

P R E F E I T U R A



RIO

Rio-Águas

Plano de Resposta às Petições dos Titulares de Dados Pessoais PRPTDP



Fundação Instituto das Águas do Município do
Rio de Janeiro - (Rio-Águas)

Novembro/2025

Assinado com senha por DANIEL BICALHO HOEFLE - ASSISTENTE I / 50543 - 05/11/2025 às 12:11:21, SIMONE PESSANHA RAMOS - ASSISTENTE I / 44009 - 05/11/2025 às 12:31:31, FELIPE CHALLUB MARTINS - ASSESSOR III / 44010 - 05/11/2025 às 12:45:23, REINALDO PINHO DA SILVEIRA - ASSISTENTE I / 47923 - 05/11/2025 às 14:51:00, BIANCA DA SILVA BALDEZ - ASSISTENTE I / 45080 - 05/11/2025 às 14:51:44, ADRIANA LUCIA NINIO - ASSISTENTE I / 44007 - 05/11/2025 às 16:42:34, WILMAR BARBOSA FERNANDES LOPES - ASSESSOR CHEFE / 50543 - 05/11/2025 às 16:43:21, ALEXANDRE FERREIRA REIS - ASSESSOR CHEFE I / 52200 - 05/11/2025 às 16:47:42, ANDREI RAYBOLT DOS SANTOS - ASSISTENTE I / 45074 - 05/11/2025 às 17:36:06, DEBORAH RAMOS DOMINGUES CARNEIRO - ASSISTENTE I / 49008 - 06/11/2025 às 09:31:59 e ELISABETE CRISTINA GONCALVES NOGUEIRA - ASSESSOR III / 49669 - 06/11/2025 às 15:47:49.
Documento Nº: 12783565-5865 - consulta à autenticidade em
<https://acesso.processo.rio/sigaex/public/app/autenticar?n=12783565-5865>



AGUCAP202507866A

SIGA

Introdução

O exercício dos direitos dos titulares de dados pessoais é um dos pilares da Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD). Tais direitos asseguram transparência, controle e autodeterminação informativa aos cidadãos, permitindo-lhes solicitar informações sobre o tratamento de seus dados pessoais, requerer correção, anonimização, exclusão, portabilidade ou ainda questionar a forma como suas informações são utilizadas.

As petições podem abranger desde simples pedidos de esclarecimento até demandas complexas que envolvem múltiplos sistemas e áreas administrativas. Assim, o atendimento adequado e tempestivo dessas solicitações requer procedimentos padronizados, comunicação clara e articulação entre o Encarregado de Dados e os setores competentes da Fundação Rio-Águas.

Deve-se destacar que o **direito de petição é pessoal e intransferível**, podendo ser exercido apenas pelo próprio titular ou por seu representante legal, mediante comprovação de legitimidade. Não são admitidos pedidos anônimos ou de terceiros não autorizados.

O descumprimento dos prazos legais ou a ausência de resposta adequada pode caracterizar infração administrativa, comprometendo a credibilidade institucional e a conformidade com a LGPD. Assim, é essencial dispor de um plano que estabeleça o fluxo completo de recebimento, análise, encaminhamento, resposta e registro das petições, assegurando rastreabilidade e *accountability*.

Neste contexto, o presente **Plano de Resposta às Petições dos Titulares de Dados Pessoais (PRPTDP)** define as diretrizes e os procedimentos para garantir que as solicitações dos titulares sejam tratadas de maneira eficiente, transparente e dentro dos prazos estabelecidos pela legislação, reforçando o compromisso da Fundação Rio-Águas com a proteção de dados pessoais e a governança em privacidade.

Objetivos

Geral

Estabelecer um processo estruturado, padronizado e rastreável para o **recebimento, análise e resposta às petições de titulares de dados pessoais**, garantindo atendimento dentro dos prazos legais, comunicação transparente e registro documental de todas as etapas do processo.



