

APOSTILA DO ALUNO

Módulo 2

Intersecções e Conflitos: Portal, LGPD e Ouvidoria

Curso: Ouvidoria, e-SIC, Portal e LGPD

Prof. Devaldo Gilini Junior

Carga horária: aproximadamente 3 horas

Objetivo geral

Compreender como conciliar transparência pública, proteção de dados pessoais, funcionamento da ouvidoria, controle social e gestão de incidentes, criando rotinas integradas e juridicamente seguras para a administração municipal.

Material de apoio para exposição, estudo de casos, debate orientado e oficina prática.

Apresentação da apostila

Esta apostila foi preparada como material de apoio ao Módulo 2 — Intersecções e Conflitos: Portal, LGPD e Ouvidoria. O objetivo é oferecer uma base conceitual e prática para que o aluno compreenda os pontos de tensão entre o direito de acesso à informação, o dever de transparência, a proteção de dados pessoais e o funcionamento das ouvidorias públicas.

A proposta não é tratar LAI e LGPD como normas incompatíveis. Ao contrário: a aula parte da ideia de que transparência e proteção de dados são deveres simultâneos da administração pública. O desafio é definir critérios, fluxos, responsabilidades e evidências para publicar o que deve ser público, proteger o que não deve ser exposto e responder adequadamente às manifestações dos cidadãos.

Como usar este material

Use as partes conceituais para revisão; os quadros práticos para aplicação no órgão; os casos em storytelling para debate em sala; e os modelos finais como ponto de partida para plano de ação institucional.

Resultados de aprendizagem esperados

- Distinguir transparência pública, controle social e proteção de dados pessoais sem tratá-los como agendas opostas.
- Aplicar critérios de ponderação para decidir quando publicar, restringir, anonimizar, tarjar ou responder por canal individual.
- Identificar riscos no tratamento de dados pessoais em ouvidorias, e-SIC, portais de transparência e canais de denúncia.
- Estruturar um fluxo mínimo de proteção ao denunciante de boa-fé e de tratamento de manifestações anônimas.
- Organizar um comitê gestor integrado e um fluxo de resposta a incidentes de segurança.
- Elaborar um plano de ação de 90 dias para melhorar a governança da informação no município.

Roteiro sugerido da aula — 3 horas

Horário	Bloco	Atividade
00:00–00:15	Abertura	Contexto, objetivos, diagnóstico inicial e combinados.
00:15–00:45	Transparência x dados	Tópicos 1 e 2: conflito aparente, hierarquia normativa e ponderação.
00:45–01:20	Ouvidoria e proteção	Tópicos 3, 4 e 5: dados na ouvidoria, denunciante e anonimato.
01:20–01:35	Intervalo / transição	Perguntas rápidas e preparação para casos.
01:35–02:10	Portal, controle social e LGPD	Tópicos 6 e 7: dados pessoais no portal e controle social responsável.
02:10–02:40	Governança integrada	Tópicos 8 e 9: comitê gestor e incidentes de segurança.
02:40–03:00	Oficina final	Matriz de decisão, plano de ação e fechamento.

Premissas normativas de partida

A Lei de Acesso à Informação estabelece o acesso como regra e o sigilo como exceção, além de exigir informação primária, íntegra, autêntica e atualizada. A LGPD, por sua vez, disciplina o tratamento de dados pessoais e protege

direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade. Já a Lei nº 13.460/2017 organiza a participação, a proteção e a defesa dos direitos dos usuários dos serviços públicos, com papel relevante para as ouvidorias.

- Transparência não significa exposição irrestrita de dados pessoais.
- Proteção de dados não autoriza opacidade indevida da administração.
- Ouvidoria não é apenas canal de reclamação; é ferramenta de escuta, integridade, melhoria do serviço e gestão de riscos.
- Portal da Transparência precisa servir ao controle social com segurança, qualidade e proporcionalidade.
- Todo tratamento de dados deve ter finalidade, necessidade, base legal, segurança e registro mínimo.

Fontes normativas principais: Constituição Federal; Lei nº 12.527/2011 (LAI); Lei nº 13.709/2018 (LGPD); Lei nº 13.460/2017; Decreto nº 7.724/2012; Decreto nº 9.492/2018; Resolução CD/ANPD nº 15/2024.

1. Transparência vs. Proteção de Dados

Ideia central

O conflito entre transparência e proteção de dados costuma ser apenas aparente. A administração deve publicar informações necessárias ao controle social e, ao mesmo tempo, limitar a exposição de dados pessoais desnecessários.

