



PROCEDIMENTO DE COMUNICAÇÃO DE INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

Alinhado ao Plano de Resposta a Incidentes de Segurança (PRIS) da CGM-Niterói

Atenção: A comunicação ao titular jamais deve revelar dados de terceiros ou detalhes de vulnerabilidade técnica do sistema da prefeitura

1. OBJETIVO

Estabelecer o fluxo, os prazos e as responsabilidades para a comunicação de incidentes de segurança com dados pessoais à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares dos dados, em conformidade com o art. 48 da LGPD, o Decreto Municipal nº 271/2025 e a Resolução CD/ANPD nº 15/2024.

2. ABRANGÊNCIA E INTEGRAÇÃO

Este procedimento é parte integrante do Plano de Resposta a Incidentes de Segurança (PRIS) da Controladoria-Geral do Município de Niterói (CGM). Ele é acionado exclusivamente *após* a etapa de "Avaliação de Impactos" do fluxo operacional do PRIS, quando se constata a ocorrência de um incidente que possa acarretar **risco ou dano relevante aos titulares**.

3. CRITÉRIOS DE AVALIAÇÃO (RISCO OU DANO RELEVANTE)

A decisão de comunicar ou não a ANPD e os titulares será fundamentada pela Equipe de Resposta a Incidentes (comitê) sob a orientação do Encarregado de Dados Setorial da CGM (DPO). O incidente será considerado de comunicação obrigatória quando afetar significativamente direitos fundamentais e envolver:

- a. Dados pessoais sensíveis;
- b. Dados de crianças, adolescentes ou idosos;
- c. Dados financeiros ou de autenticação (senhas/credenciais);
- d. Dados protegidos por sigilo legal (ex.: identidade de denunciante à CGM);
- e. Dados tratados em larga escala.

A decisão de não comunicar também deve ser documentada em relatório técnico.



4. FLUXO DE COMUNICAÇÃO À ANPD

a. Prazo: Até 3 (três) dias úteis, contados do conhecimento pelo Controlador de que o incidente afetou dados pessoais.

b. Responsável: O Encarregado pelo Tratamento de Dados Pessoais (DPO) da CGM, atuando como representante do Controlador-Geral.

c. Canal: Peticionamento Eletrônico exclusivo via sistema SEI! da ANPD, utilizando formulário próprio disponibilizado pela autoridade;

d. Conteúdo de Comunicação Inicial (mínimo obrigatório);

1. Identificação do Controlador (CGM-Niterói), do DPO e do Operador (se houver);
2. Descrição resumida do incidente e data do conhecimento;
3. Natureza e categoria dos dados afetados (discriminando vulneráveis);
4. Riscos e possíveis impactos identificados para os titulares;
5. Riscos e possíveis impactos identificados para os titulares;
6. Medidas de contenção e segurança já adotadas.

e. Comunicação Complementar: Caso as informações de comunicação inicial sejam insuficientes por conta da investigação técnica em curso, o DPO terá até 20 (vinte) dias úteis (contados da comunicação inicial) para encaminhar a complementação fundamentada à ANPD.

5. FLUXO DE COMUNICAÇÃO AOS TITULARES DE DADOS

a. Prazo: O mais rápido possível (em regra, acompanhando o prazo de 3 dias úteis da ANPD), de forma que os titulares possam adotar medidas para se proteger (ex.: trocar senhas, bloquear cartões);

b. Responsáveis: Departamento de Governança, Proteção de Dados e Transparência (DGPDT), com apoio da Assessoria de Comunicação (ASCOM);

c. Canal: Comunicação direta e individualizada. Caso a identificação individual seja inviável ou exija esforço desproporcional, a comunicação será feita por **ampla divulgação** no site oficial e mídias do município, mantida por no mínimo 3 (três) meses;

d. Conteúdo da Mensagem (Linguagem Simples e Clara):

- i. O que aconteceu e a data do conhecimento do incidente;
- ii. Quais categorias de dados específicos do titular foram expostas;
- iii. Os riscos gerados e as possíveis consequências;
- iv. As medidas de contenção tomadas pela CGM-Niterói;

- v. Recomendações práticas para o titular se proteger de fraudes;
- vi. Canais de contato direto com o DPO para dúvidas (e-mail institucional e ramal).

6. DOCUMENTAÇÃO E COMPROVAÇÃO

- a. O Encarregado de Dados Setorial (DPO) deverá juntar aos autos do processo de resposta ao incidente as cópias dos protocolos de peticionamento na ANPD.
- b. O DPO deverá emitir uma declaração formal, no processo da ANPD, atestando que os titulares foram comunicados (ou justificando a comunicação pública), em até 3 dias úteis após o encerramento da fase de comunicação.
- c. Todos os registros da decisão de comunicação, ofícios e comprovantes deverão ser mantidos arquivados pela CGM em processo com acesso restrito/sigiloso pelo prazo mínimo de 5 (cinco) anos.

7. FLUXO PRÁTICO

a. Identificação e Gatilho (Decisão)

→ Incidente confirmado com **risco ou dano relevante** aos titulares de dados (após avaliação do DPO e Comitê).

b. Comunicação à ANPD

→ **Prazo:** Até 3 dias úteis

→ **Responsável:** Encarregado de Dados (DPO)

→ **Canal:** Peticionamento via sistema SEI da ANPD

→ **Conteúdo:** Resumo do incidente, tipos de dados afetados, volume de titulares, riscos e medidas de contenção.

c. Comunicação aos Titulares de Dados

→ **Prazo:** O mais rápido possível (em regra, paralelo aos 3 dias da ANPD)

→ **Responsáveis:** DGPDT com apoio da ASCOM

→ **Canal:** E-mail/mensagem direta ou, se inviável, aviso no site oficial (por 3 meses)

→ **Conteúdo:** O que ocorreu, dados expostos, riscos, medidas adotadas, dicas de proteção ao usuário e contato do DPO.

d. Complementação de Informações (se necessário)

→ **Prazo:** Até 20 dias úteis após a comunicação inicial

→ **Ação:** Envio de laudos técnicos e detalhes adicionais à ANPD decorrentes do avanço da investigação

e. Documentação e Encerramento

→ **Ação:** Emitir declaração da ANPD atestando que os titulares foram comunicados

→ **Guarda:** Arquivar todo o processo de resposta e comprovantes sob acesso restrito por, no mínimo, 5 anos.



8. PROCEDIMENTOS PARA COMUNICAÇÃO À ANPD



https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis

Acesso ao Sistema de Peticionamento: O processo é estritamente digital. Acesse o sistema de Peticionamento Eletrônico (SEI) disponibilizado no portal da ANPD ou a plataforma **gov.br** utilizando uma conta com nível de segurança Prata ou Ouro. Caso seja o primeiro acesso no SEI da ANPD, realize o cadastro como "Usuário Externo".

Seleção do Tipo de Processo: Dentro do sistema, inicie um novo processo e selecione a opção específica para "Comunicação de Incidente de Segurança (CIS)".

Preenchimento do Formulário Oficial: Faça o download ou preencha diretamente no sistema o "Formulário de Comunicação de Incidente de Segurança com Dados Pessoais". Você deverá classificar a comunicação como:

- a. Completa:** Quando todas as informações já estão disponíveis.
- b. Preliminar:** Quando a investigação ainda está em curso e informações adicionais serão enviadas posteriormente.
- c. Complementar:** Quando for enviar os dados que faltaram na comunicação preliminar.

Inclusão das Informações Obrigatórias: Preencha o formulário detalhando de forma objetiva:

- a.** Identificação completa do Controlador de Dados e do Encarregado de Dados Setorial da CGM (DPO);
- b.** Data e hora da ocorrência do incidente e da sua descoberta;
- c.** Descrição do incidente (ex: ataque ransomware, vazamento interno, perda de equipamento);
- d.** Natureza e volume dos dados afetados (ex: dados de saúde, financeiros, credenciais) e o número estimado de titulares atingidos;
- e.** Identificação de riscos e possíveis danos aos titulares (ex: fraudes financeiras, roubo de identidade);
- f.** Medidas de segurança técnicas e administrativas que foram implementadas para conter e reverter o incidente.



Anexação de Evidências e Relatórios: Junte ao processo os documentos de suporte, como relatórios de TI, logs de auditoria, laudos forenses e, fundamentalmente, a **comprovação de que os titulares foram comunicados** (cópias de e-mails, prints de avisos no site ou comunicados à imprensa).

Assinatura e Envio (Atenção aos Prazos): Assine o documento eletronicamente no sistema e conclua o envio.

a. Comunicação Preliminar/Completa: Deve ser protocolada em até **3 (três) dias úteis**, contados a partir do momento em que o Controlador tomou conhecimento do incidente;

b. Comunicação Complementar: Deve ser enviada em até **20 (vinte) dias úteis**, contados a partir da data de comunicação inicial, caso a primeira tenha sido preliminar.

Acompanhamento: Após o envio, guarde o Número Único de Protocolo (NUP) gerado para acompanhar o andamento do processo e atender a possíveis requisições adicionais de informações por parte da ANPD.



GLOSSÁRIO

- **ANPD (Autoridade Nacional de Proteção de Dados):** Órgão da administração pública federal responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.
- **ASCOM (Assessoria de Comunicação):** Setor responsável pela gestão da comunicação interna e externa, assessoria de imprensa e publicação de notas oficiais do órgão público.
- **CGM (Controladoria-Geral do Município):** Órgão central de controle interno do Município de Niterói, responsável pela governança, transparência e proteção de dados no âmbito do município.
- **DGPDT (Departamento de Governança, Proteção de Dados e Transparência):** Unidade da CGM encarregada da gestão técnica e estratégica de governança e adequação à proteção de dados pessoais.
- **LGPD (Lei Geral de Proteção de Dados Pessoais - Lei nº 13.709/2018):** Legislação brasileira que regula as atividades de tratamento de dados pessoais por pessoas físicas ou jurídicas, públicas ou privadas.
- **NUP (Número Único de Protocolo):** Código numérico gerado em sistemas públicos de instrução processual (como o SEI) para identificar e rastrear individualmente cada processo administrativo.



- **PRIS (Plano de Resposta a Incidentes de Segurança):** Documento normativo que estabelece procedimentos operacionais padrão para detectar, responder, conter e mitigar as consequências de incidentes de segurança da informação.
- **SEI (Sistema Eletrônico de Informações):** Plataforma digital utilizada por órgãos públicos para criação, instrução, trâmite e peticionamento eletrônico de processos administrativos.
- **CIS (Comunicação de Incidente de Segurança):** Notificação formal enviada à ANPD e/ou aos titulares reportando a ocorrência de um evento adverso que comprometa a segurança de dados pessoais.
- **Controlador:** Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (no contexto, a CGM-Niterói).
- **Operador:** Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador (ex.: fornecedores contratados de software ou serviços de nuvem).
- **Encarregado pelo Tratamento de Dados Pessoais (DPO - Data Protection Officer):** Pessoa indicada pelo Controlador para atuar como canal de comunicação entre o órgão, os titulares e a ANPD, referindo-se, no âmbito deste procedimento, ao DPO desta Controladoria.
- **Titular dos Dados:** Pessoa natural (física) a quem se referem os dados pessoais que são objeto de tratamento.
- **Dados Pessoais:** Informação relacionada a pessoa natural identificada ou identificável (ex.: nome, CPF, e-mail).
- **Dados Pessoais Sensíveis:** Dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico.

