CONTROLADORIA-GERAL
DA UNIÃO

GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO

Guia de Boas Práticas na Aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) nas Ouvidorias Públicas

RENOUV
Rede Nacional de Ouvidorias

2ª Edição - Revista e Atualizada

SUMÁRIO

EXPEDIENTE

2ª Edição - Revista e Atualizada

Ariana Frances
Coordenadora-Geral da Rede Nacional de Ouvidorias

Ouvidorias do Conselho Diretivo da Renouv
Ouvidoria-Geral do Distrito Federal
Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES
Tribunal Regional Eleitoral do Ceará
Empresa de Tecnologia e Informações da Previdência - DATAPREV
Instituto Federal de Educação, Ciência e Tecnologia do Paraná - IFPR
Ouvidoria-Geral do Município de São Paulo
Secretaria da Controladoria-Geral do Estado de Pernambuco
Controladoria-Geral do Estado do Ceará
Ouvidoria-Geral do Estado do Piauí
Ouvidoria-Geral do Estado de Goiás
Ouvidoria-Geral do Estado do Rio Grande do Sul
Ouvidoria da Prefeitura Municipal de Alagoinhas – BA

Câmara Técnica de Aplicação da Lei Geral de Proteção de Dados Pessoais nas Ouvidorias
Alexandre Sanches Vicente
Coordenador

EXPEDIENTE

ELABORAÇÃO

ALEXANDRE SANCHES VICENTE
Ouvidoria-Geral do Município de Londrina (PR)
GRAYCE GONÇALVES
Ministério das Cidades
HELOÍSA CURVELLO
Controladoria-Geral da União
JULIANO AZEVEDO PAIM
Ouvidoria-Geral do Município de Vitória da Conquista (BA)
MARIA ANGÉLICA ABEN-ATHAR
Superintendência do Desenvolvimento do Centro-Oeste (SUDECO)
MARIA ELISA ANDRADE
Ouvidoria-Geral do Estado de Pernambuco
MIUCHA MAGALHÃES
Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis (IBAMA)
PAULO SÉRGIO ALMEIDA SANTOS
Ouvidoria-Geral da Universidade Federal de Mato Grosso
ROBERSON BRUNO LOBO OLIVIERI
Ouvidoria-Geral do Distrito Federal
ROBSON CARVALHO DA SILVA
Controladoria-Geral do Estado do Amazonas
TATIANA KELLY NUNES BASTOS
Ouvidoria do CEFET-MG
TATIANA APARECIDA ESTANISLAU DE SOUZA
Ouvidoria do STJ

REVISÃO

Secretaria-Executiva da Rede Nacional de Ouvidorias

EXPEDIENTE

1ª edição elaborada pelo Grupo de Trabalho da Renouv sobre a Lei Geral de Proteção de Dados Pessoais nas Ouvidorias

MARCONI MUZZIO
Coordenador
ABELARDO LOPES
Controladoria-Geral da União
ALEXANDRE SANCHES VICENTE
Ouvidoria-Geral do Município de Londrina
BRUNEI DE OLIVEIRA MAIOCHI MALFATTI
Ouvidoria do Instituto Federal Catarinense
CECÍLIA SOUZA DA FONSECA
Ouvidoria-Geral do Distrito Federal
DIEGO MENEGAZZI
Setor de dados da Ouvidoria do Instituto Federal Catarinense
JANAÍNA ANCHIETA COSTA
Ouvidoria da Universidade Federal de São Paulo
MARIANA ACCIOLY
Controladoria-Geral da União
MARIA ELISA ANDRADE
Ouvidoria-Geral do Estado de Pernambuco
PAULO SÉRGIO ALMEIDA SANTOS
Ouvidoria-Geral da Universidade Federal de Mato Grosso
ROBERSON BRUNO LOBO OLIVIERI
Ouvidoria-Geral do Distrito Federal

HISTÓRICO DE VERSÕES

Data	Versão	Descrição	Autor
30/03/2022	1.0	Primeira versão do Guia de Boas Práticas na Aplicação da Lei Geral de Proteção de Dados Pessoais nas Ouvidorias Públicas	Membros do Grupo de Trabalho Lei Geral de Proteção de Dados Pessoais nas Ouvidorias
21/11/2024	2.0	Segunda versão do Guia de Boas Práticas na Aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) nas Ouvidorias Públicas	Membros da Câmara Técnica de Aplicação da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados (LGPD), no âmbito das Ouvidorias Públicas

APRESENTAÇÃO E AGRADECIMENTOS

O Guia de Boas Práticas na Aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) nas Ouvidorias Públicas foi criado pelo Grupo de Trabalho (GT), da Rede Nacional de Ouvidorias (Renouv), dedicado a estudar o tema e torná-lo de fácil utilização. O objetivo do grupo ao elaborar esse guia era apoiar os ouvidores e ouvidoras, membros da Renouv, a atuarem em suas tarefas cotidianas atendendo à LGPD sem complicações. A primeira edição trouxe aportes valiosos para as ouvidorias da Rede, uma vez que foi além em seu papel de guia ao apresentar as melhores práticas do mercado capazes de elevar a eficiência das ouvidorias na proteção de dados pessoais. O GT foi adaptado para funcionar permanentemente sob a forma de Câmara Técnica de Aplicação da LGPD em ouvidorias. Assim, a Câmara Técnica já nasceu comprometida a atuar em benefício dos membros da Rede e a continuar com a missão de tornar o conteúdo da LGPD algo prático e fácil de ser operacionalizado, tal qual o GT que lhe deu origem.

O relançamento do **Guia de Boas Práticas na Aplicação da LGPD nas Ouvidorias Públicas**, em versão revista e atualizada, reforça a persistente necessidade de atender à demanda por orientação voltada ao nicho das ouvidorias. Se, por um lado, as ouvidorias lidam com informações pessoais sensíveis em seu dia a dia, por outro, não encontram literatura que atenda às especificidades do papel que desempenham. É a partir desse vácuo que o trabalho realizado pela Renouv assume caráter pioneiro, ao juntar orientação teórica e prática. Portanto, tornando o Guia de Boas Práticas na Aplicação da LGPD nas Ouvidorias Públicas uma ferramenta de sucesso entre ouvidores e ouvidoras.

Nesse sentido, deixar o Guia alinhado às últimas recomendações da Autoridade Nacional de Proteção de Dados (ANPD) e ilustrá-lo com exemplos práticos é antes de tudo, reconhecer os esforços empreendidos pelo Grupo de trabalho autor da 1ª edição. Seguir melhorando o que já tínhamos, retrata o nível de maturidade da Renouv. Além disso, exemplifica o espírito do trabalho em rede: somar forças e multiplicar benefícios. Por todo o exposto, é preciso registrar nossos agradecimentos a cada um dos membros participantes, tanto do Grupo de Trabalho quanto da Câmara Técnica, que tem estudado a legislação e, desta forma, compartilhado conhecimentos adquiridos na prática e oferecendo-os para fortalecer a Renouv. Permitindo, assim, que as ouvidorias melhorem seus desempenhos.

Por fim, vale dizer que o **Guia de Boas Práticas na Aplicação da LGPD** nas Ouvidorias Públicas não pretende impor como ou o que as ouvidorias da Rede devem fazer para adaptarem-se à LGPD. Sua intenção é, ao trazer boas práticas, nutrir a criatividade dos gestores e enriquecer as possibilidades de ação disponíveis de acordo com a realidade local de cada ouvidoria.

Membros da Câmara Técnica de Aplicação da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados, no âmbito das Ouvidorias Públicas

1. CONTEXTUALIZAÇÃO DAS OUVIDORIAS PÚBLICAS E A LGPD

A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, assegura direitos aos titulares de dados pessoais. Esses direitos devem ser garantidos pelos órgãos públicos dentro dos prazos e procedimentos específicos, em consonância com outras leis, como a Lei de Acesso à Informação (Lei nº 12.527/2011) e o Código de Defesa dos Usuários de Serviços Públicos (Lei nº 13.460/2017).
Dentro desse contexto, o cumprimento dos direitos dos titulares de dados é reforçado pela implementação das práticas de conformidade que constam neste Guia.

Este documento visa fornecer conceitos e diretrizes de boas práticas para as ouvidorias da Rede Nacional de Ouvidorias (Renouv), promovendo a adequação de processos e documentos às exigências da LGPD, com base nas discussões do grupo de trabalho "Lei Geral de Proteção de Dados Pessoais nas Ouvidorias".

A função das ouvidorias públicas como defensoras dos direitos dos cidadãos foi inspirada pela Declaração Universal dos Direitos Humanos, proclamada pela ONU em 1948, que consagra a figura do Ombudsman em diversos países como um canal de proteção dos direitos dos cidadãos.

No Brasil, a Emenda Constitucional n.º 19/1998 fortaleceu o papel da ouvidoria ao incluir o princípio da eficiência no artigo 37, junto aos princípios de legalidade, impessoalidade, moralidade e publicidade. Além disso, essa emenda também estabeleceu formas de participação do usuário na administração pública, incluindo entre elas o direito a reclamar sobre os serviços públicos, acessar informações e denunciar práticas abusivas.

A regulamentação da participação e defesa dos usuários de serviços públicos foi consolidada com a Lei nº 13.460/2017, também conhecida como Código de Defesa dos Usuários de Serviços Públicos, que organiza a proteção e os direitos dos cidadãos em seu relacionamento com a administração pública.

O Código de Defesa dos Usuários de Serviços Públicos especifica os direitos previstos no §3º, Art. 37 da Constituição Federal, ao regulamentar não apenas a apresentação de reclamações, mas também manifestações como "denúncias, sugestões, elogios e demais pronunciamentos de usuários que envolvem a prestação de serviços públicos e a conduta de agentes públicos na execução e fiscalização desses serviços" (art. 2º, inciso V, da Lei nº 13.460/2017). Essa lei ainda estabelece que essas manifestações devem ser direcionadas à ouvidoria do órgão ou entidade responsável.

Ao designar a ouvidoria como a unidade responsável pelo recebimento das manifestações dos usuários de serviços públicos, a Lei confere a essa estrutura a força normativa necessária para sua criação, onde ainda não implementada, e para sua consolidação, onde já existente.

Antes mesmo da edição do Código de Defesa dos Usuários de Serviços Públicos e da consolidação da ouvidoria como instância de defesa dos direitos dos usuários, muitos entes federativos já haviam implementado e regulamentado ouvidorias públicas em suas respectivas esferas de atuação. Com a Lei de Acesso à Informação (LAI) e a criação do Serviço de Informação ao Cidadão (SIC), várias ouvidorias também passaram a integrar esse serviço, aproveitando estruturas físicas e recursos humanos já existentes.

Em 16 de dezembro de 2020, a Organização das Nações Unidas (ONU) aprovou a Resolução 75/186, o que também reforçou o papel da ouvidoria na governança pública. Essa resolução além de promover a proteção dos direitos humanos, liberdades fundamentais e respeito ao Estado de Direito estabeleceu a importância do compartilhamento de informações sobre as melhores práticas para o trabalho e o funcionamento das ouvidorias.

Na atuação das ouvidorias públicas, a proteção de dados pessoais sempre foi uma preocupação. Além dos artigos 6º e 31 da LAI que abordam o tema, diversos entes federativos, incluindo a União, já promoviam salvaguardas para proteger os dados pessoais do cidadão, especialmente de denunciantes. Isso era feito por meio de normas específicas, como os Decretos nº 9.492/2018, nº 10.153/2019 e pela atualização do Decreto nº 10.890/2021, que regulamentam a proteção aos denunciantes de ilícitos na administração pública federal direta e indireta.

As normas de proteção de dados pessoais da União Europeia somam-se a esse cenário. Elas que são reconhecidas como um padrão global são atualizadas para acompanhar as transformações tecnológicas. Assim, em maio de 2018, entrou em vigor o General Data Protection Regulation (GDPR), uma evolução da Data Protection Directive (95/46/EC), com o objetivo de proteger a privacidade dos dados dos cidadãos europeus e evitar o vazamento de informações.

Diferente da diretiva de 1995, que permitia aos países da União Europeia adaptar as regras conforme suas necessidades, o GDPR exige sua aplicação uniforme nos 28 países membros.

No Brasil, a Lei Geral de Proteção de Dados (LGPD) foi sancionada em agosto de 2018, inspirada no GDPR, e seus principais dispositivos entraram em vigor em setembro de 2020. A LGPD visa regulamentar o uso de dados pessoais, proporcionando mais segurança e privacidade, permitindo o tratamento dos dados mediante autorização do titular ou com base em uma justificativa legal.

Além disso, em 10 de fevereiro de 2022, a proteção de dados pessoais foi incluída na Constituição Federal como um direito fundamental, no inciso LXXIX do art. 5º. Essa inclusão fortalece a aplicação desse direito para os cidadãos brasileiros, agora protegidos de forma permanente, uma vez que essa alteração se configura como uma cláusula pétrea, ou seja, não pode ser alterada.

Para os cidadãos, essa proteção constitucional representa mais segurança no uso de serviços digitais, seja no setor público ou privado, e reforça a confiança de que seus dados serão tratados com respeito e proteção. Esse avanço é fundamental para a construção de uma sociedade mais justa e equitativa no ambiente digital.

Portanto, a inserção da proteção de dados pessoais como direito fundamental não apenas resguarda os direitos dos cidadãos, mas também cria um ambiente mais seguro, transparente e inovador, refletindo o compromisso do Brasil com a privacidade e a dignidade humana na era digital.

2. OUVIDORIAS PÚBLICAS NO CONTEXTO DIGITAL

Em um mundo cada vez mais orientado por dados, observa-se com frequência o uso abusivo de informações pessoais, como sua comercialização ilegal. Para coibir essas práticas, são implementadas ações de proteção ao titular dos dados, incluindo a promulgação de legislações que garantem os direitos de privacidade dos indivíduos e a criação de autoridades independentes de fiscalização.

A regulamentação da proteção de dados pessoais impõe restrições ao uso indiscriminado dessas informações por instituições privadas e públicas, conferindo direitos aos titulares e alinhando as necessidades econômicas do país ao ambiente digital, já amplamente consolidado em diversos países.

As ouvidorias, como instâncias de defesa dos direitos dos usuários de serviços públicos e elementos essenciais da governança de serviços, desempenham papel fundamental na implementação da LGPD e na adaptação dos serviços públicos à evolução digital da sociedade.

Além disso, a utilização de canal eletrônicos de atendimento em ouvidorias, oferecidos pela internet, tem crescido ao longo dos anos. Fato que demonstra a preferência dos cidadãos por interações digitais com o governo.

Nesse sentido, o Estado tem se organizado para oferecer serviços em um ambiente seguro e acessível. Exemplo disso é a regulamentação dos Decreto nº 9.094 e nº 9.723. Eles simplificam o atendimento aos usuários dos serviços públicos e instituem o CPF como documento suficiente para identificação.

A Lei nº 14.129, por sua veze, estabelece princípios e diretrizes para o Governo Digital e para o aumento da eficiência pública ao promover simplificação, inovação, transformação digital e participação cidadã. O art. 18 dessa Lei determina que elementos como a Base Nacional de Serviços Públicos, as Cartas de Serviços ao Usuário (Lei nº 13.460/2017) e as Plataformas de Governo Digital são essenciais para a prestação digital de serviços públicos. Já no art. 21, inciso XI, define-se que as plataformas de atendimento digital devem incluir um sistema de ouvidoria que siga os requisitos da Lei nº 13.460/2017. E, por fim, no art. 23, inciso I, estabelece-se que o Poder Executivo federal pode instituir padrões nacionais para os componentes essenciais do Governo Digital.

Nesse contexto de digitalização de serviços, as ouvidorias precisam consolidar e organizar seus fluxos de trabalho em ambientes digitais e, ao mesmo tempo, garantir a proteção dos dados pessoais ao cidadão.

Apesar do crescimento dos atendimentos virtuais, esse Guia também vai trazer boas práticas de aplicação da LGPD nas ouvidorias relacionadas ao ambiente físico e ao atendimento presencial. Isso porque, o processo de digitalização ainda está em desenvolvimento e não devem suprimir completamente o atendimento presencial aos usuários.

Por fim, é importante ressaltar que, mesmo com o avanço da digitalização, ela não será completa. Ainda haverá arquivos históricos e outros documentos físicos os quais devem ser protegidos e tratados de acordo com LGPD.

3. CONCEITOS

As ouvidorias desempenham um papel fundamental na implementação e monitoramento da Lei Geral de Proteção de Dados (LGPD), pois atuam como uma ponte entre os titulares de dados e as organizações, sejam elas públicas ou privadas.

Para os ouvidores, é essencial compreender a LGPD e seus desdobramentos, de modo a garantir a proteção dos direitos dos titulares e assegurar o tratamento adequado dos dados pessoais. Os ouvidores devem estar habituados não apenas os princípios da LGPD, mas também suas diretrizes complementares, incluindo outras publicações e documentos técnicos como, por exemplo, o Guia de Boas Práticas1 da LGPD, do Comitê Central de Governança de Dados do Poder Executivo Federal.

Com base na LGPD e nas orientações do Guia de Boas Práticas, as ouvidorias devem atuar como defensoras da transparência, da proteção de dados e dos direitos dos titulares, sempre com foco na conformidade e segurança do tratamento de informações pessoais. Devem ainda auxiliar na identificação de falhas ou dúvidas relacionadas ao tratamento dos dados e garantir que as queixas sejam devidamente encaminhadas aos responsáveis, como o Encarregado de Proteção de Dados.

A seguir, são apresentados alguns conceitos importantes para as ouvidorias, com base na LGPD e no Guia de Boas Práticas para Implementação da LGPD na Administração Pública Federal:

Titular de Dados

O titular de dados é a pessoa física a quem os dados pessoais que estão sendo coletados ou processados se referem. A proteção dos direitos dos titulares é um dos pilares da Lei Geral de Proteção de Dados (LGPD).

Dados Pessoais

Segundo o inciso IV do artigo 4° da Lei de Acesso à Informação (LAI), dados pessoais são informações relacionadas a uma pessoa natural identificada ou identificável. Isso inclui, por exemplo, nome, CPF, endereço, e-mail e dados de localização. Toda a equipe da ouvidoria precisa ser capaz de identificar esses dados e assegurar que seu tratamento esteja protegido de acordo com a LGPD.

Dados Pessoais Sensíveis

Dados pessoais sensíveis constituem um tipo específico de dado que exige maior proteção, pois estão relacionados a características como origem racial ou étnica, convicção religiosa, opinião política, saúde, vida sexual e dados biométricos ou genéticos.