Fundamentos essenciais

- Publicidade administrativa e direito de acesso à informação.
- Finalidade, adequação, necessidade, segurança e prevenção no tratamento de dados pessoais.
- Sigilo como exceção motivada, temporária e juridicamente justificada.
- Minimização: publicar o necessário, proteger o excedente.

Aplicação prática no município

- Pergunte qual interesse público justifica a divulgação.
- Verifique se o mesmo objetivo pode ser alcançado com dado anonimizado, agregado ou tarjado.
- Registre a decisão quando houver restrição, anonimização ou publicação parcial.
- Padronize procedimentos para evitar decisões diferentes em casos iguais.

Matriz rápida de decisão

Pergunta	O que observar	Evidência recomendada
Há dever legal de publicar?	Base legal, regulamento local, orientação de controle e interesse público.	Norma, link, parecer ou checklist.
Há dado pessoal envolvido?	Identificação direta ou indireta, dados sensíveis, dados de terceiros e dados excessivos.	Registro de revisão e campos protegidos.
A publicação integral é necessária?	Proporcionalidade, minimização e possibilidade de tarja/anonimização/agregação.	Versão tarjada, justificativa ou termo de anonimização.
Quem deve decidir?	Área dona do dado, ouvidoria, encarregado, jurídico, controle interno e TI.	RACI, despacho ou ata do comitê.

Caso em storytelling para debate

A planilha que resolveu um problema e criou outro

Em um município fictício, a equipe decidiu publicar uma planilha completa de beneficiários de determinado programa para demonstrar transparência. O problema é que a planilha também continha CPF completo, endereço, telefone e dados familiares. A publicação gerou reclamações, pedidos de remoção e insegurança interna. Depois de revisar o caso, o órgão percebeu que o controle social exigia informação sobre critérios, valores, períodos, unidade responsável e base legal, mas não precisava da exposição integral de dados pessoais. A versão corrigida passou a apresentar dados agregados e campos mínimos, com consulta individual protegida por autenticação.

Lição prática: A pergunta prática não é “publica ou não publica?”. A pergunta correta é: “qual dado é necessário para o controle social e qual dado deve ser protegido?”.

Perguntas para sala

1. O que a administração deveria ter feito antes de o problema ocorrer?
2. Que dado ou etapa do fluxo era realmente necessário?
3. Quem deveria ser responsável pela decisão e pela evidência?
4. Qual controle simples poderia prevenir repetição do caso?

2. Hierarquia de Normas

Ideia central

LAI, LGPD, Lei de Ouvidorias e normas locais devem ser interpretadas de forma harmônica. Nenhuma área deve usar uma lei como desculpa automática para ignorar a outra.

Fundamentos essenciais

- Constituição como ponto de partida: publicidade, eficiência, moralidade, intimidade, vida privada e acesso à informação.
- Leis ordinárias que disciplinam dimensões diferentes do mesmo problema público.
- Regulamentos e orientações devem operacionalizar a lei, não contrariá-la.
- Norma interna municipal precisa definir fluxo, competência e evidência.

Aplicação prática no município

- Identifique a norma aplicável ao caso concreto.
- Verifique se há norma local sobre LAI, ouvidoria, portal, LGPD e segurança da informação.
- Quando houver tensão entre direitos, documente a ponderação.
- Evite respostas genéricas como “negado por LGPD” ou “publicado por transparência” sem motivação.

Matriz rápida de decisão

Pergunta	O que observar	Evidência recomendada
Há dever legal de publicar?	Base legal, regulamento local, orientação de controle e interesse público.	Norma, link, parecer ou checklist.
Há dado pessoal envolvido?	Identificação direta ou indireta, dados sensíveis, dados de terceiros e dados	Registro de revisão e campos protegidos.

Pergunta	O que observar	Evidência recomendada
	excessivos.	
A publicação integral é necessária?	Proporcionalidade, minimização e possibilidade de tarja/anonimização/agregação.	Versão tarjada, justificativa ou termo de anonimização.
Quem deve decidir?	Área dona do dado, ouvidoria, encarregado, jurídico, controle interno e TI.	RACI, despacho ou ata do comitê.

Caso em storytelling para debate

O parecer de uma linha

Uma secretaria recebeu pedido de acesso a documentos de fiscalização. A primeira resposta foi curta: “indeferido por conter dados pessoais”. O cidadão recorreu. Na revisão, a equipe percebeu que o documento continha parte pública, parte sensível e parte irrelevante ao pedido. A solução não estava em negar tudo, mas em fornecer versão com tarjas e justificar expressamente cada restrição. O recurso mostrou que a dificuldade não era a existência de conflito entre leis, e sim a falta de método para compatibilizá-las.

Lição prática: Hierarquia normativa não é decorar pirâmide; é saber aplicar Constituição, leis e regulamentos com motivação e proporcionalidade.

