

☐ Inclusão de Novo Processo
☐ Alteração de Processo Existente (ID: _____)
☐ Exclusão / Descontinuidade de Processo
2. Descrição da Operação de Tratamento
Nome do Processo / Atividade:
Descrição sucinta da atividade:
Qual a finalidade principal do tratamento dos dados?
Quem são os titulares dos dados?
☐ Servidores/Empregados ☐ Clientes/Cidadãos ☐ Fornecedores ☐ Crianças/Adolescentes ☐ Outros:
Quais dados pessoais são coletados?
(Ex.: Nome, CPF, RG, Endereço, E-mail, IP, Dados Financeiros, etc.)
Há coleta de dados sensíveis?
☐ Não
☐ Sim (Ex.: Saúde, Biometria, Origem Racial/Étnica, Dado Religioso/Sindicato/Político, etc.)
Se sim, especifique:
Os dados são compartilhados com terceiros (outros órgãos, empresas contratadas, parceiros)?
☐ Não
☐ Sim. Informe com quem e para qual finalidade:
Onde e como os dados ficam armazenados?
☐ Servidor Físico Interno
☐ Nuvem (Cloud)
☐ Arquivo em Papel / Físico
☐ Outro:
Qual o tempo estimado de guarda/retenção desses dados?
3. Validação do Encarregado / DPO
Data de Recebimento pelo DPO: //20[XX]
Parecer Técnico do DPO:
☐ Aprovado para inclusão/alteração no ROPA sem ressalvas.
☐ Aprovado com recomendações (anexar relatório).
☐ Reprovado (motivo: _____).
Base Legal Definida pelo DPO: Art. _____, Inciso _____ da LGPD.

Portaria nº 21/2026/cgm - Aprova o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) no âmbito da Controladoria-Geral do Município de Niterói, e dá outras providências.

O **CONTROLADOR-GERAL DO MUNICÍPIO DE NITERÓI**, no uso das atribuições legais e regimentais que lhe são conferidas pela legislação municipal, e

CONSIDERANDO o disposto na Lei nº 13.709, de 14 de agosto de 2018 — Lei Geral de Proteção de Dados Pessoais (LGPD), especialmente no seu art. 5º, inciso XVII, e art. 38, que preveem a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD);

CONSIDERANDO o disposto no Decreto Municipal nº 271, de 2025, do Município de Niterói, que regulamenta a aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) e estabelece as diretrizes de governança em privacidade e proteção de dados no âmbito do Poder Executivo Municipal;

CONSIDERANDO o Guia Orientativo sobre o Relatório de Impacto à Proteção de Dados Pessoais emitido pela Autoridade Nacional de Proteção de Dados (ANPD);

CONSIDERANDO a necessidade de identificar, avaliar e mitigar preventivamente os riscos às liberdades civis e aos direitos fundamentais dos titulares de dados decorrentes das atividades de fiscalização, auditoria, ouvidoria, integridade e gestão administrativa desenvolvidas no âmbito do órgão;

CONSIDERANDO os princípios da prevenção, segurança, prestação de contas e responsabilização previstos no art. 6º, incisos VIII, IX e X, da LGPD, bem como a adoção dos conceitos de *Privacy by Design* e *Privacy by Default* nos sistemas institucionais;

RESOLVE:

Art. 1º Fica aprovado o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) no âmbito da Controladoria-Geral do Município de Niterói (CGM-Niterói), referente às operações de tratamento de dados pessoais de elevado risco e relevância institucional, na forma do Anexo Único desta Portaria.

Art. 2º O RIPD aprovado por esta Portaria tem por objetivos:

I – Mapear o contexto, a necessidade e a proporcionalidade das operações de tratamento de dados pessoais realizadas no âmbito da CGM;

II – Identificar e mensurar os riscos de privacidade decorrentes dessas operações sobre os direitos dos titulares;

III – Definir salvaguardas, controles tecnológicos e medidas administrativas para mitigar a probabilidade e o impacto de potenciais incidentes de segurança.

Art. 3º Compete ao Encarregado pelo Tratamento de Dados Pessoais (DPO) da CGM, em conjunto com o Comitê Gestor de Proteção de Dados (CGPD) da CGM:

I – Acompanhar a execução do Plano de Tratamento de Riscos e Salvaguardas constante do RIPD;

II – Avaliar periodicamente a eficácia das medidas mitigadoras implementadas;

III – Orientar os servidores e colaboradores sobre a aplicação prática das salvaguardas definidas no relatório.