Tratamento de Dados Pessoais

O tratamento de dados pessoais envolve a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação e controle da informação. Além de incluir a modificação, comunicação, transferência, difusão ou extração das informações, conforme disposto no inciso X do art. 5º da LGPD. As ouvidorias, canais oficiais de comunicação diretos entre cidadãos e entidades públicas, têm uma responsabilidade especial em garantir que esses dados sejam tratados com segurança, transparência e em conformidade com a lei.

Compartilhamento de Dados

As ouvidorias podem precisar compartilhar dados pessoais com outras áreas da organização ou com entidades externas, especialmente em casos de apuração de denúncias. Esse compartilhamento, no entanto, deve estar de acordo com a base legal aplicável e ser realizado de acordo com as medidas de segurança apropriadas. O titular dos dados deve ser informado sobre o eventual compartilhamento e sobre quem serão os destinatários de seus dados.

Agentes de Tratamento: Controlador e Operador

São responsáveis pelo tratamento dos dados pessoais, sujeitos às regras da LGPD e à fiscalização da Autoridade Nacional de Proteção de Dados (ANPD):

- Controlador: a pessoa física ou jurídica que toma as decisões sobre o tratamento dos dados pessoais.
- Operador: a pessoa física ou jurídica que realiza o tratamento dos dados em nome do Controlador.

A ouvidoria deve entender a distinção entre esses dois papéis para direcionar adequadamente as demandas dos titulares de dados.

Encarregado de Dados (*DPO - Data Protection Officer*)

O Encarregado de Dados, conforme o Artigo 41 da LGPD, é a pessoa responsável por garantir o cumprimento da legislação de proteção de dados na organização. A ouvidoria deve colaborar com o encarregado para assegurar que as demandas dos titulares sejam tratadas de acordo com a lei e que as organizações respondam de forma ágil e eficiente.

Autoridade Nacional de Proteção de Dados (ANPD)

A ANPD é o órgão regulador responsável por garantir o cumprimento da LGPD. A ouvidoria deve conhecer o papel da ANPD e estar preparada para interagir com a Autoridade em casos de denúncias ou auditorias, além de ajudar a garantir que a organização esteja em conformidade com as regulamentações da ANPD.

Princípios da LGPD

As ouvidorias devem basear sua atuação nos princípios da LGPD, estabelecidos no Artigo 6º, que orientam o tratamento de dados:

- Finalidade: o tratamento de dados deve ter um propósito legítimo, específico e informado.
- Adequação: o tratamento deve ser compatível com as finalidades informadas ao titular.
- Necessidade: apenas os dados essenciais ao objetivo devem ser tratados.
- Livre Acesso: os titulares devem ter acesso fácil e gratuito às suas informações.
- Qualidade dos Dados: os dados pessoais devem ser precisos, claros e atualizados.
- Transparência: as informações devem ser claras, precisas e facilmente acessíveis aos titulares.

Finalidade e Consentimento

A LGPD exige que o tratamento de dados seja realizado com finalidade específica , ou seja, para um objetivo legítimo, claro e informado ao titular. Em muitos casos, é necessário obter o consentimento do titular para processar seus dados. A ouvidoria deve assegurar que o consentimento seja obtido de forma clara e livre, e o titular tenha o direito de revogá-lo a qualquer momento.

Direitos dos Titulares de Dados

A ouvidoria é o canal preferencial para que os titulares de dados exerçam seus direitos, garantidos pela LGPD. Os direitos incluem:

- Confirmação de existência de tratamento;
- Acesso aos dados;
- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação de dados desnecessários ou excessivos;
- Portabilidade dos dados;
- Revogação do consentimento.

As ouvidorias devem orientar os titulares sobre como exercer esses direitos e, quando necessário, interagir com o Encarregado de Dados e outras áreas internas da organização.

Segurança da Informação

O tratamento seguro dos dados é uma preocupação central na LGPD e no Guia de Boas Práticas para Implementação da LGPD na Administração Pública Federal. A ouvidoria deve assegurar a aplicação de medidas de segurança, como controle de acesso, criptografia e procedimentos para resposta a incidentes, como vazamentos de dados.

Segurança e Incidentes de Dados

A proteção dos dados requer a adoção de medidas de segurança para evitar vazamentos ou acessos não autorizados. A ouvidoria deve estar preparada para receber reclamações ou denúncias sobre incidentes de segurança e colaborar com outros setores da organização para garantir uma resposta rápida e eficaz.

Anonimização e Minimização de Dados

A LGPD e o Guia de Boas Práticas para Implementação da LGPD na Administração Pública Federal enfatizam a anonimização como uma técnica de proteção dos dados pessoais. Quando possível, as ouvidorias devem incentivar a anonimização em relatórios e a aplicação de tratamentos que preservem a identificação dos titulares. A minimização de dados é igualmente importante, garantindo que apenas as informações necessárias para o propósito da coleta sejam tratadas.

A ouvidoria deve dominar essas técnicas e garantir que os dados pessoais sejam coletados apenas quando necessário e, sempre que possível, anonimizados.

Pseudonimização de dados ou dados pseudonimizados

A pseudonimização é uma técnica prevista na LGPD e no Guia de Boas Práticas para Implementação da LGPD na Administração Pública Federal. Ela visa aumentar a privacidade dos titulares ao remover ou alterar identificadores diretos (como nome e CPF), embora possibilite reidentificação por meio de dados adicionais mantidos em separado.

Segundo a LGPD, pseudonimização é o tratamento de dados de modo que eles não possam ser diretamente vinculados a um indivíduo sem o uso de informações adicionais, mantidas separada-

mente com medidas técnicas e administrativas que garantam que os dados pessoais não sejam associados a uma pessoa identificada ou identificável.

O Guia de Boas Práticas para Implementação da LGPD na Administração Pública Federal destaca a pseudonimização como uma medida importante para reduzir riscos relacionados ao tratamento de dados pessoais, servindo como camada adicional de proteção, principalmente em cenários onde o acesso aos dados deve ser controlado.

A pseudonimização é uma prática que pode ser amplamente adotada pelas ouvidorias e outras entidades no tratamento de dados pessoais, pois protege a privacidade dos titulares ao mesmo tempo que permite a manipulação e análise dos dados. Embora os dados pseudonimizados ainda sejam considerados dados pessoais, a técnica acrescenta uma camada importante de segurança e ajuda a mitigar riscos de exposição indevida. Para que a pseudonimização seja eficaz, ela deve ser combinada com medidas técnicas e organizacionais adequadas, conforme previsto na LGPD e no Guia de Boas Práticas para Implementação da LGPD na Administração Pública Federal.

Diferença entre Pseudonimização e Anonimização

É importante distinguir a pseudonimização da anonimização:

- Anonimização: os dados são irreversivelmente alterados, fato que torna impossível a reidentificação do titular. Dados anonimizados deixam de ser considerados dados pessoais, conforme a LGPD.
- Pseudonimização: os dados podem ser reidentificados caso haja a utilização de informações adicionais, armazenadas de forma segura e separada.

Dessa forma, dados pseudonimizados continuam sendo considerados dados pessoais, pois, com as informações corretas, a identidade do titular pode ser restabelecida.

Nas ouvidorias, a pseudonimização pode ser usada para proteger a privacidade dos cidadãos que apresentam queixas ou denúncias, uma vez que permite o tratamento e a análise dos dados por equipes sem revelar imediatamente a identidade do denunciante. Informações que possibilitem a reidentificação (como nome ou CPF) podem ser mantidas em ambiente seguro e separado, acessível apenas por agentes autorizados.

Bases de dados ou banco de dados

A LGPD define um banco de dados como um "conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico" (art. 5º, IV). Em outras palavras, bancos de dados são coleções organizadas de informações que permitem criar sentido e otimizar pesquisas ou estudos, independentemente do formato (por exemplo, uma planilha no computador de um agente público ou grandes volumes de dados em nuvem ou servidor remoto). Como exemplo de banco de dados físico, há os registros funcionais dos servidores públicos, onde constam, além de dados funcionais, informações pessoais, como CPF e endereço residencial, que podem ser arquivados em armários ou prateleiras. Um exemplo de banco de dados eletrônico é a Plataforma Fala.BR, que reúne as manifestações de ouvidoria registradas.

Aplicar a LGPD nas bases de dados da ouvidoria requer um conjunto de práticas para garantir a segurança e a privacidade dos dados pessoais dos cidadãos. Assim, as ouvidorias devem adotar medidas técnicas e administrativas robustas, como políticas de controle de acesso, segurança da informação, minimização de dados e respeito aos direitos dos titulares.

Bases Legais para o Tratamento de Dados Pessoais

Os ouvidores devem ser capazes de identificar rapidamente os casos em que a LGPD exige o tratamento de dados pessoais. Com base na correlação entre o caso concreto e as hipóteses legais, será possível justificar a coleta e o uso dos dados pessoais de acordo com uma finalidade legítima, boa-fé e interesse público.

O tratamento de dados pessoais só pode ocorrer em uma das hipóteses previstas no Artigo 7º da LGPD, que incluem:

- Consentimento do titular;
- Cumprimento de obrigação legal ou regulatória;
- Execução de políticas públicas;
- Realização de estudos por órgãos de pesquisa;
- Execução de contrato;
- Exercício regular de direitos em processos judiciais, administrativos ou arbitrais;
- Proteção da vida ou incolumidade física do titular;

- Tutela da saúde, exclusivamente em procedimento realizado por profissionais e serviços de saúde ou autoridade sanitária;
- Atendimento aos interesses legítimos do controlador ou de terceiros, desde que não se sobreponham aos direitos fundamentais do titular;
- Proteção do crédito.

Os casos em que o tratamento de dados pessoais se aplica devem estar embasados em uma dessas hipóteses. Além de identificar a base legal adequada, o ouvidor deve informar os titulares sobre essa justificativa.

Relatório de Transparência

O Guia de Boas Práticas para Implementação da LGPD na Administração Pública Federal destaca recomenda que as organizações, incluindo as ouvidorias, elaborem um relatório de transparência para mostrar como os dados são tratados e quais medidas são adotadas para garantir sua proteção. Esse relatório é uma ferramenta importante para promover a confiança dos titulares e garantir uma comunicação clara sobre o uso de seus dados.

Inventário de Dados Pessoais (IDP)

É o registro das operações de tratamento de dados pessoais realizadas pelo controlador e pelo operador (LGPD, Art. 37). Trata-se de etapa necessária ao cumprimento da LGPD.

Relatório de Impacto à Proteção de Dados (RIPD)

Trata-se de documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Governança de Dados

O Guia de Boas Práticas para Implementação da LGPD na Administração Pública Federal reforça a importância de estabelecer uma governança sólida, com políticas e procedimentos claros para o tratamento de dados pessoais. As ouvidorias devem estar integradas a essa governança, com o objetivo de garantir que o tratamento de dados siga as diretrizes estabelecidas.

Incidentes de Segurança e Notificação

As ouvidorias devem ser treinadas para lidar com incidentes de segurança envolvendo dados pessoais. O Artigo 48 da LGPD exige que, em caso de incidente que possa acarretar risco ou danos aos titulares, a autoridade nacional e titulares sejam notificados. O Guia de Boas Práticas para Implementação da LGPD na Administração Pública Federal reforça a necessidade de desenvolver processos internos claros para detectar e responder a incidentes de segurança de dados.

Figura 1: Conceitos das operações de tratamento de dados pessoais (LGPD, art. 5º, X).

ACESSO
ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique.

ARMAZENAMENTO
ação ou resultado de manter ou conservar em repositório um dado.

ARQUIVAMENTO
ato ou efeito de manter registrado um dado em qualquer das fases do ciclo da informação, compreendendo os arquivos corrente, intermediário e permanente, ainda que tal informação já tenha perdido a validade ou esgotado a sua vigência.

AVALIAÇÃO
analisar o dado com o objetivo de produzir informação.

CLASSIFICAÇÃO
maneira de ordenar os dados conforme algum critério estabelecido.

COLETA
recolhimento de dados com finalidade específica.

COMUNICAÇÃO
transmitir informações pertinentes a políticas de ação sobre os dados.

CONTROLE
ação ou poder de regular, determinar ou monitorar as ações sobre o dado.

DIFUSÃO
ato ou efeito de divulgação, propagação multiplicação dos dados.

DISTRIBUIÇÃO
ato ou efeito de dispor de dados de acordo com algum critério estabelecido.

ELIMINAÇÃO
ato ou efeito de excluir ou destruir dados do repositório.

EXTRAÇÃO
ato de copiar ou retirar dados do repositório em que se encontrava.

MODIFICAÇÃO
ato ou efeito de alteração do dado.

PROCESSAMENTO
ato ou efeito de processar dados visando organizá-los para obtenção de um resultado determinado.

PRODUÇÃO
criação de bens e de serviços a partir do tratamento de dados.

RECEPÇÃO
ato de receber os dados ao final da transmissão.

REPRODUÇÃO
cópia de dado preexistente obtido por meio de qualquer processo.

TRANSFERÊNCIA
mudança de dados de uma área de armazenamento para outra, ou para terceiro.

TRANSMISSÃO
movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos etc.

UTILIZAÇÃO
ato ou efeito do aproveitamento dos dados.

Fonte: Guia de Boas Práticas da Lei Geral de Proteção de Dados do Comitê Central de Governança de Dados do Poder Executivo Federal, Brasil.

4. COMO A LGPD IMPACTA AS OUVIDORIAS PÚBLICAS

Com o advento da LGPD, as instituições públicas de todos os poderes e esferas da federação têm o dever de adequar suas ações, processos, documentos (físicos e eletrônicos) e sistemas informatizados para atender às diretrizes da Lei. Dessa forma, garantem que o tratamento de dados pessoais seja realizado necessariamente segundo as hipóteses legais previstas com a devida transparência em relação aos titulares dos dados. Além disso, é essencial que seja oferecido aos titulares um canal oficial para o exercício de seus direitos.

No caso da Plataforma Integrada de Ouvidoria e Acesso à Informação - Fala.BR - utilizada por diversas ouvidorias nas esferas federal, estadual e municipal para o recebimento e gestão de manifestações e pedidos de acesso à informação, verifica-se, em consulta ao Termo de Uso e ao Aviso de Privacidade (disponíveis em https://falabr.cgu.gov.br/publico/TermosDeUso/TermosDeUso.aspx), que as diretrizes da LGPD são devidamente seguidas.

Sob a ótica da ouvidoria, identificam-se 03 (três) efeitos da LGPD nas suas atribuições:

a) Intensificação das Ações de Proteção de Dados Pessoais e de adequação da ouvidoria à LGPD.

A primeira implicação da LGPD para as ouvidorias, independentemente de seu poder ou esfera de atuação, é a necessidade de intensificar a implementação de ações que garantam a proteção dos dados pessoais. A LAI, em seu Artigo 31, já estabelecia diretrizes para essa proteção, mas, com a LGPD, a regulamentação das especificidades da Lei tornou-se necessária. Às ouvidorias cabem realizar as adaptações em seus processos internos de trabalho, documentos (físicos e eletrônicos) e sistemas informatizados, para garantir essa proteção.

Nesse contexto, é importante que se faça um mapeamento dos dados pessoais coletados e tratados em cada ação, processo, base de dados e sistemas informatizados utilizados pela ouvidoria. A partir disso, é preciso identificar a finalidade do uso de cada um desses dados e revisar a necessidade de utilizá-los.

Nas ouvidorias em que o volume de processos a serem revisados for grande, o ouvidor deverá priorizar quais serão revisados primeiro. Essa priorização deverá ser realizada com base na análise dos riscos para a segurança dos dados pessoais, que cada operação oferecer. Caso seja identificado que o uso dos dados não está em conformidade com o princípio da finalidade da LGPD, ele deverá ser descontinuado. Já quando o uso do dado pessoal for justificado, salvaguardas devem ser implementadas, para evitar o uso incompatível com sua finalidade.

Além disso, é necessário que as ouvidorias atualizem seus sistemas informatizados, para garantir que estejam de acordo com os princípios de proteção de dados. Por sua natureza, os sistemas utilizados no registro de demandas de ouvidoria geralmente contêm uma grande quantidade de dados pessoais, incluindo dados sensíveis.

Então, as ouvidorias precisarão adequar os sistemas aos requisitos de segurança da informação e de proteção de dados pessoais definidos no âmbito da esfera e do órgão a que estejam vinculadas. Da mesma forma, as ouvidorias precisarão observar os requisitos de segurança aplicados ao manuseio de documentos em papel nos quais constem dados pessoais, uma vez que arquivos físicos também são regidos pela LGPD.

b) Ouvidoria como canal de comunicação com o titular do dado pessoal:

O segundo efeito da LGPD para a ouvidoria é, a critério de cada instituição pública, a possibilidade de ela atuar como canal de comunicação entre o titular dos dados pessoais e a Administração Pública. Essa atribuição decorre do fato de que os direitos dos titulares perante a Administração Pública já são geralmente exercidos nos prazos e procedimentos estabelecidos pela Lei de Acesso à Informação, por meio do Serviço de Informação ao Cidadão (SIC), muitas vezes vinculado às estruturas de ouvidoria. Além disso, o Código de Defesa dos Usuários de Serviços Públicos expressamente atribui à ouvidoria a responsabilidade de recepcionar manifestações dos usuários.

c) Ouvidor como encarregado de proteção de dados:

Uma terceira possibilidade para a ouvidoria, ainda que não obrigatória, é que o ouvidor atue como Encarregado de Proteção de Dados. Nesse caso, o titular da ouvidoria, indicado pelo controlador de dados da instituição, assumiria as responsabilidades do encarregado de dados. A LGPD define o encarregado como "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)" (art. 5º, inciso VII). Conforme já visto, na Administração Pública, a ouvidoria já funciona como esse canal para os usuários dos serviços públicos, cem decorrência do Código de Defesa dos Usuários de Serviços Públicos (Lei nº 13.460/2017).

Na Controladoria-Geral da União (CGU), por exemplo, a função de encarregado de dados foi atribuída ao ouvidor de abril de 2021 a fevereiro de 2023, segundo a Portaria nº 951/2021. Atualmente, a CGU designou o Secretário-Executivo Adjunto para essa função, conforme a Portaria Normativa CGU nº 056/2023.

Independentemente de a ouvidoria desempenhar diretamente a função de encarregado, sua participação na Unidade de Governança para Proteção de Dados Pessoais, quando existente, é essencial. Isso porque, mesmo que não haja um órgão colegiado específico para coordenar as ações de proteção de dados, é fundamental que a ouvidoria mantenha uma relação estreita com o setor responsável pela proteção de dados, uma vez que ela será o ponto de recepção de demandas dos titulares de dados pessoais.