Perguntas para sala

- O que a administração deveria ter feito antes de o problema ocorrer?
- Que dado ou etapa do fluxo era realmente necessário?
- Quem deveria ser responsável pela decisão e pela evidência?
- Qual controle simples poderia prevenir repetição do caso?

3. Tratamento de Dados na Ouvidoria

Ideia central

A ouvidoria trata dados pessoais em praticamente todas as etapas: recebimento, triagem, encaminhamento, resposta, relatório e arquivamento. Por isso, precisa de bases, controles, perfis de acesso e linguagem adequada.

Fundamentos essenciais

- Manifestações podem envolver reclamações, denúncias, solicitações, sugestões e elogios.
- Dados de identificação, relato, documentos anexos e informações de terceiros devem ser protegidos.
- Compartilhamento interno deve respeitar necessidade e finalidade.
- Relatórios gerenciais devem preferir dados agregados e anonimizados.

Aplicação prática no município

- Separe dados do manifestante, dados do relato e dados de terceiros.
- Restrinja acesso por perfil e registre encaminhamentos.
- Evite copiar manifestação integral quando só um resumo for suficiente.
- Defina prazos de guarda, descarte e anonimização quando cabível.

Matriz rápida de decisão

Pergunta	O que observar	Evidência recomendada
Há dever legal de publicar?	Base legal, regulamento local, orientação de controle e interesse público.	Norma, link, parecer ou checklist.
Há dado pessoal envolvido?	Identificação direta ou indireta, dados sensíveis, dados de terceiros e dados excessivos.	Registro de revisão e campos protegidos.
A publicação integral é necessária?	Proporcionalidade, minimização e possibilidade de tarja/anonimização/agregação.	Versão tarjada, justificativa ou termo de anonimização.
Quem deve decidir?	Área dona do dado, ouvidoria, encarregado, jurídico, controle interno e TI.	RACI, despacho ou ata do comitê.

Caso em storytelling para debate

O encaminhamento que expôs o cidadão

Uma ouvidoria municipal recebeu reclamação sobre atendimento em uma unidade de saúde. Para agilizar, encaminhou a manifestação integral para vários setores. O relato continha informações de saúde, endereço e detalhes familiares. A solução poderia ter sido mais simples: encaminhar apenas o resumo necessário ao gestor da unidade, preservando a identidade do manifestante quando ela não fosse essencial para apuração. A partir do episódio, a ouvidoria adotou triagem com três perguntas: quem precisa saber? o que precisa saber? por quanto tempo precisa acessar?

Lição prática: Na ouvidoria, encaminhar bem é tão importante quanto responder rápido.

Perguntas para sala

9. O que a administração deveria ter feito antes de o problema ocorrer?
10. Que dado ou etapa do fluxo era realmente necessário?
11. Quem deveria ser responsável pela decisão e pela evidência?
12. Qual controle simples poderia prevenir repetição do caso?

4. Proteção ao Denunciante de Boa-fé

Ideia central

A proteção do denunciante de boa-fé é condição para que irregularidades cheguem à administração. Sem proteção contra retaliação, o canal existe formalmente, mas perde credibilidade.

Fundamentos essenciais

- Denúncias podem envolver risco pessoal, funcional ou político para quem relata.
- A identidade do denunciante deve ser tratada com restrição e necessidade.
- Boa-fé não exige prova completa; exige relato minimamente consistente e ausência de má-fé evidente.
- Apuração deve proteger identidade, evidências e cadeia de custódia da informação.

Aplicação prática no município

- Defina quem pode acessar a identidade do denunciante.
- Separe denúncia, identificação e anexos sensíveis.
- Evite encaminhar a denúncia ao próprio denunciado sem filtros.
- Comunique ao denunciante, quando identificado, etapas gerais sem expor medidas sigilosas.

Matriz rápida de decisão

Pergunta	O que observar	Evidência recomendada
Há dever legal de publicar?	Base legal, regulamento local, orientação de controle e interesse público.	Norma, link, parecer ou checklist.
Há dado pessoal envolvido?	Identificação direta ou indireta, dados sensíveis, dados de terceiros e dados excessivos.	Registro de revisão e campos protegidos.
A publicação integral é necessária?	Proporcionalidade, minimização e possibilidade de tarja/anonimização/agregação.	Versão tarjada, justificativa ou termo de anonimização.
Quem deve decidir?	Área dona do dado, ouvidoria, encarregado, jurídico, controle interno e TI.	RACI, despacho ou ata do comitê.