Art. 4º A alteração substancial nos sistemas de informação, nos processos de trabalho, no volume de dados coletados, na introdução de novas tecnologias ou a ocorrência de incidentes de segurança relevantes ensejarão a imediata revisão e atualização do RIPD.

Art. 5º O RIPD passará por revisão ordinária a cada 12 (doze) meses, sob coordenação do Encarregado de Dados Pessoais da CGM, devendo a versão atualizada ser submetida à nova aprovação do Controlador-Geral.

Art. 6º O RIPD será disponibilizado no Portal de Transparência do Município, preservadas as informações de caráter sigiloso, segredos industriais, dados estratégicos de segurança da informação e vulnerabilidades técnicas cuja exposição possa comprometer os sistemas municipais.

Art. 7º Esta Portaria entra em vigor na data de sua publicação no Diário Oficial do Município de Niterói.

ANEXO I - Relatório de Impacto à Proteção de Dados Pessoais (RIPD) DA Controladoria-Geral do Município de Niterói (CGM) Histórico de revisões

Data	Versão	Descrição	Autor
06/10/2026	1.0	Primeira versão, elaborada a partir do Inventário de Dados Pessoais – Processo Administrativo número: NIT-050134/000785/2026	Isaque Rodrigues Lopes

1. Objetivo

Este Relatório de Impacto à Proteção de Dados Pessoais (RIPD) é a versão publicável e descreve as operações de tratamento de dados pessoais realizadas no âmbito da Controladoria-Geral do Município de Niterói (CGM) que podem gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD, bem como às liberdades civis e aos direitos fundamentais dos titulares, identificando as medidas, salvaguardas e mecanismos de mitigação de risco adotados.

O relatório abrange o conjunto de 48 processos de trabalho mapeados no ROPA da CGM (Processo nº NIT-050134/000785/2026), com destaque para as operações que concentram os maiores riscos: recepção e encaminhamento de manifestações e denúncias (Ouvidoria-Geral e Departamento de Integridade e Compliance), execução de auditorias internas governamentais (DAG), disponibilização de informações no Portal da Transparência (DGPDT) e rotinas de gestão de pessoas (Gabinete).

2. Identificação dos agentes de tratamento e do encarregado

Papel Identificação

Controlador

Prefeitura Municipal de Niterói

Encarregado Geral de Proteção de Dados
E-mail do Encarregado Geral

Anderson Peixoto de Faria
encarregadogeral.lgpd@controladoria.niteroi.rj.gov.br

Encarregado Suplente de Proteção de Dados

Isaque Rodrigues Lopes

Unidade responsável pela governança

DGPDT — Departamento de Governança, Proteção de Dados e Transparência

Encarregado de Dados Setorial da CGM - Titular

Viviane Soares da Silva

E-mail do Encarregado Setorial

Encarregadosetorial.cgm@controladoria.niteroi.rj.gov

Encarregado de Dados Setorial da CGM - Suplente

Suzana Braga Ferreiro

Operadores

Plataformas externas utilizadas como suporte ao tratamento, entre elas: Fala.BR/e-SIC (plataforma municipal de ouvidoria e acesso à informação), sistema SEI, plataforma Canva, Mailchimp e empresa terceirizada de gestão de estagiários.

3. Necessidade de elaboração do relatório

A elaboração do RIPD da CGM justifica-se pelos seguintes fatores, verificados no ROPA:

1. 9 (nove) das 48 operações mapeadas tratam dados sensíveis — dados de saúde e atestados médicos, origem racial ou étnica, convicção religiosa, opinião política, filiação sindical e dados biométricos —, sobretudo nas denúncias processadas pela Ouvidoria-Geral e pelo DIC, no processo admissional, nos atestados médicos e na execução de auditorias.

2. Os departamentos reconhecem dano potencial de natureza moral, financeira e reputacional nos processos de denúncias e ouvidoria, e dano de gravidade alta nos processos de auditoria governamental e avaliação patrimonial de dirigentes, que envolvem dados fiscais, patrimoniais e de renda;

3. Há tratamento de dados de crianças e adolescentes (certidão de nascimento para cadastro de dependentes no Gabinete) e de titulares em situação de vulnerabilidade perante denúncias (servidores denunciados, manifestantes anônimos e pseudonimizados);

4. A Ouvidoria-Geral registra expressamente que "as medidas de salvaguarda e segurança são limitadas", com controle de acesso restrito a login e senha.

