

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;

- b) Divulgação de informações pessoais ou sigilosas em relatório ou processo público;
 c) Perda ou furto de equipamentos e documentos;
 d) Acesso indevido a sistemas, pastas ou contas institucionais;
 e) Sequestro, alteração, destruição ou indisponibilidade de dados; e
 f) Exposição de identidade de denunciante ou de informações protegidas por sigilo.

2. Responsáveis e atribuições

A aprovação do plano deverá identificar quem atua como controlador em cada tratamento, considerando a organização municipal; não se presume que a CGM ou o encarregado exerçam essa função isoladamente.

Responsável proposto	Atribuições
CGM	Assegurar recursos, decidir medidas institucionais e garantir o cumprimento das obrigações de comunicação.
DGPDT	Acionar os envolvidos, manter a cronologia, coordenar providências e acompanhar os prazos.
Encarregado pelo tratamento de dados pessoais	Orientar a avaliação dos impactos aos titulares e conduzir a interlocução com a ANPD e os titulares, em nome do controlador, conforme suas atribuições.
TI	Conter o incidente, preservar evidências técnicas, investigar causas e recuperar os serviços.
Departamento da CGM afetado	Identificar os processos, documentos, dados e titulares envolvidos; executar medidas administrativas.
DCAP	Apoiar a análise das obrigações legais, do sigilo e da fundamentação das decisões.
ASCOM	Apoiar a elaboração de mensagens claras, sem divulgar dados pessoais ou informações protegidas.
Servidores e fornecedores	Reportar imediatamente suspeitas e colaborar com a apuração, sem destruir evidências.

Deverão ser designados titulares e substitutos, com contatos atualizados e forma de acionamento emergencial.

3. Fluxo operacional de resposta

Identificação → Registro e acionamento → Contenção → Avaliação de risco → Comunicação, quando exigida → Recuperação → Encerramento e melhoria.

As etapas podem ocorrer simultaneamente. A investigação completa não é condição para realizar a comunicação legalmente exigida.

Etapas	Providências	Responsáveis propostos	Prazo ou referência
1. Identificar e reportar	Comunicar a suspeita pelo canal institucional (e-mail), indicando o ocorrido, o horário, os sistemas ou documentos envolvidos e as medidas já adotadas.	Pessoa que identificou o evento; Chefia	Imediatamente após a identificação.
2. Registrar e acionar	Abrir registro com identificador único; anotar a data da ocorrência, quando conhecida, da detecção e do conhecimento pelo controlador de que dados pessoais foram afetados; acionar coordenação, TI e encarregado.	Comitê de Resposta a Incidentes (CRI)	Imediatamente; meta interna proposta de até 2 horas para o acionamento.
3. Conter e preservar	Restringir acessos, suspender compartilhamentos, revogar credenciais ou isolar equipamentos, conforme orientação técnica; preservar registros e documentos.	TI e departamento afetado	Início imediato, conforme a criticidade.
4. Avaliar impactos	Identificar categorias de dados, titulares, extensão, consequências possíveis e necessidade de comunicação. Registrar a fundamentação.	Encarregado, TI, departamento afetado e apoio jurídico	Avaliação inicial proposta em até 24 horas, sem ultrapassar os prazos legais.
5. Comunicar	Encaminhar comunicações à ANPD e aos titulares quando houver risco ou dano relevante; guardar protocolos e comprovações.	Controlador, por meio do encarregado de tratamento de dados	Conforme os prazos legais descritos na seção 5.
6. Corrigir e recuperar	Eliminar a causa, corrigir vulnerabilidades, restaurar dados e validar a segurança antes de retomar os serviços.	TI e departamento afetado	Conforme plano técnico documentado.
7. Encerrar e melhorar	Consolidar relatório, registrar consequências, medidas corretivas, responsáveis e pendências; atualizar controles e capacitação.	Coordenação e autoridade competente	Proposta: relatório em até 10 dias úteis após a estabilização.

Cuidados imediatos

- a) Não apagar mensagens, registros de acesso ou arquivos relacionados ao incidente.
 b) Não formatar equipamentos nem executar intervenções sem orientação técnica.
 c) Não encaminhar dados expostos a grupos, contas pessoais ou canais não autorizados.
 d) Não realizar divulgação pública por iniciativa individual.
 e) Restringir o acesso às evidências às pessoas necessárias à resposta, mantendo registro de sua coleta e movimentação.