Caso em storytelling para debate

A denúncia que foi parar na mesa errada

Um servidor relatou possível direcionamento em contratação. Por falta de fluxo, a denúncia foi encaminhada integralmente à chefia mencionada no relato. O denunciante passou a temer retaliação e o canal perdeu confiança. Na revisão do processo, o órgão criou triagem prévia, restrição de identidade e encaminhamento por extrato objetivo. A denúncia passou a ser tratada como informação sensível, não como simples expediente administrativo.

Lição prática: Proteger o denunciante não é proteger acusação falsa; é proteger o canal para que fatos relevantes possam ser apurados com segurança.

Perguntas para sala

13. O que a administração deveria ter feito antes de o problema ocorrer?
14. Que dado ou etapa do fluxo era realmente necessário?
15. Quem deveria ser responsável pela decisão e pela evidência?
16. Qual controle simples poderia prevenir repetição do caso?

5. Anonimato nas Manifestações

Ideia central

Manifestação anônima exige tratamento cuidadoso. O anonimato pode limitar a resposta individual, mas não impede análise de risco, registro, triagem e encaminhamento quando houver elementos mínimos.

Fundamentos essenciais

- Identificação do requerente não deve ter exigências que inviabilizem a manifestação.
- Denúncias anônimas podem indicar riscos relevantes e merecer análise preliminar.
- Ausência de identificação pode limitar complementação e comunicação de resultado.
- O foco inicial deve ser a plausibilidade do relato e a existência de elementos verificáveis.

Aplicação prática no município

- Não descarte automaticamente manifestação anônima.
- Classifique como comunicação de irregularidade ou denúncia anônima, conforme norma aplicável.
- Busque elementos mínimos: local, data aproximada, envolvidos, documento, contrato, unidade ou fato verificável.
- Evite conclusões precipitadas: anonimato não prova verdade nem falsidade.

Matriz rápida de decisão

Pergunta	O que observar	Evidência recomendada
Há dever legal de publicar?	Base legal, regulamento local, orientação de controle e interesse público.	Norma, link, parecer ou checklist.
Há dado pessoal envolvido?	Identificação direta ou indireta, dados sensíveis, dados de terceiros e dados excessivos.	Registro de revisão e campos protegidos.
A publicação integral é necessária?	Proporcionalidade, minimização e possibilidade de tarja/anonimização/agregação.	Versão tarjada, justificativa ou termo de anonimização.
Quem deve decidir?	Área dona do dado, ouvidoria, encarregado, jurídico, controle interno e TI.	RACI, despacho ou ata do comitê.

Caso em storytelling para debate

O bilhete sem nome que evitou prejuízo

A ouvidoria recebeu relato anônimo dizendo que determinado serviço estava sendo pago sem entrega integral. A mensagem era curta, mas indicava contrato, mês e local. Em vez de arquivar, a equipe fez verificação preliminar com documentos públicos e registros de fiscalização. Encontrou inconsistências e acionou controle interno. O autor nunca foi identificado, mas o relato continha elementos verificáveis. O caso ensinou que anonimato não substitui prova, mas pode ser ponto de partida para controle.

Lição prática: Manifestação anônima não deve ser condenada pelo formulário; deve ser avaliada pelo conteúdo verificável.

Perguntas para sala

17. O que a administração deveria ter feito antes de o problema ocorrer?
18. Que dado ou etapa do fluxo era realmente necessário?
19. Quem deveria ser responsável pela decisão e pela evidência?
20. Qual controle simples poderia prevenir repetição do caso?

6. Dados Pessoais no Portal da Transparência

Ideia central

O portal deve publicar dados necessários ao controle social, especialmente sobre receitas, despesas, licitações, contratos, pessoal e políticas públicas. A publicação, porém, deve observar necessidade, proporcionalidade e segurança.

Fundamentos essenciais

- Informações sobre uso de recursos públicos têm forte interesse público.
- Dados pessoais desnecessários, sensíveis ou excessivos devem ser ocultados, anonimizados ou agregados.
- Documentos integrais devem passar por revisão antes da publicação.
- O portal precisa de atualização, rastreabilidade e padronização de campos.

Aplicação prática no município

- Revise PDFs antes da publicação para localizar CPF, RG, endereço, assinatura, telefone, e-mail pessoal, dados bancários e dados sensíveis.
- Use tarja quando o documento precisar ser publicado, mas contiver dado pessoal excessivo.
- Crie lista de campos permitidos e proibidos por tipo de conteúdo.
- Mantenha registro de data, fonte, responsável e versão publicada.