Específicos

- Assegurar o **cumprimento dos prazos** previstos na LGPD (15 dias, prorrogáveis uma única vez por igual período, mediante justificativa).
- Garantir que as **petições sejam encaminhadas ao setor competente** para análise técnica e devolução da resposta ao Encarregado.
- Estabelecer que, **em caso de descumprimento de prazos**, o setor responsável apresente **justificativa formal de prorrogação** ao Encarregado.
- Determinar que, **em nova ocorrência de atraso**, o Encarregado de Dados comunique o fato ao **Encarregado Geral do Município**, com relatório circunstanciado.
- Promover a **transparência e o direito à informação** aos titulares, conforme os princípios da LGPD e do Decreto Rio nº 54.984/2024.
- Fortalecer a **governança em privacidade e proteção de dados pessoais** na Fundação Rio-Águas.
- Aprimorar continuamente os procedimentos de atendimento às solicitações dos titulares, incorporando lições aprendidas e boas práticas administrativas.

A proteção de dados pessoais é dever da Administração Pública e pressupõe o alinhamento às normas da LGPD, ao Decreto Rio nº 54.984/2024 e às orientações da ANPD. A aplicação desses conceitos fundamenta o PRPTDP e orienta a atuação institucional em resposta a petições dos titulares.

Definições e Conceitos Fundamentais da LGPD

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 - LGPD) estabelece diretrizes e princípios para o tratamento de dados pessoais no Brasil. A seguir, apresentam-se os principais termos, conceitos e princípios que orientam este Plano:

Dados

- **Dado Pessoal:** Qualquer informação relacionada a pessoa natural identificada ou identificável, como nome, CPF, RG, endereço, telefone ou combinação de dados que possibilite a identificação do titular.
- **Dado Pessoal Sensível:** Informações que exigem maior proteção, como origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, dados referentes à saúde, vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural.
- **Dado Anonimizado:** Informação que passou por processo técnico que retira a possibilidade de associação, direta ou indireta, a um indivíduo de forma **irreversível**.
- **Anonimização:** Procedimento técnico que torna os dados pessoais impossíveis de identificar, de forma irreversível.



- **Pseudonimização:** Substituição de informações identificáveis por identificadores artificiais (como códigos), sendo possível reverter a anonimização por meio do acesso a uma base separada mantida pelo controlador.
- **Banco de Dados:** Conjunto estruturado de dados pessoais, em suporte físico ou eletrônico.
- **Bloqueio:** Suspensão temporária de qualquer operação de tratamento.
- **Eliminação:** Exclusão de dado ou conjunto de dados armazenados.

Agentes de Tratamento

- **Titular:** Pessoa natural a quem se referem os dados pessoais.
- **Agentes de Tratamento:** Incluem o **Controlador** e o **Operador**.
 - **Controlador:** Pessoa física ou jurídica, de direito público ou privado, responsável pelas decisões referentes ao tratamento de dados pessoais.
 - **Operador:** Pessoa física ou jurídica que realiza o tratamento em nome do Controlador, seguindo suas instruções.
 - **Controladoria Conjunta:** Situação em que dois ou mais Controladores compartilham responsabilidades sobre finalidades e meios do tratamento.
- **Encarregado de Dados (DPO):** Pessoa indicada pelo Controlador para atuar como canal de comunicação entre titulares, Controlador e a Autoridade Nacional de Proteção de Dados (ANPD), além de orientar boas práticas e monitorar o tratamento.

Tratamento de Dados

- **Tratamento:** Toda operação realizada com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, modificação, comunicação, transferência ou difusão.
- **Consentimento:** Manifestação **livre, informada e inequívoca** pela qual o titular concorda com o tratamento de seus dados para uma finalidade específica.
- **Transferência Internacional de Dados:** Envio de dados pessoais para país estrangeiro ou organismo internacional.
- **Uso Compartilhado de Dados:** Comunicação, difusão ou tratamento compartilhado de dados entre órgãos públicos ou entre estes e entidades privadas, quando permitido pela LGPD.
- **Bases Legais:** Hipóteses que autorizam o tratamento de dados pessoais (art. 7º da LGPD) e de dados sensíveis (art. 11 da LGPD), incluindo consentimento e outras finalidades legítimas previstas em lei.



