MANUAL

Política de Gestão de Riscos no contexto da privacidade para a Administração Pública do Município de São Paulo (Controle 19)

Portaria CGM/SP nº 27/2026

Programa de Governança em Privacidade e 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

Marcos Augusto Carboni

Equipe da Coordenadoria de Proteção de Dados Pessoais

Coordenador

Edson Joaquim Raimundo de Araujo Júnior

Elaboração

Fábio Fernandes Libonati

João Francisco Resende

Thiago Ryuichi Hirata

Revisão

Alana Leite Catuzzati

Arte e Diagramação

Marília Miquelin de Oliveira

Versão 01

Junho de 2026

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	06/2026

Sumário

1. Apresentação

Este manual foi elaborado com o objetivo de auxiliar os agentes públicos responsáveis por implementar os controles previstos na Portaria CGM nº 27/2026, que regulamenta o modelo de Programa de Governança em Privacidade e Proteção de Dados Pessoais da Administração Pública Municipal (PGPP). O foco deste manual é a implementação do "*Controle 19 – Política de Gestão de Riscos no contexto da privacidade*".

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. Conceitos iniciais

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 Administração Municipal na aplicação dos conceitos às suas diferentes realidades.

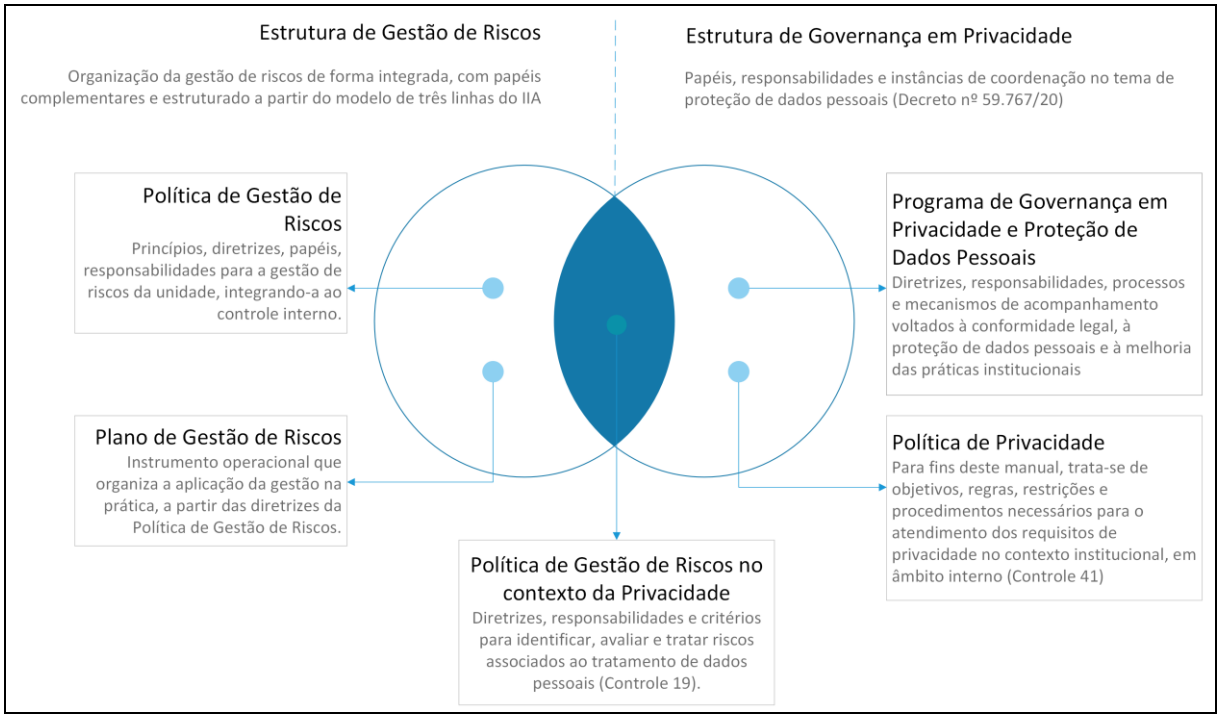
Inicialmente, faz-se necessário delimitar o entendimento sobre os principais conceitos adotados neste manual, em especial aqueles relacionados às estruturas de Governança da Privacidade e de Gestão de Riscos na Administração Pública Municipal. Nesse sentido, serão explicados brevemente as expressões:

- Política de Gestão de Riscos;
- Plano de Gestão de Riscos;
- Política de Privacidade; e
- Programa de Governança em Privacidade e Proteção de Dados Pessoais.

A definição prévia desses conceitos é fundamental para assegurar uniformidade de entendimento na aplicação das diretrizes estabelecidas no âmbito da Administração Pública Municipal. A partir desse enquadramento conceitual, torna-se possível construir o entendimento específico da Política de Gestão de Riscos no contexto da privacidade.

A Figura 1 ilustra, de maneira geral, como os principais conceitos se encontram relacionados no contexto da gestão de riscos e no contexto da privacidade, ambos em âmbito municipal.

Figura 1: Gestão de Riscos no contexto da privacidade



Fonte: CGM/CPD[1]

2.1. Estrutura de Governança da Privacidade na Administração Pública Municipal

A estrutura de Governança da Privacidade na Administração Pública Municipal é estabelecida pelo Decreto Municipal nº 59.767/2020, que define papéis, responsabilidades e instâncias de coordenação no âmbito do Município de São Paulo. Nos termos do Decreto, cada órgão e entidade deve designar encarregado pelo tratamento de dados pessoais, que atuará como canal de comunicação entre o órgão ou a entidade, os titulares de dados pessoais e a Agência Nacional de Proteção de Dados (ANPD), além de apoiar e orientar internamente sobre o tema.

Essa estrutura é operacionalizada e monitorada por meio do Programa de Governança em Privacidade e Proteção de Dados Pessoais (PGPP), instituído pela Portaria CGM nº 27/2026, que estabelece controles e mecanismos de acompanhamento das práticas de privacidade adotadas pelos órgãos municipais, promovendo a melhoria contínua da governança em privacidade.

[1] Para mais informações sobre o modelo de três linhas do IIA consulte o tópico "2.2. Estrutura de Gestão de Riscos na Administração Pública Municipal" deste Manual

Para mais informações, consulte as referências elencadas aqui[2].

2.1.1. Programa de Governança em Privacidade e Proteção de Dados Pessoais

O Programa de Governança em Privacidade e Proteção de Dados Pessoais (PGPP) é o instrumento mais amplo da estrutura de proteção de dados pessoais do órgão ou entidade. Ele reúne diretrizes, responsabilidades, processos e mecanismos de acompanhamento voltados à conformidade legal, à proteção dos dados pessoais e à melhoria contínua das práticas institucionais. No âmbito da Administração Pública Municipal de São Paulo, ela corresponde ao conjunto dos 70 controles do Diagnóstico de Maturidade.

Nesse contexto, tanto a Política de Privacidade quanto a Política e o Plano de Gestão de Riscos em Privacidade constituem elementos do Programa, representados pelos Controles 41, 19 e 18, respectivamente. A Política de Privacidade estabelece diretrizes específicas sobre o tratamento de dados pessoais no âmbito interno à unidade, enquanto a Política e o Plano de Gestão de Riscos em Privacidade permitem identificar, analisar, avaliar e tratar os riscos associados às atividades de tratamento de dados pessoais.

Uma particularidade da gestão de riscos em privacidade é que os seus resultados podem orientar e fundamentar a elaboração, a implementação e o aprimoramento do próprio Programa de Governança em Privacidade, ao indicar prioridades, necessidades de controle e ações de melhoria. Essa abordagem está alinhada às boas práticas descritas pelo National Institute of Standards and Technology (NIST), que integra a privacidade à gestão de riscos organizacionais como parte da governança institucional.

Para mais informações, consulte as referências elencadas aqui[3].

---

[2] Referências [1]:
[1] 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: 12/01/2026.
[1] SÃO PAULO (Cidade). Portaria CGM/SP nº 27, de 22 de Junho de 2026. Regulamenta o modelo de Programa de Governança em Privacidade e Proteção de Dados Pessoais da Administração Pública Municipal (PGPP), assim como o procedimento do Diagnóstico de Maturidade em Proteção de Dados Pessoais. Disponível em: <https://legislacao.prefeitura.sp.gov.br/portaria-controladoria-geral-do-municipio-cgm-27-de-22-de-junho-de-2026>. Acesso em: 23/06/2026.
[3] Referências [2]:

2.1.2. Política de Privacidade

A ABNT NBR ISO/IEC 29100:2024 esclarece que a expressão Política de Privacidade é utilizada na prática com diferentes significados, podendo referir-se tanto a políticas internas quanto a instrumentos voltados ao público externo.

No âmbito do PGPP, o conceito de Política de Privacidade adotado corresponde à política interna da unidade, direcionada aos seus colaboradores. Essa política reúne objetivos, regras, obrigações, restrições e procedimentos necessários para o atendimento dos requisitos de privacidade no contexto institucional. Nesse sentido, a Política de Privacidade interna é objeto do Controle 41.

Esse conceito difere da política externa, voltada ao público em geral, cuja finalidade é informar de forma clara e acessível sobre as operações de tratamento de dados pessoais realizadas pela unidade. No âmbito do PGPP, a política externa adota a denominação de Aviso de Privacidade, sendo objeto do Controle 12, já disciplinado em Manual próprio, seguindo-se as recomendações da ABNT NBR ISO/IEC 29184:2021.

Essa distinção está alinhada às orientações da ABNT NBR ISO/IEC 29100:2024, ao diferenciar instrumentos internos de governança daqueles voltados à transparência e à comunicação com os titulares de dados.

Para mais informações, consulte as referências elencadas aqui[4].

---

[2] SÃO PAULO (Cidade). Portaria CGM/SP nº 27, de 22 de Junho de 2026. Regulamenta o modelo de Programa de Governança em Privacidade e Proteção de Dados Pessoais da Administração Pública Municipal (PGPP), assim como o procedimento do Diagnóstico de Maturidade em Proteção de Dados Pessoais. Disponível em: <https://legislacao.prefeitura.sp.gov.br/portaria-controladoria-geral-do-municipio-cgm-27-de-22-de-junho-de-2026>. Acesso em: 23/06/2026.

[2] 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: 12/01/2026.

[4] Referências [3]:

[3] ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 29100:2024. Tecnologia da informação – Técnicas de segurança – Estrutura de privacidade. Rio de Janeiro: ABNT, 2024.

[3] ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 29184:2021. Tecnologia da informação – Avisos de privacidade on-line e consentimento. Rio de Janeiro: ABNT, 2021.