Matriz rápida de decisão

Pergunta	O que observar	Evidência recomendada
Há dever legal de publicar?	Base legal, regulamento local, orientação de controle e interesse público.	Norma, link, parecer ou checklist.
Há dado pessoal envolvido?	Identificação direta ou indireta, dados sensíveis, dados de terceiros e dados excessivos.	Registro de revisão e campos protegidos.
A publicação integral é necessária?	Proporcionalidade, minimização e possibilidade de tarja/anonimização/agregação.	Versão tarjada, justificativa ou termo de anonimização.
Quem deve decidir?	Área dona do dado, ouvidoria, encarregado, jurídico, controle interno e TI.	RACI, despacho ou ata do comitê.

Caso em storytelling para debate

O contrato público e o anexo esquecido

Uma prefeitura publicou contrato e aditivos corretamente no portal, mas esqueceu que um anexo continha documentos pessoais de representantes e terceiros. O arquivo ficou disponível por meses. Quando o problema foi percebido, a equipe removeu o documento, republicou versão tarjada e criou uma etapa obrigatória de revisão antes de publicar novos anexos. O erro não estava na transparência do contrato, mas na ausência de controle sobre o que vinha junto.

Lição prática: O portal deve ser transparente sobre o ato público, não sobre dados pessoais que chegaram por acidente no processo.

Perguntas para sala

21. O que a administração deveria ter feito antes de o problema ocorrer?
22. Que dado ou etapa do fluxo era realmente necessário?
23. Quem deveria ser responsável pela decisão e pela evidência?
24. Qual controle simples poderia prevenir repetição do caso?

7. Controle Social e a LGPD

Ideia central

A LGPD não enfraquece o controle social. Ela qualifica a forma de publicar e de acessar informações, estimulando dados úteis, confiáveis e proporcionais.

Fundamentos essenciais

- Controle social depende de informação compreensível, íntegra e atualizada.
- Dados abertos e painéis podem fortalecer fiscalização sem exposição indevida de pessoas.
- Acesso individualizado pode ser necessário em alguns casos; em outros, dado agregado é suficiente.
- Transparência de critérios e decisões é tão importante quanto transparência de bases brutas.

Aplicação prática no município

- Publique metodologia, critérios, responsáveis, valores, datas e resultados.
- Prefira bases estruturadas com campos necessários e dicionário de dados.
- Crie trilha para pedido de informação complementar quando o portal não bastar.
- Explique ao cidadão por que determinado dado pessoal foi protegido.

Matriz rápida de decisão

Pergunta	O que observar	Evidência recomendada
Há dever legal de publicar?	Base legal, regulamento local, orientação de controle e interesse público.	Norma, link, parecer ou checklist.
Há dado pessoal envolvido?	Identificação direta ou indireta, dados sensíveis, dados de terceiros e dados excessivos.	Registro de revisão e campos protegidos.
A publicação integral é necessária?	Proporcionalidade, minimização e possibilidade de tarja/anonimização/agregação.	Versão tarjada, justificativa ou termo de anonimização.
Quem deve decidir?	Área dona do dado, ouvidoria, encarregado, jurídico, controle interno e TI.	RACI, despacho ou ata do comitê.

Caso em storytelling para debate

O cidadão que queria fiscalizar a política pública

Um cidadão pediu lista nominal completa de famílias atendidas por um programa social, com endereço e composição familiar. A área social temeu negar tudo. A solução foi oferecer dados agregados por bairro, critérios de elegibilidade, quantidade de atendidos, valores executados, responsáveis e forma de auditoria, além de canal para denúncia de irregularidade específica. O controle social foi preservado sem expor famílias vulneráveis.

Lição prática: Controle social não é curiosidade sobre pessoas; é fiscalização sobre critérios, recursos, decisões e resultados.

Perguntas para sala

25. O que a administração deveria ter feito antes de o problema ocorrer?
26. Que dado ou etapa do fluxo era realmente necessário?
27. Quem deveria ser responsável pela decisão e pela evidência?
28. Qual controle simples poderia prevenir repetição do caso?

8. Comitê Gestor Integrado

Ideia central

Os temas de portal, LAI, LGPD e ouvidoria não devem funcionar em ilhas. Um comitê integrado ajuda a resolver conflitos, definir padrões, priorizar riscos e acompanhar planos de ação.

Fundamentos essenciais

- As decisões envolvem múltiplas áreas: ouvidoria, controle interno, procuradoria, TI, comunicação, gestão documental, encarregado de dados e unidades finalísticas.
- Comitê não substitui responsabilidades legais, mas organiza coordenação.
- Agenda fixa evita que conflitos sejam resolvidos apenas quando viram crise.
- Registro de decisões fortalece prestação de contas.

Aplicação prática no município

- Defina composição mínima e periodicidade.
- Crie pauta fixa: pedidos recorrentes, riscos LGPD, incidentes, portal, denúncias e plano de ação.
- Mantenha ata, responsáveis, prazos e evidências.
- Leve decisões complexas para parecer técnico-jurídico quando necessário.