4. Avaliação de risco ou dano relevante

A avaliação deverá considerar as consequências possíveis para as pessoas, e não apenas o impacto nos sistemas.

Segundo a Resolução CD/ANPD nº 15/2024, o incidente pode acarretar risco ou dano relevante quando puder afetar significativamente interesses e direitos fundamentais e, **cumulativamente**, envolver pelo menos um dos seguintes critérios:

- a) Dados pessoais sensíveis;
 b) Dados de crianças, adolescentes ou idosos;
 c) Dados financeiros;
 d) Dados de autenticação em sistemas;
 e) Dados protegidos por sigilo legal, judicial ou profissional; e
 f) Dados tratados em larga escala.

Entre os possíveis impactos estão discriminação, fraude, roubo de identidade, danos à reputação, violação da integridade física ou impedimento de exercer direitos e utilizar serviços. A exposição de denunciantes ou de pessoas envolvidas em procedimentos sigilosos merece análise especialmente cuidadosa. **A decisão de comunicar ou de não comunicar deverá ser fundamentada e registrada.** A inexistência de dano já comprovado não afasta a obrigação quando houver possibilidade de risco ou dano relevante.

5. Estabelecimento de procedimento de comunicação à ANPD e aos titulares

A CGM deverá instituir e submeter à aprovação da autoridade competente procedimento formal, integrado à governança municipal de proteção de dados, para avaliar e comunicar incidentes de segurança que possam acarretar risco ou dano relevante aos titulares, nos termos do art. 48 da LGPD e da Resolução CD/ANPD nº 15/2024. O procedimento deverá identificar o controlador responsável, o encarregado ou representante constituído, seus substitutos, os canais de comunicação e os responsáveis pela elaboração e envio das informações, assegurando a comunicação à ANPD e aos titulares em até **três dias úteis contados do conhecimento pelo controlador de que o incidente afetou dados pessoais**, ressalvada, para a comunicação à ANPD, a existência de prazo previsto em legislação específica. Deverá prever comunicação inicial à ANPD com as informações disponíveis e complementação fundamentada em até **vinte dias úteis da comunicação inicial**, sem aguardar a conclusão da investigação; comunicação aos titulares em linguagem simples, direta e individualizada sempre que possível; divulgação ampla por pelo menos

três meses quando a comunicação individual for inviável ou os titulares não puderem ser identificados; e guarda dos protocolos, comprovações e decisões em registro de acesso controlado.

5.1. Comunicação à ANPD

O encarregado ou representante legalmente constituído deverá utilizar o **procedimento oficial de peticionamento eletrônico na ANPD**, com formulário e comprovação de representação, conforme as orientações da Autoridade.

A comunicação deverá contemplar:

- Identificação do controlador, do encarregado ou representante e do operador, quando aplicável.
- Descrição do incidente, datas de ocorrência e conhecimento e causa, se identificada.
- Natureza e categorias de dados afetados.
- Número de titulares afetados, discriminando crianças, adolescentes e idosos quando aplicável.
- Total de titulares cujos dados são tratados nas atividades afetadas.
- Riscos e possíveis impactos aos titulares.
- Medidas de proteção existentes e medidas adotadas após o incidente.
- Providências para reverter ou mitigar os efeitos.
- Justificativa de eventual atraso.

As informações ainda não disponíveis deverão ser identificadas e posteriormente complementadas, de maneira fundamentada, no prazo regulamentar. Informações protegidas por lei deverão receber tratamento adequado, com solicitação fundamentada de sigilo à ANPD quando cabível.

5.2. Comunicação aos titulares

A mensagem deverá informar, em linguagem simples:

- Quais categorias de dados foram afetadas.
- A data em que o incidente se tornou conhecido.
- Os riscos e possíveis consequências.
- As medidas de segurança e de mitigação adotadas.
- Recomendações de proteção, quando cabíveis.
- O canal para esclarecimentos e o contato do encarregado, quando aplicável.
- A justificativa de eventual atraso.