5. As manifestações de ouvidoria são encaminhadas via Fala.BR a órgãos e entidades municipais; dados do Portal da Transparência são publicados em aberto; contratos e dados de fornecedores transitam por sistemas municipais e pelos sistemas eletrônicos da Prefeitura e do TCE/RJ.

4. Descrição do tratamento e do contexto

4.1 Escopo do tratamento

1. Dados de identificação (nome, CPF, RG, CNH, passaporte, título de eleitor), dados de contato, dados profissionais e funcionais (cargo, matrícula, histórico funcional), dados financeiros e patrimoniais (salário, conta bancária, bens declarados, imposto de renda) e dados eletrônicos (IP, logs, cookies);

2. Dados de saúde e atestados médicos, dados biométricos, origem racial ou étnica, convicção religiosa, opinião política e filiação sindical, tratados de forma direta (atestados, admissional, denúncias) ou incidental (documentos auditados, manifestações);

3. Municípios, servidores da CGM e de outros órgãos, estagiários, fornecedores, candidatos a vagas, agentes públicos de alto nível (secretários e dirigentes) e crianças e adolescentes;

4. O tratamento é contínuo. A Ouvidoria-Geral concentra o maior volume, com manifestações diárias por múltiplos canais (WhatsApp, e-mail, Fala.BR, presencial, postal);

5. Armazenamento em sistemas corporativos municipais, nuvem (fornecedores) e arquivos físicos;

6. Não foram identificadas decisões tomadas exclusivamente com base em tratamento automatizado.

4.2 Fluxo típico das operações de maior risco

1. Recepção e encaminhamento de denúncias (Ouvidoria-Geral e DIC): a manifestação é enviada pelo cidadão por WhatsApp, e-mail, Fala.BR, presencialmente ou por carta; é registrada na plataforma e na base de dados; os dados são encaminhados aos órgãos competentes pelo Fala.BR para as devidas tratativas; as respostas conclusivas retornam pelo mesmo canal. Denúncias anônimas e pseudonimizadas exigem tratamento diferenciado da identidade do manifestante. Não há prazo de retenção definido — a unidade declara "guarda permanente no arquivo geral".

2. Auditoria e avaliação patrimonial (DAG): dados chegam por SEI, e-mail e documentos fornecidos pela unidade auditada; são armazenados em sistema corporativo, nuvem e computadores locais; resultados são compartilhados com órgãos auditados e órgãos de controle externo (TCE/RJ). Retenção e descarte não definidos especificamente para o processo.

3. Transparência ativa (DGPDT): publicação, no Portal da Transparência, de dados identificadores, financeiros, patrimoniais, funcionais e logs de acesso, com base legal de cumprimento de obrigação legal, com possível tratamento de dados sensíveis sujeito a guarda de até 100 anos.

4.3 Contexto de relacionamento com os titulares

1. Titulares exercem seus direitos via DGPDT, Fala.BR (Ouvidoria-Geral) e e-SIC; os pedidos de acesso à informação têm guarda prevista de 100 anos conforme a LAI.

5. Partes interessadas consultadas

1. DGPDT — Departamento de Governança, Proteção de Dados e Transparência: central do programa de privacidade, responsável pela condução do levantamento, pelo atendimento a titulares e pelas denúncias sobre LGPD.

2. Unidades mapeadas: DIC, DACE, DCAP, Ouvidoria-Geral (OGM), Assessoria de Comunicação, Gabinete, DGPDT e DAG, que responderam ao formulário de mapeamento no 2º semestre de 2026.

3. Encarregado de dados: responsável pela revisão e homologação deste relatório juntamente com o Comitê Gestor de Proteção de Dados da CGM.

4. Controlador-Geral: responsável pela aprovação final deste relatório por meio de Portaria a ser publicada em Diário Oficial.

6. Necessidade e proporcionalidade

1. A maior parte das unidades declara coletar o estritamente necessário; contudo, algumas admitem excessos — caso do processo de execução de auditorias, no qual o Departamento reconhece que os documentos analisados "podem conter dados pessoais, inclusive sensíveis, que não guardam relação direta com o objeto da auditoria", recomendando-se minimização por ocultação de campos, anonimização ou disponibilização apenas das informações necessárias;

2. Nos processos de consultoria e avaliação processual (DCAP), o setor apenas consulta dados em processos eletrônicos sem manter armazenamento próprio — **prática a ser mantida e registrada como boa referência**;

3. A publicação no Portal da Transparência deve conciliar o dever legal de publicidade com o princípio da necessidade, tarjando dados pessoais que não sejam de publicação obrigatória (ex.: CPF, endereço e dados de dependentes).