[3] SÃO PAULO (Cidade). Manual sobre Aviso de Privacidade e Cookies no contexto da Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo (Controle 12), Versão 1.0, 2025. Disponível

2.2. Estrutura de Gestão de Riscos na Administração Pública Municipal

A estrutura de Gestão de Riscos na Administração Pública Municipal se conecta ao sistema de controle interno, do qual a Controladoria Geral do Município (CGM) ocupa o papel de órgão central. Nesse sentido, destaca-se a Política de Gestão de Riscos da CGM, formalizada pela Portaria CGM nº 49/2023 e seu respectivo manual, que estabelecem uma estrutura baseada no Modelo de Três Linhas do IIA (Institute of Internal Auditors).

Esse modelo organiza a gestão de riscos de forma integrada, com papéis complementares, distinguindo: (i) quem executa e controla os processos (1ª linha), (ii) quem coordena e orienta a gestão de riscos e controles (2ª linha) e (iii) quem avalia, de forma independente, a efetividade do sistema (3ª linha), evitando sobreposições e lacunas de responsabilidade.

Nesse arranjo, o Comitê de Gestão de Riscos (alta administração) cumpre o papel de direcionamento e decisão: define objetivos, estabelece diretrizes, aprova critérios (como apetite a risco) e acompanha resultados. O Núcleo Especializado de Gestão de Riscos (2ª Linha) atua como instância de coordenação e suporte: aplica a metodologia, consolida informações, orienta e capacita as áreas, monitora a evolução dos riscos e acompanha planos de ação e controles. Já os Gestores dos Riscos (1ª Linha), nas áreas finalísticas e de apoio, são responsáveis por identificar e avaliar os riscos dos processos sob sua gestão e implementar as respostas, reportando periodicamente ao Núcleo e ajustando controles conforme necessário. Por fim, a CGM (3ª Linha) é responsável por avaliar de forma independente a efetividade do sistema de gestão de riscos e de controles internos.

em: < https://prefeitura.sp.gov.br/documents/d/controladoria_geral/manual-controle-12-v2-pdf >. Acesso em: 12/01/2026.

Figura 2: Estrutura de Gestão de Riscos da Administração Pública Municipal

Fonte: Manual de Gestão de Riscos da CGM

Para mais informações, consulte as referências elencadas aqui[5].

2.2.1. Política de Gestão de Riscos

A Política de Gestão de Riscos estabelece os princípios, diretrizes, papéis e responsabilidades para a gestão de riscos no órgão ou entidade, orientando sua aplicação de forma sistemática, estruturada e contínua, em integração com a governança e os controles internos, conforme as diretrizes da ABNT NBR ISO 31000.

Essa perspectiva também é reforçada pela Instrução Normativa Conjunta CGU/MPOG nº 01/2016, importante referência nacional sobre a gestão de riscos. Nesse sentido, o normativo determina a sistematização das práticas de gestão de riscos, controles internos e governança (Art. 1º), a observância do princípio de atuação sistemática, estruturada e oportuna, subordinada

[5] Referências [4]:
[4] SÃO PAULO (Cidade). Portaria Controladoria Geral do Município – CGM nº 49 de 27 de novembro de 2023. Institui a Política de Gestão de Riscos da Controladoria Geral do Município de São Paulo. Disponível em: <https://legislacao.prefeitura.sp.gov.br/leis/portaria-controladoria-geral-do-municipio-cgm-49-de-27-de-novembro-de-2023>. Acesso em: 12/01/2026.
[4] 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: 12/01/2026.
[4] THE INSTITUTE OF INTERNAL AUDITORS (IIA). Modelo das Três Linhas do IIA. Lake Mary, FL: The Institute of Internal Auditors, 2020. Disponível em: <https://iiabrasil.org.br/korbilload/upl/editorHTML/uploadDireto/20200758glob-th-editorHTML-00000013-20082020141130.pdf>. Acesso em: 16/01/2026.

ao interesse público (Art. 14, I), e a gestão integrada entre riscos e controles internos, com foco no cidadão e na sociedade (Art. 22).

Além disso, a IN Conjunta CGU/MPOG nº 01/2016 define Política de Gestão de Riscos como a "declaração das intenções e diretrizes gerais" da organização relacionadas à gestão de riscos (Art. 2º, XII). No mesmo normativo, a política é operacionalizada por responsabilidades e competências institucionais. Cabe ao gestor de risco assegurar que o risco seja gerenciado conforme a política e monitorá-lo ao longo do tempo, para manter níveis adequados de risco (Art. 20, § 2º, I e II). Por outro lado, compete ao Comitê de Governança, Riscos e Controles aprovar a política, diretrizes, metodologias e mecanismos de comunicação e institucionalização da gestão de riscos e dos controles internos (Art. 23, § 2º, VII).

Para mais informações, consulte as referências elencadas aqui[6].

2.2.2. Plano de Gestão de Riscos

O Plano de Gestão de Riscos é o instrumento operacional que organiza a aplicação da gestão de riscos na prática e deve estar alinhado à Política de Gestão de Riscos do órgão ou entidade, observando suas diretrizes, critérios e responsabilidades, conforme orienta a ABNT NBR ISO 31000:2018.

Sua execução é conduzida pela 1ª linha (Gestores dos Riscos), que realizam a identificação, análise, avaliação e tratamento dos riscos nos processos sob sua gestão, com coordenação e suporte da 2ª linha (Núcleo Especializado de Gestão de Riscos), responsável por orientar a metodologia, consolidar informações e acompanhar a implementação. As decisões de maior relevância, bem como a priorização e validação de critérios, são submetidas à instância de direção (Comitê de Gestão de Riscos), em linha com a abordagem de integração entre gestão

[6] Referências [5]:
[5] ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO nº 31000:2018. Gestão de riscos – Diretrizes. Rio de Janeiro: ABNT, 2018.
[5] BRASIL. Ministério do Planejamento, Orçamento e Gestão (MPOG) e Controladoria-Geral da União (CGU). Instrução Normativa Conjunta nº 1, de 10 de maio de 2016. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal. Brasília, DF, 10 mai. 2016. Diário Oficial da União, Seção 1, p. 14, 11 mai. 2016. Disponível em: <https://www.gov.br/mj/pt-br/acesso-a-informacao/governanca/Gestao-de-Riscos/biblioteca/Normativos/instrucao-normativa-conjunta-no-1-de-10-de-maio-de-2016-imprensa-nacional.pdf/view>. Acesso em: 15/01/2026

de riscos, controles internos e governança prevista pelo Modelo de Três Linhas do IIA e pela Instrução Normativa Conjunta CGU/MPOG nº 01/2016.

Na etapa de identificação, o plano orienta o levantamento dos eventos de risco vinculados aos objetivos e processos, incluindo causas e consequências. Na análise, define-se como estimar probabilidade e impacto e registrar o nível de risco (inerente, isto é, sem considerar eventuais controles aplicados para sua mitigação). Na avaliação, os riscos são comparados a critérios definidos pelo Comitê de Gestão de Riscos (por exemplo, níveis aceitáveis e prioridades), para selecionar aqueles que exigem resposta. Por fim, no tratamento, o plano consolida as respostas aprovadas (mitigar, evitar, compartilhar ou aceitar) e detalha controles e ações, com responsáveis, prazos, indicadores e forma de monitoramento, permitindo acompanhar a efetividade das medidas e atualizar periodicamente o mapa de riscos e os planos de ação.

Para mais informações, consulte as referências elencadas aqui[7].

2.3. Resumo: Política de Gestão de Riscos no contexto da privacidade

A Política de Gestão de Riscos no contexto da privacidade encontra fundamento na própria LGPD, especialmente no Art. 50, ao prever regras de boas práticas e de governança que incluam mecanismos internos de supervisão e de mitigação de riscos relacionados ao tratamento de dados pessoais. Em complemento, o Art. 50, § 2º, I, "d" indica que o programa de governança em privacidade pode estabelecer políticas e salvaguardas adequadas com base em um processo de avaliação sistemática de impactos e riscos à privacidade, considerando a natureza das operações e a probabilidade e gravidade de danos aos titulares.

Nesse sentido, a política tem como objetivo institucionalizar a gestão de riscos em privacidade na unidade, definindo diretrizes, responsabilidades e critérios para identificar, analisar, avaliar

[7] Referências [6]:
[6] ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO nº 31000:2018. Gestão de riscos – Diretrizes. Rio de Janeiro: ABNT, 2018.
[6] BRASIL. Ministério do Planejamento, Orçamento e Gestão (MPOG) e Controladoria-Geral da União (CGU). Instrução Normativa Conjunta nº 1, de 10 de maio de 2016. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal. Brasília, DF, 10 mai. 2016. Diário Oficial da União, Seção 1, p. 14, 11 mai. 2016. Disponível em: <https://www.gov.br/mj/pt-br/acesso-a-informacao/governanca/Gestao-de-Riscos/biblioteca/Normativos/instrucao-normativa-conjunta-no-1-de-10-de-maio-de-2016-imprensa-nacional.pdf/view>. Acesso em: 15/01/2026

e tratar riscos associados ao tratamento de dados pessoais. Sua principal peculiaridade é que a avaliação de riscos deve considerar não apenas efeitos para a organização (como conformidade e reputação), mas também os impactos sobre os titulares de dados pessoais e seus direitos, o que confere contornos próprios à análise e à priorização de medidas. Tais particularidades são apresentadas pela ABNT NBR ISO/IEC nº 27557:2023, que adapta a ABNT NBR ISO nº 31000:2018 para o contexto da privacidade.

Embora dialogue com outros instrumentos, a Política de Gestão de Riscos no contexto da privacidade não se confunde com eles. Ela não se confunde com a Política de Privacidade, que é voltada a regras e orientações internas, nem com o Programa de Governança em Privacidade, que é mais amplo e abrange a estrutura de governança, papéis, controles e mecanismos contínuos de acompanhamento.

Também não se confunde com a Política/Plano de Gestão de Riscos corporativos em geral, pois a gestão de riscos em privacidade é um caso particular dessa disciplina, aplicando seus métodos e princípios ao tratamento de dados pessoais, com foco específico nos riscos e impactos à privacidade. No âmbito do PGPP, a Política de Gestão de Riscos no contexto da privacidade é objeto do Controle 19, enquanto o Plano de Gestão de Riscos em Privacidade é tratado no Controle 18, o qual já possui manual publicado.

Apesar das diferenças, é importante que o tema seja tratado de forma integrada e sistematizada. No âmbito da União, o Framework de Privacidade e Segurança da Informação (PPSI 2.0), desenvolvido pela Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (MGI/SGD), é uma referência útil para compreender como estruturar a governança em privacidade e em segurança da informação. O guia enfatiza que a maturidade nesses temas depende da existência de um sistema institucional de gestão de riscos e de controles internos. Nesse sentido, recomenda que os processos de gestão de riscos de privacidade e de segurança da informação estejam alinhados ao modelo institucional do órgão, destacando que podem ser incorporados aos processos institucionais já existentes (medidas 0.13 e 0.17).

