***: preenchimento manual e livre, conforme explicado neste manual. Visa identificar os principais riscos no processo e

realizar análise sobre suas respectivas causas e consequências (para os indivíduos e para a organização como um todo), sendo que cada risco deve estar registrado em uma linha diferente da planilha;

- ***"Probabilidade",*** **e** ***"Impacto"****:* preenchimento manual, a partir de opções de uma lista, conforme explicado neste manual. Busca avaliar os riscos identificados;

- ***"Risco Inerente"****:* preenchimento automático, conforme explicado neste manual. Traz o resultado da avaliação sobre os riscos identificados;

- ***"Ação"****:* preenchimento manual, a partir de opções de uma lista, conforme explicado neste manual. Busca avaliar o tipo de ação adequada para os riscos identificados;

- ***"Controle"****:* preenchimento manual e livre, conforme explicado neste manual. Visa identificar os controles existentes para os riscos identificados;

- ***"Efetividade do controle"****:* preenchimento manual, a partir de opções de uma lista, conforme explicado neste manual. Busca avaliar a efetividade dos controles existentes sobre os riscos identificados;

- ***"Risco Residual"****:* preenchimento automático, conforme explicado neste manual. Traz o resultado da avaliação sobre os riscos identificados após a ação dos controles;

A tabela a seguir traz exemplo de como a planilha deve ser preenchida.

Tabela 03: Preenchimento das colunas da aba "18. Gestão de Riscos – Parte 2"

Coluna da planilha	Descrição	Tipo de resposta	Exemplo
Área	Identificação da área ou setor do gestor do processo	Lista – escolher opção da lista	*Controladoria Geral do Município de São Paulo / Assessoria de Comunicação*
Processo	Identificação do nome do processo	Lista – escolher opção da lista	*Publicação de Relatórios da Auditoria Geral do Município, Notas Técnicas e Notas de Monitoramento*
Principais Atividades	Identificação das principais atividades do processo	Campo automático - não preencher	*1. Recebimento do documento para publicização; 2. Revisão do documento; 3. Publicação do documento.*

Fluxo dos dados pessoais	Descrição do fluxo dos dados pessoais no processo	Campo automático - não preencher	*1. Transmissão dos dados pessoais entre áreas da CGM; 2. Armazenamento dos dados pessoais; 3. Publicação dos dados pessoais*
Dados pessoais	Descrição de todos os dados pessoais tratados	Campo automático - não preencher	*Nome; Registro Funcional; CPF*
Finalidade	Identificação da finalidade do tratamento de dados pessoais	Campo automático - não preencher	*Dar ampla publicidade aos resultados da auditoria geral, garantindo transparência e acesso facilitado às informações*
Descrição do Risco	Identificação dos riscos associados ao processo	Livre – sem restrições	*Vazamento de dados pessoais em relatórios públicos*
Causa	Descrição da causa do risco	Livre – sem restrições	*Ausência de procedimento para descaracterização de dados pessoais*
Consequência	Descrição da consequência do risco	Livre – sem restrições	*Dano individual pela perda de dignidade; Dano reputacional e financeiro ao órgão*
Probabilidade	Avaliação quanto à probabilidade de ocorrência do risco	Lista – escolher opção da lista	*Alto*
Impacto	Avaliação quanto ao impacto do risco	Lista – escolher opção da lista	*Alto*
Risco Inerente	Cálculo automático do risco inerente	Campo automático - não preencher	*Alto*
Ação	Avaliação quanto à resposta ao risco inerente	Lista – escolher opção da lista	*Mitigar*
Controle	Identificação dos controles existentes	Livre – sem restrições	*Processo de revisão ad hoc dos documentos*
Efetividade do controle	Avaliação quanto à efetividade dos controles existentes	Lista – escolher opção da lista	*Fraco*
Risco Residual	Cálculo automático do risco residual	Campo automático - não preencher	*Alto*

Fonte: CGM/CPD

6. Referências bibliográficas

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC nº 27001:2022. Segurança da informação, segurança cibernética e proteção à privacidade – Sistemas de gestão da segurança da informação – Requisitos. Rio de Janeiro: ABNT, 2022.