De aqui em diante, esse Guia - específico para as ouvidorias - abordará os riscos e as melhores práticas relacionados ao que a LGPD implica às ouvidorias. Por isso, será necessário focar nos casos "a" e "b" mencionados acima. São eles: a "intensificação das ações de Proteção de Dados Pessoais e de adequação da ouvidoria à LGPD" e "ouvidoria como canal de comunicação com o titular do dado pessoal" respectivamente.

As orientações que serão disponibilizadas têm o objetivo alinhar as ações, os processos, os documentos físicos e eletrônicos, bem como os sistemas informação às diretrizes da LGPD. Essas orientações visam também apoiar na proteção dos dados pessoais que devem receber tratamento, além de auxiliar no atendimento aos titulares de dados que buscam as ouvidorias para exercer os direitos regulamentados pela LGPD.

5. BASE LEGAL PARA TRATAMENTO DE DADOS PESSOAIS PELAS OUVIDORIAS PÚBLICAS

Base legal ou hipóteses de tratamento de Dados Pessoais são as circunstâncias expressamente previstas no Artigo 7°, da LGPD que autorizam o tratamento de dados pessoais.

Observe na figura a seguir, extraída do Guia de Boas Práticas para Implementação da LGPD na Administração Pública Federal apresenta, o resumo das hipóteses de tratamento autorizadas pela LGPD.

Figura 2. Hipóteses de tratamento de dados pessoais previstas no art. 7º, da LGPD.

Hipóteses de Tratamento	Dispositivo Legal Para o Tratamento de Dados Pessoais	Dispositivo Legal Para o Tratamento Dados Pessoais Sensíveis
Hipótese 1: Mediante consentimento do titular	LGPD, art. 7º, I	LGPD, art.11, I
Hipótese 2: Para o cumprimento de obrigação legal ou regulatória	LGPD, art. 7º, II	LGPD, art. 11, II, "a"
Hipótese 3: Para a execução de políticas públicas	LGPD, art. 7º, III	LGPD, art. 11, II, "b"
Hipótese 4: Para a realização de estudos por órgão de pesquisa	LGPD, art. 7º, IV	LGPD, art. 11, II, "c"
Hipótese 5: Para a execução ou preparação de contrato	LGPD, art. 7º, V	Não se aplica
Hipótese 6: Para o exercício de direitos em processo judicial, administrativo ou arbitral	LGPD, art. 7º, VI	LGPD, art. 11, II, "d"
Hipótese 7: Para a proteção da vida ou da incolumidade física do titular ou terceiro	LGPD, art. 7º, VII	LGPD, art. 11, II, "e"
Hipótese 8: Para a tutela da saúde do titular	LGPD, art. 7º, VIII	LGPD, art. 11, II, "f"
Hipótese 9: Para atender interesses legítimos do controlador ou de terceiro	LGPD, art. 7º, IX	Não se aplica
Hipótese 10: Para proteção do crédito	LGPD, art. 7º, X	Não se aplica
Hipótese 11: Para a garantia da prevenção à fraude e à segurança do titular	Não se aplica	LGPD, art. 11, II, "g"

Fonte: Guia de Boas Práticas da Lei Geral de Proteção de Dados do Comitê Central de Governança de Dados do Poder Executivo Federal, Brasil.

No contexto da ouvidoria pública, as bases legais que autorizam o tratamento de dados pessoais e dados sensíveis são:

1. O cumprimento de obrigação legal ou regulatória, previsto nos artigos 7º, II, e 11, II, "a"; e
2. A execução de políticas públicas, conforme disposto nos artigos 7º, III, e 11, II, "b".

Desse contexto entende-se que o consentimento, tratado nos Artigos 7º, I e 11, I da LGPD, não deve ser a base legal escolhida para justificar o tratamento dos dados pessoais nos processos típicos de ouvidoria.

O Guia Orientativo para Tratamento de Dados Pessoais pelo Poder Público da ANPD define consentimento como a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade específica". Isso significa que o titular pode revogar seu consentimento a qualquer momento, o que não é compatível com a natureza das atividades da ouvidoria. O Poder Público realiza suas ações para cumprir obrigações e atribuições legais, as quais podem exigir o tratamento de dados pessoais. A ANPD destaca que, nesse contexto, "o órgão ou a entidade exerce prerrogativas estatais, que impõem suas demandas aos titulares em uma relação desequilibrada, em que o cidadão não possui condições efetivas de se manifestar livremente sobre o uso de seus dados".

Assim, as informações pessoais coletadas pela ouvidoria para o registro de manifestações e no cadastro de sistemas informatizados são necessárias para que os órgãos tomem providências em relação ao que foi apresentado pelos cidadãos, seja na forma de denúncia, reclamação, solicitação, entre outras. Essa coleta se baseia na obrigação legal e regulatória disposta no artigo 12, parágrafo único, da Lei nº 13.460/2017, que impõe à administração pública a resolução das manifestações dos usuários.

Além disso, o tratamento de dados pessoais relacionado à análise de manifestações sobre serviços públicos pode gerar decisões administrativas e até melhorias nos processos e serviços. Dependendo do contexto, isso pode ser enquadrado na hipótese legal de execução de políticas públicas (art. 7º, inciso III, e art. 11, inciso II, "b"). É importante ressaltar que cada tratamento de dados exige uma base legal específica e um mesmo tratamento de dados não pode ter duas bases legais.

Quanto à execução de políticas públicas, a ouvidoria pode utilizar dados pessoais coletados para traçar o perfil socioeconômico dos usuários, o que ajudaria na definição de estratégias de atuação, aumentando a eficácia da política pública de ouvidoria.

Por fim, para afastar a hipótese de consentimento nas manifestações de ouvidoria, é relevante observar que a Lei nº 13.460/2017 determina que as manifestações sobre a prestação de serviços públicos devem ser, obrigatoriamente, identificadas. Adicionalmente, o § 1º do art. 10-A, incluído pela Lei nº 14.129/2021, determina que cadastros e formulários exigidos para a prestação de serviços públicos devem incluir campo para o CPF, de preenchimento obrigatório para cidadãos brasileiros e estrangeiros.

Entretanto, essa prerrogativa de dispensar o consentimento só se aplica se for respeitado o princípio da finalidade, explícito no inciso I do art. 6º da LGPD. Segundo o Guia da ANPD, o tratamento de dados deve ocorrer para fins legítimos, específicos e informados ao titular, sem possibilidade de tratamento posterior incompatível com essas finalidades. Além disso, no setor público, o tratamento de dados pessoais deve atender a uma "finalidade pública", conforme previsto no art. 23 da LGPD.

Ainda que o consentimento não seja a base legal mais apropriada para o tratamento de dados pelo Poder Público, ele pode ser eventualmente usado quando o tratamento de dados for opcional e a ouvidoria atuar fora de suas atribuições típicas. Por exemplo, uma organização sem fins lucrativos que ofereça capacitação gratuita a cidadãos para exercer o controle social pode solicitar os e-mails de usuários da ouvidoria para convidá-los ao evento. Nesse caso, o compartilhamento dos dados só seria permitido mediante consentimento dos titulares.

Diante disso, é crucial que as ouvidorias apresentem o Termo de Uso e a Política de Privacidade aos cidadãos ao registrar uma manifestação ou realizar o cadastro em sistemas informatizados, quando aplicável. Além disso, é recomendável que essas informações sejam fornecidas em respostas a e-mails de usuários, quando esse for um dos canais de ouvidoria. Para auxiliar na elaboração desses documentos, sugere-se o uso do Guia de Elaboração de Termo de Uso e Política de Privacidade para serviços públicos, desenvolvido pelo Comitê Central de Governança de Dados do Poder Executivo Federal.

6. DIREITOS DOS TITULARES DE DADOS PESSOAIS E SEU EXERCÍCIO

A LAI já havia estabelecido, em seu art. 31, já havia estabelecido, em seu art. 31, diretrizes e procedimentos básicos para o tratamento de dados pessoais no setor público. A LGPD, no art. 23, §3º, reconhece o avanço conquistado até então e estabelece que os prazos e procedimentos para o exercício dos direitos dos titulares no âmbito público devem observar a legislação específica, incluindo a LAI.

Com isso, entende-se que o exercício dos direitos dos titulares de dados pessoais, previstos no art. 18, incisos I, II, VII e VIII, e no art. 20, § 1º, da LGPD, equivale ao direito fundamental de acesso à informação garantido pela LAI. Assim, esses direitos estarão sujeitos aos prazos e procedimentos já estipulados pela Lei de Acesso à Informação.

Nesse contexto, para exercer esses direitos, o titular dos dados pessoais deverá utilizar o Serviço de Informação ao Cidadão (SIC), conforme previsto na LAI, e seguir os respectivos prazos e procedimentos.

A Tabela 1 apresenta os direitos que serão exercidos conforme regramento da LAI:

Direitos que seguirão regramento LAI	
Direitos do titular de dados pessoais	**Dispositivo na LGPD**
Receber confirmação da existência de tratamento de seus dados pessoais	Art. 18, I
Acessar seus dados pessoais	Art. 18, II
Receber informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de seus dados pessoais, quando aplicável	Art. 18, VII
Receber informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa	Art. 18, VIII
Receber informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial	Art. 20, §1º

Tabela 1. Direitos que seguirão regramento LAI. Referência LGPD.

Para os demais direitos garantidos pela LGPD, poderá ser adotado o Código de Defesa dos Usuários de Serviços Públicos (Lei nº 13.460/2017). Sabe-se que esses direitos não se configuram como direito de acesso à informação, derivam da autodeterminação informativa e incluem a revisão de decisões tomadas exclusivamente com base em tratamento automatizado. Esse entendimento é reforçado pelo O Guia de Boas Práticas para Implementação da LGPD na Administração Pública Federal que diferencia o exercício dos direitos dos titulares entre o acesso à informação (transparência passiva) e as petições e manifestações via ouvidoria.

No âmbito administrativo, a LGPD se refere expressamente à LAI, à Lei de Processo Administrativo (Lei nº 9.784/1999) e à Lei do Habeas Data (Lei nº 9.507/1997) como referências não exclusivas para o exercício dos direitos dos titulares. Apesar de citar essa legislação, a LGPD não exige a aplicação exclusiva desses normativos. O Código de Defesa dos Usuários de Serviços Públicos, por ser mais ágil e vantajoso para os titulares, pode ser adotado para solicitações de providências e reclamações relativas ao tratamento de dados.

Direitos que seguirão regramento do Código de Defesa dos Usuários de Serviços Públicos	
Direitos do titular de dados pessoais	**Dispositivo na LGPD**
Solicitar correção de dados incompletos, inexatos ou desatualizados	Art. 18, III
Solicitar a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD	Art. 18, IV
Solicitar a eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da LGPD (não aplicável em Ouvidoria)	Art. 18, VI
Solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade	Art. 20

Tabela 2. Direitos que seguirão regramento do Código de Defesa dos Usuários de Serviços Públicos. Referência LGPD.

Especificamente acerca do direito de solicitar a eliminação dos dados pessoais tratados com o consentimento do titular, tratado no art. 18, inciso VI, da LGPD, é importante esclarecer que ele não se aplica aos dados coletados pela ouvidoria. Isso decorre do fato de que, conforme já descrito no item 3 deste Guia, o consentimento não é a base legal adequada para o tratamento de dados pessoais em ouvidoria, desde que ela esteja atuando no cumprimento de suas obrigações e atribuições legais ou na execução da política pública.

Contudo, convém ressaltar que o art. 18, §2º da LGPD prevê o direito de o titular se opor ao tratamento de seus dados, ao determinar que "o titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei".

Além dos direitos dos titulares apresentados nas Tabelas 1 e 2, em conformidade com o princípio da transparência, o órgão deverá disponibilizar e divulgar amplamente as informações sobre a identidade e contatos do encarregado de dados pessoais, bem como suas atribuições. Portanto, os dados de contato do encarregado — incluindo nome, cargo, horários e locais de atendimento, telefone e e-mail para esclarecimentos — deverão ser acessíveis no site institucional do órgão e da ouvidoria.

De modo complementar, o titular dos dados, no exercício de seus direitos previstos na LGPD, deverá manifestar-se diretamente ao controlador responsável pelo tratamento dos dados pessoais do órgão, por meio dos canais oficiais. E, caso entenda que a manifestação não tenha sido atendida pelo controlador, o titular pode apresentar petição à Autoridade Nacional de Proteção de Dados, com a comprovação da ausência de atendimento.

Compreendida a diferença entre os direitos de acesso à informação em transparência passiva e os meios de registrar manifestações à administração pública, é essencial que o órgão defina ferramentas e fluxos internos para o atendimento aos titulares de dados pessoais. Essa definição deve envolver o Serviço de Informação ao Cidadão e a Ouvidoria e estabelecer uma coordenação eficaz entre esses setores e o encarregado de dados. Finalmente, a equipe de ouvidoria deverá ser capacitada para acolher esses pedidos e manifestações, com ampla divulgação dos canais de atendimento.

7. AGENTES DE TRATAMENTO E DEMAIS ENVOLVIDOS NO EXERCÍCIO DOS DIREITOS DOS TITULARES

A atuação dos agentes de tratamento e demais envolvidos no exercício dos direitos dos titulares, no contexto da ouvidoria como canal oficial de atendimento, deve ser estruturada para garantir a conformidade com a LGPD, a LAI e com o Código de Defesa dos Usuários de Serviços Públicos. A ouvidoria é responsável pelo Sistema de Informação ao Cidadão e pelo registro e acompanhamento de manifestações dos usuários. Ela também atua como um ponto chave para garantir que os direitos dos titulares de dados sejam respeitados e exercidos de forma eficaz.

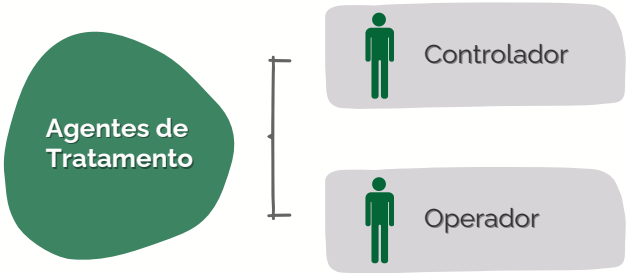
Os atores envolvidos com a proteção de dados são: o titular dos dados pessoais, os agentes de tratamento (controlador e operador), o encarregado e o ouvidor.

Ainda nesse contexto, o ouvidor deve conhecer as atribuições da Autoridade Nacional de Proteção de Dados Pessoais, bem como as circunstâncias que podem levar à criação de uma Unidade de Governança para Proteção de Dados Pessoais, na forma de comissões, comitês, grupos de trabalho, entre outros.

Nesta seção será demonstrada a distinção e o relacionamento entre os agentes de tratamento, tendo como base o Guia Orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado, publicado pela ANPD.

De acordo com a LGPD, os agentes de tratamento podem ser controladores ou operadores:

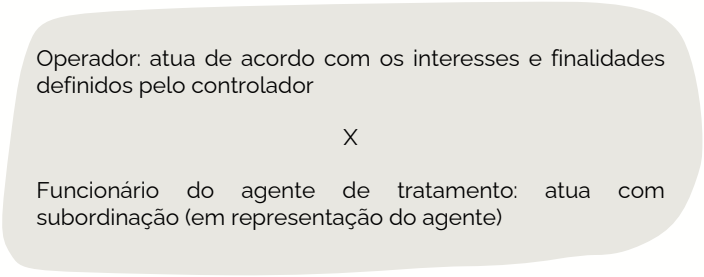
Figura 3. Agentes de tratamento.



Os conceitos de controlador e operador se diferenciam principalmente pelo poder de decisão, que pertence ao controlador. Em segundo lugar, se diferenciam pelo dever de observância que o operador tem de só atuar seguindo as instruções do controlador.

A Figura 4, extraída do Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, da ANPD, destaca a distinção entre o funcionário do controlador e o operador de dados pessoais:

Figura 4. Distinção entre o funcionário do controlador e o operador de dados pessoais.



Fonte: Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado. ANPD. Maio, 2021. Página 06

Por exemplo, no contexto de uma ouvidoria, a organização pública ou privada que mantém a ouvidoria (ministério, agência reguladora, empresa etc.) atua como controladora, enquanto a própria ouvidoria e seus funcionários ou terceiros que auxiliam nas atividades, atuam como operadores.

Funções dos Agentes de Tratamento na Ouvidoria

Os agentes de tratamento desempenham papéis importantes para garantir o cumprimento da LGPD e o respeito aos direitos dos titulares de dados. A seguir, destacam-se algumas dessas funções, considerando a relação entre o SIC e o Código de Defesa dos Usuários de Serviços Públicos.

a) Coleta e Tratamento de Dados

A ouvidoria recebe, registra e processa manifestações, que podem conter dados pessoais. É essencial que a coleta de dados siga os princípios da necessidade, transparência e finalidade, conforme definido pela LGPD.

A base legal para o tratamento de dados pela ouvidoria pode ser o cumprimento de obrigação legal (responder a solicitações com base na LAI ou tratar reclamações de usuários) ou o exercício regular de direitos , especialmente nos casos de denúncias ou queixas relacionadas ao serviço público.

b) Atendimento aos Direitos dos Titulares

A ouvidoria é o canal para o exercício dos direitos dos titulares, previstos no Art. 18 da LGPD, como:

- Confirmação da existência de tratamento;
- Acesso aos dados pessoais;
- Correção de dados incompletos ou incorretos;
- Anonimização, bloqueio ou eliminação de dados desnecessários;
- Portabilidade de dados;
- Informação sobre o compartilhamento de dados.

A ouvidoria, como agente de tratamento, deve criar procedimentos claros e ágeis para permitir que os titulares exerçam esses direitos. Isso inclui fornecer orientações e permitir que os titulares possam solicitar essas ações de forma segura e eficiente.

c) Transparência e Informação ao Titular

A ouvidoria deve garantir a transparência em relação ao tratamento de dados pessoais. Isso significa fornecer informações claras sobre como os dados são coletados, para que são usados, com quem são compartilhados, conforme a LGPD e a LAI.

A ouvidoria deve disponibilizar informações sobre o uso de dados pessoais em local acessível ao titular, incluindo nelas a finalidade e a base legal do tratamento.

d) Segurança da Informação e Proteção de Dados

Os agentes de tratamento devem assegurar que qualquer incidente de segurança que comprometa os dados seja notificado à ANPD e, quando necessário, ao titular dos dados.

e) Minimização de Dados

A ouvidoria deve garantir que os dados pessoais coletados sejam mínimos e necessários para o tratamento adequado das manifestações e das demandas dos titulares. Isso está em linha com o princípio da minimização previsto na LGPD, ao estabelecer que apenas os dados estritamente necessários ao alcançar da finalidade pretendida devem ser tratados.