7. Garantia dos direitos dos titulares

Direito

Como é garantido

Confirmação de tratamento e acesso aos dados

Via DGPDT, Ouvidoria-Geral, Fala.BR e e-SIC (Lei nº 12.527/2011 e LGPD)

Correção de dados incompletos, inexatos ou desatualizados

Por solicitação à Ouvidoria-Geral e ao DGPDT e correção nos sistemas corporativos

Anonimização, bloqueio ou eliminação de dados desnecessários

Aplicável conforme os prazos de retenção; hoje limitada pela ausência de prazos definidos em várias operações

Portabilidade

Não aplicável na maioria das operações; avaliar caso a caso

Informação sobre compartilhamento

Este RIPD e o ROPA; informar aos titulares os destinatários típicos (órgãos municipais via Fala.BR, TCE/RJ, Portal da Transparência)

Revisão de decisões automatizadas

Não aplicável — não há decisões exclusivamente automatizadas

8. Análise dos riscos

8.1 Escopo, premissas e avaliação dos riscos:

8.1.1 Escopo:

O art. 5º, XVII da LGPD preconiza que o Relatório de Impacto de Proteção de Dados Pessoais (RIPD) deve descrever "medidas, salvaguardas e mecanismos de mitigação de risco. Antes de definir tais medidas, salvaguardas e mecanismos, é necessário identificar os riscos que geram impacto potencial sobre o titular dos dados pessoais. Por este motivo, segue abaixo o Plano de Análise de Riscos, com a metodologia sugerida no presente documento. Para cada risco identificado, define-se: a probabilidade de ocorrência do evento de risco, o possível impacto caso o risco ocorra, avaliando o nível potencial de risco para cada evento. Para fins da presente análise, apenas os riscos ao cumprimento das legislações e melhores práticas da proteção de dados pessoais são considerados. Não serão considerados todos os possíveis riscos de segurança da informação incidentes - até porque a análise deverá incluir o tratamento de dados pessoais que ocorra em documentos físicos e digitais, independentemente do meio em que se encontrem.

8.1.2 Premissas:

A identificação e avaliação de riscos envolvem elencar os eventos de risco, a probabilidade, o impacto e o nível de risco, considerando a realidade específica de cada agente de tratamento. Abaixo, é destacada a análise dos parâmetros escalares que foram utilizados para representar os níveis de probabilidade e impacto que, após a multiplicação, resultarão nos níveis de risco, que direcionarão a aplicação de medidas de segurança. As tabelas abaixo apresentam os critérios de enquadramento e a matriz de Probabilidade x Impacto dos riscos, instrumento de apoio para a definição dos critérios de classificação do nível e priorização de risco:

Impacto	Crítérios
MUITO BAIXO - 1	Acontecimentos que não produzam qualquer desconforto perceptível aos titulares de dados pessoais, sem gerar riscos às liberdades civis e aos direitos fundamentais dos titulares. Dados pessoais anonimizados ou agregados, sem possibilidade de reidentificação.
BAIXO - 2	Acontecimentos que não produzam desconforto significativo aos titulares de dados pessoais, sem gerar riscos às liberdades civis e aos direitos fundamentais dos titulares. Dados pessoais pseudonimizados (desde que a chave para reidentificação do titular também não tenha sido comprometida), dados pessoais de difícil identificação (ex.: endereços IP).
MÉDIO - 3	Acontecimentos que produzam desconforto aos titulares, sem prejuízos financeiros e sem gerar riscos às liberdades civis e aos direitos fundamentais dos titulares. Dados pessoais imediatamente identificáveis (ex.: nome, e-mail, CPF, endereço), combinados, ou não, com informações comportamentais (ex.: histórico de atividades, preferências).
ALTO - 4	Acontecimentos que produzam restrição relevante às liberdades civis e aos direitos fundamentais dos titulares, de difícil reversão, ou prejuízos financeiros significativos. Dados pessoais de crianças, adolescentes ou outras categorias de vulneráveis, dados pessoais sensíveis ou que possam gerar discriminação ao titular.
MUITO ALTO - 5	Acontecimentos que produzam restrição grave e possivelmente irreversível às liberdades civis e aos direitos fundamentais dos titulares, com potencial de dano à vida, à integridade física ou à dignidade da pessoa. Volume elevado de titulares afetados, dados pessoais sensíveis em grande volume ou de crianças, adolescentes ou outras categorias de vulneráveis, ou tratamento enquadrado como de alto risco.