Matriz rápida de decisão

Pergunta	O que observar	Evidência recomendada
Há dever legal de publicar?	Base legal, regulamento local, orientação de controle e interesse público.	Norma, link, parecer ou checklist.
Há dado pessoal envolvido?	Identificação direta ou indireta, dados sensíveis, dados de terceiros e dados excessivos.	Registro de revisão e campos protegidos.
A publicação integral é necessária?	Proporcionalidade, minimização e possibilidade de tarja/anonimização/agregação.	Versão tarjada, justificativa ou termo de anonimização.
Quem deve decidir?	Área dona do dado, ouvidoria, encarregado, jurídico, controle interno e TI.	RACI, despacho ou ata do comitê.

Caso em storytelling para debate

A reunião que economizou cem e-mails

Em um município, cada pedido sensível gerava troca interminável de e-mails entre ouvidoria, jurídico, TI e comunicação. As respostas saíam tarde e de forma desigual. Com a criação de uma reunião mensal curta, os casos repetitivos viraram orientação padrão, o portal recebeu melhorias e a ouvidoria reduziu retrabalho. O comitê não criou burocracia; ele organizou a burocracia que já existia.

Lição prática: Comitê bom não é reunião para conversar; é rotina para decidir, registrar e destravar.

Perguntas para sala

29. O que a administração deveria ter feito antes de o problema ocorrer?
30. Que dado ou etapa do fluxo era realmente necessário?
31. Quem deveria ser responsável pela decisão e pela evidência?
32. Qual controle simples poderia prevenir repetição do caso?

9. Gestão de Incidentes de Segurança

Ideia central

Incidente de segurança exige preparação antes da crise. O órgão deve saber identificar, conter, avaliar risco, acionar responsáveis, comunicar quando necessário e aprender com o ocorrido.

Fundamentos essenciais

- Incidente pode comprometer confidencialidade, integridade ou disponibilidade de dados pessoais.
- A comunicação à ANPD e aos titulares depende da avaliação de risco ou dano relevante.
- Registros e evidências são essenciais para responsabilização e prestação de contas.
- Correção de causa raiz é parte do processo, não etapa opcional.

Aplicação prática no município

- Crie formulário de registro de incidente.
- Defina equipe de resposta: TI, encarregado, jurídico, comunicação, controle interno e área afetada.
- Classifique gravidade, dados envolvidos, titulares afetados e medidas de contenção.
- Após o incidente, revise permissões, contratos, backups, logs, treinamento e plano de continuidade.

Matriz rápida de decisão

Pergunta	O que observar	Evidência recomendada
Há dever legal de publicar?	Base legal, regulamento local, orientação de controle e interesse público.	Norma, link, parecer ou checklist.
Há dado pessoal envolvido?	Identificação direta ou indireta, dados sensíveis, dados de terceiros e dados excessivos.	Registro de revisão e campos protegidos.
A publicação integral é necessária?	Proporcionalidade, minimização e possibilidade de tarja/anonimização/agregação.	Versão tarjada, justificativa ou termo de anonimização.

Pergunta	O que observar	Evidência recomendada
Quem deve decidir?	Área dona do dado, ouvidoria, encarregado, jurídico, controle interno e TI.	RACI, despacho ou ata do comitê.

Caso em storytelling para debate

O pendrive que virou incidente

Um servidor perdeu um pendrive com planilhas de atendimento. Ninguém sabia se havia senha, cópia, backup ou quais dados estavam no arquivo. O caso revelou que o problema não era apenas o pendrive, mas a falta de inventário, criptografia, orientação e fluxo de resposta. Depois disso, o órgão criou registro de incidentes, proibiu armazenamento inseguro e definiu acionamento imediato da TI e do encarregado.

Lição prática: Incidente não começa quando vaza na imprensa; começa quando o órgão perde controle sobre o dado.

Perguntas para sala

33. O que a administração deveria ter feito antes de o problema ocorrer?
34. Que dado ou etapa do fluxo era realmente necessário?
35. Quem deveria ser responsável pela decisão e pela evidência?
36. Qual controle simples poderia prevenir repetição do caso?

Ferramentas práticas para aplicação

1. Matriz LAI x LGPD para decisões difíceis

Etapa	Pergunta de controle	Decisão possível
1. Finalidade	Qual é a finalidade da divulgação ou do acesso?	Publicar, responder via SIC, encaminhar à ouvidoria ou restringir.
2. Base jurídica	Qual norma autoriza ou exige o tratamento?	LAI, LGPD, norma setorial, contrato, obrigação legal ou interesse público.
3. Necessidade	Todos os dados são necessários para a finalidade?	Remover excessos, tarjar, agregar ou anonimizar.
4. Risco	Há risco à intimidade, segurança, denunciante ou titular?	Aplicar restrição, controle de acesso ou consulta individual.
5. Evidência	Como a decisão será comprovada?	Despacho motivado, checklist, ata, parecer, log ou versão publicada.