Código de Defesa dos Usuários de Serviços Públicos e Papel da Ouvidoria

O Código de Defesa dos Usuários de Serviços Públicos (Lei nº 13.460/2017) fortalece direito de o usuário de serviços públicos acessar informação e de ser tratado com transparência e eficiência. A ouvidoria deve garantir que os usuários possam exercer esses direitos, por exemplo:

- Apresentando reclamações sobre a prestação de serviços públicos;
- Acompanhando o andamento das demandas;
- Recebendo resposta em tempo adequado.
- A LGPD adiciona ao rol de funções da ouvidoria a função de proteger os dados pessoais no contexto das manifestações. Portanto, os agentes de tratamento nas ouvidorias devem:
- Respeitar os prazos estabelecidos pelo Código para resposta aos usuários;
- Garantir que o tratamento de dados seja seguro e que nenhum dado pessoal do titular seja exposto de forma inadequada.

Envolvimento dos Demais Responsáveis pelo Tratamento de Dados

Além dos agentes diretamente envolvidos no tratamento, outros atores também desempenham papéis cruciais na proteção dos dados pessoais nas ouvidorias:

a) Encarregado pelo Tratamento de Dados (DPO)

A LGPD exige que as organizações, incluindo as ouvidorias, nomeiem um DPO. Este profissional será o responsável por:

- Garantir que a ouvidoria e demais setores da instituição estejam em conformidade com a LGPD;
- Interagir com os titulares de dados e com a ANPD;
- Supervisionar a implementação de políticas de privacidade e proteção de dados.

b) Autoridade Nacional de Proteção de Dados

A ANPD é a entidade responsável pela fiscalização do cumprimento da LGPD. A ouvidoria, como canal de atendimento ao titular e agente de tratamento, deve estar preparada para prestar contas à ANPD, para elaborar relatórios e atender a determinações regulatórias.

8. RELAÇÃO ENTRE A LEI DE ACESSO À INFORMAÇÃO E A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

A LAI já previa, em seu art. 31, procedimentos e diretrizes para o tratamento de informações pessoais no âmbito público. Dentre eles, o tratamento transparente dos dados, a garantia expressa aos direitos de personalidade e o consentimento do titular para a sua disponibilização a terceiros. Dessa maneira, atribui, inclusive, a regulamento específico, a disposição sobre os procedimentos para tratamento de informação pessoal.

Existe, portanto, uma convergência entre a LGPD e a LAI, pois ambas visam garantir a publicidade e o uso responsável de dados pessoais. E essa compatibilidade atribui maior segurança jurídica às políticas públicas.

O intuito da Lei Geral de Proteção de Dados é reduzir a assimetria de poder entre o cidadão, do lado "mais fraco" e Poder Público, do lado "mais forte", garantindo um fluxo adequado de informações, o que é essencial para a construção de uma sociedade mais justa e transparente.

A utilização de dados para a construção de políticas públicas baseadas em evidências é fundamental para otimização dos serviços públicos oferecidos. E, para que essa utilização possa ocorrer, a LGPD estabeleceu as bases legais, permitindo que o Poder Público atue de forma mais ágil e eficiente, promovendo um melhor atendimento à sociedade.

Todavia, o desafio é estabelecer um equilíbrio entre a proteção de dados pessoais e a necessidade de acesso à informação. Para que essa interação ocorra, é preciso estabelecer diretrizes claras.

Para melhor compreensão do exercício dos direitos consubstanciados na LGPD e na LAI, apresenta-se o seguinte exemplo: um cidadão, pai de paciente maior de 18 (dezoito) anos internado em hospital de determinada rede estadual de saúde, ao requisitar acesso às informações referentes ao plantão médico daquele hospital ou de quaisquer outras unidades de saúde daquele Estado, faz uso do seu direito fundamental de acesso à informação, consubstanciado na LAI. Se, por outro lado, esse mesmo pai deseja obter acesso ao prontuário médico de seu filho, estará diante de um dado pessoal cujo acesso é protegido pela Lei Geral de Proteção de Dados Pessoais.

Diferentemente, quanto à publicação ativa de informações na internet, por vezes, para cumprimento do princípio constitucional da publicidade, a administração pública necessita dar transparência a dados pessoais, a exemplo de beneficiários de auxílios financeiros. Por isso, os portais de transparência fomentam o controle social, garantindo que os dados sejam utilizados de maneira adequada e promovem uma gestão pública mais responsável.

No Guia Orientativo Tratamento de Dados Pessoais pelo Poder Público, a ANPD se posiciona no sentido de que a divulgação pública de dados pessoais, quando necessária ao atendimento ao princípio da publicidade, também deve ser realizada em conformidade com as disposições da LGPD. O que significa dizer que, "em termos práticos, considerando o reforço protetivo trazido pela LGPD ao titular de dados, é necessário realizar uma avaliação sobre os riscos e os impactos para os titulares dos dados pessoais bem como sobre as medidas mais adequadas para mitigar possíveis danos decorrentes do tratamento de dados pessoais", reforçando, com maior detalhamento, a necessidade já prevista na LAI. Para aprofundamento sobre o tema, recomenda-se a leitura do Guia referenciado acima.

Em decorrência das dúvidas em relação à publicação de informações pessoais no âmbito da administração pública, é possível que ocorra, também, o indeferimento equivocado de pedidos de acesso à informação, nos Serviços de Informação ao Cidadão, sob a alegação de infringir a LGPD. Um exemplo desta situação são as informações sobre servidores públicos.

Acerca dessas informações, em específico, é possível esclarecer que informações de servidores públicos referentes às suas atividades laborais, como escala de trabalho, gozo de férias, realização de viagens a trabalho e recebimento de diárias, geralmente, são informações públicas. Diferentemente, o número do cadastro de pessoa física e a classificação estatística internacional de doenças e problemas relacionados com a saúde (CID) que provocaram afastamentos para tratamento médico de servidores, estas sim, são informações pessoais, pois não decorrem diretamente das atividades laborais do servidor.

Nesse sentido, a Controladoria-Geral da União emitiu o Enunciado nº 04, de 10 de março de 2022, com seguinte teor:

> *Nos pedidos de acesso à informação e respectivos recursos, as decisões que tratam da publicidade de dados de pessoas naturais devem ser fundamentadas nos arts. 3º e 31 da Lei nº 12.527/2011 (Lei de Acesso à Informação), vez que:*
>
> *A LAI, por ser mais específica, é a norma de regência processual e material a ser aplicada no processamento desta espécie de processo administrativo; e*
>
> *A LAI, a Lei nº 14.129/2021 (Lei de Governo Digital) e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) são sistematicamente compatíveis entre si e harmonizam os direitos fundamentais do acesso à informação, da intimidade e da proteção aos dados pessoais, não havendo antinomia entre seus dispositivos."*

Por todo o exposto, a implementação da LGPD, promove a transparência e segurança na gestão das informações pessoais, aumentando a confiança da população nas instituições públicas.

9. GESTÃO DE RISCOS APLICADAS ÀS OUVIDORIAS

A gestão de riscos, enquanto metodologia que auxilia na prevenção do impacto provocado por possíveis intercorrências no processo de trabalho, é extremamente necessária na implementação de boas práticas, para aplicação da LGPD.

A aplicação de salvaguardas, com foco na proteção do sigilo dos dados pessoais do manifestante, é uma medida que a maioria das ouvidorias já adota há anos, com o objetivo de resguardar o cidadão. Essas medidas têm o intuito de transmitir segurança e confiabilidade nos serviços de ouvidoria. Assim, o usuário sente-se seguro para informar seus dados pessoais e prestar informações relevantes para o atendimento da sua demanda.

Como já mencionado, com o advento da LAI e da LGPD, as salvaguardas foram intensificadas e sistematizadas, com adoção de providências mais eficientes. E, nesse contexto, a gestão de riscos se tornou um importante instrumento que auxilia na detecção de possíveis riscos de vazamento de dados, bem como de erros operacionais intencionais ou não.

Tendo em conta a gestão de risco, o levantamento dos riscos, no âmbito das ouvidorias bem como o mapeamento de processos e a definição de um plano de ação, para aplicação da LGPD, são considerados como exemplos de boas práticas.

É importante destacar que a "Privacidade desde a Concepção" (privacy by design) pode ser aplicada ao gerenciamento de riscos. Isso porque, o termo propõe incorporar a privacidade e a proteção de dados pessoais em todos os projetos e processos desenvolvidos por uma organização, desde a sua concepção. Essa metodologia implica adotar uma postura proativa, em vez de reativa, ou seja, o gerenciamento deve se respaldar na prevenção do risco e não na sua remediação.

Considerando os riscos levantados, teremos mais clareza sobre onde devemos atuar e envidar mais esforços. De acordo com a metodologia "Privacidade desde a Concepção", deve-se priorizar a realização de ações mitigadoras nos riscos classificados como extre-

mos e altos. Em outras palavras, aqueles riscos que apresentam maior probabilidade de acontecer e cujo impacto nos processos de trabalho é mais alto.

Nesse mesmo contexto, após identificar riscos potenciais ou já materializados, deve-se elaborar o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), disposto no §3ª do artigo 4º, da LGPD. Para apoiar os órgãos da administração pública federal, o Comitê Central de Governança de Dados do Poder Executivo Federal disponibilizou Guia e um formato modelo para elaboração do RIPD. Ambos podem ser utilizados como referência, uma vez que consolidam diversas referências de publicações e de outros documentos técnicos já existentes, que poderão ser utilizados como referencial também na análise das demais esferas administrativas, além do Poder Executivo Federal.

Além do Guia Orientativo Tratamento de Dados Pessoais pelo Poder Público, recomenda-se o uso dos seguintes materiais sobre como aplicar a Gestão de Riscos:

- Gestão de Riscos – Avaliação da Maturidade – elaborado pelo Tribunal de Contas da União (TCU)

- Metodologia de Gestão de Riscos – elaborada pela ControladoriaGeral da União CGU)

- Guia de Avaliação de Riscos de Segurança e Privacidade - Lei Geral de Proteção de Dados Pessoais (LGPD) – elaborado pelo Comitê Central de Governança de Dados do Poder Executivo Federal

- COSO. Committee of Sponsoring Organizations of the Treadway Commission. Gerenciamento de Riscos Corporativos – Estrutura Integrada. 2017.

- COSO. Committee of Sponsoring Organizations of the Treadway Commission. Risk Assessment in Practice.

10. PASSO A PASSO PARA ADEQUAÇÃO DAS OUVIDORIAS À LGPD

Nessa seção, serão apresentados os passos necessários para adequação das ouvidorias à LGPD, com as providências iniciais para sua realização.

São eles: (1) mapear os dados pessoais sob a responsabilidade da ouvidoria; (2) mapear processos e ações da ouvidoria; (3) identificar os riscos relevantes envolvidos em cada um desses processos; (4) analisar quais ações de resposta poderão ser adotadas; (5) revisar os processos e ações relacionadas aos riscos relevantes identificados e (6) adequar os documentos internos e termos de contrato.

Importante esclarecer que a depender da estrutura e organização de cada ouvidoria, bem como do órgão ao qual está vinculada, os referidos passos podem ser realizados em ritmo mais acelerado ou mais lento. Ainda, dentro de cada um desses passos, a abrangência da ação pode ser ampliada gradativamente, de maneira incremental, a partir de uma priorização com base numa análise dos riscos mais relevantes.

Passo 1: Mapear os dados pessoais sob a responsabilidade da ouvidoria

Sob a coordenação da Unidade de Governança para Proteção de Dados Pessoais do órgão, é recomendável que seja elaborado o Inventário de Dados Pessoais a partir de uma priorização por meio de uma análise de riscos, documento fundamental para registro do tratamento de dados pessoais realizados pela instituição.

O inventário se faz necessário, dentre outros motivos, para o fiel cumprimento do art. 37 da LGPD, que dispõe que o "controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse" e consiste, também, uma forma efetiva de levantar quais dados pessoais são tratados, onde e como estão armazenados, quais operações são realizadas com eles e, ainda, com qual finalidade.

É recomendável que esse processo de mapeamento seja articulado com a governança de dados de um ponto de vista mais abrangente na organização. Dessa forma, o inventário elaborado pode não ser restrito apenas à identificação dos dados pessoais, mas a todas as operações envolvendo dados na instituição. Isso porque os sistemas podem ser alterados e passar a coletar dados pessoais, devendo observar a LGPD desde a sua concepção.

De acordo com o Guia de Elaboração de Inventário de Dados Pessoais - Lei Geral de Proteção de Dados Pessoais (guia_inventario_dados_pessoais.pdf), elaborado pelo Ministério da Gestão e Inovação em Serviços Públicos, o Inventário deve descrever informações em relação ao tratamento de dados pessoais realizado pelo órgão ou entidade, tais como:

- atores envolvidos (agentes de tratamento e o encarregado);
- finalidade (o que a instituição faz com o dado pessoal com base em atribuição legal);
- base legal do tratamento (arts. 7º e 11 da LGPD);
- previsão legal (dispositivos legais ou normativos que determinam o tratamento dos dados)
- dados pessoais tratados pela instituição;
- categoria dos titulares dos dados pessoais;
- tempo de retenção dos dados pessoais;
- instituições com as quais os dados pessoais são compartilhados;
- transferência internacional de dados (art. 33 LGPD);
- medidas de segurança atualmente adotadas.

Importante observar que devem ser identificados os dados pessoais constantes em quaisquer meios, físicos ou eletrônicos. Para tanto, deve-se identificar a existência, por exemplo, de documentação em papel arquivada na ouvidoria, onde constem dados pessoais do usuário, como formulários de atendimento presencial, de cadastro ou, até mesmo, formulários de manifestações, comumente utilizados em urnas coletoras e em ações itinerantes de ouvidoria.

Especificamente, no tocante à finalidade, importante mencionar que o mapeamento deve considerar todo o fluxo de dados, isso porque um mesmo dado pode ser tratado para finalidades diferentes, por setores diferentes sempre sendo exigida a base legal para cada finalidade.

Passo 2: Mapear processos e ações da ouvidoria

O mapeamento do processo é uma técnica que busca identificar falhas e potencialidades, para posterior correção e disseminação, respectivamente. E, assim, evitar a utilização de procedimentos isolados que não consideram o processo como um todo, ao fazer com que os trabalhos sejam conduzidos de forma mais integrada, proporcionando alcance de resultados com mais eficiência.

Com o advento da LGPD, o mapeamento de processos ganha ainda maior importância. Isso porque, a partir da análise detalhada de cada etapa dos processos é possível a identificação da ocorrência de tratamento de dados pessoais, na forma de coleta, produção, acesso ou quaisquer formas de tratamento de que trata o art. 5º, inciso X da Lei.

Uma vez identificados os processos e respectivas etapas em que ocorrem tratamentos de dados pessoais, é necessário avaliar a sua conformidade aos princípios, diretrizes e direitos previstos na Lei Geral de Proteção de Dados Pessoais. Caso estejam em desconformidade, será o caso de prever adequação para tanto.

Inclusive, é recomendável que o Inventário de Dados citado no passo 1 seja realizado em consonância com o mapeamento de processos ou, até mesmo, de forma concomitante.

Passo 3: Identificar os riscos relevantes envolvidos em cada um desses processos

Conforme a ABNT, a gestão de riscos consiste em "atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos" (ABNT NBR ISO/IEC 31000:2018).

Em adição, de acordo com o COSO 2017, modelo internacional de referência em gestão de riscos aplicável às instituições públicas, o gerenciamento de riscos corporativos está baseado na manutenção de práticas alinhadas às estratégias e objetivos das organizações, as quais, por sua vez, devem estar adaptadas a ambientes de negócios globais e altamente dependentes de tecnologia. Nesse sentido, o modelo ressalta a importância de se analisar o risco na definição das estratégias e para o desenvolvimento das organizações.

No que concerne aos sistemas informatizados utilizados pelas ouvidorias, faz-se essencial a atuação conjunta da ouvidoria com a área de tecnologia do órgão, para a avaliação dos riscos de segurança e privacidade.

Importante reforçar que nesses sistemas as ouvidorias tramitam não apenas informações pessoais como a identificação dos manifestantes que, nos termos do §7º. art. 10, da Lei nº 13.460, *"é informação pessoal protegida com restrição de acesso nos termos da Lei nº 12.527, de 18 de novembro de 2011"*, como também o teor das manifestações apresentadas, cujo acesso só deve ser permitido com a finalidade de apuração ou para tomada de providência acerca do que foi apresentado.

A título exemplificativo, a Lei nº 16.420, de 17 de setembro de 2018, aplicável ao Poder Executivo do Estado de Pernambuco, atribui à Ouvidoria-Geral e às ouvidorias dos órgãos e entidades estaduais o dever, dentre outros, de *"garantir o sigilo, a discrição e a fidedignidade quanto ao conteúdo e providências das manifestações recebidas"*.

De maneira similar, a Norma Modelo para Criação de Unidades de Ouvidoria da Rede Nacional de Ouvidorias trata do sigilo das manifestações quando estabelece a necessidade de estrutura adequada para atendimento ao usuário, com vistas a resguardá-lo. Ademais, quando dispõe sobre a possibilidade de utilização de base de dados e sistema informatizado cedidos por órgãos públicos, estabelece o dever de obedecer a critérios técnicos que garantam a segurança e o sigilo dos dados.

Com o intuito de fornecer, aos responsáveis pelo tratamento de dados pessoais do Poder Executivo Federal, orientação para identificar lacunas de segurança da informação e de privacidade sobre os sistemas, contratos e processos da instituição, o Comitê Central de Governança de Dados do Poder Executivo Federal publicou o Guia de Avaliação de Riscos de Segurança e Privacidade, que poderá ser utilizado como referência nesta avaliação de sistemas, inclusive, os de registro e tramitação de manifestações de ouvidoria.

Passo 4: Analisar quais ações de resposta poderão ser adotadas

A Lei Geral de Proteção de Dados Pessoais, em seu artigo 50, estabelece que os controladores e operadores, no âmbito de suas competências, deverão formular regras de boas práticas e de governança.

Especificamente, a alínea 'g', inciso I, §2º, do mesmo artigo determina que planos de resposta a incidentes e remediação deverão constar nos programas de governança em privacidade que poderão ser instituídos pelos mencionados agentes de tratamento. E, além deste plano, há outros controles aplicáveis na formulação de respostas ao risco, como controle de acesso, desenvolvimento seguro, gestão de continuidade, entre outros.