O presente manual apresenta, no Capítulo 3, resultados de pesquisa e exemplos observados em outros entes públicos, com alternativas de implementação desse instrumento no setor público.

Para mais informações, consulte as referências elencadas aqui[8].

[8] Referências [7]:

[7] 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.

[7] BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Guia do Framework de Privacidade e Segurança da Informação – Programa de Privacidade e Segurança da Informação, versão 1.0, 2025. Disponível em: <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi-2.0/arquivos/guiafwppsi2-0-v1-0-22nov2025.pdf> Acesso em: 12/01/2026.

[7] SÃO PAULO (Cidade). Manual sobre Gestão de Riscos em Privacidade para a Administração Pública do Município de São Paulo (Controle 18), Versão 1.0, 2025. Disponível em: <https://prefeitura.sp.gov.br/documents/d/controladoria_geral/manual-controle-18-_v3-pdf> Acesso em: 12/01/2026.

3. Implementação da Política de Gestão de Riscos no contexto da privacidade

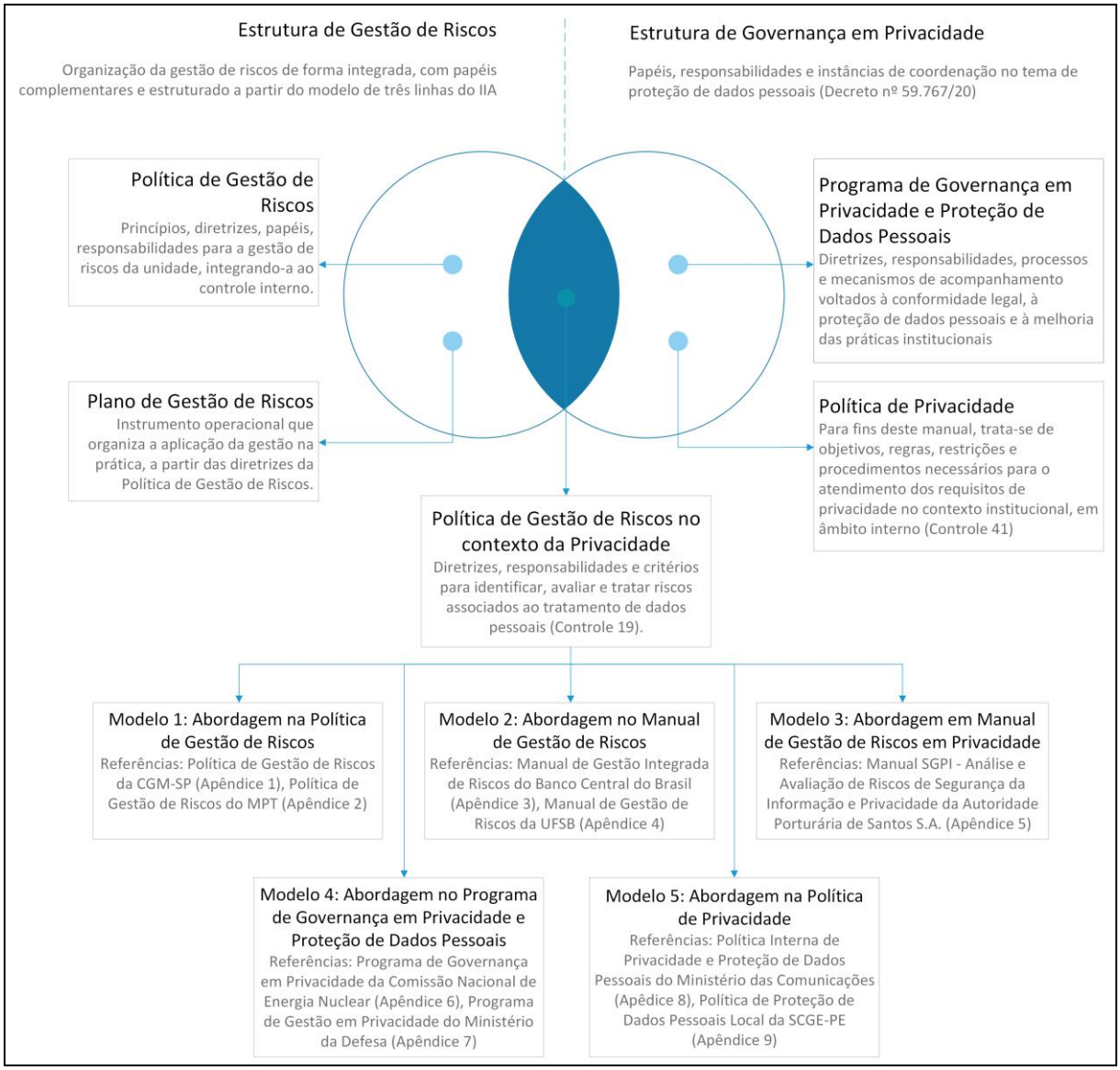
O presente capítulo apresenta exemplos de outros entes públicos e as diferentes formas pelas quais implementaram a Política de Gestão de Riscos no contexto da privacidade. Ao final, será apresentada uma breve análise do conteúdo das políticas examinadas, bem como sugestões de competências e responsabilidades para sua elaboração, formalização e aprovação.

3.1. Exemplos de implementação em outros entes públicos

Este manual realizou pesquisa em normas técnicas e em boas práticas de outros entes públicos para identificar diferentes formas de implementar a Política de Gestão de Riscos no contexto da privacidade. Observou-se que, na prática, a gestão de riscos em privacidade pode ser tratada de maneiras distintas, ora como parte da gestão de riscos corporativa, ora como conteúdo detalhado em instrumentos específicos de privacidade, mantendo-se, em qualquer caso, a necessidade de **sistematização e integração** com o modelo geral de gestão de riscos da organização.

Em síntese, os casos analisados indicam que o tema da gestão de riscos em privacidade pode constar diretamente na Política de Gestão de Riscos, ou ser incorporado por meio do Manual de Gestão de Riscos, seja ele geral (com seção específica de privacidade) ou específico para riscos em privacidade. Quando a gestão de riscos em privacidade é tratada principalmente no âmbito da governança de privacidade (por meio do Programa de Governança ou da Política de Privacidade) é fundamental que esses instrumentos estejam alinhados à política institucional de gestão de riscos e conectados aos seus mecanismos de registro, priorização, monitoramento e reporte. A Figura 3 apresenta as diferentes abordagens para implementação da Política de Gestão de Riscos no contexto da Privacidade.

Figura 3: Abordagens para implementação da Política de Gestão de Riscos no contexto da Privacidade



Fonte: CGM/CPD

Independentemente da forma e abordagem utilizada, é importante destacar o conteúdo da Política de Gestão de Riscos no contexto da privacidade, que deve conter elementos mínimos, como a definição de princípios, objetivos, diretrizes, competências e responsabilidades, conforme descrito no item 3.2.

3.1.1. Modelo 1: Abordagem na Política de Gestão de Riscos

Nessa abordagem, a Política de Gestão de Riscos do órgão ou entidade já incorpora, de forma explícita, o tema da privacidade no seu escopo. Em geral, isso ocorre quando a política

reconhece a privacidade como uma categoria de risco relevante (ao lado de riscos operacionais, legais, tecnológicos etc.) e prevê, por exemplo, critérios próprios para avaliar impactos sobre titulares, responsabilidades envolvidas no tema e a necessidade de considerar dados pessoais nos processos e projetos.

Nesse sentido, destaca-se o art. 18 da IN Conjunta MPOG/CGU nº 01/2016, que sugere tipologias de riscos a serem consideradas. Observa-se que a norma, editada anteriormente à LGPD, não contempla explicitamente riscos à privacidade e à proteção de dados pessoais, embora admita a consideração de outras tipologias além daquelas expressamente elencadas. A vantagem é manter um único instrumento normativo, com visão integrada de riscos. Também ajuda explicitar como a privacidade se conecta a temas correlatos, como segurança da informação, gestão de terceiros e resposta a incidentes.

Pontos de atenção
É importante garantir que essa incorporação não fique restrita à redação da política, de forma genérica. Ela deve se refletir à prática da estrutura de gestão de riscos da unidade, evitando que riscos de privacidade sejam tratados de forma informal ou fora do ciclo corporativo. Recomenda-se o detalhamento das práticas em manual operacional.
Referências
• Apêndice 1: Política de Gestão de Riscos da Controladoria Geral do Município de São Paulo • Apêndice 2: Política de Gestão de Riscos do Ministério Público do Trabalho

3.1.2. Modelo 2: Abordagem no Manual de Gestão de Riscos

Nessa abordagem, a Política de Gestão de Riscos permanece corporativa e mais principiológica, sendo complementada por um manual que detalha sua aplicação, incluindo os riscos de privacidade. Normalmente, o manual apresenta orientações práticas para equipes, podendo detalhar as particularidades da avaliação dos impactos aos titulares de dados pessoais. A vantagem é dar operacionalidade sem inflar a política.

Pontos de atenção
Deve-se assegurar coerência entre a política e o manual (mesmos conceitos, critérios e fluxos) e evitar que o manual crie procedimentos que não se conectem ao ciclo corporativo (registro, priorização, reporte e monitoramento), principalmente no detalhamento da gestão dos riscos de privacidade.
Referências
• Apêndice 3: Manual de Gestão Integrada de Riscos do Banco Central do Brasil

- Apêndice 4: Manual de Gestão de Riscos da Universidade Federal do Sul da Bahia

3.1.3. Modelo 3: Abordagem em Manual de Gestão de Riscos em Privacidade

Nessa abordagem, a Política de Gestão de Riscos é corporativa e é complementada por um manual específico de gestão de riscos em privacidade, com orientações operacionais completas. Em geral, esse manual descreve o processo ponta a ponta aplicado ao tratamento de dados pessoais: como mapear processos e operações de tratamento, como identificar ameaças e vulnerabilidades, como avaliar impactos aos titulares, como selecionar controles e como acompanhar indicadores e planos de ação. Costuma trazer modelos prontos (matriz, registro de riscos, plano de tratamento, *checklists*), facilitando a aplicação por áreas com diferentes níveis de maturidade.

Pontos de atenção
Recomenda-se evitar que o tema fique isolado. O manual específico deve adotar critérios compatíveis com os corporativos e prever como seus resultados serão registrados, reportados e monitorados nas instâncias de gestão de riscos do órgão. Além disso, é importante definir a governança de atualização do manual (quem revisa, com que periodicidade, como incorporar lições aprendidas e incidentes) e como ele se conecta aos demais instrumentos do Programa de Governança em Privacidade.
Referências
• Apêndice 5: Manual SGPI – Análise e Avaliação de Riscos de Segurança da Informação e Privacidade da Autoridade Portuária de Santos S.A.