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC nº 27002:2022. Segurança da informação, segurança cibernética e proteção à privacidade – Controles de segurança da informação. Rio de Janeiro: ABNT, 2022.

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC nº 27557:2023. Segurança da Informação, segurança cibernética e proteção da privacidade – Aplicação da ABNT NBR ISO 31000:2018 para gestão de riscos de privacidade organizacional. Rio de Janeiro: ABNT, 2023.

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC nº 27701:2020. 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, 2020.

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC nº 29100:2020. Tecnologia da informação – técnicas de segurança – estrutura de privacidade. Rio de Janeiro: ABNT, 2020.

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO nº 31000:2018. Gestão de riscos – Diretrizes. Rio de Janeiro: ABNT, 2018.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). Metodologia de Governança de Processos. V. 1.0. Brasília, abril de 2024. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/metodologia_anpd_vf_consolidada.pdf> Acesso em: 27/11/2024

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). Resolução CD/ANPD nº 8 de 05/09/2023. Institui a Política de Governança de Processos da Autoridade Nacional de Proteção de Dados (ANPD). Disponível em: <https://www.in.gov.br/web/dou/-/resolucao-cd/anpd-n-8-de-5-de-setembro-de-2023-508638337> Acesso em: 29/10/2024.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Guia de Elaboração de Inventário de Dados Pessoais. Programa de Privacidade e Segurança da Informação (PPSI). Versão 2.0. Brasília, março de 2023. Disponível em: <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_inventario_dados_pessoais.pdf> Acesso em: 02/12/2024

BRASIL. Lei Federal nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, Diário Oficial da União, 15 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 29/10/2024.

CENTER INTERNET SECURITY. Controles CIS, Versão 8, 2021. Disponível em: <https://www.cisecurity.org/> Acesso em: 04/03/2024

INSTITUTO DOS AUDITORES INTERNOS DO BRASIL (IIA Brasil). Modelo das 3 linhas do IIA 2020, IIA Brasil, 2021. Disponível em: https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-portuguese.pdf Acesso em 07/05/2025

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST Privacy Framework: a Tool for Improving Privacy Through Enterprise Risk Management, Versão 1.0, 2020. Disponível em: <https://doi.org/10.6028/NIST.CSWP.01162020pt> Acesso em: 04/03/2024

REALE, Miguel. Filosofia do Direito. 11ª ed. São Paulo: Saraiva, 1986.

SÃO PAULO (Cidade). Decreto Municipal 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 Geral de Proteção de Dados Pessoais (LGPD) - no âmbito da Administração Municipal direta e indireta. São Paulo, Diário Oficial da Cidade de São Paulo, 15 de setembro de 2020. Disponível em: <https://legislacao.prefeitura.sp.gov.br/leis/decreto-59767-de-15-de-setembro-de-2020>. Acesso em: 29/10/2024.

SÃO PAULO (Cidade). Guia Orientativo sobre a Privacidade e a Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo, versão 01, 2023. Disponível em: https://www.prefeitura.sp.gov.br/cidade/secretarias/upload/controladoria_geral/GuiaOrientativosobreaPrivacidadeeaProtecaodeDadosPessoaisparaaAdministracaoPublicadoMunicipiodeSaoPaulo_publicacao_26_01_2023.pdf Acesso em: 21/03/2024

SÃO PAULO (Cidade). Guia Orientativo sobre a Instrução Normativa CGM/SP nº 01/2022 para a Administração Pública do Município de São Paulo, versão 01, 2023. Disponível em: < https://www.prefeitura.sp.gov.br/cidade/secretarias/upload/controladoria_geral/GuiaOrientativosobreaInstrucaoNormativaCGM-SPn%C2%BA01-2022paraaAdministracaoPublicadoMunicipiodeSaoPaulo_publicacao_26_01_2023.pdf> Acesso em: 21/03/2024

SÃO PAULO (Cidade). Instrução Normativa CGM/SP 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. São Paulo, Diário Oficial da Cidade, 22 de julho de 2022. Disponível em: <https://legislacao.prefeitura.sp.gov.br/leis/instrucao-normativa-controladoria-geral-do-municipio-cgm-1-de-21-de-julho-de-2022>. Acesso em: 29/10/2024.