2. Fluxo recomendado para publicar documento no portal

37. Área responsável identifica documento e finalidade da publicação.
38. Servidor responsável verifica se há dados pessoais, dados sensíveis ou informações sigilosas.
39. Quando houver dados excessivos, prepara versão tarjada ou anonimizada.
40. Área jurídica, encarregado ou controle interno é consultado em casos sensíveis.
41. Documento é publicado com data, fonte, responsável e categoria correta.
42. Portal mantém histórico e registro da versão publicada.

43. Correções posteriores são registradas, sem apagar trilha de auditoria.

3. Fluxo recomendado para manifestações de ouvidoria

44. Receber e protocolar a manifestação no canal oficial.
45. Classificar: reclamação, denúncia, solicitação, sugestão, elogio ou comunicação de irregularidade.
46. Separar dados de identificação, relato, anexos e dados de terceiros.
47. Verificar necessidade de proteção de identidade ou restrição de acesso.
48. Encaminhar apenas o conteúdo necessário à unidade responsável.
49. Responder com linguagem clara, motivação e orientação sobre recurso ou complementação.
50. Registrar aprendizados para melhoria de serviços, portal e comunicação institucional.

4. Checklist mínimo do comitê gestor integrado

Item	Sim/Não	Evidência
Há designação formal dos membros?		
Participam ouvidoria, e-SIC, encarregado, TI, controle interno, comunicação e jurídico?		
Existe calendário de reuniões?		
Há pauta fixa para portal, LGPD, manifestações, incidentes e plano de ação?		
As decisões são registradas em ata?		
Há painel de pendências com responsável e prazo?		
Casos sensíveis geram orientação padrão para evitar decisões divergentes?		

5. Registro simplificado de incidente de segurança

Campo	Descrição
Data e hora da identificação	Quando o incidente foi percebido.
Unidade afetada	Secretaria, setor, sistema ou processo envolvido.
Descrição do evento	O que ocorreu, como foi descoberto e qual o estado atual.
Dados envolvidos	Tipo de dado pessoal, dado sensível, volume aproximado e titulares afetados.
Medidas de contenção	Ações imediatas adotadas para reduzir impacto.
Avaliação de risco/dano	Possível impacto aos titulares e à administração.
Responsáveis acionados	TI, encarregado, jurídico, controle interno, comunicação e área demandante.
Comunicação externa	Necessidade de comunicar ANPD, titulares ou outros órgãos.
Correção de causa raiz	Medidas estruturais para evitar reincidência.

Oficina prática final — plano de ação de 90 dias

A oficina final serve para transformar o conteúdo em ação institucional. A turma deve escolher um problema concreto do órgão e montar um plano com responsáveis, prazos, evidências e indicadores.

Passo 1 — Diagnóstico rápido

Eixo	Pergunta	Nota 0–2
Portal	Documentos são publicados com revisão de dados pessoais?	
Ouvidoria	Há triagem e proteção de identidade quando necessário?	
e-SIC	Respostas são motivadas e preservam dados pessoais excessivos?	
LGPD	Existe encarregado, canal e fluxo mínimo?	
Incidentes	Há procedimento escrito de identificação, contenção e comunicação?	
Governança	Há comitê ou rotina integrada?	
Indicadores	Há KPIs de prazo, qualidade, risco e reincidência?	

Pontuação sugerida: 0 = inexistente; 1 = existe parcialmente; 2 = existe e é aplicado com evidência.

Passo 2 — Mapa de prioridades

Problema identificado	Risco	Impacto	Ação prioritária	Responsável

Passo 3 — Plano 30/60/90 dias

Prazo	Entrega	Responsável	Evidência de conclusão	KPI associado
30 dias	Criar checklist de publicação no portal.		Checklist aprovado e usado em 3 publicações.	% documentos revisados antes da publicação.
60 dias	Formalizar fluxo de ouvidoria com proteção de identidade.		Fluxo publicado internamente e treinamento realizado.	% manifestações triadas com classificação correta.
90 dias	Implantar rotina do comitê integrado.		Ata mensal, painel de pendências e plano atualizado.	% ações concluídas no prazo.

Indicadores sugeridos

Indicador	Fórmula simples	Periodicidade	Uso gerencial
Tempo médio de resposta do e-SIC	Soma dos dias de resposta / número de pedidos respondidos.	Mensal	Identificar gargalos e áreas com atraso.
Taxa de respostas com complementação/recurso	Pedidos com recurso ou complementação / total de	Mensal	Medir qualidade da resposta.