3.1.4. Modelo 4: Abordagem no Programa de Governança em Privacidade

Nessa abordagem, a Política de Gestão de Riscos é corporativa e, em paralelo, o Programa de Governança em Privacidade descreve como a gestão de riscos em privacidade será conduzida e monitorada. A vantagem é tratar os riscos de privacidade como parte estruturante do próprio Programa de Governança em Privacidade, podendo sinalizar prioridades, necessidades de controle e ações de melhoria. Isso se alinha ao disposto no item 2.1.1., no qual se explicou que a gestão de riscos de privacidade tem forte relação com a estruturação do Programa de Governança em Privacidade.

Pontos de atenção
É essencial evitar duplicidade de instâncias e critérios. O Programa de Governança deve articular o tema da privacidade, mas mantendo alinhamento com o processo corporativo de gestão de riscos (critérios de aceitação/apetite, escalonamento, reporte e monitoramento). Também convém deixar claro como a gestão de

riscos em privacidade se integra a comitês já existentes e como os resultados alimentam o mapa institucional de riscos e os planos corporativos de ação.
Referências
• Apêndice 6: Programa de Governança em Privacidade da Comissão Nacional de Energia Nuclear • Apêndice 7: Programa de Gestão em Privacidade do Ministério da Defesa

3.1.5. Modelo 5: Abordagem na Política de Privacidade

Nessa abordagem, a Política de Gestão de Riscos é corporativa, e, em paralelo, a Política de Privacidade (interna) passa a detalhar procedimentos e salvaguardas relacionados à gestão de riscos em privacidade. Na prática, esse documento pode trazer regras e rotinas internas para tratar riscos. Em alguns casos, também apresenta como a unidade realiza avaliações de risco/impacto e quando aciona instâncias responsáveis.

Pontos de atenção
É necessário garantir que os riscos e medidas definidos na Política de Privacidade sejam incorporados ao ciclo corporativo de gestão de riscos e que o detalhamento não gere fragmentação ou sobreposição com outros instrumentos (por exemplo, Aviso de Privacidade, políticas de segurança da informação e normas de contratação/terceiros). A Política de Privacidade deve manter seu foco principal (regras internas e orientação de conduta), sem substituir a metodologia e o acompanhamento próprios da gestão de riscos corporativa.
Referências
• Apêndice 8: Política Interna de Privacidade e Proteção de Dados Pessoais do Ministério das Comunicações • Apêndice 9: Política de Proteção de Dados Pessoais Local da Secretaria da Controladoria Geral do Estado de Pernambuco

3.2. Conteúdo da política de gestão de riscos no contexto da privacidade

O conteúdo de uma Política de Gestão de Riscos no contexto da privacidade deve deixar claro o que a organização pretende alcançar, como o processo de gestão de riscos será conduzido e quem é responsável por cada etapa. Como referência, a IN Conjunta MPOG/CGU nº 01/2016 apresenta requisitos mínimos para políticas de gestão de riscos em sentido geral. Contudo, seus elementos são plenamente aplicáveis à gestão de riscos em privacidade, por se tratar de um caso particular da gestão de riscos organizacionais, com foco nos riscos associados ao tratamento de dados pessoais.

Tabela 1: Conteúdo mínimo da Política de Gestão de Riscos em privacidade

Conteúdo mínimo da Política de Gestão de Riscos em privacidade	**Fundamento (IN Conjunta MPOG/CGU nº 01/2016)**
Princípios e objetivos organizacionais	Art. 17, I
Diretrizes sobre integração da gestão de riscos ao planejamento estratégico, processos e políticas do órgão	Art. 17, II, "a"
Diretrizes sobre como e com que periodicidade serão identificados, analisados/avaliados, tratados e monitorados os riscos	Art. 17, II, "b"
Diretrizes sobre como será medido o desempenho da gestão de riscos	Art. 17, II, "c"
Diretrizes sobre como serão integradas/articuladas as instâncias responsáveis pela gestão de riscos	Art. 17, II, "d"
Diretrizes sobre metodologia e ferramentas de apoio à gestão de riscos	Art. 17, II, "e"
Diretrizes sobre desenvolvimento e capacitação contínua dos agentes públicos em gestão de riscos	Art. 17, II, "f"
Competências e responsabilidades para a efetivação da gestão de riscos no órgão	Art. 17, III

Fonte: IN Conjunta MPOG/CGU nº 01/2016

Para visualizar exemplos de políticas de gestão de riscos no contexto do setor público, consulte os Apêndices 1 a 9, que reúnem casos de outros entes. Esses normativos apresentam estruturas e soluções próprias, que podem servir como referência e inspirar a elaboração ou o aprimoramento da política a ser adotada por cada órgão ou entidade, conforme seu contexto e nível de maturidade.

3.3. Competências e responsabilidades

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

(i) Comitê de Gestão de Riscos da unidade;
(ii) Núcleo Especializado de Gestão de Riscos da unidade; e
(iii) Encarregado pelo tratamento de dados pessoais

O Comitê de Gestão de Riscos representa a alta administração da unidade e aqueles responsáveis pelo seu planejamento estratégico. Cabe a este colegiado decidir e aprovar a política de gestão de riscos. Por sua vez, o Núcleo Especializado de Gestão de Riscos se situa abaixo do Comitê e deve ser presidido pelo Responsável pelo Controle Interno (RCI) da unidade. Suas funções envolvem subsidiar as decisões do Comitê, além de supervisionar a implementação da gestão de riscos, incluindo a definição da política. Para mais informações sobre a atuação desses atores, consulte o Manual de Gestão de Riscos da CGM, p.7-11.

Por fim, tem-se a atuação específica relacionada ao tema da privacidade e da proteção de dados pessoais pelo Encarregado pelo Tratamento de Dados Pessoais do órgão ou da entidade. Este ator tem a função de realizar a interlocução do tema da privacidade com a estrutura de gestão de riscos da unidade, orientando os demais atores sobre a abordagem que será adotada.

3.4. Formalização e aprovação

Para a finalização do trabalho, sugere-se que a abordagem adotada seja validada pela alta administração da unidade e que seja formalizada, independentemente da opção escolhida. Recomenda-se a publicação de Portarias para Políticas de Gestão de Riscos, Políticas de Privacidade e Programas de Governança em Privacidade. A formalização da aprovação de manuais operacionais também é importante para a institucionalização das práticas.

4. Referências

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 29100:2024. Tecnologia da informação – Técnicas de segurança – Estrutura de privacidade. Rio de Janeiro: ABNT, 2024.

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 29184:2021. Tecnologia da informação – Avisos de privacidade on-line e consentimento. Rio de Janeiro: ABNT, 2021.

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

BRASIL. Autoridade Portuária de Santos – Santos Port Authority (SPA). Manual SGPI – Análise e Avaliação de Riscos de Segurança da Informação e Privacidade. Versão 1.0. [S.l.]: SPA, 2022. 29 p. Disponível em: <https://intranet.portodesantos.com.br/docs_codesp/doc_codesp_pdf_site.asp?id=139250>. Acesso em: 15/01/2026.

BRASIL. Autoridade Portuária de Santos S.A. Política de Gestão de Riscos – Pol.SERCI.GCO.004. Santos, SP: Autoridade Portuária de Santos, v. 3.0, aprovada em 26/06/2025; CONSAD nº 090/2025, 22 p. Disponível em: <https://intranet.portodesantos.com.br/docs_codesp/doc_codesp_pdf_site.asp?id=132453>. Acesso em: 15/01/2026.

BRASIL. Banco Central do Brasil. Gestão Integrada de Riscos 2024. Versão 2.0, de 14 de novembro de 2024. Disponível em: <https://www.bcb.gov.br/content/acessoinformacao/riscos-controles/manual_gestao_integrada_riscos.pdf>. Acesso em: 12/01/2026

BRASIL. Banco Central do Brasil. Resolução BCB nº 70, de 11 de fevereiro de 2021. Institui a Política de Gestão Integrada de Riscos do Banco Central do Brasil (PGR-BCB). Disponível em: < https://aprendervalor.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=70>. Acesso em: 12/01/2026

BRASIL. Comissão Nacional de Energia Nuclear (CNEN). Portaria PR/CNEN nº 35, de 2021. Aprova o Programa de Governança em Privacidade da Comissão Nacional de Energia Nuclear (PGP/CNEN). Diário Oficial da União, Brasília, DF, 18/06/2021. Disponível em: <https://www.gov.br/cnen/pt-br/acesso-a-informacao/institucional/copy_of_PGPCNEN.pdf>. Acesso em: 15/01/2026.

BRASIL. Comissão Nacional de Energia Nuclear (CNEN). Portaria CNEN-PR nº 013, de 23 de março de 2018. Aprova a Política de Gestão de Riscos da Comissão Nacional de Energia Nuclear. Diário Oficial da União, Brasília, DF, 23 mar. 2018. 7 p. Disponível em: <https://www.gov.br/cnen/pt-br/avulsos/port-cnen-pr-013-2018-pdf>. Acesso em: 15/01/2026.

BRASIL. Ministério da Defesa. Resolução CG-MD nº 3, de 25 de novembro de 2024. Aprova a Política de Gestão de Riscos do Ministério da Defesa – PGR-MD. Diário Oficial da União, Brasília, DF, 10 dez. 2024, Seção 1, p. 35. Disponível em: <https://www.gov.br/defesa/pt-br/acesso-a-informacao/governanca/colegiados/governanca-md/resolucoes-1/arquivos/resolucao-cg-md-no-3-de-25-de-novembro-de-2024-dou-imprensa-nacional.pdf>. Acesso em: 15/01/2026

BRASIL. Ministério da Defesa. Programa de Gestão em Privacidade. Brasília: Ministério da Defesa, 1ª ed., 2023. Disponível em: <https://www.gov.br/defesa/pt-br/acesso-a-informacao/lei-geral-de-protecao-de-dados-pessoais-lgpd/arquivos/ProgramadeGestoemPrivacidade.pdf>. Acesso em: 15/01/2026

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Guia do Framework de Privacidade e Segurança da Informação – Programa de Privacidade e Segurança da Informação, versão 1.0, 2025. Disponível em: <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi-2.0/arquivos/guiafwppsi2-0-v1-0-22nov2025.pdf> Acesso em: 12/01/2026

BRASIL. Ministério das Comunicações. Política Interna de Privacidade e Proteção de Dados Pessoais. Brasília, DF: Ministério das Comunicações, 2024. Disponível em: <https://www.gov.br/mcom/pt-br/acesso-a-informacao/transparencia-e-prestacao-de-contas/privacidade-e-protecao-de-dados-pessoais/Politica_Privacidade1.pdf>. Acesso em: 15/01/2026.