SÃO PAULO (Cidade). 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. São Paulo, Diário Oficial da Cidade, 27 de dezembro de 2024. Disponível em:

<https://legislacao.prefeitura.sp.gov.br/leis/instrucao-normativa-controladoria-geral-do-municipio-cgm-2-de-23-de-dezembro-de-2024>. Acesso em: 30/12/2024

SÃO PAULO (Cidade). Manual de Gestão de Riscos 2023. Versão 01. 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: 09/04/2025

7. Anexo I - Identificação de riscos

O texto a seguir foi retirado em sua integralidade do "*Guia Orientativo sobre a Privacidade e a Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo, versão 01, 2023*".

"E como identificar os riscos que tragam perigo ou inconveniente no que se refere à segurança da informação, à privacidade e à proteção de dados pessoais?"

Nos termos previstos pela ABNT NBR ISO nº 31000:2018[1], na etapa de "*identificação de riscos*", os seguintes "*fatores"* devem ser considerados:

(i) *"Fontes tangíveis e intangíveis de risco"*: as "*fontes tangíveis*" são fontes palpáveis, físicas, como portões, catracas, cadeados, "*hardware"* e pessoas, enquanto as "*fontes intangíveis*" são fontes que não são alcançáveis pelo tato, como processos e tecnologias. Nesse sentido, imagine a hipótese de um portão ou catraca para impedir o acesso de pessoas não autorizadas a um determinado ambiente que contenha informações, porém o portão não está trancado ou a catraca está liberada. Trata-se, neste caso, de "*fontes tangíveis*". Ou, ainda, que a organização tenha adquirido certa tecnologia para proteger informações que estão armazenadas em um servidor, porém a tecnologia não foi configurada corretamente, por não ter havido a implementação de processos de verificação, ou mesmo porque os profissionais não foram treinados com o intuito da obtenção do máximo grau de usabilidade da tecnologia. Trata-se, neste caso, de "*fontes intangíveis*";

(ii) "*Causas"* e *"eventos":* as "*causas"* ocasionam determinados "*eventos*", que, por sua vez, podem gerar um perigo e/ou um inconveniente. É neste contexto que há a importância da realização de um mapeamento dos "*eventos*" que geram "*riscos*" efetivos ou potenciais a um processo, assim

[1] Item 6.4.2, "identificação de riscos", da norma ABNT NBR ISO nº 31000:2018.

como a importância do conhecimento de suas "*causas*". Nesse sentido, por exemplo, na hipótese de João ser responsável por uma catraca, necessitar se ausentar a fim de ir ao banheiro e decidir deixar a catraca liberada, no intuito de não impedir a entrada de algum funcionário, tem-se como "*evento*" a liberação da catraca, que possui como "*causa*", em seu turno, a ausência de designação de outro funcionário que substitua João em suas tarefas;

(iii) "*Ameaças*" e "*oportunidades*": uma *"ameaça"* é um "*evento*" que tem o potencial de comprometer "*ativos*", como as "*fatores temporais*", indicados pela ABNT NBR ISO nº 31000:2018. As "*oportunidades*", em seu turno, podem ser definidas como um hiato ("*gap*") entre um contexto presente e um contexto futuro em que é possível visualizar alguma vantagem;

(iv) "*Vulnerabilidades"* e *"capacidades"*: a "*vulnerabilidade"* representa uma fraqueza que pode ser explorada com consequências negativas, ou seja, é um ponto fraco existente, por exemplo, em um recurso tecnológico ou mesmo em um recurso humano, como as "*limitações de conhecimento e de confiabilidade da informação"* e os "*vieses, hipóteses e crenças dos envolvidos*", descritas pela ABNT NBR ISO nº 31000:2018. A "*capacidade*", por sua vez, é a aptidão para a execução de uma determinada ação. Neste contexto, é a aptidão em proteger a privacidade e os dados pessoais; e

(v) *"Mudança nos contextos externos e internos":* o "*contexto externo*" diz respeito ao contexto em que uma determinada organização existe e atua, podendo estar relacionado, por exemplo, aos fatores sociais, culturais, políticos, jurídicos, tecnológicos, econômicos e ambientais que afetam os processos da organização. Um exemplo de "*mudança de contexto externo*" que afetou a todas as organizações é a própria LGPD, que alterou o trato de todos com a privacidade e com os dados pessoais. O "*contexto interno*", por sua vez, diz respeito ao contexto existente no interior da organização, como, entre outros, os elementos relacionados a sua estrutura e a sua cultura organizacional, além de seus recursos humanos, físicos, tecnológicos e

informacionais. Nesse sentido, as "*mudanças*" nesses contextos podem ser "*causas*" de "*eventos*" que venham a gerar um risco efetivo ou potencial a um processo; e

(vi) "*Natureza e valor dos ativos*": um "*ativo*" é algo que possui valor para a organização e que, portanto, requer proteção. Identificar a natureza e o valor de determinado ativo significa classificá-lo a partir de um contexto pré-determinado ("*natureza*") e também classificá-lo a partir da valoração pré-determinada de um ativo para a organização ("*valor*").

É importante ressaltar, como o próprio termo anglófono "*likelihood"* indica, que não há como se dizer sobre um "*risco zero*", uma vez que sempre haverá riscos em qualquer ambiente. A função da gestão de riscos aplicada à segurança da informação é minimizar a probabilidade de ocorrência de eventos danosos – quer para a organização, quer para o usuário. Essa mitigação é possível com a alocação dos recursos necessários à organização – o que inclui, por exemplo, os recursos humanos, com as suas competências e experiências, assim como por boas práticas aplicadas aos processos, aos métodos e as ferramentas a serem empregadas.

Nesse sentido, as seguintes "*etapas"* podem ser aplicadas no processo de "*identificação de riscos*":

(i) Identificação dos "*ativos*": como mencionado, um "*ativo*" é algo que possui valor para a organização e que, portanto, requer proteção. No presente contexto, os "*ativos*" são as "*informações*" havidas pela Administração Pública do Município, que necessitam de proteção. As informações possuem valor intrínseco, ou seja, não se resumem em sua representação em dados, enquanto representados pela linguagem. Assim, as ideias e os conceitos contidos nas informações são "*formas intangíveis*" do valor havido nas informações. A identificação das "*informações*" requer, nesse sentido, um "*mapeamento de processos*", como explicitado anteriormente, a fim de que haja a identificação das "*informações*" existentes nos processos que afetam a privacidade e que contenham dados pessoais;

(ii) Identificação das "*ameaças*": a identificação das "*ameaças*" pode ser realizada por uma análise sobre os "*eventos*" anteriores e sobre os processos realizados pela organização. Essas "*ameaças*" podem ser de natureza humana ou de ordem natural e se classificam de acordo com a sua natureza acidental ou intencional. As "*ameaças*" podem resultar na modificação, na perda ou no furto de "*informações*" e até mesmo na paralisação dos serviços que estão sendo executados;

(iii) Identificação das "*vulnerabilidades*": a identificação das "*vulnerabilidades*" depende da compreensão sobre as "*ameaças*" que afetam cada área da organização, como o uso não controlado de "*softwares"* e o uso de conexões de rede desprotegidas. Como já mencionado, a "*vulnerabilidade*" representa uma fraqueza que pode ser explorada e que possua "*consequências*" negativas, ou seja, é um ponto fraco existente em um processo de uma organização;

(iv) Identificação dos "*controles*" já existentes: a identificação dos "*controles*" existentes consiste na verificação sobre quais medidas estão sendo adotadas no tratamento dos "*ativos*" de modo a manter e/ou modificar o "*risco*". Concomitantemente à identificação dos "*controles*" existentes, é importante que a verificação de sua eficácia e de sua eficiência sejam realizadas, uma vez que um "*controle*" ineficaz ou ineficiente pode ser causa de "*vulnerabilidades*". Ademais, poderá ser preciso, como se verá, adiante, que "*controles*" suplementares sejam aplicados, caso os "*controles*" iniciais falhem ou sejam insuficientes; e

(v) Identificação das *"consequências*": uma "*consequência*" é o resultado de um "*evento*". As "*consequências*" podem ser negativas, positivas, ou indiferentes ao objetivo de proteção do "*ativo*" considerado – neste caso, as "*informações*". Uma "*consequência*" pode ser, por exemplo, a perda da eficácia e da efetividade da proteção. Assim, a identificação das "*consequências*" visa a apresentar os cenários decorrentes de um "*evento*" que resulte na ocorrência de um "*risco*", isto de modo a considerar, por exemplo, os danos à privacidade e à proteção de

dados pessoais e os eventuais reparos necessários ao retorno da prestação de um serviço, em caso da ocorrência do "*evento*".

Apresentados os principais "*fatores*" e as "*principais etapas*" a uma "*identificação de riscos*", exemplifica-se, a seguir, quadro de "*ameaças*" e de "*vulnerabilidades*" que podem estar presentes nos recursos humanos, físicos, tecnológicos e informacionais de uma organização:

Tabela I – Exemplos de ameaças e de vulnerabilidades aos recursos humanos

Ameaça	**Vulnerabilidade**
Indisponibilidade de recursos humanos	Ausência de recursos humanos
Erro durante o uso	Treinamento insuficiente
Destruição de equipamentos ou mídia	Procedimento de recrutamento inadequado

Tabela II – Exemplos de ameaças e vulnerabilidades aos recursos físicos, tecnológicos e informacionais

Ameaça	**Vulnerabilidade**
Inundação	Localização em área suscetível à inundação
Interrupção do suprimento de energia	Fornecimento de energia instável
Destruição de equipamento ou mídia	Uso inadequado
Erro durante o uso	Inexistência de política de uso de correspondência eletrônica
Repúdio de ações	Atribuição inadequada das responsabilidades pela segurança da informação
Furto de equipamentos	Inexistência de controle sobre ativos fora das dependências da organização
Furto de mídia ou documentos	Armazenamento não protegido
Destruição de equipamento ou mídia	Falta de uma rotina de substituição periódica
Poeira, corrosão e congelamento	Sensibilidade à umidade e sujeira
Erro durante o uso de *software*	Datas incorretas
Abuso de direitos	Atribuição errônea de direitos de acesso
Forjamento de direitos	Gestão de senhas incorreto

8. Anexo II - Exemplos de riscos de privacidade

O texto a seguir foi retirado em sua integralidade do "*Guia Orientativo sobre a Instrução Normativa CGM/SP nº 01/2022 para a Administração Pública do Município de São Paulo, versão 01, 2023*".

Tabela II – Exemplos de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais

Identificação	Risco	Escopo
1	Acesso não autorizado	Acesso indevido (permissão indevida) a um ambiente físico ou lógico.
2	Modificação não autorizada	Usuário sem permissão de alteração para um determinado registro realiza modificação não autorizada.
3	Perda	Perdas provocadas tanto por ações intencionais de usuários oriundas de uma exclusão indevida ou devida e não comunicada, quanto por ações não intencionais, como falhas em sistemas e sobrescrita de dados.
4	Roubo	Dados roubados nas dependências internas do controlador/operador, como falhas nos controles de segurança dos sistemas, a exemplo da ausência ou fraca criptografia e falha de sistema que permita escalação de privilégio.
5	Remoção não autorizada	Usuário sem permissão para retirar ou copiar dados pessoais para outro local.
6	Coleta excessiva	Coleta de dados pessoais em quantidade superior ao necessário à finalidade da atividade a qual terá o tratamento de dados pessoais.
7	Informação insuficiente sobre a finalidade do tratamento	O tratamento de dados pessoais deve atender a uma finalidade específica a ser informada de forma transparente ao titular de dados pessoais.
8	Tratamento sem consentimento do titular de dados pessoais na hipótese em que o tratamento não esteja previsto em normas aplicáveis	Controlador de dados pessoais não obtém o consentimento do titular de dados pessoais para realizar um tratamento de dados sem norma que lhe diga respeito.
9	Falha em considerar os direitos do titular de dados pessoais	Falha na garantia de atendimento dos direitos do titular, conforme descritos, sobretudo, entre os arts. 9º e 17 a 23 da LGPD.
10	Compartilhar dados pessoais com terceiros sem o consentimento do titular na hipótese em que o consentimento esteja previsto em normas aplicáveis	Organização compartilha os dados pessoais sem hipótese de tratamento de dados que lhe autoriza.

11	Retenção prolongada de dados pessoais sem necessidade	O término da prestação de um serviço ou do prazo da retenção dos dados pessoais para fins legais deve culminar com a exclusão e/ou descarte seguro dos dados pessoais.
12	Associação indevida, direta ou indireta, de dados pessoais ao titular	A realização de todo tratamento de dados pessoais deve estar em conformidade com as normas aplicáveis. Qualquer tratamento que não atenda esse requisito pode produzir dados pessoais e informações pessoais com associações indevidas.
13	Erro de processamento	Dados de entrada que não são corretamente validados e operações de tratamento automatizadas de sistema que alteram de maneira indevida a composição do dado armazenado, a exemplo de execução de *script* de banco de dados que atualiza dado pessoal com dado equivocado e ausência de validação dos dados de entrada.
14	Reidentificação de dados pseudonimizados	Dados pessoais podem ser reidentificados por cruzamento de dados pessoais.
15	Exposição a vulnerabilidades diversas	Existência de vulnerabilidade que, uma vez explorada, pode gerar outras vulnerabilidades ou mesmo outros riscos

9. Anexo III – Tratamento de riscos

O texto a seguir foi retirado em sua integralidade do "*Guia Orientativo sobre a Privacidade e a Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo, versão 01, 2023*".

Conforme a norma ABNT NBR ISO/IEC nº 27002:2022, um "*controle*" é uma medida apta a manter ou modificar um risco[2]. Assim, um "*controle*" pode reduzir ou eliminar a probabilidade e/ou o impacto de um risco identificado, analisado e avaliado.

Nesse sentido, pode um "*controle*" dizer respeito a todo o contexto de incidência da privacidade e da proteção de dados pessoais no âmbito da organização, ou mesmo ser aplicado a contextos específicos de incidência, a partir dos contextos internos e externos que influenciam nos distintos processos da organização.

Os "*controles*" devem estar todos em conformidade com os "*princípios*"[3] que devem orientar toda a organização diante da privacidade e da proteção de dados pessoais. Por "*princípios*", é possível entender as "*verdades ou juízos fundamentais, que servem de alicerce ou de garantia de certeza a um conjunto de juízos, ordenados em um sistema de conceitos relativos à dada porção da realidade*"[4].

Nesse sentido, a norma ABNT NBR ISO/IEC nº 29100:2020 lhes dispôs do seguinte modo:

(i) consentimento e escolha: o "*consentimento*" é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais, enquanto a "*escolha*" é o momento prévio em que o titular age em direção ao seu consentimento. No âmbito da LGPD, está especialmente relacionado ao seu art. 7º, inc. I, e ao seu art. 11, inc. I, que dispõem, respectivamente, das hipóteses de tratamento de dados pessoais e de dados pessoais sensíveis pelo consentimento;

[2] Item 0.3, "controles", da norma ABNT NBR ISO/IEC nº 27002:2022.
[3] Item 5.1, "visão geral dos princípios de privacidade", da norma ABNT NBR ISO/IEC nº 29100:2020.
[4] REALE, Miguel. Filosofia do Direito. 11ª ed. São Paulo: Saraiva, 1986, p 60.

(ii) legitimidade e especificação de objetivo: a "*legitimidade*" consiste na competência legal ou contratual para o tratamento de dados pessoais, enquanto a "*especificação do objetivo"* trata-se da determinação da finalidade do tratamento, inclusive ao titular. No âmbito da LGPD, está especificamente relacionado ao seu art. 6º, inc. I, relativo ao princípio da finalidade;

(iii) limitação da coleta: a "*limitação da coleta*" dispõe da necessidade da realização de um tratamento sempre pautado em propósitos legítimos, específicos, explícitos e informados ao titular, sem a possibilidade de tratamento posterior de forma incompatível com esses propósitos. No âmbito da LGPD, está também especificamente relacionado ao seu art. 6º, inc. I, relativo ao princípio da finalidade;

(iv) minimização de dados pessoais: a "*minimização de dados pessoais*", apesar de relacionado ao princípio da limitação da coleta, diz respeito à limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados. No âmbito da LGPD, está especificamente relacionado ao seu art. 6º, inc. III, relativo ao princípio da necessidade;

(v) limitação do uso, da retenção e da divulgação: a "*limitação do uso, da retenção e da divulgação*", estreitamente relacionada ao princípio da "*limitação da coleta*", refere-se, pois, também à necessidade da realização de um tratamento sempre pautado em propósitos legítimos, específicos, explícitos e informados ao titular, sem a possibilidade de tratamento posterior de forma incompatível com esses propósitos. No mesmo sentido, no âmbito da LGPD, está também especificamente relacionado ao seu art. 6º, inc. I, relativo ao princípio da finalidade;

(vi) precisão e qualidade: a "*precisão e qualidade*" diz respeito à necessidade da garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento. No âmbito da LGPD, está relacionado ao seu art. 6º, inc. V, relativo ao princípio da qualidade dos dados;

(vii) abertura, transparência e notificação: a "*abertura, transparência e notificação*" traz a ideia da necessidade da garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento. No âmbito da LGPD, está relacionado ao seu art. 6º, inc. VI, relativo ao princípio da transparência;

(viii) participação individual e acesso: a "*participação individual e acesso*" diz respeito à necessidade da garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais. No âmbito da LGPD, está relacionado ao seu art. 6º, inc. IV, relativo ao princípio do livre acesso;

(ix) responsabilização: a "*responsabilização*" traz a necessidade da demonstração, pelos agentes de tratamento, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas relativas à segurança da informação, à privacidade e à proteção de dados pessoais e, inclusive, da eficácia dessas medidas. No âmbito da LGPD, está relacionado ao seu art. 6º, inc. X, relativo ao princípio da responsabilização e prestação de contas;

(x) segurança da informação: a "*segurança da informação*" é aqui trazida com a ideia da utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. No âmbito da LGPD, está relacionado ao seu art. 6º, inc. VII, relativo ao princípio da segurança;

(xi) *compliance* com a privacidade: o "*compliance com a privacidade*" indica, de modo geral, a necessidade da conformidade e da demonstração da conformidade, pelo agente de tratamento, ao sistema normativo de salvaguarda à privacidade e à proteção de dados pessoais vigente. No âmbito da LGPD, para além dos princípios supracitados, é possível a abrangência, neste princípio da norma ABNT NBR ISO/IEC nº 29100:2020, de todos os demais – dos princípios da adequação, da

prevenção e da não discriminação, respectivamente presentes no art. 6º, incs. II, VIII e IX.

10. Apêndice I – Análise SWOT (Manual de Gestão de Riscos da CGM)

O Manual de Gestão de Riscos da CGM sugere que a gestão de riscos deve se iniciar com o estudo do contexto do órgão. Para isso, propõe a utilização da ferramenta da Análise SWOT (*Strengths*: Forças, *Weaknesses*: Fraquezas, *Opportunities*: Oportunidades, *Threats*: Ameaças). Trata-se de uma ferramenta de gestão que auxilia no entendimento do cenário em que o órgão se encontra, facilitando a tomada de decisões estratégicas. Isso é importante para personalizar a gestão de riscos ao contexto de cada órgão.

Figura 08: Análise SWOT

Fonte: Manual de Gestão de Riscos da CGM 2023

A utilização da ferramenta facilita o estudo dos ambientes interno e externo do órgão, fornecendo informações importantes para a elaboração de seu planejamento estratégico. Isso permite avaliar cenários e embasar a tomada de decisões, inclusive a de priorização de processos-chave do órgão.

Nesse sentido, o Manual de Gestão de Riscos da CGM também aponta a necessidade do mapeamento dos processos. O manual sugere que "*para aumentar a eficiência e efetividade da gestão de riscos, é essencial* ***selecionar os processos-chave*** *com base nas atividades operacionais, táticas e estratégicas*" (grifo nosso). Conforme a evolução da maturidade do órgão, o manual recomenda expandir o escopo do mapeamento aos demais processos não prioritários. O objetivo do mapeamento é também de retratar o contexto do órgão.