Indicador	Fórmula simples	Periodicidade	Uso gerencial
	pedidos.		
Documentos revisados antes da publicação	Documentos com checklist / documentos publicados.	Mensal	Reduzir exposição indevida de dados pessoais.
Incidentes registrados e tratados	Incidentes com registro completo / incidentes identificados.	Mensal	Garantir rastreabilidade e resposta.
Ações do plano concluídas no prazo	Ações concluídas no prazo / total de ações previstas.	Mensal	Monitorar efetividade do comitê gestor.
Manifestações recorrentes por tema	Total de manifestações por assunto/unidade.	Mensal	Converter ouvidoria em melhoria de serviço.

Modelos de textos úteis

Modelo 1 — Justificativa para tarja/anonimização

Texto-base
O documento é disponibilizado em atendimento ao dever de transparência e ao direito de acesso à informação. Foram ocultados exclusivamente dados pessoais não necessários à finalidade de controle social, em observância aos princípios da finalidade, necessidade, segurança e prevenção previstos na legislação de proteção de dados pessoais.

Modelo 2 — Resposta orientativa ao cidadão

Texto-base
A informação solicitada está disponível no Portal da Transparência no seguinte caminho: [indicar caminho]. Para preservar dados pessoais de terceiros que não são necessários à finalidade do pedido, foram disponibilizados os campos essenciais ao controle social. Caso necessite de informação complementar, apresente novo pedido indicando o dado específico e a finalidade de acesso, para análise conforme a legislação aplicável.

Modelo 3 — Encaminhamento interno de manifestação com proteção de identidade

Texto-base
Encaminha-se extrato da manifestação para análise técnica da unidade, preservando-se a identidade do manifestante por não ser necessária à apuração inicial. Solicita-se manifestação objetiva sobre os fatos narrados, indicação de providências adotadas e documentos comprobatórios, sem tentativa de identificação do cidadão.

Glossário essencial

Termo	Significado prático
Anonimização	Técnica que impede ou dificulta a identificação do titular a partir do dado tratado.
Dado pessoal	Informação relacionada a pessoa natural identificada ou identificável.
Dado sensível	Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, saúde, vida sexual, dado genético ou biométrico,

Termo	Significado prático
	entre outros.
e-SIC	Canal para pedidos de acesso à informação com procedimento e prazos próprios.
Encarregado	Pessoa indicada para atuar como canal entre controlador, titulares e ANPD.
Manifestação	Reclamação, denúncia, sugestão, elogio ou solicitação apresentada pelo usuário do serviço público.
Minimização	Uso do menor conjunto de dados necessário para cumprir a finalidade legítima.
Pseudonimização	Tratamento que dificulta associação direta do dado ao titular sem informação adicional separada.
Tarja	Ocultação de trecho específico de documento para proteger dado pessoal ou informação sigilosa.

Referências normativas e institucionais

- Constituição da República Federativa do Brasil de 1988 — princípios da administração pública, direito de acesso à informação e proteção à intimidade e vida privada.
- Lei nº 12.527/2011 — Lei de Acesso à Informação (LAI). Fonte: Planalto.
- Decreto nº 7.724/2012 — regulamenta a LAI no âmbito do Poder Executivo federal. Fonte: Planalto.
- Lei nº 13.460/2017 — participação, proteção e defesa dos direitos do usuário dos serviços públicos. Fonte: Planalto.
- Decreto nº 9.492/2018 — Sistema de Ouvidoria do Poder Executivo federal e procedimentos de ouvidoria. Fonte: Planalto.
- Lei nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais (LGPD). Fonte: Planalto.
- Autoridade Nacional de Proteção de Dados — regulamentações, guias e canais oficiais. Fonte: gov.br/anpd.
- Resolução CD/ANPD nº 15/2024 — Regulamento de Comunicação de Incidente de Segurança. Fonte: ANPD/Diário Oficial da União.
- Lei nº 12.846/2013 — responsabilização administrativa e civil de pessoas jurídicas por atos contra a administração pública, relevante para canais de denúncia e integridade.

Fechamento

Síntese final

A boa administração municipal não escolhe entre transparência e proteção de dados. Ela organiza processos para fazer as duas coisas bem: publica o que deve ser público, protege o que deve ser protegido, responde ao cidadão com qualidade e registra evidências das decisões tomadas.

Material elaborado com base no conteúdo do Módulo 2 — Intersecções e Conflitos: Portal, LGPD e Ouvidoria, no novo layout UNYFLEX 2026, e em fontes normativas oficiais consultadas em junho de 2026.