Neste contexto, elaborado o Inventário de Dados Pessoais da organização e a Avaliação de Riscos de Segurança e Privacidade, ambos tratados nos itens anteriores deste Guia, é necessário planejar as respostas aos riscos relevantes identificados. Trata-se de etapa necessária à implementação da gestão de riscos, denominada Plano de Tratamento de Riscos, com foco na adoção de controles preventivos, atenuantes ou de recuperação.

Algumas das respostas aos riscos poderão corresponder a ajustes nos procedimentos de ouvidoria já existentes ou a criação de novos fluxos de comunicação. Como, por exemplo, para garantir que todas as partes interessadas sejam informadas sempre que houver mudanças em atualizações de software e outros componentes das soluções de tecnologia da informação e comunicação. E, nos casos de respostas que ensejem mudanças das soluções de tecnologia da informação e comunicação utilizadas pela ouvidoria, será necessária, mais uma vez, a análise conjunta com a área de tecnologia da organização.

Passo 5: Revisar os processos e ações relacionadas aos riscos relevantes identificados

Identificados os riscos relevantes dos processos e sistemas de ouvidoria, o próximo passo deverá ser a revisão destes processos, com o intuito de corrigir procedimentos e/ ou implantar controles que visem reduzir os riscos relevantes identificados. Em relação àqueles associados aos sistemas, deve-se buscar junto à área de tecnologia formas de mitigá-los.

Essa revisão deverá constar nos planos de resposta a incidentes e remediação, de que dispõe a Lei Geral de Proteção de Dados (LGPD), já abordado neste Guia.

Passo 6: Adequar os documentos internos e termos de contrato

Assim como os processos e ações da ouvidoria precisarão ser revisadas após identificação dos riscos, os documentos e demais registros da área também deverão ser objeto de análise e ajuste, caso necessário.

Exemplos de documentos que poderão necessitar de adequação, no âmbito das ouvidorias, são os relatórios produzidos, em especial, relatórios gerenciais e termos de confidencialidade e sigilo. Deve-se observar que relatórios com informações estatísticas, apesar de apresentarem menor risco de conter divulgação indevida de dados pessoais, deverão, também, ser objeto de análise neste momento.

Essa necessidade de revisão aplica-se, também, a roteiros, scripts e materiais de orientação que sejam utilizados como referência às atividades de ouvidoria.

Nesse contexto, é importante que se faça a revisão dos termos dos contratos firmados pela ouvidoria para suporte e desenvolvimento de sistemas de tecnologia da informação e comunicação, bem como para serviços de consultoria e fornecimento de mão de obra.

Independentemente do seu objeto, se para sua execução for necessário o acesso à base de dados de ouvidoria, deverá ser incluída cláusula de proteção de dados pessoais e confidencialidade das manifestações nos respectivos contratos. Ou seja, nessa formalização devem constar cláusulas que assegurem a adoção das medidas de segurança pertinentes, bem como que vedem o compartilhamento com terceiros. A depender do tratamento dos dados realizado pela empresa contratada, ela pode ser considerada operadora dos dados, tratado no Capítulo 7 deste Guia, tendo responsabilidades sobre o tratamento dos dados pessoais.

A mesma análise deverá ser realizada e as adequações providenciadas, se necessário, em relação a outras formas de parcerias distintas da contratação, como formalização de convênios, termos de parceria e congêneres.

Por fim, importante mencionar que, em consonância com a LAI e o princípio da transparência previsto na LGPD, esses documentos devem ser publicados, de forma a permitir aos titulares de dados conhecerem as práticas e os agentes de tratamento de seus dados.

11. BOAS PRÁTICAS APLICADAS À OUVIDORIA PARA ATENDIMENTO À LGPD

A aplicação de boas práticas ao fluxo de uma o uvidoria para atendimento à LGPD envolve o desenvolvimento de procedimentos e mecanismos que garantam a conformidade com a legislação, a proteção de dados pessoais e o exercício dos direitos dos titulares. As ouvidorias, por lidarem diretamente com os dados dos cidadãos em manifestações, reclamações, denúncias e pedidos de acesso à informação, devem adotar práticas sólidas para preservar a privacidade e a segurança desses dados.

A seguir as principais boas práticas que podem ser aplicadas ao fluxo de trabalho de uma ouvidoria para atendimento à LGPD:

Mapeamento de Dados Pessoais

O primeiro passo para garantir a conformidade com a LGPD é realizar um mapeamento completo dos dados pessoais que a ouvidoria coleta, processa e armazena. Isso inclui:

- Identificar quais tipos de dados são coletados (nome, CPF, endereço, dados sensíveis etc.);
- Definir a finalidade de cada coleta (responder à manifestação, apurar denúncias etc.);
- Verificar onde e como esses dados são armazenados (bancos de dados, arquivos físicos, sistemas internos etc.);
- Identificar quem tem acesso a esses dados e como eles são tratados.
- Produzir o Inventário de Dados Pessoais;

Este mapeamento garante que a ouvidoria compreenda todo o ciclo de vida dos dados pessoais e aplique as medidas adequadas de segurança e proteção.

Política de Privacidade e Termos de Consentimento

A ouvidoria deve adotar uma política de privacidade clara e acessível, que informe os cidadãos sobre:

- Quais dados estão sendo coletados;
- Para que finalidade os dados serão utilizados;
- Como os dados serão armazenados e protegidos;
- Com quem os dados podem ser compartilhados (quando aplicável);
- Quais são os direitos dos titulares de dados e como podem ser exercidos.

Além disso, é essencial obter o consentimento dos titulares, quando necessário, de maneira transparente, e garantir que os cidadãos sejam informados sobre seus direitos em relação ao tratamento dos seus dados.

Treinamento e Sensibilização da Equipe

Os colaboradores da ouvidoria devem ser treinados para entender as obrigações impostas pela LGPD e a importância da proteção de dados pessoais. O treinamento deve abordar:

- Boas práticas de segurança da informação;
- Procedimentos para tratar solicitações de titulares (acesso, correção, eliminação de dados etc.);
- Como lidar com incidentes de segurança (como vazamento de dados) e como reportá-los à ANPD, se necessário.

A sensibilização contínua é essencial para que todos os envolvidos compreendam a seriedade da proteção de dados.

Minimização da Coleta de Dados

A minimização de dados é um dos princípios da LGPD e deve ser aplicado no fluxo da ouvidoria. Isso significa que a ouvidoria só deve coletar os dados pessoais estritamente necessários para o atendimento da demanda, evitando o acúmulo de informações desnecessárias. Por exemplo, se o objetivo da manifestação puder ser atendido sem a coleta de informações sensíveis, esses dados não devem ser solicitados.

Segurança da Informação

É fundamental que a ouvidoria implemente medidas de segurança adequadas para proteger os dados pessoais, conforme o princípio da segurança previsto na LGPD. Algumas práticas recomendadas incluem:

- Criptografia de dados, tanto em repouso quanto em trânsito;
- Controle de acesso rigoroso, garantindo que apenas pessoas autorizadas possam acessar os dados pessoais;
- Backups regulares e seguros dos dados armazenados;
- Implementação de firewalls e sistemas de monitoramento para detectar e prevenir acessos não autorizados ou atividades suspeitas.

Fluxo de Atendimento a Solicitações dos Titulares

A ouvidoria deve implementar um procedimento estruturado para atender às solicitações dos titulares de dados, como previsto na LGPD. O fluxo deve prever:

- Confirmação da existência de tratamento de dados pessoais, a pedido do titular;
- Fornecimento de cópia dos dados pessoais armazenados pela ouvidoria, quando solicitado;
- Correção de dados incorretos, incompletos ou desatualizados;
- Anonimização, bloqueio ou eliminação de dados que não sejam mais necessários ou quando o titular solicitar (desde que não haja impedimento legal);
- Portabilidade dos dados, quando aplicável.

Esses processos devem ser simples, acessíveis e rápidos, respeitando os prazos estabelecidos na legislação.

Pseudonimização e Anonimização de Dados

Uma boa prática recomendada para proteger os dados dos cidadãos é a pseudonimização ou anonimização dos dados pessoais, sempre que possível. Essas técnicas reduzem o risco de exposição de dados, especialmente em casos de vazamento ou acessos não autorizados.

- Pseudonimização: os dados são alterados de forma que não possam ser atribuídos diretamente a um indivíduo sem o uso de informações adicionais.
- Anonimização: os dados são irreversivelmente desidentificados, de modo que não possam ser ligados a uma pessoa específica.

Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

A ouvidoria deve avaliar a necessidade de elaborar um RIPD, especialmente em casos de tratamento de dados sensíveis ou de grande volume de informações pessoais. O RIPD é um documento que analisa os riscos envolvidos no tratamento de dados e define as medidas de mitigação para garantir a proteção.
Processos de Gestão de Incidentes

A ouvidoria deve ter um processo estabelecido para gestão de incidentes envolvendo dados pessoais, como vazamentos ou acessos não autorizados. Este processo deve prever:

- A notificação imediata à ANPD e, quando necessário, aos titulares dos dados afetados;
- Ações corretivas rápidas para conter o incidente e mitigar os danos;
- Registro e documentação dos incidentes para futura análise e melhoria dos processos.

Auditorias e Revisões Periódicas

A conformidade com a LGPD não é estática, por isso a ouvidoria deve realizar auditorias periódicas para verificar se as políticas e procedimentos de proteção de dados estão sendo seguidos corretamente. Além disso, a revisão constante das práticas adotadas é necessária para se adaptar às novas exigências legais ou tecnológicas.

Nomeação de um Encarregado de Proteção de Dados (DPO)

A ouvidoria deve designar um DPO, responsável por:

- Monitorar a conformidade da ouvidoria com a LGPD;
- Ser o ponto de contato com a Autoridade Nacional de Proteção de Dados;

- Coordenar o atendimento às solicitações dos titulares e o tratamento dos dados dentro da organização.

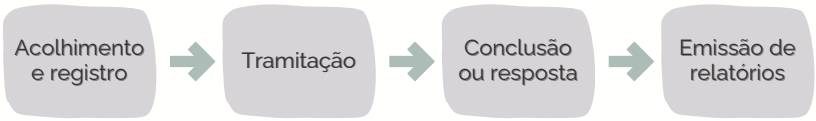
O DPO desempenha um papel essencial na criação de uma cultura de privacidade e proteção de dados dentro da instituição.

Conclusão

Aplicar boas práticas ao fluxo de atendimento da ouvidoria para conformidade com a LGPD envolve a adoção de políticas transparentes, a implementação de medidas de segurança e a criação de um ambiente que respeite os direitos dos titulares de dados. Com essas medidas, a ouvidoria pode garantir que o tratamento de dados pessoais seja feito de maneira segura, eficiente e em conformidade com a legislação, reforçando a confiança dos cidadãos no processo de atendimento e proteção de seus direitos.

Em seguida, serão apresentados riscos e boas práticas relacionadas, especificamente, a cada etapa deste fluxo, que contempla (1) acolhimento e registro, (2) tramitação, (3) conclusão ou resposta e (4) emissão de relatórios, conforme Figura 5:

Figura 5. Etapas do fluxo das manifestações de ouvidoria



11.1. BOAS PRÁTICAS RELACIONADAS AO RISCO DE ACESSO NÃO AUTORIZADO AOS SISTEMAS E DOCUMENTOS DA OUVIDORIA

Pela exigência disposta no Código de Defesa dos Usuários, quanto à obrigatoriedade de identificação na apresentação de manifestações à ouvidoria, bem como para permitir que as providências necessárias sejam tomadas pelos órgãos em relação a essas manifestações, a ouvidoria trata dados pessoais e dados pessoais sensíveis em suas atividades.

Diante disto, algumas medidas se fazem necessárias para garantir a proteção desses dados armazenados.

Nesse contexto, as primeiras boas práticas que serão apresentadas neste Guia são aquelas relacionadas a mitigar o risco de acesso não autorizado desses dados, que podem estar não apenas no sistema informatizado, como também em documentos em papel ou salvos na área de trabalho dos computadores dos servidores, por exemplo.

Risco: Acesso não autorizado ao sistema informatizado de ouvidoria, inclusive, à sua base de dados.

Este risco consiste, de maneira geral, no acesso não autorizado de pessoas ao sistema informatizado em uso pela ouvidoria, incluindo-se, neste contexto, o acesso diretamente à base de dados de ouvidoria por servidores e colaboradores responsáveis pela manutenção e evolução do sistema.

Será considerado neste risco, também, o acesso ilegal ao sistema por hackers.

Boas práticas: Utilizar sistema informatizado com controle efetivo de acesso, e demais requisitos de segurança necessários para mitigar o risco de invasão.

Sabe-se que a Política de Segurança da Informação tem como objetivo limitar a exposição ao risco a níveis aceitáveis e buscar continuamente a disponibilidade, a integridade, a confidencialidade, a autenticidade. Neste contexto, deve-se ater às questões de controle de acesso, garantindo que os usuários tenham acesso apenas aos recursos necessários à execução do seu trabalho e da audibilidade, que consiste na garantia de rastreabilidade de usuários e processos por meio de registro detalhado.

O controle de acesso também é considerado uma medida de segurança que tem como objetivo proteger equipamentos, softwares, arquivos de dados, modificação ou divulgação de informações, entre outros e, basicamente, são classificados em controles de acesso físicos ou lógicos.

O controle de acesso físico busca proteger o acesso de pessoas em determinado local e é composto de uma barreira, uma porta, fechaduras, catracas, chaves, entre outros. Já o controle de acesso lógico, tem como objetivo garantir a segurança das informações, além disso, deve garantir que apenas usuários autorizados tenham acesso ao sistema.

Em outras palavras, o controle de acesso é um conjunto de procedimentos e medidas com o objetivo de proteger as informações de um sistema contra as tentativas de acesso não autorizadas por outras pessoas. É um exemplo de controle, o acesso ao sistema mediante login e senha, para validar que essa determinada pessoa possui acesso autorizado ao sistema.

Ainda com relação ao controle de acesso, é importante implantá-los e estar atento para que credenciais de acesso legítimas não sejam obtidas e utilizadas por pessoas não autorizadas. Práticas inseguras como o registro de senhas em arquivos de texto em computadores pessoais ou pastas compartilhadas podem ser causas de vazamento de dados de sistemas. Para evitar que isso aconteça, é recomendável que o órgão mantenha uma política de gestão de senhas e atualização periódica obrigatória.

Nesse contexto, devem constar na Política de Segurança da Informação do órgão e, principalmente, estarem em pleno funcionamento no sistema informatizado, requisitos de segurança disponíveis que impeçam, efetivamente, a invasão à base de dados por ação de hackers, como exemplos, a instituição de senha forte de acesso e o ambiente protegido.

Uma senha forte deve conter, por exemplo, um composto de letras maiúsculas e minúsculas, números e símbolos e, deve ainda, formar uma sequência aleatória, ou seja, uma frase que não tenha nenhum sentido lógico. É uma boa prática, também, que essa senha seja alterada, preferencialmente, de 3 em 3 meses.

Boas práticas: Submeter à assinatura de termo de confidencialidade aos colaboradores que realizam ações de suporte e manutenção de tecnologia da informação e comunicação.

A importância do termo de confidencialidade no contexto das ouvidorias será ressaltada, também, na etapa de acolhimento e registro de manifestações, em relação aos colaboradores que estarão autorizados a realizar este acolhimento e, consequentemente, a coleta de dados pessoais dos usuários do serviço.

No contexto do risco de vazamento, pretende-se ainda incluir a prática de assinatura destes termos por aqueles que acessam o sistema e, até mesmo a sua base de dados diretamente, quando realizam operações de manutenção e evolução do sistema. Aqui estão

se tratando daqueles que dão o suporte e o apoio em tecnologia da informação e comunicação necessários às atividades de ouvidoria.

A obrigação de sigilo, inclusive da assinatura do termo de confidencialidade, deve ser incluída entre as cláusulas contratuais, caso esse serviço de suporte seja prestado por meio de uma contratação de empresa especializada.

É interessante, ainda, que o próprio sistema informatizado utilizado pela ouvidoria mostre avisos aos usuários relembrando sobre a Política de Privacidade da instituição e a obrigação de sigilo.

Risco: Acesso não autorizado aos documentos e informações de ouvidoria armazenados em meios eletrônicos.

Além dos dados pessoais que constem no sistema informatizado, a ouvidoria deverá proteger, do risco de acesso por pessoa não autorizada, os dados que, porventura, constem em documentos armazenados nas redes internas ou, na área de trabalhos dos computadores dos servidores e colaboradores da ouvidoria.

Boas práticas: Possuir sistema de gestão documental para armazenamento e acesso a documentos de ouvidoria em meio eletrônico.

Para um armazenamento seguro de documentos eletrônicos da ouvidoria, em especial, aqueles que, porventura, contenham dados pessoais dos manifestantes, é aconselhável que a organização possua um sistema de gestão de documentos.

Desta forma, além de deixá-los armazenados em um único local, é possível controlar o acesso a eles e, ainda, deixar as informações com acesso restrito, para que somente aquelas pessoas autorizadas possam acessá-las.

Ademais, neste sistema também ficam centralizadas as informações de um determinado processo, facilitando, sobremaneira, as tarefas do dia a dia.

Caso a organização não disponibilize de um sistema de gestão documental, pode seguir algumas boas práticas quanto ao armazenamento dos arquivos em rede interna, conforme abaixo:

- Organizar uma pasta para cada processo e dentro organizar subpasta;

- Nomear as pastas;
- Atribuir identificação específica aos documentos eletrônicos e aos escaneados;
- Utilizar caracteres simples;
- Não abreviar;
- Colocar data nos documentos com mais de uma edição;
- Ativar a indexação do seu sistema operacional.

Risco: Acesso não autorizado aos documentos e informações de ouvidoria reproduzidos em meio distinto ao sistema informatizado de ouvidoria, como impresso em papel ou copiado e encaminhado por correio eletrônico (e-mail) e whatsapp.

Não obstante a digitalização do serviço de ouvidoria estar em crescente expansão, não apenas, especificamente, com o sistema informatizado de ouvidoria, como também, com o uso de outros sistemas de tramitação de processos, a exemplo do Sistema Eletrônico de Informação (SEI), é compreensível que as ouvidorias estejam em níveis distintos de maturidade nesse processo, remanescendo situações em que o registro e a tramitação de manifestações ocorram em meio físico.