Dessa forma, observa-se que a priorização dos processos pode ser feita com base no planejamento estratégico do órgão, utilizando-se de ferramentas de gestão que forneçam uma visão sistêmica sobre os seus processos mais relevantes.

11. Apêndice II – Impacto no resultado organizacional (Metodologia de Governança de Processos da ANPD)

A Metodologia de Governança de Processos da ANPD apresentou critérios próprios para a priorização de processos para análise detalhada (no caso, para a realização de modelagem de processos – BPM – *Business Process Modeling*). Nesse sentido, para fins de exemplificação, citam-se os critérios utilizados por essa metodologia, que também podem ser utilizados como referência:

- **Grau de relacionamento com os macroprocessos**: avalia se o processo tem impacto direto nos macroprocessos finalísticos, gerenciais e de suporte do órgão;

- **Alinhamento estratégico e resultados institucionais**: avalia se o processo tem relação com o planejamento estratégico, com políticas públicas ou com metas do Plano Plurianual do órgão;

- **Objeto de recomendação ou determinação de órgão de controle**: avalia se o processo é objeto de recomendação do Tribunal de Contas de União, da Controladoria Geral da União ou do Ministério Público;

- **Quantidade de atores do processo**: avalia a quantidade de atores envolvidos no processo; e

- **Impacto institucional**: avalia o impacto institucional do processo, sob a perspectiva: da demanda processual anual; da visibilidade e do impacto para o cidadão/ cliente; da informalidade e fragmentariedade do fluxo processual; do alto grau de conflitos de responsabilidade e de competências entre diferentes setores; da disponibilidade de tempo dos executores e gestores para a transformação do processo; e do alto risco de impacto institucional junto à sociedade e ao governo.

Figura 09: Critérios de priorização de processos da ANPD

ANPD — CRITÉRIOS DE PRIORIZAÇÃO DE PROCESSOS PARA INICIATIVA BPM

CRITÉRIOS DE PRIORIZAÇÃO	PONTUAÇÃO (para as marcações SIM)
Grau de relacionamento com os Macroprocessos	**Quantidade de pontos - 21**
Impacta diretamente os macroprocessos finalísticos	10
Impacta diretamente os macroprocessos gerenciais	7
Impacta diretamente os macroprocessos de suporte	4
Alinhamento estratégico e resultados institucionais	**Quantidade de pontos - 20**
Relacionado ao Planejamento Estratégico da ANPD	12
Relacionado à Política Pública da ANPD	5
Relacionado à meta do Plano Plurianual - PPA da ANPD	3
Objeto de recomendação/determinação de órgão de controle	**Quantidade de pontos - 24**
Relacionada à recomendação constante em Acórdão do TCU	8
Relacionada à recomendação exarada pela Controladoria Geral da União - CGU	8
Relacionada à recomendação exarada por Ministério Público	8
Quantidade de atores do processo	**Quantidade de pontos - 10**
6 (seis) ou mais atores	5
4 (quatro) a 5 (cinco) atores	3
até 3 (três) atores	2
Impacto institucional	**Quantidade de pontos - 25**
Alta demanda processual anual	5
Alta visibilidade e impacto para o cidadão/cliente	5
Fluxos processuais fragmentados, informais (baixo nível de normatização e manualização) ou com baixo nível de uniformidade e padronização de atos e procedimentos	2
Alto grau de conflitos de responsabilidades e competências entre diferentes setores	3
Disponibilidade de tempo dos executores e gestores para a transformação do processo	5
Alto risco de impacto institucional junto à sociedade e ao governo	5
PONTUAÇÃO TOTAL	100

Fonte: Metodologia de Governança de Processos da ANPD

Através da priorização dos processos, a ANPD busca identificar aqueles que representam maiores impactos no resultado organizacional, ao mesmo tempo em que pondera a complexidade, a oportunidade e a conveniência de se priorizar cada processo. A lista de processos priorizados deve ser submetida para deliberação superior, que poderá realizar as alterações pertinentes, para que se determine então a lista final de processos que serão modelados.

PREFEITURA DE
SÃO PAULO