A comunicação deverá ser direta e individualizada, quando possível, por canal usual de contato com o titular. Não deverá revelar dados de terceiros, identidades de denunciante ou detalhes técnicos que ampliem a vulnerabilidade.

O encarregado deverá juntar ao processo de comunicação à ANPD **declaração de que os titulares foram comunicados, indicando os meios utilizados, em até três dias úteis contados do término do prazo regulamentar para comunicação aos titulares**.

6. Registro e documentação

Cada incidente, **inclusive aquele não comunicado à ANPD e aos titulares**, deverá possuir registro contendo:

- Identificador e cronologia do evento.
- Descrição e circunstâncias.
- Dados e titulares envolvidos.
- Avaliação de risco e consequências possíveis.
- Medidas de contenção, correção e recuperação.
- Evidências preservadas e responsáveis por sua guarda.
- Fundamentação da decisão de comunicar ou não comunicar.
- Comunicações, protocolos e comprovações.
- Causas identificadas e ações preventivas.
- Aprovação do encerramento e pendências de acompanhamento.

Os registros dos incidentes deverão ser mantidos por **no mínimo cinco anos**, observadas outras obrigações aplicáveis de guarda documental e as restrições de acesso.

7. Implantação e acompanhamento do PRIS:

Determinação/Recomendação — medida de atendimento proposta	O que fazer	Como fazer	Quem vai fazer	Quando fazer
Formalização da resposta a incidentes	Aprovar o plano e definir responsabilidades	Registrar em processo administrativo e editar ato competente, com titulares e substitutos	Controlador-Geral e encarregado da CGM	Até 15 dias
Organização do acionamento	Instituir canal interno e fluxo emergencial	Definir contatos, escalonamento e formulário de registro	CGM e TI	Até 15 dias
Comunicação à ANPD e aos titulares	Aprovar procedimento e modelos de comunicação	Preparar formulários, comprovar representação e organizar acesso ao canal oficial	Controlador, encarregado e apoio jurídico	Até 30 dias
Preparação das equipes	Capacitar servidores e fornecedores envolvidos	Realizar orientação e exercício com caso fictício	Encarregado e TI	Até 45 dias
Teste e melhoria	Verificar o funcionamento do Plano	Simular incidente, medir tempos, registrar falhas e corrigir o fluxo	Coordenação de resposta	Até 60 dias; depois, revisão anual e após incidentes relevantes

FUNDAÇÃO MUNICIPAL DE SAÚDE
Atos da Presidente
PROCESSO SELETIVO PÚBLICO SIMPLIFICADO
EDITAL 005/2025
CONTRATAÇÃO XI

A Presidente da FUNDAÇÃO MUNICIPAL DE SAÚDE, através da Superintendência de Gestão do Trabalho e Educação em Saúde, informa que se encontra disponível no Sítio Eletrônico www.saude.niteroi.rj.gov.br a convocação para contratação dos candidatos habilitados no Processo Seletivo Público Simplificado, Edital N° 005/2025, para atuarem na Rede Especializada Ambulatorial vinculada à Vice-Presidência de Atenção Coletiva, Ambulatorial e da Família (VIPACAF), com vistas a atender à necessidade temporária de excepcional interesse público da Fundação Municipal de Saúde de Niterói.

Os candidatos habilitados deverão apresentar os documentos solicitados, nos moldes item 7.4 do Edital, na Superintendência de Gestão do Trabalho e Educação em Saúde, situada à Avenida Ernani do Amaral Peixoto, 286 – 5° andar – Centro – Niterói – RJ, sendo imprescindível a observância do disposto nos itens 7.5 e 7.11 do instrumento convocatório para a garantia da efetivação das contratações

Inscrição	Nome do Cargo	Nome do Profissional	Data e horário para assinatura do contrato
00040	Generalista	GABRIELA ARAUJO BRUZZI DE SOUZA LIMA	27/10/2026 às 13:00h
00057	Reumatologista	ISIS REIS CARVALHO	27/10/2026 às 13:00h

SUPERINTENDÊNCIA DE GESTÃO DO TRABALHO E EDUCAÇÃO EM SAÚDE – SUGETE