BRASIL. Ministério das Comunicações (MCom). Resolução CTIR nº 1/2021/SEI-MCTIC – Política de Gestão de Riscos e Controle Interno do Ministério das Comunicações. Boletim de Serviço nº 90, p. 1-4, 2021. Disponível em: <https://www.gov.br/mcom/pt-br/acesso-a-informacao/legislacao/ResoluoCTIRn1Boletimdeservion90.pdf>. Acesso em: 15/01/2026.

BRASIL. Ministério do Planejamento, Orçamento e Gestão (MPOG) e Controladoria-Geral da União (CGU). Instrução Normativa Conjunta nº 1, de 10 de maio de 2016. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal. Brasília, DF, 10 mai. 2016. Diário Oficial da União, Seção 1, p. 14, 11 mai. 2016. Disponível em: <https://www.gov.br/mj/pt-br/acesso-a-informacao/governanca/Gestao-de-Riscos/biblioteca/Normativos/instrucao-normativa-conjunta-no-1-de-10-de-maio-de-2016-imprensa-nacional.pdf/view>. Acesso em: 15/01/2026

BRASIL. Ministério Público do Trabalho. Manual de Gestão de Riscos / Anderson Luiz Corrêa da Silva, Carlos Eduardo Correa Roque, Helder Santos Amorim, Ricardo Augusto de Andrade Franco, organizadores. – Brasília: Ministério Público do Trabalho, 2023. Disponível em: <https://mpt.mp.br/pgt/secretaria-de-integridade-e-gestao-de-riscos/manual-de-gestao-de-riscos.pdf> Acesso em: 12/01/2026

BRASIL. Ministério Público do Trabalho. Plano de Gestão de Riscos 2024-2026. <https://mpt.mp.br/pgt/secretaria-de-integridade-e-gestao-de-riscos/plano-de-gestao-de-riscos.pdf>. Acesso em: 12/01/2026

BRASIL. Ministério Público do Trabalho. Portaria MPT nº 890/2023. Institui a Política de Gestão de Riscos no âmbito do Ministério Público do Trabalho. Disponível em: <https://mpt.mp.br/pgt/secretaria-de-integridade-e-gestao-de-riscos/politica-de-gestao-de-riscos.pdf>. Acesso em: 12/01/2026

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: 12/01/2026.

BRASIL. Universidade Federal do Sul da Bahia – UFSB. Política de Gestão de Riscos (PGR-UFSB). Portaria nº 34/2020. Itabuna: Reitoria da Universidade Federal do Sul da Bahia, 2020. Disponível em: <https://ufsb.edu.br/propa/images/UFSB_Pol%C3%ADtica_de_Gest%C3%A3o_de_Riscos_ATUALIZADA.pdf>. Acesso em: 15/01/2026

BRASIL. Universidade Federal do Sul da Bahia – UFSB. Manual de Gestão de Riscos Estratégicos. Itabuna: Pró-Reitoria de Planejamento (PROPLAN) / Coordenação de Governança, Riscos e Controles (CGRC), 1ª ed., 2024. Disponível em: <https://ufsb.edu.br/proplan/images/Coordena%C3%A7%C3%A3o_CGRC/manual_gest%C3%A3o_de_riscos_estrategicos.pdf>. Acesso em: 15/01/2026.

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: 12/01/2026.

PERNAMBUCO. Decreto nº 49.265/20. Institui a Política Estadual de Proteção de Dados Pessoais do Poder Executivo Estadual em consonância com a Lei Federal nº 13.709/18 (Lei de Proteção de Dados Pessoais). Disponível em: <https://legis.alepe.pe.gov.br/texto.aspx?id=51399>. Acesso em: 13/01/2026.

PERNAMBUCO. Secretaria da Controladoria Geral do Estado. Instrução de Serviço Interno SCGE nº 2/2024. Disponível em: <https://www.scge.pe.gov.br/wp-content/uploads/2025/03/Politica-de-Protecao-de-Dados-Pessoais-Local-PPDPL-SCGE.pdf>. Acesso em: 13/01/2026.

PERNAMBUCO. Secretaria da Controladoria Geral do Estado. Portaria SCGE nº 026/2021. Aprova Politica de Proteção de Dados Pessoais Locais – PPDPL da SCGE. Disponível em: <https://www.scge.pe.gov.br/wp-content/uploads/2021/03/Anexo-Unico-Portaria-SCGE-no-026-2021-_Politicia-de-Protecao-de-Dados-Pessoais-Local-PPDPL-da-SCGE.pdf>. Acesso em: 13/01/2026.

PERNAMBUCO. Secretaria da Controladoria Geral do Estado. Portaria SCGE nº 45/2022. Aprova a Política de Gestão de Riscos (PGR) da Secretaria da Controladoria-Geral do Estado de Pernambuco. Disponível em: <https://www.scge.pe.gov.br/wp-content/uploads/2023/06/2.-Politica-de-Gestao-de-Riscos-da-SCGE-VF_Anexo-Unico.pdf>. Acesso em: 15/01/2026

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: 12/01/2026.

SÃO PAULO (Cidade). Portaria CGM/SP nº 27, de 22 de Junho de 2026. Regulamenta o modelo de Programa de Governança em Privacidade e Proteção de Dados Pessoais da Administração Pública Municipal (PGPP), assim como o procedimento do Diagnóstico de Maturidade em Proteção de Dados Pessoais. Disponível em: <https://legislacao.prefeitura.sp.gov.br/portaria-controladoria-geral-do-municipio-cgm-27-de-22-de-junho-de-2026>. Acesso em: 23/06/2026.

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: 12/01/2026.

SÃO PAULO (Cidade). Manual sobre Aviso de Privacidade e Cookies no contexto da Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo (Controle 12), Versão 1.0, 2025. Disponível em: < https://prefeitura.sp.gov.br/documents/d/controladoria_geral/manual-controle-12-v2-pdf >. Acesso em: 12/01/2026

SÃO PAULO (Cidade). Manual sobre Gestão de Riscos em Privacidade para a Administração Pública do Município de São Paulo (Controle 18), Versão 1.0, 2025. Disponível em: <https://prefeitura.sp.gov.br/documents/d/controladoria_geral/manual-controle-18-_v3-pdf> Acesso em: 12/01/2026

SÃO PAULO (Cidade). Portaria Controladoria Geral do Município – CGM nº 49 de 27 de novembro de 2023. Institui a Política de Gestão de Riscos da Controladoria Geral do Município de São Paulo. Disponível em: < https://legislacao.prefeitura.sp.gov.br/leis/portaria-controladoria-geral-do-municipio-cgm-49-de-27-de-novembro-de-2023>. Acesso em: 12/01/2026

THE INSTITUTE OF INTERNAL AUDITORS (IIA). Modelo das Três Linhas do IIA. Lake Mary, FL: The Institute of Internal Auditors, 2020. Disponível em: <https://iiabrasil.org.br/korbilload/upl/editorHTML/uploadDireto/20200758glob-th-editorHTML-00000013-20082020141130.pdf>. Acesso em: 16/01/2026.

Apêndice 1: Política de Gestão de Riscos da Controladoria Geral do Município de São Paulo

A Política de Gestão de Riscos da Controladoria Geral do Município de São Paulo (CGM) foi instituída pela Portaria CGM nº 49/2023. Da análise do normativo, observa-se que a CGM adotou uma política integrada para todo o órgão, com metodologia aplicável a diferentes temas, incluindo a proteção de dados pessoais.

Essa opção é reforçada pela menção expressa do Art. 9º, XI, ao atribuir ao Núcleo Especializado de Gestão de Riscos e Controles Internos a competência de manter a compatibilidade entre a metodologia aplicada à gestão de riscos e às práticas internas adotadas de Proteção de Dados Pessoais e Segurança da Informação. A inclusão explícita do tema evidencia sua relevância e contribui para orientar a integração da privacidade ao sistema de gestão de riscos institucional.

> Art. 9º Compete ao Núcleo Especializado de Gestão de Riscos e Controles Internos: (Redação dada pela Portaria CGM nº 56/2025) [...]
>
> XI - manter a compatibilidade entre a metodologia aplicada à gestão de riscos e práticas internas adotadas para Integridade, Proteção de Dados Pessoais e Segurança da Informação. (Incluído pela Portaria CGM nº 56/2025)
>
> Fonte: Portaria CGM nº 49/2023

Por sua vez, o Manual de Gestão de Riscos da CGM (2023) reforça a premissa de desenvolver um sistema de gestão de riscos abrangente, concebido para funcionar de maneira harmônica e sinérgica, favorecendo o amadurecimento do sistema de forma eficiente e consistente. Essa diretriz fortalece a ideia de que a gestão de riscos deve ser tratada como um processo institucional contínuo, capaz de incorporar temas específicos (como privacidade) sem fragmentar a governança e os mecanismos de acompanhamento.

> As orientações aqui apresentadas têm por premissa o desenvolvimento de um sistema de gestão de riscos abrangente, e que funcione de forma harmônica e sinérgica, propiciando o amadurecimento do sistema de modo eficiente e consistente.
>
> Fonte: Manual de Gestão de Riscos da CGM (2023)

Para mais informações, consulte as referências elencadas aqui[9].

[9] Referências [8]:
[8] SÃO PAULO (Cidade). Portaria Controladoria Geral do Município – CGM nº 49 de 27 de novembro de 2023. Institui a Política de Gestão de Riscos da Controladoria Geral do Município de São Paulo. Disponível em: <https://legislacao.prefeitura.sp.gov.br/leis/portaria-controladoria-geral-do-municipio-cgm-49-de-27-de-novembro-de-2023>. Acesso em: 12/01/2026.
[8] 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: 12/01/2026.

Apêndice 2: Política de Gestão de Riscos do Ministério Público do Trabalho

A Política de Gestão de Riscos do Ministério Público do Trabalho (MPT) foi instituída pela Portaria nº 890/2023. Da análise do normativo, observa-se que o MPT optou por explicitar categorias de riscos a serem consideradas pela instituição, sem prejuízo da identificação de outras, incluindo a categoria de "riscos de privacidade de dados pessoais" (Art. 3º, IX). Essa opção é relevante porque orienta a atuação das unidades ao indicar, de forma prévia, um conjunto de categorias que deve ser observado, conferindo visibilidade ao tema da proteção de dados pessoais no âmbito da gestão de riscos.

> Art. 3º Para os fins desta Portaria, destacam-se as seguintes categorias de riscos, sem prejuízo da identificação de outras: [...]
>
> IX. Riscos de Privacidade de Dados Pessoais: decorrentes de eventos que tenham efeito na privacidade de dados pessoais tratados pela instituição
>
> Fonte: Portaria nº 890/2023

O Art. 3º, IX, define riscos de privacidade de dados pessoais como aqueles decorrentes de eventos que tenham efeito na privacidade de dados pessoais tratados pela instituição. Em linha com essa diretriz, o Manual de Gestão de Riscos do MPT (2023) detalha o processo institucional de gestão de riscos e prevê que, após a etapa de identificação, cada risco deve ser classificado conforme sua natureza, incluindo expressamente a categoria de privacidade de dados. Essa vinculação entre política e manual reforça a institucionalização do tema, ao assegurar que os riscos de privacidade sejam registrados e tratados no mesmo fluxo metodológico aplicável às demais categorias de risco.