E, até mesmo em ouvidorias que utilizam sistema informatizado, é possível existir situações de indisponibilidade do sistema em uso, o que as levam a utilizar outras formas de registro e tramitação, dentre elas aquelas em meio físico, com documentação impressa em papel.

Outras duas circunstâncias que podem ensejar a produção de documentos de ouvidoria em meio distinto do sistema: a realização de ação itinerante e a captação de manifestações por meio de urnas coletoras.

Nesse contexto é importante estar claro que arquivos físicos também são regidos pela LGPD. Assim, se a ouvidoria recebe manifestações em formulários em papel e os coloca em um espaço sem segurança, por exemplo, apoiado em uma mesa em uma sala de acesso público e esses documentos se perdem, trata-se de incidente de segurança tanto quanto uma invasão em sistemas informatizados.

Boa prática: Levantar os fluxos de trabalho e estabelecer procedimentos considerando o eventual uso e armazenamento de documentos onde constem dados pessoais dos manifestantes, em meios físicos.

As ouvidorias devem buscar implantar mecanismos e o desenvolvimento de uma cultura de proteção dos dados pessoais do cidadão, independente do canal e do suporte utilizado para registro, seja ele físico, lógico ou analógico. Para isto, como já mencionado, é essencial manter uma boa gestão dos documentos eletrônicos armazenados nas redes internas, na área de trabalho dos computadores, encaminhados por e-mail, entre outros.

Especificamente, quanto aos documentos arquivados em meio físico, é importante que eles sejam mantidos em armários fechados e que haja barreiras físicas de proteção, a exemplo de cadeados, com a atenção à guarda das chaves.

Nesse sentido, entende-se como uma boa prática o levantamento dos fluxos de trabalho e estabelecimento de procedimentos adequados considerando o eventual uso e armazenamento de documentos onde constem dados pessoais dos manifestantes, em todos os formatos aplicáveis, como consta no primeiro passo para a adequação das ouvidorias à LGPD, de que trata capítulo 10 deste Guia.

A adequação ou a criação dos procedimentos deve considerar, além dos aspectos relacionados à LGPD, as normas arquivísticas e de segurança da informação vigentes e aplicáveis em todos os casos e para todas as ferramentas envolvidas na execução. Para isto, seguem algumas dicas:

Dica 1: Quando for indispensável a reprodução de dados em formatos distintos, por exemplo, de papel para documento eletrônico, observar os mecanismos de segurança previstos para os dois suportes.

Dica 2: Quando da utilização de outros meios, diferentes do sistema de ouvidoria, como e-mail ou Sistema SEI, inserir mecanismos que dificultem a reprodução ou utilização das informações ali presentes, tais como mensagem em formato "imagem" ou inserção de marca d`água.

Dica 3: O sistema de ouvidoria deve prever, em seus mecanismos de rastreabilidade, o registro dos dados e informações gravadas e/ou distribuídas em outra ferramenta. Tal procedimento visa à rastreabilidade dos dados pessoais e à mitigação de riscos decorrentes da falha na segurança.

Dica 4: Fomentar a importância e as vantagens de uso do sistema de ouvidoria para fins de atendimento, evitando a utilização de mecanismos como e-mail e sistemas diversos para cadastro e tramitação de demandas, dando preferência à disposição dos dados coletados e tramitados exclusivamente no sistema informatizado de ouvidoria.

Boa prática: No caso de acolhimento de manifestações em formulários em papel, observar requisitos de segurança da informação, como a coleta e acesso apenas por atendente autorizado.

Nos casos das ouvidorias que utilizarem como canal de captação de manifestações as urnas coletoras, onde as manifestações estarão registradas em um formulário em papel, os seguintes requisitos de segurança devem ser observados:

- O material utilizado na confecção da urna não deve ser transparente, evitando assim que seja possível a leitura dos formulários que estejam nela depositados; assim, ela pode ser translúcida ou adesivada;
- A urna deverá estar, permanentemente, trancada com cadeado;
- A coleta deverá ser realizada, exclusivamente, por servidor da ouvidoria ou aquele por ela autorizado, com termo de confidencialidade devidamente assinado;
- A frequência de recolhimento deve ser pré-estabelecida e deverá estar afixada, junto à urna, para conhecimento do usuário.

Estas medidas visam evitar os riscos, por exemplo, de extravio de formulários dentro das urnas ou do não depósito de novos formulários, pelos usuários da ouvidoria, visto a urna estar cheia.

De toda forma, é importante reforçar que a coleta de manifestações por meio de urnas não permite a verificação da titularidade, impedindo assim, o exercício de alguns direitos previstos na LGPD, como de correção de dados incompletos, inexatos ou desatualizados, tratados em capítulo específico neste Guia.

Boas práticas: Nos casos de formulários em papel utilizados em ações itinerantes de ouvidoria, importante que a sua coleta seja realizada, exclusivamente, por servidor ou colaborador da ouvidoria devidamente autorizado e o mesmo se aplica àquele que fará a transferência dos dados do meio físico para o sistema informatizado de ouvidoria.

Em ações itinerantes, é importante também observar os cuidados com a guarda e manuseio dos formulários de manifestações coletados, para que não haja seu extravio ou acesso de pessoa não autorizada.

É bem comum, nessas ações, que haja o engajamento de servidores e colaboradores de outras áreas, distintas da ouvidoria, com o intuito de ampliar o seu alcance. Todavia, é importante reforçar que, mesmo nessas ações, a coleta dos dados pessoais deve ser realizada, exclusivamente, por servidor. Na possibilidade de coleta por colaborador, ou seja, funcionários terceirizados ou estagiários, é importante que tenham, previamente, assinado termo de confidencialidade.

11.2. BOAS PRÁTICAS E RISCOS ASSOCIADOS ÀS ETAPAS DO PROCESSO DE TRATAMENTO DE MANIFESTAÇÕES DE OUVIDORIA

Nesta seção, estão reunidos os riscos e boas práticas identificados no processo de tratamento de manifestações de ouvidoria, especificamente, em cada uma de suas etapas, sendo elas o acolhimento e registro, a tramitação, a conclusão ou resposta e a emissão de relatórios.

Não obstante essa disposição por etapas, é possível que um risco possa vir a ocorrer em mais de uma delas, estando apresentada aqui aquela considerada a que havia maior probabilidade de ocorrência do risco.

Etapa Acolhimento e registro

A etapa ou o momento de acolhimento e registro da demanda é o modo habitual por meio do qual os usuários que procuram a ouvidoria realizam o primeiro contato com o atendimento em si. Nessa etapa, as demandas dos usuários são recepcionadas em forma de reclamações, denúncias, solicitação de providências, elogios, dentre outras, culminando no conhecimento da alta gestão a fim de tomada de ações.

A coleta de dados realizada nesta etapa constitui-se em uma das operações de tratamento realizada durante o contato inicial dos(as) cidadãos(ãs) nas ouvidorias.

Importante observar que a coleta de dados deverá estar pautada no princípio da necessidade, como forma de assegurar ao titular que não sejam solicitados dados desnecessários ou excessivos diante da demanda apresentada, bem como que os seus dados não sejam utilizados para outros fins.

Como boas práticas, de maneira geral, no cadastro inicial do cidadão, se houver, e no registro da manifestação realizados nas ouvidorias, elencam-se as seguintes ações a serem incorporadas ao trabalho da equipe da ouvidoria e objeto de atualização, sempre que necessário:

1. A rotina de conferência dos dados coletados deverá ser realizada de forma atenta e minuciosa, com o objetivo de evitar erros na identificação do cidadão(ã);
2. Tendo em vista o princípio da necessidade, a ouvidoria coletará os dados estritamente necessários ao atendimento da demanda apresentada pelo titular do dado e adotará medidas internas, que visem à proteção dos dados coletados de acessos não autorizados, de situações acidentais ou ilícitas. Desta forma, medidas de segurança deverão ser adotadas nos sistemas e procedimentos de coleta e armazenamento dos dados utilizados pela ouvidoria;
3. Nos sistemas informatizados de autoatendimento das ouvidorias, deverá ser esclarecido ao titular dos dados a finalidade e a necessidade de coleta dos dados, bem como a forma que ocorrerá o tratamento dos dados no âmbito do órgão e as medidas de contenção ou mitigação dos riscos associadas às violações de segurança, à luz do princípio da transparência previsto na Lei nº 13.709 de 14 de agosto de 2018, Lei Geral de Proteção de Dados (LGPD) e
4. No caso da coleta de dados pessoais ou pessoais sensíveis complementares, para fins de estudo do perfil do usuário dos serviços, para adequação de canais de atendimento e melhoria de políticas públicas, por exemplo, o titular deverá ser comunicado sobre essa possibilidade de utilização do dado no ato da coleta com clareza e objetividade.

A partir desse ponto, passam a ser apresentadas as boas práticas correlacionadas a riscos identificados na etapa de acolhimento e registro de manifestações de ouvidoria.

A observância dos princípios da necessidade e finalidade é de extrema importância em todas as etapas do fluxo da manifestação de ouvidoria, sobremaneira, na etapa de acolhimento e registro, quando ocorre a coleta dos dados pessoais.

Nesse sentido, a ANPD, posiciona-se no Guia Orientativo Tratamento de Dados Pessoais pelo Poder Público que, "muitas vezes, a coleta indiscriminada de dados pessoais é o ponto principal a ser considerado, de modo que, ao invés de eventual e posterior atribuição de sigilo, a proteção será mais efetiva com a própria dispensa da coleta ou com a eliminação da informação"

Riscos: Inexistência, não apresentação ou falta de clareza do Termo de Uso e da Política de Privacidade.

Este risco corresponde a não apresentação do Termo de Uso e da Política de Privacidade ao titular do dado pessoal no ato de cadastro, junto à ouvidoria ou de registro de manifestações, que pode se dar pela inexistência dos instrumentos ou pela não disponibilização no momento.

Pode haver, ainda, a apresentação do Termo de Uso e da Política de Privacidade, porém, pode não existir clareza na linguagem, dificultando ou, até mesmo, impedindo a compreensão.

E ambas as situações podem ocasionar, inclusive, a inibição do registro de manifestações pelo titular, em razão da insegurança gerada ao usuário, pelo desconhecimento do uso que será dado à informação.

Boas práticas: Elaborar e apresentar ao usuário do serviço de ouvidoria, no ato de cadastro, junto à ouvidoria, se houver, ou de registro de manifestações, o Termo de Uso e a Política de Privacidade do serviço.

Em atenção ao princípio da transparência, o cidadão necessita ter ciência da finalidade com qual serão utilizados os seus dados pessoais, inclusive, com qual temporalidade. Para isso, ao utilizar os serviços da ouvidoria, o usuário deve confirmar que leu, compreendeu e tem ciência dos termos e políticas aplicáveis, ficando a eles vinculado.

O Termo de Uso é o documento legal por meio do qual o órgão deverá definir as regras da utilização dos serviços informatizados de ouvidoria. Igualmente, por intermédio da Política de Privacidade, o órgão deve esclarecer como os dados pessoais dos usuários serão tratados.

Portanto, é imprescindível que a instituição elabore Termo de Uso e Política de Privacidade no tocante aos serviços de ouvidoria do órgão

e divulgue no sítio eletrônico oficial e, nele também, deve ser feita ampla divulgação, caso haja posterior atualização desses documentos.

Nos casos das ouvidorias que utilizam cadastro prévio para realização de manifestações, a ciência do usuário no Termo de Uso e na Política de Privacidade poderá ser requisitada uma única vez, no ato do cadastro e não a cada manifestação registrada.

Para elaboração do Termo de Uso e da Política de Privacidade, pode ser utilizado, de maneira referencial, o Guia de Elaboração de Termo de Uso e Política de Privacidade para serviços públicos, publicado pelo Comitê Central de Governança de Dados do Poder Executivo Federal.

Risco: Coleta de dados realizada por atendente não autorizado.

Nesse caso, o risco decorre da ausência de compromisso dessa pessoa com os protocolos adotados pelo setor e a responsabilização direta sobre as informações coletadas.

Boas práticas: Definir os servidores e colaboradores das equipes que estarão autorizados a realizar os atendimentos aos titulares dos dados, promover as ações de capacitação necessárias e garantir a ciência do dever de sigilo por meio de assinatura de termo de confidencialidade ou documento análogo pelos colaboradores.

A ouvidoria deverá definir os perfis de acesso ao sistema informatizado, junto com a área de tecnologia da informação, com permissões específicas e compatíveis com a finalidade da utilização do dado.

Recomenda-se, inclusive, de acordo com o quantitativo de servidores que compõem a equipe, definir perfis distintos para as diversas operações que podem ser realizadas na ferramenta, a exemplo de cadastro, consulta, encaminhamentos, resposta, administração, gestão, entre outros.

No contexto específico da LGPD, ou seja, na coleta de dados pessoais na etapa de acolhimento do fluxo da manifestação de ouvidoria, especificamente, quanto ao atendimento presencial do titular, é importante que seja realizada a seleção de quais servidores e colaboradores estarão autorizados para realização deste atendimento e haja a devida comunicação à equipe.

E, após essa definição, é importante observar se os colaboradores já assinaram o termo de confidencialidade, como mais uma medida de proteção dos dados pessoais.

Importante ressaltar que, nos casos de servidores públicos, os estatutos de servidores federais, estaduais e municipais, e em alguns casos, códigos de ética específicos de determinadas carreiras, em geral, já preveem a obrigação do sigilo profissional e, por este motivo, o termo de confidencialidade não se faz necessário.

Diferentemente, quanto aos colaboradores que atuam sob contrato de fornecimento de mão-de-obra especializada, a referida obrigação deve constar no contrato administrativo firmado com a pessoa jurídica e, neste caso, pela ausência de vínculo do colaborador com a administração pública, o termo de confidencialidade torna-se indispensável.

Tal procedimento se aplica caso o relacionamento do colaborador com o órgão público se dê por meio de outras formas de parcerias, como estágios, convênios e termos de cooperação, se for o caso.

Concomitantemente às definições e implementações em relação aos perfis e autorizações de acessos aos sistemas e informações de ouvidoria, devem ser realizadas orientações constantes, promovidas capacitações periódicas e incentivado o estudo e a participação de cursos e demais eventos voltados à ouvidoria, à proteção de dados pessoas e à ética profissional.

Risco: Impossibilidade, via sistema informatizado, de verificação e autenticação da titularidade do usuário do serviço de ouvidoria.

Para o exercício dos direitos previstos na LGPD, por meio das ouvidorias Públicas, se faz necessário não apenas a identificação do titular do dado pessoal, como também a sua verificação e autenticação.

Isso se faz necessário para, entre outros, mitigar o risco de, equivocadamente, fornecer dados pessoais de um cidadão para outrem.

Boa prática: Implantar funcionalidade no sistema informatizado de ouvidoria que permita a verificação e autenticidade da titularidade do usuário do serviço de ouvidoria.

Para que o titular possa exercer os direitos de que trata a LGPD por meio eletrônico, sem que precise, necessariamente, direcionar-se presencialmente a um ponto de atendimento, para identificação, os sistemas de ouvidoria devem contar com ferramenta que permita essa verificação e autenticação com segurança.

A verificação da autenticidade da identidade do titular contribui para a segurança e efetividade do processo de atendimento às manifestações registradas para o exercício dos direitos previstos na LGPD.

Neste contexto, as ouvidorias que utilizam o FalaBR, e atendam ao requisito de verificação do cadastro do usuário pela validação do selo Gov.BR já atendem a este requisito e, aquelas que possuam sistema próprio e específico, podem considerar a utilização do login único do Governo Federal – o gov.br -, disponibilizado gratuitamente a Estados e Municípios

A conta Gov.BR é um meio de acesso digital do usuário aos serviços públicos digitais que garante a identificação de cada cidadão que acessa os serviços digitais do governo federal. Por meio de processo simples de adesão, junto ao Ministério da Economia, é possível utilizar a funcionalidade no sistema informatizado de ouvidoria já em uso.

Para aquelas ouvidorias que optem por utilizar o Gov.BR em seus sistemas informatizados, uma recomendação importante é que escolham, entre os níveis de autenticação bronze, prata e ouro disponíveis, o nível verificado – Prata ou Nível Comprovado Ouro.

O procedimento para solicitação de integração ao gov.br inicia-se com o encaminhamento de e-mail ao endereço atendimentogovbr@economia.gov.br.

ATENÇÃO!

Nos casos de ouvidorias que utilizem outro mecanismo eletrônico de verificação, lembramos que, nos termos do art. 28 da Lei 14.129/2021, o Cadastro de Pessoas Físicas (CPF) e o Cadastro Nacional da Pessoa Jurídica (CNPJ) são os números suficientes para identificação do cidadão ou da pessoa jurídica. Assim, esses devem ser os únicos números de identificação solicitados na etapa de acolhimento e registro, bem como nos cadastros dos sistemas informatizados de ouvidoria, se houver.

Não obstante a aplicação da Lei aos Estados, Distrito Federal e Municípios depender de regulamentação em atos normativos próprios, é recomendável que sejam seguidos os mesmos parâmetros, de forma a garantir maior uniformidade de atendimento aos usuários dos serviços públicos, de maneira geral.

Nos atendimentos presenciais, é importante que essa verificação de titularidade seja realizada pelo atendente autorizado, por meio da apresentação de documento oficial. Uma boa prática, nos atendimentos presenciais, é a elaboração e aplicação de check list ou roteiro, com o intuito de garantir que essa verificação seja realizada.

Enquanto não implantada funcionalidade que permita a verificação e autenticação eletrônica, recomenda-se às ouvidorias que só respondam a pedidos de que tratam art. 18 e 20 da LGPD mediante atendimento presencial, no qual a verificação poderá ser realizada por atendente autorizado. Contudo, importante ficar claro que essa deve ser uma medida provisória, devendo ser providenciada a adequação do sistema informatizado em uso com a maior brevidade possível.

Etapa Tramitação

A tramitação é a movimentação de documentos ou processo, tanto interno ou externamente na entidade. No caso específico da ouvidoria, a tramitação está associada à fase de condução das manifestações recepcionadas junto às unidades técnicas com vistas a apurar e tomar providências em relação às manifestações registradas.