Fonte: Critérios para determinar o impacto dos riscos - <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi-2.0/arquivos/modelo-de-ripd-v1-0-31072026.pdf>

Probabilidade	Crítérios
MUITO BAIXA - 1	Improvável. Acontecimentos que ocorrem, em média, menos de uma vez a cada dois anos.
BAIXA - 2	Pouco provável. Acontecimentos que ocorrem, em média, pelo menos uma vez a cada ano.
MÉDIA - 3	Provável. Acontecimentos que ocorrem, em média, pelo menos uma vez a cada semestre.
ALTA - 4	Muito provável. Acontecimentos que ocorrem, em média, pelo menos uma vez ao mês.
MUITO ALTA - 5	Praticamente certa. Acontecimentos que ocorrem, em média, mais de uma vez ao mês.

Fonte: Critérios para determinar a probabilidade dos riscos - <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi-2.0/arquivos/modelo-de-ripd-v1-0-31072026.pdf>

8.1.3 Nível de Risco

A matriz a seguir apresenta o nível de risco resultante da combinação entre os níveis de impacto e de probabilidade, calculado pela multiplicação entre ambos (Nível de Risco = Impacto x Probabilidade). Cada nível resultante é classificado em uma das quatro faixas a seguir, identificadas na matriz pelas cores correspondentes:

1. Pequeno (níveis 1 a 3) - indicado em verde: risco aceitável, dentro do apetite a risco do órgão ou entidade;
2. Moderado (níveis 4 a 6) - indicado em amarelo: risco aceitável, podendo ser reduzido caso o custo da medida seja proporcional ao benefício esperado;
3. Alto (níveis 8 a 12) - indicado em laranja: risco inaceitável, exigindo a implementação de controles com custo-benefício adequado;
4. Crítico (níveis 15 a 25) - indicado em vermelho: risco inaceitável, exigindo a implementação imediata de controles com custo-benefício adequado.

IMPACTO \ PROBABILIDADE	[1]	[2]	[3]	[4]	[5]
[5]	5	10	15	20	25
[4]	4	8	12	16	20
[3]	3	6	9	12	15
[2]	2	4	6	8	10
[1]	1	2	3	4	5

Fonte: Matriz para determinar o nível de risco - <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi-2.0/arquivos/modelo-de-ripd-v1-0-31072026.pdf>

Resultado da avaliação do risco:

ID	Risco referente ao tratamento de dados pessoais	P	I	N	Aceitável?
R01	Exposição de dados de denunciante anônimos ou pseudonimizados, com risco de retaliação, por falha no controle de identidade nos encaminhamentos via Fala.BR	4	5	20	Não
R02	Vazamento ou uso indevido de registros fotográficos e arquivos mantidos em dispositivos privados de servidores e em cópias na nuvem	2	4	8	Não
R03	Publicação excessiva de dados pessoais no Portal da Transparência, incluindo dados sensíveis e de dependentes (crianças e adolescentes), sem tarjamento adequado	2	5	10	Não
R04	Retenção indefinida de dados ("guarda permanente", "não definido") em violação ao princípio da necessidade e ao art. 16 da LGPD, aumentando a superfície de ataque	5	5	25	Não
R05	Vazamento de dados fiscais, patrimoniais e sensíveis incidentais durante auditorias e avaliação patrimonial de dirigentes, com dano reconhecido como de gravidade alta	2	5	10	Não
R06	Quebra de sigilo em rotinas de gestão de pessoas (atestados médicos, folha de ponto, férias) com armazenamento híbrido físico e digital e chaves físicas	2	3	6	Com monitoramento
R07	Indisponibilidade de dados essenciais por inexistência de plano de contingência e backups uniformes entre unidades	2	3	6	Com monitoramento

Medidas para tratamento dos riscos

ID	Medidas propostas	Prazo sugerido
R01	Instituir fluxo padrão de anonimização na origem das denúncias anônimas/pseudonimizadas; limitar a identidade do manifestante ao eventual necessário para respostas conclusivas	Imediato

R02	Proibir armazenamento em dispositivos privados; instituir repositório institucional único com backup	Curto prazo (90 dias)
R03	Revisar rotinas de publicação com tarjamento de dados não obrigatórios (CPF, endereço, dados de dependentes); alinhar à regulamentação de transparência e à proteção reforçada de crianças e adolescentes (art. 14, LGPD)	Curto prazo (90 dias)
R04	Definir tabela de temporalidade aplicável a cada operação e rotina de descarte seguro; rever a prática de "guarda permanente"	Médio prazo (180 dias)
R05	Restringir papéis de trabalho de auditoria ao necessário; ocultar ou anonimizar dados irrelevantes ao objeto; tramitar apenas por SEI com restrição de acesso	Imediato
R06/R07	Uniformizar controles mínimos (login individual, pasta restrita, armário trancado, backup institucional); elaborar plano de resposta a incidentes alinhado à Resolução CD/ANPD nº 15/2024	Médio prazo (180 dias)

9. Aprovação e revisão

Este RIPD deve ser formalmente aprovado pelo Controlador-Geral e pelo encarregado pelo tratamento de dados pessoais da CGM. O relatório será revisado, no mínimo, anualmente ou sempre que ocorrer alteração relevante nas operações de tratamento, nova introdução de tecnologia, mudança normativa ou ocorrência de incidente significativo.

Portaria nº 22/CGM/2026 - Aprova o Plano de Resposta a Incidentes de Dados Pessoais (PRIS) no âmbito da Controladoria-Geral do Município de Niterói e dá outras providências.

O **CONTROLADOR-GERAL DO MUNICÍPIO DE NITERÓI**, no uso das suas atribuições legais e regimentais que lhe são conferidas pela legislação municipal em vigor, e

CONSIDERANDO o disposto na Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), especialmente em seu art. 48, que estabelece o dever do controlador de comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares;

CONSIDERANDO a Resolução CD/ANPD nº 15, de 24 de abril de 2024, que aprova o Regulamento de Comunicação de Incidente de Segurança e define os parâmetros para avaliação de risco ou dano relevante;

CONSIDERANDO o Acórdão nº 003931/2025-PLENV do Tribunal de Contas do Estado do Rio de Janeiro (TCE-RJ), que determina a adoção de medidas de governança e segurança da informação no tratamento de dados pessoais;

CONSIDERANDO o disposto no Decreto Municipal nº 271, de 2025, do Município de Niterói, que regulamenta a aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) no âmbito do Poder Executivo Municipal e estabelece expressamente a obrigatoriedade de elaboração e implementação de um Plano de Resposta a Incidentes de Segurança em todos os órgãos e entidades municipais;

CONSIDERANDO a necessidade de estabelecer procedimentos céleres e padronizados para identificar, conter, avaliar, comunicar e tratar incidentes de segurança da informação e de privacidade no âmbito da Controladoria-Geral do Município de Niterói (CGM);

RESOLVE:

Art. 1º Fica aprovado o **Plano de Resposta a Incidentes de Dados Pessoais (PRIS)** da Controladoria-Geral do Município de Niterói (CGM), na forma do **Anexo Único** desta Portaria.

Art. 2º O PRIS tem como objetivo proteger os direitos dos titulares e mitigar os impactos de eventos que comprometam a confidencialidade, a integridade ou a disponibilidade de dados pessoais custodiados pela CGM, em documentos físicos, sistemas corporativos, processos administrativos, correio eletrônico, equipamentos e demais serviços utilizados pela Controladoria.

Art. 3º As disposições do Plano de Resposta a Incidentes de Dados Pessoais (PRIS) aplicam-se a todos os servidores, empregados públicos, ocupantes de cargos em comissão, estagiários, colaboradores, prestadores de serviços e fornecedores que, em nome da CGM-Niterói, realizem o tratamento de dados pessoais.

Art. 4º Para os fins do disposto nesta Portaria, considera-se incidente de segurança qualquer evento adverso, confirmado ou sob suspeita, que resulte em violação de segurança da informação, tal como, mas não limitado a:

- I - Envio de documentos com dados pessoais a destinatário indevido;
- II - Divulgação de informações pessoais ou sigilosas em relatório ou processo público;
- III - Perda ou furto de equipamentos e documentos;
- IV - Acesso indevido a sistemas, pastas ou contas institucionais;
- V - Sequestro (ransomware), alteração, destruição ou indisponibilidade de dados; e
- VI - Exposição da identidade de denunciante ou de informações protegidas por sigilo no âmbito das apurações da CGM.

Art. 5º Fica constituído, em caráter permanente, o Comitê de Resposta a Incidentes, que será acionado imediatamente após a detecção de uma suspeita de incidente, composto pelos seguintes membros titulares:

- I - Controlador-Geral do Município;
- II - Representante do Departamento de Governança, Proteção de Dados e Transparência (DGPDT);
- III - Encarregado pelo Tratamento de Dados Pessoais (DPO) da CGM;
- IV - Representante da área de Tecnologia da Informação (TI) que apoie à CGM; e
- V - Representante do Departamento diretamente afetado pelo incidente.

Parágrafo Único. O Comitê de Resposta a Incidentes (CRI) deverá se reunir, em caráter emergencial, em até 02 (duas) horas após o acionamento para coordenar as ações de contenção e deliberação.

Art. 6º Compete ao Encarregado pelo Tratamento de Dados Pessoais (DPO):

- I - Orientar a avaliação técnica dos impactos aos titulares;
- II - Conduzir a interlocução oficial com a Autoridade Nacional de Proteção de Dados (ANPD) e com os titulares afetados, em nome do Controlador de dados; e
- III - Assegurar que as comunicações legais sejam realizadas nos prazos estipulados pela Resolução CD/ANPD nº 15/2024.

Art. 7º Qualquer pessoa submetida a esta Portaria que tome conhecimento de um possível incidente de segurança deverá reportar o fato imediatamente à sua chefia imediata e ao Departamento de Governança, Proteção de Dados e Transparência (DGPDT), preferencialmente por meio do canal institucional de correio eletrônico, abstendo-se de compartilhar informações detalhadas do evento em grupos não oficiais, aplicativos de mensagens de uso pessoal ou publicamente.

Art. 8º É expressamente vedado, em caso de suspeita ou confirmação de incidente, antes da devida orientação técnica da área de TI:

- I - Apagar mensagens, registros de acesso (logs) ou arquivos relacionados ao incidente;
- II - Formatar equipamentos ou executar intervenções técnicas por conta própria; e
- III - Encaminhar os dados expostos a contas pessoais ou canais não autorizados para fins de arquivamento.

Art. 9º Todos os incidentes, inclusive aqueles que, após avaliação fundamentada, não demandarem notificação à ANPD ou aos titulares, deverão ser rigorosamente registrados e documentados em processo administrativo sigiloso, cujos autos deverão ser preservados pelo prazo mínimo de 5 (cinco) anos.

Art. 10. O Departamento de Governança, Proteção de Dados e Transparência (DGPDT) deverá, no prazo de até 45 (quarenta e cinco) dias contados da publicação desta Portaria, promover capacitação específica sobre as diretrizes deste Plano a todos os servidores e fornecedores envolvidos.

Art. 11. O Plano de Resposta a Incidentes de Dados Pessoais (PRIS) será submetido a exercícios de simulação em até 60 (sessenta) dias após a sua aprovação, e posteriormente avaliado e revisado anualmente, ou sempre que ocorrer um incidente relevante.

Art. 12. Esta Portaria entra em vigor na data de sua publicação.

ANEXO I - PLANO DE RESPOSTA A INCIDENTES DE DADOS PESSOAIS (PRIS)

A finalidade deste Plano é estabelecer procedimentos para identificar, conter, avaliar, comunicar e tratar incidentes envolvendo dados pessoais no âmbito da CGM, como medida de governança em apoio ao atendimento à Lei Geral de Proteção de Dados, ao Decreto Municipal nº 271/2025 e ao Acórdão nº 003931/2025-PLENV do TCE-RJ.

1. Objetivo e abrangência

Proteger os direitos dos titulares e reduzir os impactos de eventos que comprometam a confidencialidade, a integridade ou a disponibilidade de dados pessoais, em documentos físicos, sistemas, processos administrativos, correio eletrônico, equipamentos e serviços utilizados pela CGM.

O plano abrange servidores, colaboradores, prestadores de serviços e fornecedores que tratam dados pessoais nas atividades da Controladoria, incluindo auditorias, procedimentos correcionais, manifestações de ouvidoria e demais atividades aplicáveis.

São exemplos de incidentes:

- a) Envio de documentos com dados pessoais a destinatário indevido;