> Cada risco identificado deve ser classificado conforme sua natureza: estratégico, operacional, de conformidade, de integridade, de recursos humanos, de reputação, de segurança institucional, de tecnologia da informação ou de privacidade de dados (conforme classificação prevista no art. 3º da Política de Gestão de Riscos do MPT – Portaria PGT n. 890/2023)
>
> Fonte: Manual de Gestão de Riscos do MPT (2023)

Para mais informações, consulte as referências elencadas aqui[10].

[10] Referências [9]:
[9] BRASIL. Ministério Público do Trabalho. Portaria MPT nº 890/2023. Institui a Política de Gestão de Riscos no âmbito do Ministério Público do Trabalho. Disponível em: <https://mpt.mp.br/pgt/secretaria-de-integridade-e-gestao-de-riscos/politica-de-gestao-de-riscos.pdf>. Acesso em: 12/01/2026.
[9] BRASIL. Ministério Público do Trabalho. Manual de Gestão de Riscos / Anderson Luiz Corrêa da Silva, Carlos Eduardo Correa Roque, Helder Santos Amorim, Ricardo Augusto de Andrade Franco, organizadores. – Brasília: Ministério Público do Trabalho, 2023. Disponível em: <https://mpt.mp.br/pgt/secretaria-de-integridade-e-gestao-de-riscos/manual-de-gestao-de-riscos.pdf> Acesso em: 12/01/2026.
[9] BRASIL. Ministério Público do Trabalho. Plano de Gestão de Riscos 2024-2026. <https://mpt.mp.br/pgt/secretaria-de-integridade-e-gestao-de-riscos/plano-de-gestao-de-riscos.pdf>. Acesso em: 12/01/2026.

Apêndice 3: Manual de Gestão Integrada de Riscos do Banco Central do Brasil

A Política de Gestão de Riscos do Banco Central do Brasil (BCB) foi instituída pela Resolução BCB nº 70/2021. Da análise do normativo, observa-se que o BCB adotou uma política integrada de gestão de riscos, aplicável a toda a instituição (Art. 1º). A própria nomenclatura "gestão integrada" reforça a ideia de padronização e de aplicação transversal, envolvendo diferentes atores e diferentes tipos de riscos no âmbito institucional. O Art. 1º destaca, nesse sentido, que a gestão integrada de riscos é um processo conduzido pela Diretoria Colegiada, pelo corpo gerencial e por todos os servidores, voltado, entre outros aspectos, a identificar eventos em potencial capazes de afetar a instituição.

> Art. 1º Gestão integrada de riscos é o processo conduzido pela Diretoria Colegiada, corpo gerencial e todos os servidores, aplicado no estabelecimento e na implantação de estratégias que são formuladas para:
>
> I - identificar em toda a Instituição eventos em potencial capazes de afetá-la;
>
> Fonte: Resolução BCB nº 70/2021

Embora a política não trate expressamente de privacidade e proteção de dados pessoais, o tema aparece de forma mais detalhada no Manual de Gestão Integrada de Riscos (2024). O manual diferencia riscos de origem financeira e riscos organizacionais e, no âmbito dos riscos operacionais, adota uma taxonomia com categorias específicas. Nesse arranjo, os riscos relacionados à proteção de dados pessoais são tratados no escopo de riscos à integridade, que incluem eventos com impacto tanto sobre o titular de dados pessoais quanto sobre a instituição. O manual também explicita que riscos cibernéticos, ainda que considerados no conjunto de riscos operacionais corporativos, recebem tratamento específico no âmbito da Segurança da Informação, o que evidencia uma articulação entre o processo corporativo de riscos e instrumentos especializados para temas com maior complexidade técnica.

> Dentre os tipos de risco à integridade, mas não limitados a eles, destacam-se os riscos à proteção de dados e informações armazenadas pela instituição, em especial aos dados pessoais. Esse tipo de risco pode ser descrito como potencial evento que gera impacto sobre o titular de dados pessoais e sobre o BC. [...] Importante ressaltar que os riscos

cibernéticos, ainda que considerados dentro do escopo dos riscos operacionais corporativos, possuem um tratamento específico no BC.

Fonte: Manual de Gestão Integrada de Riscos (2024)

Para mais informações, consulte as referências elencadas aqui[11].

[11] Referências [10]:
[10] BRASIL. Banco Central do Brasil. Resolução BCB nº 70, de 11 de fevereiro de 2021. Institui a Política de Gestão Integrada de Riscos do Banco Central do Brasil (PGR-BCB). Disponível em: <https://aprendervalor.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=70>. Acesso em: 12/01/2026.
[10] BRASIL. Banco Central do Brasil. Gestão Integrada de Riscos 2024. Versão 2.0, de 14 de novembro de 2024. Disponível em: <https://www.bcb.gov.br/content/acessoinformacao/riscos-controles/manual_gestao_integrada_riscos.pdf>. Acesso em: 12/01/2026.

Apêndice 4: Manual de Gestão de Riscos da Universidade Federal do Sul da Bahia

A Universidade Federal do Sul da Bahia (UFSB) aprovou sua Política de Gestão de Riscos por meio da Portaria nº 34/2020. Embora o normativo não mencione diretamente o tema da privacidade, observa-se que ele prevê uma estrutura que permite incorporar o assunto por meio da definição institucional de categorias de risco. Nesse sentido, ao tratar das responsabilidades dos agentes envolvidos, a política atribui ao Comitê de Governança, Gestão de Riscos e Controle Interno a competência de aprovar as categorias de riscos a serem gerenciados (Art. 14, II, "c").

> Art. 14 Para efetivação da gestão de riscos no âmbito da instituição, ficam estabelecidas as responsabilidades dos diversos agentes envolvidos no processo de gerenciamento de riscos: [...]
>
> II - Comitê de Governança, Gestão de Riscos e Controle Interno: [...]
>
> c) aprovar as categorias de riscos a serem gerenciados;
>
> Fonte: Portaria nº 34/2020

Por sua vez, o Manual de Gestão de Riscos da UFSB (2024) explicita essas categorias e inclui, de forma expressa, referências à privacidade e proteção de dados pessoais. O manual orienta que os riscos sejam classificados por categoria para apoiar a organização na identificação dos principais fatores que podem afetá-la, destacando que um mesmo risco pode se relacionar a mais de uma tipologia. Entre as categorias, inclui-se "Segurança da informação", cuja descrição abrange eventos relacionados à confidencialidade, disponibilidade e integridade da informação, bem como à privacidade e proteção de dados e informações da instituição e de pessoas. Essa solução mostra como o tema pode ser incorporado de modo prático no nível metodológico, mesmo quando a política corporativa não detalha explicitamente a privacidade.

> 2.2 Categoria do evento
>
> Os riscos também devem ser classificados quanto a sua categoria, o que auxilia na organização a entender quais os principais fatores de riscos que a podem afetar. Para auxiliar nessa categorização, é importante avaliar as causas do risco, para saber a que matéria se relacionam (financeiro, legal, imagem, infraestrutura, político etc.), de forma

a identificar a tipologia mais adequada. Vale lembrar que, não raro, um risco pode estar relacionado a mais de uma tipologia, contudo, sempre existirá uma que é mais dominante em detrimento às demais. As categorias adotadas como referência são:

Origem: Interna
Categoria: Segurança da informação
Descrição: Eventos associados a confidencialidade, disponibilidade e integridade da informação, privacidade e proteção de dados e informações da instituição e de pessoas.

Fonte: Manual de Gestão de Riscos da UFSB (2024)

Para mais informações, consulte as referências elencadas aqui[12].

[12] Referências [11]:
[11] BRASIL. Universidade Federal do Sul da Bahia – UFSB. Política de Gestão de Riscos (PGR-UFSB). Portaria nº 34/2020. Itabuna: Reitoria da Universidade Federal do Sul da Bahia, 2020. Disponível em: <https://ufsb.edu.br/propa/images/UFSB_Pol%C3%ADtica_de_Gest%C3%A3o_de_Riscos_ATUALIZADA.pdf>. Acesso em: 15/01/2026
[11] BRASIL. Universidade Federal do Sul da Bahia – UFSB. Manual de Gestão de Riscos Estratégicos. Itabuna: Pró-Reitoria de Planejamento (PROPLAN) / Coordenação de Governança, Riscos e Controles (CGRC), 1ª ed., 2024. Disponível em: <https://ufsb.edu.br/proplan/images/Coordena%C3%A7%C3%A3o_CGRC/manual_gest%C3%A3o_de_riscos_estrategicos.pdf>. Acesso em: 15/01/2026.

Apêndice 5: Manual SGPI – Análise e Avaliação de Riscos de Segurança da Informação e Privacidade da Autoridade Portuária de Santos S.A.

A Política de Gestão de Riscos da Autoridade Portuária de Santos S.A. (APS) (2025) não menciona expressamente o tema da privacidade. O normativo institui a Política como parte de um conjunto de instrumentos de governança e de gestão voltados a apoiar a concepção, implementação e melhoria contínua da estrutura organizacional da Companhia.

> 1. Fica instituída a Política de Gestão de Riscos ("Política"), a qual faz parte de um conjunto de instrumentos de governança e de gestão que suportam a concepção, implementação e melhoria contínua na estrutura organizacional da Autoridade Portuária de Santos S.A. ("APS" ou "Companhia").
>
> 2. Esta Política de Gestão de Riscos tem por finalidade estabelecer a estrutura e o processo de governança corporativa dos riscos, os princípios, diretrizes e responsabilidades que orientam a gestão de riscos e controles internos de forma integrada, objetivando o atingimento dos objetivos estratégicos da APS, bem como a consolidação de um ambiente que respeite os valores, interesses e expectativas da Companhia e de todas as partes interessadas, tendo o cidadão e a sociedade como principais vetores. [...]
>
> 4. Os dispositivos da presente Política aplicam-se e devem ser utilizados por todos os membros dos órgãos estatutários e empregados da APS e, poderão ser utilizados como base conceitual quando da ausência de normativos específicos. [...]
>
> 6. Outros normativos internos serão compostos pelo detalhamento dos procedimentos e metodologias com a aplicação dos objetivos estabelecidos nesta Política para uma efetiva gestão de riscos.
>
> Fonte: Política de Gestão de Riscos da Autoridade Portuária de Santos S.A. (APS) (2025)

Ainda assim, observa-se a adoção de instrumento complementar voltado ao tema: o Manual para Avaliação de Riscos de Segurança da Informação e Privacidade (2022), que estabelece uma metodologia específica para esse contexto. O manual delimita seu escopo à avaliação de riscos relacionados à segurança da informação e privacidade, sem abranger riscos corporativos e de processos, que permanecem disciplinados em normativos próprios. Ao mesmo tempo, a

solução preserva a integração com a Política de Gestão de Riscos, ao posicionar o manual como instrumento especializado dentro do sistema institucional de gestão de riscos.

> O presente Manual tem por objetivo definir as regras de elaboração do relatório de Análise e Avaliação de Riscos de Segurança da Informação e Privacidade da SPA. Este manual trata da avaliação técnica e específica dos riscos relacionados à segurança da informação e privacidade, não abrangendo a avaliação de riscos corporativos e de processos tratados em normativos próprios.
>
> Fonte: Manual para Avaliação de Riscos de Segurança da Informação e Privacidade (2022)

Para mais informações, consulte as referências elencadas aqui[13].

[13] Referências [12]

[12] BRASIL. Autoridade Portuária de Santos S.A. Política de Gestão de Riscos – Pol.SERCI.GCO.004. Santos, SP: Autoridade Portuária de Santos, v. 3.0, aprovada em 26/06/2025; CONSAD nº 090/2025, 22 p. Disponível em: <https://intranet.portodesantos.com.br/docs_codesp/doc_codesp_pdf_site.asp?id=132453>. Acesso em: 15/01/2026.

[12] BRASIL. Autoridade Portuária de Santos – Santos Port Authority (SPA). Manual SGPI – Análise e Avaliação de Riscos de Segurança da Informação e Privacidade. Versão 1.0. [S.l.]: SPA, 2022. 29 p. Disponível em: <https://intranet.portodesantos.com.br/docs_codesp/doc_codesp_pdf_site.asp?id=139250>. Acesso em: 15/01/2026.

Apêndice 6: Programa de Governança em Privacidade da Comissão Nacional de Energia Nuclear

A Política de Gestão de Riscos da Comissão Nacional de Energia Nuclear (CNEN) foi instituída pela Portaria CNEN-PR nº 13/2018. O normativo estabelece a gestão de riscos na instituição (Art. 1º) e define como finalidade estabelecer princípios, diretrizes e responsabilidades, além de orientar os processos de identificação, avaliação, tratamento, monitoramento, comunicação e a incorporação da visão de riscos à tomada de decisões estratégicas, em conformidade com os objetivos da CNEN (Art. 4º). O parágrafo único do Art. 4º reforça que a gestão de riscos deve estar integrada aos processos de planejamento estratégico, tático e operacional, à gestão e à cultura organizacional. Adicionalmente, o Art. 5º prevê que o gerenciamento de riscos seja implantado gradualmente em todas as áreas, com priorização dos processos que impactam diretamente os objetivos organizacionais.

> Art. 1º Fica instituída a Política de Gestão de Riscos, que estabelece a Gestão de Riscos na Comissão Nacional de Energia Nuclear - CNEN.
>
> Art. 4º Estabelecer princípios, diretrizes e responsabilidades da Gestão de Riscos, bem como orientar os processos de identificação, avaliação, tratamento, monitoramento e comunicação dos riscos inerentes às atividades, incorporando a visão de riscos à tomada de decisões estratégicas e em conformidade com os objetivos da CNEN.
>
> Parágrafo único. A Gestão de Riscos deverá estar integrada aos processos de planejamento estratégico, tático e operacional, à gestão e à cultura organizacional da CNEN.
>
> Art. 5º O gerenciamento de riscos deverá ser implantado de forma gradual em todas as áreas da CNEN, sendo priorizados os processos que impactam diretamente os objetivos organizacionais.
>
> Fonte: Portaria CNEN-PR nº 13/2018

Por sua vez, o Programa de Governança em Privacidade da CNEN (2021) vincula expressamente a gestão de riscos em privacidade à política institucional de riscos. Ao tratar do tema “Gestão de Riscos”, o documento destaca que a implementação do programa depende da

mitigação de riscos associados e explicita que a avaliação e o gerenciamento desses riscos devem ser realizados conforme o plano de implementação e em alinhamento com a Política de Riscos da CNEN (Art. 10). Essa abordagem ilustra uma forma de integração em que o programa de governança em privacidade incorpora a gestão de riscos em privacidade como componente próprio, porém conectado ao modelo corporativo de riscos já adotado pela instituição.

> 10. GESTÃO DE RISCOS
>
> Para que um Programa de Governança em Privacidade seja bem implementado, é essencial mitigar os riscos associados. De acordo com o Plano de Implementação a ser definido (item cronograma) e com a Política de Riscos da CNEN, a avaliação e o gerenciamento dos riscos deverão ser feitos, considerando o seu grau de ameaça à implementação do PGP/CNEN.
>
> Fonte: Programa de Governança em Privacidade da CNEN (2021)

Para mais informações, consulte as referências elencadas aqui[14].

[14] Referências [13]:
[13] BRASIL. Comissão Nacional de Energia Nuclear (CNEN). Portaria PR/CNEN nº 35, de 2021. Aprova o Programa de Governança em Privacidade da Comissão Nacional de Energia Nuclear (PGP/CNEN). Diário Oficial da União, Brasília, DF, 18/06/2021. Disponível em: <https://www.gov.br/cnen/pt-br/acesso-a-informacao/institucional/copy_of_PGPCNEN.pdf>. Acesso em: 15/01/2026.
[13] BRASIL. Comissão Nacional de Energia Nuclear (CNEN). Portaria CNEN-PR nº 013, de 23 de março de 2018. Aprova a Política de Gestão de Riscos da Comissão Nacional de Energia Nuclear. Diário Oficial da União, Brasília, DF, 23 mar. 2018. 7 p. Disponível em: <https://www.gov.br/cnen/pt-br/avulsos/port-cnen-pr-013-2018-pdf>. Acesso em: 15/01/2026.

Apêndice 7: Programa de Gestão em Privacidade do Ministério da Defesa

A Política de Gestão de Riscos do Ministério da Defesa foi aprovada pela Resolução CG-MD nº 3/2024. O normativo estabelece que a política tem por finalidade definir princípios, objetivos e diretrizes e instituir o sistema de gestão de riscos relacionado aos objetivos estratégicos, projetos, processos e recursos do Ministério (Art. 1º). O parágrafo único do mesmo artigo reforça que a gestão de riscos está integrada ao Planejamento Estratégico Organizacional, abrangendo as três linhas de defesa e os órgãos que integram o Ministério da Defesa, com exceção dos Comandos da Marinha, do Exército e da Aeronáutica.

> Art. 1º Esta Resolução aprova a Política de Gestão de Riscos do Ministério da Defesa - PGR-MD, que tem por finalidade estabelecer princípios, objetivos, diretrizes e instituir o sistema de gestão de riscos relacionados aos objetivos estratégicos organizacionais, projetos, processos e recursos no âmbito do Ministério da Defesa.
>
> Parágrafo único. A gestão de riscos está integrada ao processo de Planejamento Estratégico Organizacional do Ministério da Defesa, abrangendo as três linhas de defesa da gestão e todos os órgãos que integram o Ministério da Defesa, exceto os Comandos da Marinha, do Exército e da Aeronáutica.
>
> Fonte: Resolução CG-MD nº 3/2024

Embora a política não detalhe tipologias específicas de riscos de privacidade, o Programa de Gestão em Privacidade (2023) explicita a necessidade de alinhamento da gestão de riscos em privacidade ao modelo corporativo. O documento registra que as definições e conceitos ali apresentados servem de referência para ilustrar a identificação e avaliação de riscos no Relatório de Impacto à Proteção de Dados Pessoais (RIPD) e destaca que o gerenciamento de riscos relacionado ao tratamento de dados pessoais deve ser realizado em harmonia com a Política de Gestão de Riscos do Ministério, em consonância com a lógica de integração prevista na IN Conjunta MPOG/CGU nº 01/2016. Essa abordagem evidencia uma solução em que a privacidade é operacionalizada por instrumentos próprios (como o RIPD), mantendo-se conectada ao sistema institucional de gestão de riscos.

> As definições e conceitos de riscos adotados neste documento são utilizados como forma de ilustrar a identificação e avaliação de riscos realizada no Relatório de Impacto à Proteção de Dados Pessoais - RIPD. Desse modo, é importante destacar que o

gerenciamento de riscos relacionado ao tratamento dos dados pessoais deve ser realizado em harmonia com a Política de Gestão de Riscos do Ministério da Defesa, caso instituída, conforme preconizado pela Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016.

Fonte: Programa de Gestão em Privacidade (2023)

Para mais informações, consulte as referências elencadas aqui[15].

[15] Referências [14]:
[14] BRASIL. Ministério da Defesa. Resolução CG-MD nº 3, de 25 de novembro de 2024. Aprova a Política de Gestão de Riscos do Ministério da Defesa – PGR-MD. Diário Oficial da União, Brasília, DF, 10 dez. 2024, Seção 1, p. 35. Disponível em: <https://www.gov.br/defesa/pt-br/acesso-a-informacao/governanca/colegiados/governanca-md/resolucoes-1/arquivos/resolucao-cg-md-no-3-de-25-de-novembro-de-2024-dou-imprensa-nacional.pdf>. Acesso em: 15/01/2026
[14] BRASIL. Ministério da Defesa. Programa de Gestão em Privacidade. Brasília: Ministério da Defesa, 1ª ed., 2023. Disponível em: <https://www.gov.br/defesa/pt-br/acesso-a-informacao/lei-geral-de-protecao-de-dados-pessoais-lgpd/arquivos/ProgramadeGestoemPrivacidade.pdf>. Acesso em: 15/01/2026

Apêndice 8: Política Interna de Privacidade e Proteção de Dados Pessoais do Ministério das Comunicações

O Ministério das Comunicações (MCom) aprovou sua Política de Gestão de Riscos e Controle Interno por meio da Resolução nº CTIR nº 1/2021/SEI-MCTIC. O normativo estabelece como finalidade definir princípios, diretrizes e responsabilidades mínimas para a gestão de riscos e de controles internos relacionados aos planos estratégicos, programas, projetos e processos do Ministério (Art. 1º). O parágrafo único reforça que a gestão de riscos deve estar alinhada aos modelos de governança e de gestão, ao planejamento estratégico e à cadeia de valor institucionalizada no âmbito do MCom.