Neste sentido, algumas boas práticas podem ser implementadas a fim de mitigar os riscos relacionados a esta etapa, a exemplo da rotina de conferência e revisão dos dados coletados antes de proceder à tramitação da manifestação para a área responsável, bem como as seguintes:

a) No caso da necessidade de esclarecimentos adicionais, demandado pelo responsável pela informação no órgão ou do acréscimo de dados pelo titular, após etapa de acolhimento e registro pela ouvidoria, deverá ser observado o princípio da necessidade, devendo ser coletados apenas os dados pessoais estritamente necessários para o atendimento da demanda. Nesse sentido, nas situações em que o gestor da área solicitar dados pessoais do titular

adicionais para análise da demanda, a ouvidoria deverá solicitar a justificativa com o intuito de resguardar os princípios da necessidade, adequação e finalidade do tratamento de dados e a proteção do usuário, nos termos do Código de Defesa dos Usuários de Serviços Públicos.

b) Além da solicitação de justificativa pelo gestor para coleta adicional de dados na etapa de tramitação, também é uma boa prática questioná-lo se o dado necessário já não está disponível no órgão em algum outro banco de dados.

c) Nos sistemas de tramitação de manifestações orienta-se que seja apresentado aos servidores e colaboradores da ouvidoria um campo específico, para preenchimento da finalidade a que se propõe a utilização dos dados coletados, a fim de reforçar a cultura do não aproveitamento dos dados para finalidade incompatível.

Desse ponto em diante, apresentam-se boas práticas especificamente relacionadas a riscos identificados na etapa de tramitação de manifestações de ouvidoria.

Risco: Utilização dos dados coletados para finalidade incompatível.

Este risco pode ocorrer pelo desconhecimento do servidor ou colaborador da Política de Privacidade do órgão, onde devem constar as possíveis formas de utilização dos dados pessoais coletados.

Boa prática: Divulgar amplamente a Política de Privacidade no órgão e comunicar ao titular de dados pessoais alterações no Termo de Uso, quando houver.

A Política de Privacidade é um documento que deve esclarecer como todo o órgão, inclusive a ouvidoria, lida com as informações coletadas de seus usuários, limitando as ações dos servidores públicos e colaboradores no uso desses dados.

Desta forma, além de devidamente instituída, é essencial que haja ampla disseminação interna da Política de Privacidade e ações contínuas de capacitação, bem como exista procedimento formal de apuração de conduta irregular de servidores e colaboradores, no caso específico, relacionado a uso de dados pessoais de maneira incompatível com aquela definida na Política de Privacidade do órgão.

Importante, também, observar que quaisquer alterações no Termo de Uso e na Política de Privacidade precisam ser comunicadas aos usuários da ouvidoria. O envio de e-mails e a divulgação no sítio eletrônico oficial da ouvidoria são exemplos de como pode se dar essa comunicação.

Risco: Modificação indevida dos dados realizada por servidor ou colaborador da ouvidoria ou por erro do sistema informatizado de ouvidoria

Dentre as operações de tratamento, entende-se como modificação o ato ou efeito de alteração do dado, sendo, inclusive, direito assegurado ao titular, previsto no inciso III, art. 18 da LGPD, a correção de dados incompletos, inexatos ou desatualizados.

Todavia, a modificação deve ocorrer mediante provocação do titular ou se verificada incongruência com outra base, por exemplo, e não, deliberadamente, por servidor ou colaborador da ouvidoria.
Outra causa possível para a ocorrência deste risco é a modificação decorrente de erro do servidor ou colaborador da ouvidoria ou, ainda, por erro do sistema informatizado de ouvidoria.

Boa Prática: Definir bloqueios no sistema a fim de evitar modificações indevidas dos dados e dispor de registro de *logs* no sistema informatizado de ouvidoria.

Para evitar a modificação indevida de dados pessoais, comprometendo sua integridade, é desejável que o sistema informatizado de ouvidoria possua bloqueios que impeçam essa operação, sendo permitida, apenas, a alguns perfis de usuários do sistema, que possuam maiores permissões e que poderão realizar essa operação, exclusivamente, mediante solicitação do titular de dados pessoais ou se forem detectadas inconsistências a partir de outras bases.

Em adição, é necessário que os sistemas possuam registro de logs, que corresponde aos registros de atividades que um usuário realiza dentro do sistema. Eles, geralmente, estão registrados de forma cronológica por data e hora e é possível monitorar as atividades que são realizadas no sistema, sendo muito úteis em verificações futuras. Além disso, há a possibilidade de saber quem acessou o sistema na data e hora, quem realizou alterações de registro e o que foi alterado. Também pode ajudar a identificar quando um sistema está sendo atacado por hackers, pois há como registrar falhas de autenticação e identificar de qual endereço de IP está sendo acessado.

Os arquivos de logs devem ser protegidos com total segurança para que não haja alterações em suas informações. Como boa prática, um arquivo de registro de logs deve conter as seguintes informações:

- Datas e hora de entrada e saída do sistema;
- Identificação dos usuários;
- Em caso de Sistemas Web, devem ser armazenados o IP de acesso;
- Registros das tentativas de acesso (aceitas e rejeitadas) ao sistema;
- Informações que foram incluídas, alteradas e excluídas.

Ainda, é importante que os logs sejam monitorados e revisados com frequência, principalmente para evitar possíveis ataques de hackers e corrigir possíveis falhas de segurança que o sistema possa ter. O registro de logs, geralmente, não fica visível aos usuários do sistema, até mesmo por questões de privacidade das informações que são registradas e, dependendo do tamanho do log, pode se tornar inviável carregar as informações para a tela do usuário. Entretanto, o setor de tecnologia da informação deve ter acessos a essas informações e monitorar, constantemente, possíveis falhas de segurança.

Além disso, os registros de logs também devem ser feitos nos servidores de tecnologia da informação que estão hospedados nos sistemas para fins de acompanhamento de realização de backup ou outras alterações de infraestrutura que possam ocorrer.

Em síntese, os logs são informações fundamentais que a área de tecnologia da informação deve manter com total segurança, seja para verificar possíveis invasões dentro do sistema ou servidor de Tecnologia da Informação e Comunicação (TIC), como para verificar quem realizou uma determinada alteração nas informações contidas no sistema.

Identificado o servidor ou colaborador de ouvidoria que deu causa à modificação indevida de dados pessoais, deve ser dado conhecimento à área de apuração para tomada de providências necessárias à devida apuração do ocorrido.

Diferentemente, para evitar modificação de dados por força de erro do sistema informatizado, se faz necessária a manutenção de uma boa governança de tecnologia da informação, que tem papel essencial para a ouvidoria digital. Assim, possuir documentação de sistemas, infraestrutura e banco de dados ajuda, sobremaneira, a evitar erros que possam ocorrer durante os processos.

Ainda, para garantir a integridade dos dados é preciso que a organização possua logs de alterações de backup, pois caso seja necessária a restauração de algum backup, é importante que não afete nenhuma solicitação já realizada pela ouvidoria.

Risco: Perda dos dados por falha na infraestrutura de Tecnologia da Informação.

Este risco se refere à falha ou indisponibilidade do sistema informatizado que acarrete a eliminação indevida de dados armazenados.

Boa Prática: Buscar, junto à área de Tecnologia da Informação, a disponibilidade de infraestrutura adequada para suporte ao funcionamento do sistema informatizado de ouvidoria e ao banco de dados.

Para garantir a segurança dos dados armazenados no sistema informatizado em uso pela ouvidoria, é necessário, além do atendimento aos requisitos constantes na Política de Segurança da Informação, que ele seja acompanhado por equipe especializada que garanta sua manutenção.

Nesse contexto, não apenas o sistema, como toda a infraestrutura de tecnologia que dá suporte ao seu funcionamento, deve ser garantida pelo órgão ao qual a ouvidoria está vinculada.

A infraestrutura de tecnologia consiste em um conjunto de componentes necessários para a operação e gerenciamento de serviços de tecnologia que são, além do software, as máquinas e equipamentos utilizados, o gerenciamento de dados e serviço e as redes.

Para tanto, são necessários investimentos em pessoal, sistemas e equipamentos e, para tanto, deverá o gestor máximo do órgão compreender a importância do tema, e envidar esforços no sentido de prover a infraestrutura adequada.
Risco: Perda dos dados por extravio de documentos em papel.

Este risco se refere especificamente ao extravio de documentos da ouvidoria que constem em pastas ou papel, como exemplo, formulários de manifestação preenchidos, relatórios de manifestação impressos a partir do sistema informatizado e relatórios gerenciais de ouvidoria que estejam em meio físico.

Boa Prática Convém implantar controles e definir o perímetro de segurança para proteção das áreas onde estejam os documentos em papel.

De acordo com a ISO 27002, convém que as informações que constem em papel sejam guardadas em lugar seguro, como cofres ou arquivos trancáveis, especialmente, quando o ambiente estiver trancado ou desocupado, ou seja, fora do horário de funcionamento da ouvidoria.

Importante, ainda, para proteção do ambiente físico, que portas e janelas sejam trancadas quando estiverem sem um servidor da equipe de ouvidoria no ambiente, bem como haja proteção externa nessas janelas, especialmente, quando a sala da ouvidoria fica localizada no térreo.

Ainda nesse contexto, importante que o ambiente físico contenha proteção contra incêndio, como portas corta-fogo e inundações.

Por fim, importante observar, quando do uso de impressoras a autorização de uso, bem como a retirada imediata de documentos que contenham informações pessoais desses equipamentos.

Risco: Vazamento de dados por pessoa com acesso autorizado, de forma deliberada ou não.

O vazamento, neste contexto, consiste em pessoa autorizada acessar os dados de ouvidoria e/ou dar acesso, de forma deliberada ou não, a terceiro não autorizado.

Boas práticas: Manter ações de capacitação e orientação constantes, disseminação do Código de Ética aplicável e fomento à Política Correicional.

De maneira análoga à modificação de dados por servidor ou colaborador da ouvidoria, de maneira deliberada ou não, no caso de identificado o vazamento de dados pessoais, deverá ser dado conhecimento do fato à área de tratamento de incidentes de TIC e à área de apuração. Além disso, o fato deverá ser comunicado aos titulares, de acordo com as disposições da ANPD, bem como será necessária a elaboração do já mencionado Plano de Resposta a Incidentes de Segurança.

Para coibir conduta irregular do servidor da ouvidoria, bem como dos gestores que respondem às manifestações e pedidos de acesso à informação que contenham dados pessoais existentes, apresenta-se como uma boa prática o fomento à Política Correicional, nos termos da legislação aplicável ao ente federativo, que preveja as sanções àquele que utilize o dado com finalidade inapropriada.

Uma vez existente a política e definidos os procedimentos, ao ser detectado indício de conduta irregular do servidor, devem-se adotar medidas urgentes de comunicação ao órgão correicionais, para que sejam adotadas as medidas cabíveis.

No caso de a conduta irregular ser cometida por colaborador de ouvidoria, que nela atua sob formalização de contrato administrativo, deverão ser aplicadas as sanções previstas no termo contratual.

Neste contexto, é importante que haja o alinhamento da ouvidoria com o Programa de Integridade do órgão ao qual está vinculada, se já instituído e a proposição de medidas capazes de mitigar os riscos associados às suas atividades.

Poderá a ouvidoria, ainda, contribuir com a criação de indicadores capazes de demonstrar os ajustes necessários à prevenção, detecção e apuração de condutas inadequadas no âmbito do órgão.

E por fim, para coibir desvios de condutas, apresenta-se como uma boa prática a atuação preventiva com ações de capacitação e orientação constantes e disseminação do Código de Ética aplicável.

Risco: Vazamento de dados decorrente do registro e tramitação de manifestações em meio físico ou por e-mail, nos quais não é possível o rastreamento de quem teve acesso.

Este risco está sendo aqui abordado no contexto da tramitação física (em papel) ou eletrônica, especificamente, por meio de e-mail, de manifestações, sendo essas situações em que não existem meios de controle efetivo de quais servidores e colaboradores, ou até mesmo terceiros, tiveram acesso àquelas informações.

Boa prática: Dar preferência ao registro e tramitação de manifestações por sistema informatizado, a exemplo do Fala.BR, disponibilizado gratuitamente pela Ouvidoria-Geral da União.

Num contexto de crescente digitalização de serviços públicos, a ouvidoria é impulsionada a se adequar a esta realidade, não apenas pela ampliação do acesso ao serviço, como também, considerando os requisitos de proteção de dados pessoais, de observância obrigatória, previstos na LAI e, mais recentemente, na LGPD.

Nesse sentido, consiste em boa prática dispor de sistema informatizado para registro, tramitação e conclusão de manifestações, utilizando-se de documentos em meio físico ou o uso do correio eletrônico apenas de maneira residual ou excepcional.

O Fala.BR é a plataforma integrada de ouvidoria e acesso à informação do Poder Executivo Federal, desenvolvido pela Controladoria-Geral da União (CGU), que permite a qualquer cidadão encaminhar manifestações e pedidos de acesso à informação pela mesma ferramenta.

Qualquer Estado ou Município pode utilizar a plataforma gratuitamente, devendo, para tanto, fazer a adesão à Rede Nacional de Ouvidorias e ao sistema Fala.BR propriamente dito.

Conforme orientações da Ouvidoria-Geral da União (OGU), para adesão é necessário o preenchimento e envio de Termo de Adesão Eletrônico constante no site www.gov.br/ouvidorias.

Etapa Conclusão ou Resposta

A etapa de conclusão ou resposta consiste no momento do fluxo da manifestação, em que a área ou gestor responsável pelo processo, serviço ou informação, encaminha a resposta da manifestação à ouvidoria, a qual, por sua vez, deverá analisá-la.

Nesta análise, que deve anteceder o encaminhamento ao usuário, a ouvidoria pode propor complementações ou alterações na resposta, inclusive, para garantir a sua compreensão pelo usuário.

Importante observar alguns riscos potenciais que podem ocorrer nesta etapa e, a critério de cada ouvidoria, realizar ações que visem a mitigá-los, como as boas práticas dispostas a seguir:

Risco: Acesso a titular de dado a dado pessoal de outrem.

Na etapa de acolhimento e registro é possível, observados os princípios da finalidade e necessidade, que tenha havido a coleta de dados pessoais do usuário do serviço de ouvidoria. Da mesma forma, existe a possibilidade de, na resposta do gestor, conter outros dados pessoais, os quais são encaminhados ao titular como parte das providências adotadas.

Neste contexto, o risco ora apresentado consiste em encaminhar a resposta da manifestação que contenha dados pessoais a terceiros, e não ao titular dos dados.

Boa prática: Realizar conferência dos dados pessoais contidos na resposta do gestor antes de encaminhar resposta ao manifestante.

No recebimento da resposta do encarregado ou área competente com dados pessoais, o ouvidor deverá observar se os dados correspondem ao titular que ingressou com a demanda e, em negativo, retornar a demanda para o encarregado ou área competente para análise e correção.

A resposta final deve ser emitida sempre ao titular dos dados pessoais constantes na inicial. O cuidado do ouvidor, ao realizar a análise final antes de encaminhar a resposta ao demandante, deverá realizar um *check-list* básico, confirmando os dados pessoais entre outras informações coletadas na inicial, para assegurar que está encaminhando a resposta ao real titular dos dados pessoais. Em caso de conflito de dados, deve-se reportar ao setor que elaborou a resposta para que possa reavaliar o documento e realizar as correções necessárias.

Importante reforçar que a existência de dados pessoais não pode ser argumento para a negativa do pedido de acesso à informação, reiterando o argumento do início do Guia de harmonia entre LAI e LGPD.

Risco: Ausência de informações estruturadas que permitam a tomada de decisão pelo Controlador quanto às manifestações apresentadas pelos titulares de dados pessoais.

Em qualquer ação, processo ou projeto, a informação correta é essencial para que os gestores consigam decidir da melhor forma. Nesse contexto, este risco consiste na ausência das informações e conhecimentos necessários para a tomada de decisão do controlador quanto ao requerimento do titular do exercício de direitos de que tratam a LGPD.

Boa prática: Criar Unidade de Governança para Proteção de Dados Pessoais para subsidiar a tomada de decisão pelo controlador.

Para tomada de decisão, no que concerne à proteção de dados pessoais, são necessárias informações relacionadas, entre outros, à própria LGPD, LAI, Lei de Defesa dos Usuários de Serviços Públicos, Marco Civil da Internet, gestão de riscos e processos.

Quanto à segurança da informação, são informações relevantes para a tomada de decisão as boas práticas produzidas pela *International Organization for Standardization* (ISO), em especial, as ISO 31000, 31010, 27001, 27002, 27004, 27005, 27701, 29100.

Neste contexto, considerando a multidisciplinaridade dos conhecimentos e informações necessárias, é interessante que o órgão disponha de Unidade de Governança para Proteção de Dados Pessoais, na forma de comissões, comitês, grupos de trabalho, entre outros, não apenas para coordenar e orientar a implementação das ações necessárias à adequação à LGPD, como já mencionado neste Guia, mas também para assessorar o controlador e o encarregado na tomada de decisão em relação às manifestações dos titulares de dados.

É aconselhável, ainda, que a composição da referida unidade contemple pessoas envolvidas na governança de dados mais ampla da instituição, para que as decisões a respeito de dados pessoais estejam em consonância com outras medidas relativas à gestão de dados de forma geral.

<u>Etapa Emissão de Relatórios</u>

Uma das atribuições precípuas da ouvidoria, realizada de maneira concomitante com os processos de atendimento, é a proposição de correção e melhorias nos serviços e políticas públicas, que se dá, em geral, por meio da produção de informações estratégicas e emissão de relatórios gerenciais.

O Modelo de Maturidade em Ouvidoria Pública (MMOuP), desenvolvido pela Controladoria-Geral da União, com consultoria do Programa da União Europeia para Coesão Social na América Latina (EUROsociAL), atribui nível otimizado no objetivo gestão estratégica de informações, às ouvidorias que realizam *"(...) análises quantitativas e qualitativas dos dados coletados, segundo metodologia científica*

transparente e validada e por meio de parâmetros definidos em conjunto por ela e pelos gestores responsáveis pela tomada de decisão".

Além disso, o modelo considera estar no nível máximo de maturidade no elemento "produção de informações estratégicas", as ouvidorias que "além do encaminhamento dos processos de manifestações de ouvidoria, a unidade produz anualmente o Relatório de Gestão de que tratam os artigos 14 e 15 da Lei 13.460, de 2017, e instituiu rotinas de comunicação aos gestores dos serviços, periodicamente ou em decorrência de eventos concretos por ela identificados. Adicionalmente, dados quantitativos relacionados às avaliações de serviços e manifestações são disponibilizados automaticamente aos gestores por meio de painéis gerenciais".

Em adição, independentemente do processo regular de análise dos dados, sempre que uma informação considerada estratégica para o órgão é levada ao conhecimento da ouvidoria por meio de uma manifestação ou por outras formas, deverá a ouvidoria realizar a análise de maneira sistêmica, considerando, inclusive, dados de outros processos ou sistemas, externos à ouvidoria e registrá-la em relatório temático, que deverá ser encaminhado tempestivamente aos gestores, para tomada de decisão.