Governança e Fiscalização

- **Autoridade Nacional de Proteção de Dados (ANPD):** Órgão da Administração Pública responsável por zelar, implementar, regular e fiscalizar a aplicação da LGPD, podendo aplicar sanções.
- **Relatório de Impacto à Proteção de Dados (RIPD):** Documento elaborado pelo Controlador que descreve processos de tratamento e avalia riscos, salvaguardas e medidas de mitigação.
- **Privacy by Design (Privacidade desde a Concepção):** Integração de requisitos de privacidade no desenvolvimento de produtos, serviços e processos desde a sua criação.
- **Privacy by Default (Privacidade por Padrão):** Garantia de que, por padrão, apenas os dados estritamente necessários sejam coletados e tratados.
- **Princípios da LGPD:** As atividades de tratamento devem observar a boa-fé e os seguintes princípios:
 - Finalidade
 - Adequação
 - Necessidade
 - Livre Acesso
 - Qualidade dos Dados
 - Transparência
 - Segurança
 - Prevenção
 - Não Discriminação
 - Responsabilização e Prestação de Contas

Governança Municipal (Decreto Rio nº 54.984/2024)

- **Encarregado de Dados (DPO):** Responsável pela coordenação da proteção de dados na Fundação Rio-Águas, comunicação com a ANPD e orientação de boas práticas.
- **Comitê de Privacidade e Proteção de Dados Pessoais:** Grupo de apoio ao DPO, encarregado de avaliar processos, apoiar a implantação do Programa de Governança e analisar incidentes.

Compartilhamento e Direitos dos Titulares

- **Compartilhamento de Dados:** Deve ser formalizado por contrato, convênio ou ato normativo, observando finalidade, necessidade, transparência e medidas de segurança. É vedada a transferência a entidades privadas, salvo exceções legais.
- **Direito de Petição dos Titulares:** Os titulares podem exercer seus direitos de forma gratuita mediante requerimento expresso, atendido no prazo de até 15 dias, prorrogável mediante justificativa.



Incidente de Segurança e Vazamento de Dados Pessoais

Definição

Um **Incidente de Segurança** é qualquer evento indesejado ou inesperado que comprometa a segurança de dados pessoais, podendo resultar em:

- Acesso não autorizado;
- Destruição, perda ou alteração (acidental ou ilícita);
- Comunicação ou outro tratamento inadequado ou ilícito.

O **Vazamento de Dados** é um tipo específico de incidente em que informações privadas e sigilosas são expostas publicamente ou a terceiros sem autorização. Esse cenário pode permitir que dados sejam acessados, comercializados, utilizados em golpes, extorsões ou causem danos à imagem institucional.

Causas e Fatores de Vazamento de Dados

Causas mais comuns

1. **Ataques maliciosos** - como *malwares* e *ransomwares*, que sequestram dados e exigem resgate.
2. **Falhas técnicas ou de sistema** - decorrentes de indisponibilidade, bugs ou falta de manutenção.
3. **Erro humano** - ações acidentais de servidores, colaboradores ou terceiros.

Fatores que facilitam ataques

- Uso de credenciais comprometidas;
- Falhas de configuração em ambientes de nuvem;
- Vulnerabilidades em softwares de terceiros;
- Práticas de *phishing* e engenharia social.

Medidas Preventivas e Estrutura de Governança

A **LGPD** determina que os Agentes de Tratamento (Controlador e Operador) adotem medidas de segurança técnicas e administrativas para proteger os dados pessoais.

Medidas Preventivas

Área	Medidas Preventivas
Tecnologia	Implementar soluções de proteção contra códigos maliciosos homologadas, com atualizações automáticas de antivírus e firewall corporativo.
	Utilizar criptografia de disco (BitLocker) em estações de trabalho.



Área	Medidas Preventivas
Tecnologia	<p>Utilizar criptografia SMB em servidores físicos.</p> <p>Aplicar controle inteligente de aplicativos para bloquear execuções não autorizadas.</p> <p>Ativar proteção baseada em reputação e mitigação contra <i>exploits</i>.</p> <p>Assegurar o isolamento do núcleo habilitado para integridade do sistema.</p> <p>Auditar periodicamente as configurações e chaves de criptografia.</p> <p>Utilizar autenticação multifator (MFA) para sistemas críticos e serviços em nuvem.</p> <p>Aplicar de patches de segurança e firmware conforme recomendações dos fabricantes.</p> <p>Adotar mecanismos de auditoria e monitoramento contínuo de acessos, incidentes e registros de rede.</p> <p>Coagir a instalação de softwares não homologados e o uso de mídias externas sem verificação de antivírus.</p> <p>Utilizar protocolos WPA3 ou superior em redes sem fio e a configuração segura de ambientes de nuvem com criptografia em repouso e em trânsito.</p> <p>Realizar backups completos e incrementais, com verificação de integridade e testes periódicos de restauração.</p>
Infraestrutura	<p>Atualizar continuamente sistemas, softwares e hardwares.</p> <p>Armazenar documentos físicos em armários trancados, com controle de chaves e acesso restrito e eliminar os mesmos com segurança conforme temporalidade.</p> <p>Assegurar o controle físico de acesso a salas de servidores, com registro de entrada e saída de pessoas autorizadas.</p> <p>Instalar equipamentos de rede em locais protegidos contra acesso indevido.</p> <p>Reprimir a instalação de <i>access points</i> ou roteadores sem coordenação do Suporte de TI.</p> <p>Implementar redundância de energia e conectividade, garantindo continuidade dos serviços essenciais.</p> <p>Analisar vulnerabilidade e efetuar testes de recuperação periodicamente.</p> <p>Restaurar ao estado de fábrica os equipamentos antes do descarte.</p> <p>Manter cópias de segurança armazenadas de forma segura, com definição de ciclos de retenção e cronogramas de verificação.</p>
Acesso e Controle	<p>Manter autenticação individual e intransferível para cada usuário.</p> <p>Excluir contas inativas e atualizar imediatamente credenciais comprometidas.</p> <p>Estabelecer regras de criação e renovação de senhas (mínimo 10 caracteres, letras, números e símbolos).</p> <p>Bloquear contas inativas e forçar a troca de senhas a cada 60 dias.</p> <p>Orientar que senhas não sejam armazenadas em navegadores ou transmitidas por e-mail.</p> <p>Adotar controle de tentativas de autenticação (máximo de 3 antes do bloqueio).</p>



Área	Medidas Preventivas
Acesso e Controle	Implementar registro e rastreabilidade de acessos a sistemas e bancos de dados. Controlar concessão de acessos privilegiados e revisar perfis de usuários periodicamente.
Pessoas e Cultura	Promover treinamentos e fomentar a capacitação em LGPD e em relação aos riscos em segurança da informação entre os colaboradores. Vedar o uso de e-mails pessoais para tratar de assuntos institucionais. Reforçar o uso ético e seguro de dados pessoais e dos ativos tecnológicos na cultura organizacional. Orientar que os usuários internos deverão reportar imediatamente problemas e situações de possível risco ao Comitê de Privacidade e/ou Suporte de TI Promover condições para o Comitê de Privacidade planejar e acompanhar a execução das políticas internas e avaliar incidentes.
Governança	Estabelecer e atualizar periodicamente os instrumentos de gestão da LGPD. Formalizar matriz de responsabilidades entre titulares das pastas, fiscais de contrato, operadores, agentes de monitoramento de riscos e encarregados. Registrar e avaliar todos os incidentes em fluxo institucional. Fiscalizar as cláusulas dos Contratos Administrativos e congêneres referentes à LGPD. Emitir Orientações do Controlador aos Operadores. Celebrar Termos de Compartilhamento de Dados Pessoais. Aplicar anonimização em relatórios e bases de dados que contenham informações pessoais sensíveis para fins de ampla divulgação e compartilhamento com pessoas jurídicas de direito privado, bem como em respostas à requerimentos LAI.

Estrutura Municipal de Resposta a Petições dos Titulares

O **Programa Municipal de Proteção de Dados Pessoais** contempla, entre suas diretrizes, a coordenação do atendimento aos direitos dos titulares, conforme previsto no art. 18 da Lei nº 13.709/2018 (LGPD) e no Decreto Rio nº 54.984/2024, que objetiva garantir que as petições dos titulares - relacionadas à confirmação da existência de tratamento, acesso, correção, exclusão, anonimização, portabilidade, revogação de consentimento ou demais direitos - sejam tratadas de forma uniforme, transparente e tempestiva.

Fluxo de Comunicação em Caso de Petições dos Titulares

1. O titular ou seu representante legal encaminha, com vistas ao **Recebimento da Petição**, a solicitação ao **Encarregado de Dados** da Fundação Rio-Águas, utilizando o formulário padronizado ou canais oficiais (Portal de Privacidade ou Central 1746).



2. O Encarregado procede com o **Registro e Encaminhamento** da solicitação em processo eletrônico, classifica o tipo de direito invocado e encaminha a demanda ao **setor competente** para análise e resposta técnica.
3. O setor competente analisa a solicitação, elabora a resposta e devolve ao Encarregado dentro do prazo de **7 dias úteis**.
4. Caso o prazo legal de 15 dias não possa ser cumprido, o setor deve apresentar **justificativa formal** ao Encarregado, que informará o titular e concederá **prorrogação por igual período**.
5. **Acompanhamento e Comunicação** contempla:
 - o Se o prazo prorrogado também for descumprido, o Encarregado comunicará o fato ao Encarregado Geral do Município, com relatório das medidas adotadas.
 - o O Comitê de Privacidade e Proteção de Dados Pessoais acompanhará os casos de reincidência e recomendará melhorias aos fluxos internos.
6. Após o envio da resposta ao titular, o processo é **arquivado** com registro das datas de recebimento, encaminhamento, resposta e comunicação final, garantindo rastreabilidade e evidência de conformidade.

Consequências e Responsabilidade Legal

- Sanções administrativas (inclusive multas).
- Perdas financeiras (contratuais, operacionais ou de imagem).
- Quebra de confiança com usuários e titulares de dados.
- Danos à reputação institucional.
- Ações judiciais individuais ou coletivas.

O **Controlador** ou **Operador** responde por danos patrimoniais ou morais decorrentes de incidentes, salvo se comprovar que:

- Não realizou o tratamento em questão;
- Houve tratamento, mas sem violação à legislação;
- O dano decorreu exclusivamente de culpa do titular ou de terceiros.

Compartilhamento de Dados Pessoais

Requisitos internos:

- **Formalização** por processo administrativo, contrato ou convênio;
- **Necessidade e finalidade** específicas e compatíveis com a coleta original;
- **Base legal e prazo** de utilização definidos;
- **Segurança e transparência** garantidas;
- **Publicidade** das hipóteses de compartilhamento no site institucional.



Compartilhamento com órgãos de controle:

Permitido com Judiciário, Legislativo, Tribunais de Contas, Ministério Público e outras autoridades, desde que:

- Não envolva reserva de jurisdição;
- Seja restrito às atribuições legais do órgão requisitante;
- Seja formalizado em processo auditável.

Vedação a entidades privadas:

É proibida a transferência de dados pessoais a entes privados, exceto quando:

- For para execução descentralizada de atividade pública;
- Envolver dados publicamente acessíveis;
- Estiver respaldada por previsão legal ou contratual;
- For exclusiva para prevenção de fraudes ou proteção do titular.

Tramitação de documentos

- **Para outros poderes/entes públicos:** deve seguir os parâmetros de compartilhamento.
- **Entre órgãos municipais:** a tramitação física ou digital é atividade administrativa legítima e necessária para a execução de atribuições públicas.

Tratamento de Resposta a Incidentes

Recebida a notificação de possível incidente de segurança, o Encarregado, deverá proceder a caracterização dos dados vinculados ao episódio e encaminhar para o Comitê de Privacidade e Proteção de Dados Pessoais com objetivo de:

- **Identificação:** Verificar se os dados pertencem à Fundação Rio-Águas e se são dados pessoais.
- **Confirmação:** Avaliar se houve risco ou dano relevante aos titulares.
- **Avaliação:** Classificar a gravidade (alta, média ou baixa) conforme impacto, tipo e volume de dados.
- **Parecer Técnico:** Registrar evidências, causas, ações corretivas e preventivas.
- **Comunicação:** Notificar Encarregado Geral, ANPD e titulares em até 3 dias úteis, se aplicável.
- **Relatório Final:** Consolidar resultados, eficácia das medidas e lições aprendidas no Programa de Governança em Privacidade.



Tratamento de Resposta a Petição dos Titulares

Direito de Petição

- O direito pode ser exercido **pelo titular dos dados pessoais** ou por **representante legal** devidamente autorizado.
- As solicitações devem ser **encaminhadas ao Encarregado de Proteção de Dados Pessoais** da Fundação Rio-Águas, preferencialmente por meio do **formulário padronizado** (anexo), disponível no Portal de Privacidade e na Central de Atendimento 1746.
- O atendimento é **gratuito** e deve ocorrer **em até 15 (quinze) dias**, prorrogável **por igual período**, mediante justificativa formal.
- **Não serão aceitas** petições **anônimas** ou apresentadas por **terceiros não autorizados**.

Deverá ser empregado o formulário padronizado disponível no site:

<https://fundacaorioaguas.prefeitura.rio/programa-de-governanca-em-privacidade-e-protecao-de-dados-pessoais/>

Recebimento e Registro

O **Encarregado de Dados** recebe a petição via formulário ou canal oficial (e-mail, protocolo, 1746).

A solicitação é **registrada em processo eletrônico** com número, data de recebimento e tipo de pedido (acesso, correção, exclusão, etc.).

O Encarregado realiza **análise preliminar** para confirmar:

- A identidade do titular ou de seu representante;
- A legitimidade da solicitação;
- A clareza e completude das informações apresentadas.

Encaminhamento aos Setores Competentes

Após o registro, o Encarregado encaminha a petição às áreas técnica, jurídica e administrativa envolvidas no tratamento dos dados pessoais objeto da solicitação do titular.

Os setores competentes devem **analisar internamente a solicitação**, identificar os dados pessoais envolvidos e **elaborar a resposta técnica** em linguagem clara, precisa e fundamentada.

O prazo para retorno ao Encarregado é de **até 7 dias úteis**, de modo a permitir a consolidação e envio da resposta final ao titular dentro do prazo legal.



Controle de Prazos e Prorrogação

Caso o setor competente **não consiga atender no prazo inicial**, deverá **comunicar formalmente o Encarregado** antes do término do prazo, apresentando **justificativa fundamentada** e estimativa do tempo adicional necessário.

O Encarregado avaliará a justificativa e, se procedente, **prorrogará o prazo por mais 15 dias**, comunicando o titular sobre o motivo da prorrogação e o novo prazo previsto.

Se o **prazo prorrogado também for descumprido**, o Encarregado deverá **comunicar o fato ao Encarregado Geral do Município**, relatando a ocorrência, as razões do descumprimento e as providências cabíveis.

Resposta ao Titular

O Encarregado **consolida a resposta técnica** recebida do setor responsável, verifica sua conformidade com a LGPD e prepara a **resposta formal ao titular**.

A resposta deve conter:

- O resultado do pedido (atendido, parcialmente atendido ou indeferido);
- Os fundamentos legais e técnicos;
- Eventuais orientações complementares;
- Informações sobre recursos ou novos pedidos.

A comunicação ao titular será feita por **e-mail institucional, carta registrada ou outro meio seguro**, assegurando a comprovação do envio.

Arquivamento e Registro Final

Todo o processo deve ser **documentado e arquivado**, contendo:

- Petição original;
- Registros de encaminhamentos;
- Pareceres e comunicações internas;
- Resposta final encaminhada ao titular.

Os registros serão **mantidos por, no mínimo, 5 anos** para fins de auditoria, controle interno e prestação de contas.

Acompanhamento e Relatórios

O Encarregado consolidará **relatórios semestrais** sobre o número, natureza e tempo de resposta das petições, bem como eventuais ocorrências de atraso e suas causas.



Esses relatórios subsidiarão o **Programa de Governança em Privacidade e Proteção de Dados Pessoais** da Fundação Rio-Águas, orientando medidas de aperfeiçoamento contínuo.

Fluxograma