> Art. 1º Aprovar a Política de Gestão de Riscos PGR, que tem por finalidade estabelecer os princípios, diretrizes e responsabilidades mínimas a serem observadas e seguidas para a gestão de riscos e de controles internos referentes aos planos estratégicos, programas, projetos e processos do Ministério das Comunicações.
>
> Parágrafo único. A gestão de riscos deve alinhar-se aos modelos de governança corporativa e de gestão, ao planejamento estratégico, e à cadeia de valor institucionalizados no âmbito do Ministério das Comunicações, observadas suas atribuições e competências regimentais.
>
> Fonte: Resolução nº CTIR nº 1/2021/SEI-MCTIC

Embora a política corporativa não mencione expressamente o tema da privacidade, a Política Interna de Privacidade e Proteção de Dados Pessoais (2024) do MCom estabelece essa conexão ao orientar que os servidores e demais agentes abrangidos devem compreender os riscos relacionados ao tratamento de dados pessoais e adotar os processos de gestão de risco definidos na Política de Gestão de Riscos e Controle Interno do Ministério. Essa abordagem evidencia uma solução em que a privacidade é disciplinada em instrumento próprio, mas subordinada e integrada ao modelo institucional de gestão de riscos e controles internos.

> 6. Diretrizes Gerais
>
> Cabe aos servidores e demais curadores de dados pessoais aos quais a política se aplica, enumerados anteriormente, conhecer, aderir, cumprir e fazer cumprir a Política de Privacidade do Ministério das Comunicações, conforme as diretrizes gerais a seguir.

- Conhecer, aderir, cumprir e fazer cumprir o Programa de Governança em Privacidade do Ministério das Comunicações.

- Compreender os riscos relacionados ao tratamento de dados pessoais e sua relação com os benefícios ao titular de dados e à sociedade resultantes dos serviços prestados. Adotar os processos de gestão de risco determinados pelo Ministério das Comunicações em sua Política de Gestão de Riscos e Controle Interno - RESOLUÇÃO Nº CTIR nº 1/2021/SEI-MCTIC.

Fonte: Política Interna de Privacidade e Proteção de Dados Pessoais (2024)

Para mais informações, consulte as referências elencadas aqui[16].

[16] Referências [15]:
[15] BRASIL. Ministério das Comunicações. Política Interna de Privacidade e Proteção de Dados Pessoais. Brasília, DF: Ministério das Comunicações, 2024. Disponível em: <https://www.gov.br/mcom/pt-br/acesso-a-informacao/transparencia-e-prestacao-de-contas/privacidade-e-protecao-de-dados-pessoais/Politica_Privacidade1.pdf>. Acesso em: 15/01/2026.
[15] BRASIL. Ministério das Comunicações (MCom). Resolução CTIR nº 1/2021/SEI-MCTIC – Política de Gestão de Riscos e Controle Interno do Ministério das Comunicações. Boletim de Serviço nº 90, p. 1-4, 2021. Disponível em: <https://www.gov.br/mcom/pt-br/acesso-a-informacao/legislacao/ResoluoCTIRn1Boletimdeservion90.pdf>. Acesso em: 15/01/2026.

Apêndice 9: Política de Proteção de Dados Pessoais Local da Secretaria da Controladoria Geral do Estado de Pernambuco

A Política de Gestão de Riscos da Secretaria da Controladoria-Geral do Estado de Pernambuco (SCGE/PE) foi aprovada pela Portaria SCGE nº 45/2022, com aplicação a todas as áreas da Secretaria (Art. 1º), mas não detalha o tratamento dos riscos em privacidade.

> Art. 1º A presente Política de Gestão de Riscos (PGR) é aplicável a todas as áreas desta Secretaria da Controladoria-Geral do Estado de Pernambuco (SCGE/PE).
>
> Fonte: Portaria SCGE nº 45/2022

Por sua vez, a Política Estadual de Proteção de Dados Pessoais, instituída pelo Decreto nº 49.265/2020, determinou que órgãos e entidades elaborem suas Políticas de Proteção de Dados Pessoais Locais (PPDPL), a serem aprovadas pelo dirigente máximo, devendo contemplar, no mínimo, o processo de gerenciamento de riscos (Art. 6º, §1º, III). Essa exigência cria uma conexão direta entre a governança de privacidade e a institucionalização da gestão de riscos como componente obrigatório das políticas locais.

> Art. 6º Os órgãos e as entidades da Administração Pública Estadual direta, autárquica e fundacional deverão estabelecer suas respectivas Políticas de Proteção de Dados Pessoais Locais – PPDPL a serem aprovadas pelo dirigente máximo.
>
> § 1º As Políticas de Proteção de Dados Pessoais Locais – PPDPL deverão considerar as prioridades previstas no Plano Quadrienal Estratégico de Proteção de Dados Pessoais – PPDP e deverão estabelecer, no mínimo: [...]
>
> III - processo de gerenciamento de riscos;
>
> Fonte: Decreto nº 49.265/2020

No caso da SCGE/PE, a PPDPL aprovada pela Portaria SCGE nº 026/2021 incorporou de forma expressa diretrizes, metodologias e competências sobre gestão de riscos em privacidade. Entre os dispositivos, destacam-se: a diretriz de gestão de riscos sistematizada, suportada por metodologias técnicas, e a orientação de priorização de processos conforme relevância e impacto estratégico (Art. 5º, VI e parágrafo único); a previsão de instrumentos para sustentar o

modelo, incluindo metodologia baseada em referenciais como COSO e normas ISO (com menção a ISO 31000, 31010, 27001, 27002, 27004, 27005, 27701 e 29100), além do apoio por solução tecnológica (Art. 7º); e a atribuição de responsabilidade à autoridade máxima pela definição final da gestão de riscos e controles internos quanto à adequação à LGPD na Secretaria, conforme o decreto estadual (Art. 9º).

> Art. 5º São diretrizes da PPDPL-SCGE: [...]
>
> VI - a gestão de riscos sistematizada e suportada pelas premissas de metodologias técnicas;
>
> Parágrafo único. O modelo de gestão de gerenciamento de riscos deve seguir o método de priorização de processos, considerando sua relevância e impacto na estratégia da Secretaria.
>
> Art. 7º São instrumentos da PPDPL-SCGE: [...]
>
> II - a metodologia: o modelo de gestão de riscos da Secretaria deve ser estruturado com base do Committee of Sponsoring Organizations of the Treadway Commission – COSO e nas boas práticas produzidas pela International Organization for Standardization, em especial, as ISO 31000, 31010, 27001, 27002, 27004, 27005, 27701, 29100; [...]
>
> V - a solução tecnológica: o processo de gestão de riscos deve ser apoiado por adequado suporte de tecnologia da informação.
>
> Art. 9º O Secretário da Controladoria-Geral do Estado, enquanto representante legal, terá responsabilidade pela definição final da gestão dos riscos e controles internos quanto à adequação à LGPD na Secretaria, nos termos do art. 12 do Decreto Estadual nº 49.265, de 06 de agosto de 2020.
>
> Fonte: Portaria SCGE nº 026/2021

Posteriormente, a política local foi atualizada pela Instrução de Serviço Interno SCGE nº 2/2024, mantendo a ênfase na gestão de riscos e detalhando competências institucionais. A norma preserva a diretriz de gestão de riscos sistematizada (Art. 6º, VI) e reafirma a responsabilidade da autoridade máxima quanto à definição final da gestão de riscos e controles internos para adequação à LGPD (Art. 9º). Além disso, explicita atribuições do encarregado de dados pessoais, incluindo instituir e coordenar ciclos de avaliação de riscos de segurança da

informação e privacidade, monitorar planos de implementação de controles internos e apoiar a elaboração e revisão do método de avaliação de riscos (Art. 15), bem como competências da Diretoria de Tecnologia da Informação do Controle Interno, como elaborar o método de avaliação de riscos (Art. 16). Esse conjunto demonstra uma abordagem em que a gestão de riscos em privacidade é tratada de forma estruturada no âmbito da política local de proteção de dados, com forte detalhamento de metodologia e responsabilidades.

> Art. 6º São diretrizes da PPDPL-SCGE: [...]
>
> VI – a gestão de riscos sistematizada e suportada pelas premissas de metodologias técnicas.
>
> Art. 9º A autoridade máxima da Secretaria da Controladoria-Geral do Estado, enquanto representante legal, terá responsabilidade pela definição final da gestão dos riscos e controles internos quanto à adequação à LGPD neste órgão, nos termos do art. 12 do Decreto Estadual nº 49.265, de 06 de agosto de 2020
>
> Art. 15. Compete ao encarregado de dados pessoais, além das ações descritas no Decreto nº 49.265/2020, as seguintes:
>
> IX – instituir e coordenar os ciclos de avaliação de riscos de segurança da informação e privacidade;
>
> X – instituir, coordenar e monitorar os Planos de Implementação de Controles Internos elaborados com as medidas de controle interno necessárias para a mitigação dos principais riscos encontrados nos processos organizacionais do órgão, e suas revisões
>
> XIV – apoiar a elaboração do Método de Avaliação de Riscos de SI&P previsto na Portaria SCGE nº 14, de 22 de abril de 2022, bem como, de suas revisões; e
>
> Art. 16. Compete à Diretoria de Tecnologia da Informação do Controle Interno - DTCI: [...]
>
> XIII – elaborar o Método de Avaliação de Riscos de SI&P;
>
> Fonte: Instrução de Serviço Interno SCGE nº 2/2024

Para mais informações, consulte as referências elencadas aqui[17].

[17] Referências [16]:

[16] PERNAMBUCO. Decreto nº 49.265/20. Institui a Política Estadual de Proteção de Dados Pessoais do Poder Executivo Estadual em consonância com a Lei Federal nº 13.709/18 (Lei de Proteção de Dados Pessoais). Disponível em: <https://legis.alepe.pe.gov.br/texto.aspx?id=51399>. Acesso em: 13/01/2026.

[16] PERNAMBUCO. Secretaria da Controladoria Geral do Estado. Instrução de Serviço Interno SCGE nº 2/2024. Disponível em: <https://www.scge.pe.gov.br/wp-content/uploads/2025/03/Politica-de-Protecao-de-Dados-Pessoais-Local-PPDPL-SCGE.pdf>. Acesso em: 13/01/2026.

[16] PERNAMBUCO. Secretaria da Controladoria Geral do Estado. Portaria SCGE nº 026/2021. Aprova Politica de Proteção de Dados Pessoais Locais – PPDPL da SCGE. Disponível em: <https://www.scge.pe.gov.br/wp-content/uploads/2021/03/Anexo-Unico-Portaria-SCGE-no-026-2021-_Politicia-de-Protecao-de-Dados-Pessoais-Local-PPDPL-da-SCGE.pdf>. Acesso em: 13/01/2026.

[16] PERNAMBUCO. Secretaria da Controladoria Geral do Estado. Portaria SCGE nº 45/2022. Aprova a Política de Gestão de Riscos (PGR) da Secretaria da Controladoria-Geral do Estado de Pernambuco. Disponível em: <https://www.scge.pe.gov.br/wp-content/uploads/2023/06/2.-Politica-de-Gestao-de-Riscos-da-SCGE-VF_Anexo-Unico.pdf>. Acesso em: 15/01/2026

PREFEITURA DE
SÃO PAULO