Nesse contexto, a temática da proteção de dados pessoais, com o advento da LGPD, passa formalmente a integrar os temas que poderão ser apresentados à ouvidoria pelos seus usuários ou, conforme denomina a Lei, pelos titulares de dados pessoais. Assim, como ocorre com os demais temas a ela apresentados, espera-se da ouvidoria a proposição de aprimoramento dos serviços e das políticas públicas voltadas à proteção dos dados pessoais a partir da análise das manifestações registradas na ouvidoria.

Como nas demais etapas do fluxo da ouvidoria, alguns riscos relacionados à proteção de dados são identificados na etapa de emissão de relatórios, e algumas medidas poderão ser implementadas, com o fim de mitigá-los, como as que serão tratadas a seguir.

Risco: Na avaliação dos dados para produção de análises estatísticas e relatórios gerenciais, dispor de dados pessoais em documentos preparatórios ou versões internas do documento.

O acesso aos dados pessoais dos usuários da ouvidoria armazenados no sistema informatizado de ouvidoria deve ser controlado pela infraestrutura de segurança da informação, como permissões de acesso.

Aqueles que acessam os dados para realização de avaliações, análises e emissões de relatórios gerenciais e estatísticos devem zelar pela confidencialidade dos dados e a privacidade dos usuários não apenas no produto final daquele trabalho, onde constem os dados, como também em toda documentação preparatória emitida ou consultada.

Como exemplo desta documentação preparatória é possível citar planilhas com dados das manifestações, documentos em rascunho ou versões anteriores antes da finalização.

Boa prática: Garantir que o armazenamento de arquivos de ouvidoria obedeça a Política de Segurança da Informação do órgão.

A Política de Segurança da Informação reúne as sistemáticas e procedimentos de segurança da informação aplicáveis no âmbito do órgão público, para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados e informações tratadas, além de visar garantir a consistência, a privacidade e a confiabilidade dos dados e informações.

Exemplo prático de procedimento de segurança que poderá constar na Política para mitigar o risco analisado é limitar os modelos de extração de dados gerenciais do sistema a fim de que os campos de qualificação não sejam exportáveis.

Nesse contexto, poderão as ouvidorias fomentar e contribuir com a instituição de Política de Segurança da Informação, no âmbito dos órgãos aos quais estão vinculadas e, ainda, naqueles em que já tenha havido a referida instituição, que nela estejam contempladas questões específicas relacionadas ao tratamento de dados pessoais, conforme diretrizes da LGPD.

Constarão nesta Política os requisitos de segurança para o armazenamento de documentos, entre eles, aqueles utilizados em ouvidoria, como planilhas e relatórios de manifestações, bem como os tópicos a seguir:

a) Procedimentos de prevenção e detecção de vírus;

b) Gestão de riscos;
c) Classificação das informações como confidencial, restrito ostensivo;
d) Políticas de acesso aos sistemas;
e) Plano de treinamento de segurança da informação;
f) Plano de Respostas a Incidentes de Segurança;
g) Padrões mínimos de qualidade;
h) Consequências de violações de dados.

Boa prática: Garantir que o princípio da necessidade norteie todas as ações da ouvidoria, inclusive a realização de análises estatísticas e produção de relatórios gerenciais.

É importante que o princípio da necessidade norteie todas as ações da ouvidoria, inclusive a produção de análises estatísticas e relatórios gerenciais, nas quais devem constar, mesmo em documentos preparatórios ou versões internas do documento, exclusivamente, os dados necessários à análise a ser realizada.

Risco: Na emissão de relatórios gerenciais e estatísticos, equivocadamente, divulgar dados pessoais.

A divulgação de dados pessoais em relatórios elaborados pela ouvidoria só será possível se atender aos princípios da finalidade, adequação e necessidade. Caso ocorra qualquer divulgação, sem a observância desses, ensejará não apenas o descumprimento da LGPD e responsabilização do agente que deu causa, como também a perda da credibilidade da ouvidoria perante seu usuário.

Boa prática: Sistema informatizado de ouvidoria dispor de funcionalidade que permita a pseudonimização dos dados em consonância com a finalidade de tratamento.

Com a utilização da técnica de pseudonimização, o dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. Do ponto de vista da segurança da informação, essa técnica visa a contribuir para haver uma maior segurança dos dados, diminuindo os possíveis danos causados por um vazamento.

No contexto da ouvidoria, é importante que o sistema informatizado utilizado possua esta funcionalidade a ser aplicada aos dados pessoais excessivos e desnecessários, visando a proteção no caso das manifestações do tipo denúncias, conforme Resolução nº 3/2019 da Rede Nacional de Ouvidorias, que estabelece a Norma Modelo sobre Medidas Gerais de Salvaguarda à Identidade de Denunciantes

em prejuízo de ampliação para outras tipologias, de acordo com a especificidade da ouvidoria.

O sistema Fala.BR, já apresentado neste Guia, realiza o processo de pseudonimização de denúncias e informações sobre sua operacionalização estão disponíveis no Manual do sistema disponibilizado na Wiki da CGU.

Além disso, em âmbito federal, Portaria CGU nº 581, de 09 de março de 2021, que estabelece orientações para o exercício das competências das unidades do Sistema de Ouvidoria do Poder Executivo federal, entre outros, dispõe sobre o processo de pseudononimização de denúncias, especificamente, em seus artigos 34 e 35.

Esta Portaria estabelece como elementos de identificação, no mínimo, dados cadastrais, atributos genéticos, atributos biométricos e dados biográficos e, como meios de pseudonimização a serem adotados, dentre outros, produção de extrato, produção de versão tarjada e redução a termo de gravação ou relato descritivo de imagem.

Boa prática: Realizar conferência dos relatórios gerenciais, por superior ou par, a fim de garantir que não haja divulgação de dados pessoais sem observância dos princípios da finalidade, adequação e necessidade.

Ao emitir um relatório ou documento gerencial em ouvidoria, é necessário analisar, cuidadosamente, se o dado pessoal ali contido é necessário para a análise e providência em relação à demanda apresentada. Caso contrário, os dados não devem constar no relatório ou documento.

É possível exemplificar, com a situação comumente apresentada à ouvidoria, na qual, o número do CPF do titular consta na demanda, porém, não é necessário para seu atendimento. Neste caso, poderá ser aplicada técnica para mascarar os dados, da seguinte forma: ***000. ***- **.

No caso de relatórios gerados automaticamente nos sistemas informatizados de ouvidoria, uma vez que eles correspondem a uma extração dos dados cadastrados no próprio sistema, faz-se necessário que o procedimento de pseudonimização, quando aplicável, ocorra de maneira adequada nas etapas iniciais do fluxo de ouvidoria para que, na etapa final de emissão de relatórios, não haja divulgação equivocada de dados pessoais cadastrados.

Importante, ainda, com o advento da LGPD, que os relatórios comumente emitidos sejam revisados, com o intuito de identificar a divulgação indevida de dados pessoais.

É possível, também, que os relatórios de ouvidoria sejam gerados em ferramentas de edição de textos como Microsoft Word ou LibreOffice Writer, a partir de consultas aos sistemas de ouvidoria, o que pode aumentar, sobremaneira, o risco da divulgação indevida de dados pessoais. Formas de mitigar esse risco são a inclusão de etapas revisionais, por superior hierárquico ou um par, bem como estabelecimento de modelo padrão de relatórios, sempre que possível

11.3. BOAS PRÁTICAS RELACIONADAS AO COMPARTILHAMENTO DE DADOS ENTRE OUVIDORIAS

Nesta seção, abordamos o risco do compartilhamento de dados pessoais entre ouvidorias sem informar ao titular a finalidade desse compartilhamento. Esse risco refere-se à troca de dados entre diferentes ouvidorias (controladores distintos), sem que o titular seja previamente informado ou tenha consentido, o que pode resultar no uso indevido de seus dados. Embora esse risco também se aplique à tramitação interna, aqui o foco é na transferência de dados entre ouvidorias de órgãos distintos.

A LGPD, nos artigos 7º, 23º e 26º, estabelece que o compartilhamento de dados deve ser respaldado por bases legais adequadas, e o titular deve ser informado sobre a finalidade do tratamento. A Resolução nº 03/2019 da Rede Nacional de Ouvidorias, em seus §§ 5º e 6º, reforça que o consentimento do denunciante é necessário para o compartilhamento de denúncias com elementos identificáveis entre ouvidorias, ou, na ausência de consentimento, os dados devem ser pseudonimizados. Além disso, o Guia Orientativo sobre Tratamento de Dados Pessoais pelo Poder Público, da ANPD, destaca a importância de justificar o compartilhamento, assegurar transparência e proteger os direitos do titular.

No caso de denúncias, proteções adicionais são aplicadas de acordo com as Leis nº 13.460/2017 e 13.608/2018, que regulamentam o serviço telefônico de denúncias e a recompensa por informações que auxiliem investigações policiais. Essas proteções são complementadas pelo Decreto nº 10.153/2019 e pela Norma Modelo de Salvaguarda à Identidade de Denunciantes, aprovada pela Resolução nº 03/2019 da Rede Nacional de Ouvidorias, garantindo a confidencialidade e segurança do denunciante.

Boas Práticas:

- **Solicitar Consentimento para Compartilhamento de Dados:** Sempre que possível, solicitar o consentimento do titular ao compartilhar dados pessoais entre ouvidorias. Em casos de denúncias com elementos identificáveis, o compartilhamento só deve ocorrer com o consentimento do denunciante ou, em sua ausência, após a pseudonimização dos dados.

- **Formalizar Parcerias entre Ouvidorias:** Estabelecer convênios, contratos ou outros acordos formais para o compartilhamento de dados entre ouvidorias, conforme previsto pela ANPD. Essas parcerias e a finalidade do compartilhamento devem ser comunicadas ao titular no Termo de Uso.

- **Transparência e Comunicação:** Informar claramente os titulares sobre os Termos de Uso e quando seus dados podem ser compartilhados com outras instituições. Na ausência de um ato formal ou consentimento, a ouvidoria deve orientar o usuário sobre o órgão competente, sem compartilhar dados pessoais.

- **Minimização de Dados:** Compartilhar apenas os dados estritamente necessários para a demanda, seguindo o princípio de minimização de dados da LGPD, reduzindo o risco de exposição indevida.

- **Anonimização e Pseudonimização:** Sempre que possível, implementar anonimização ou pseudonimização antes de compartilhar dados entre ouvidorias, mesmo quando o consentimento é obtido.

- **Treinamento Contínuo:** Manter um programa contínuo de capacitação dos colaboradores sobre proteção de dados e boas práticas de compartilhamento.

- **Monitoramento:** Implementar um sistema de monitoramento para rastrear o compartilhamento de dados pessoais, garantindo transparência e responsabilização.

- **Política de Retenção de Dados:** Definir uma política clara de retenção e descarte de dados, limitando o compartilhamento de informações apenas ao necessário.

- **Revisão Periódica dos Termos de Uso:** Atualizar regularmente os Termos de Uso para garantir que estejam em conformidade com a legislação vigente e melhores práticas de proteção de dados.

- **Canal de Comunicação para Titulares:** Fortalecer canais de comunicação para que os titulares possam exercer seus direitos, como solicitar informações sobre o compartilhamento de seus dados ou pedir sua exclusão.

- **Plano de Resposta a Incidentes:** Desenvolver um plano de resposta a incidentes de segurança relacionados ao compartilhamento de dados, incluindo medidas de mitigação em caso de vazamento ou uso indevido.

12. CONSIDERAÇÕES FINAIS

O presente Guia de Boas Práticas foi elaborado com o objetivo de apoiar as ouvidorias Públicas na aplicação da Lei Geral de Proteção de Dados Pessoais, apresentando conceitos da Lei, bem como orientações contidas nos guias produzidos pela ANPD e pelo Comitê Central de Governança de Dados do Poder Executivo Federal, aplicadas ao contexto de atuação das ouvidorias públicas.

Este Guia traz, inicialmente, uma importante contextualização das ouvidorias públicas e o advento da Lei Geral de Proteção de Dados Pessoais e as ouvidorias digitais. Em seguida, discorre sobre conceitos da própria LGPD e outros conceitos relevantes correlacionados à ouvidoria para então tratar das possíveis implicações da Lei na sua atuação.

O Guia também esclarece a base legal para tratamento de dados pessoais pelas ouvidorias públicas, aborda os direitos dos titulares de dados pessoais e traz orientações sobre os agentes de tratamento. Por oportuno, este material trata também da relação entre a LAI e a LGPD e a importância de a ouvidoria conhecer os riscos relevantes relacionados às suas atividades.

E após todo este conteúdo, o Guia apresenta, em termos práticos e objetivos, um passo a passo inicial para adequação das ouvidoria s à LGPD e um rol de riscos e respectivas boas práticas que visam mitigá-los . Estas boas práticas estão divididas em três partes, sendo elas aquelas relacionadas ao acesso não autorizado aos sistemas e documentos da ouvidoria , às etapas do fluxo de manifestações de ouvidoria e ao compartilhamento de dados entre ouvidorias.

Por fim, cabe ressaltar que este é um documento da Rede Nacional de Ouvidoria desenvolvido por ouvidorias públicas para ouvidorias Públicas, que deverá estar em constante atualização e aperfeiçoamento a partir da contribuição de todas as ouvidorias integrantes da Rede.

REFERÊNCIAS

Associação Brasileira de Normas Técnicas. NBR ISO/IEC 31000:2018. Gestão de riscos – Diretrizes. Rio de Janeiro. 2018.

Associação Brasileira de Normas Técnicas. NBR 27002:2013. Tecnologia da informação - Técnicas de segurança - Código de Prática para controles de segurança da informação. Rio de Janeiro. 2013.

Artigo LGPD e LAI: uma análise sobre a relação entre elas. Disponível em: LGPD e LAI: uma análise sobre a relação entre elas — LGPD - Lei Geral de Proteção de Dados Pessoais | Serpro

BRASIL. Autoridade Nacional de Proteção de Dados. Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte. 1ª ed. Brasília; 2021. Disponível em: guia-vf.pdf (www.gov.br)

BRASIL. Autoridade Nacional de Proteção de Dados. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. 1ª ed. Brasília; 2021. Disponível em: 2021.05.27GuiaAgentesdeTratamento_Final.pdf (www.gov.br)

BRASIL. Autoridade Nacional de Proteção de Dados. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. 2ª ed. Brasília; 2022. Disponível em: Documentos e Publicações — Autoridade Nacional de Proteção de Dados (www.gov.br)

BRASIL. Autoridade Nacional de Proteção de Dados. Guia Orientativo Tratamento de Dados Pessoais pelo Poder Público. 1ª ed. Brasília; 2022. Disponível em: BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal: Centro Gráfico, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.html

BRASIL. Controladoria-Geral da União – CGU. Enunciado n. 4, de 10 de março de 2022. Disponível em: https://repositorio.cgu.gov.br/handle/1/67735

BRASIL. Controladoria-Geral da União. Modelo de Maturidade em Ouvidoria, 2021. Disponível em: https://www.gov.br/ouvidorias/pt-br/ouvidorias/modelo-de-maturidade-em-ouvidoria-publica

BRASIL. Controladoria-Geral da União – CGU. Metodologia de gestão de riscos. Brasília, abril de 2018. Disponível em: https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/institucionais/arquivos/cgu-metodologia-gestao-riscos-2018.pdf

BRASIL. Comitê Central de Governança de Dados do Poder Executivo Federal. Guia de Boas Práticas - Lei Geral de Proteção de Dados Pessoais (LGPD). Agosto, 2020. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_inventario_dados_pessoais.pdf

BRASIL. Comitê Central de Governança de Dados do Poder Executivo Federal. Guia de Avaliação de Riscos de Segurança e Privacidade - Lei Geral de Proteção de Dados Pessoais. Versão 1.0 Brasília, novembro de 2020. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_avaliacao_riscos.pdf

BRASIL. Comitê Central de Governança de Dados do Poder Executivo Federal. Guia de Resposta a Incidentes de Segurança. Lei Geral de Proteção de Dados Pessoais (LGPD). Versão 1.0 Brasília, setembro de 2021. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_resposta_incidentes.pdf

BRASIL. Comitê Central de Governança de Dados do Poder Executivo Federal. Guia de elaboração de Termo de Uso e Política de Privacidade para serviços públicos. Lei Geral de Proteção de Dados Pessoais (LGPD). Versão 1.2. Brasília, setembro de 2021. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_tupp.pdf

BRASIL, Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). [Internet]. Diário Oficial da União, Brasília; 2017. [citado 2021 dez. 14]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

BRASIL. Lei nº 13.460, de 26 de junho de 2017. Dispõe sobre a participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13460.htm

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Guia de Elaboração de Inventário de Dados Pessoais. Versão 2.0. Brasília, março de 2023. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_inventario_dados_pessoais.pdf

BRASIL. Portaria nº 581, de 9 de março de 2021. CGU. Disponível em: https://www.gov.br/ouvidorias/pt-br/ouvidorias/legislacao/portarias/portaria-no-581-consolidada-v2.pdf

BRASIL. Rede Nacional de Ouvidorias - Renouv. Norma Modelo para Criação de Unidades de Ouvidoria da Rede Nacional de Ouvidorias. Disponível em: NORMAMODELODECRIAODEOUVIDORIASFINAL.docx

BRASIL. Resolução nº 7, de 30 de novembro de 2021. Coordenação Geral da Rede Nacional de Ouvidorias. Controladoria-Geral da União. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-n-7-de-30-de-novembro-de-2021-364253953

COSO – Gerenciamento de riscos corporativos – integrado com estratégia e performance - Sumário Executivo - 2017.

MINAS GERAIS. Controladoria-Geral do Estado. Guia Metodológico da Gestão de Riscos Estratégicos. Minas Gerais, maio de 2020. Disponível em: https://bancodoconhecimento.conaci.org.br/bitstream/123456789/271/1/Guia_Metodologico_de_Gestao_de_Riscos_Estratégicos.pdf

PERNAMBUCO. Lei nº 16.420, de 17 de setembro de 2018. Dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública estadual. Disponível em: https://legis.alepe.pe.gov.br/texto.aspx?tiponorma=1&numero=16420&complemento=0&ano=2018&tipo=&url=

Supremo Tribunal Federal. ADI nº 6393 MC /DF. Relator: Ministra Rosa Weber. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5896399

ONU. Resolução 75/186. Disponível em: https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F75%2F186&Language=S&DeviceType=Mobile

UNICEF. Declaração Universal das Nações Unidas. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos