PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

LGPD

PGP
série

FECHO FINAL

Privacy Washing no Setor Público

Por que o ecossistema documental do PGP
é o antídoto contra o abismo entre
discurso e prática.

Privacy Washing no Setor Público

Por que o ecossistema documental do PGP é o antídoto contra o abismo entre discurso e prática.

Conclusão da série composta pelo artigo principal (Regulamentação, Política Interna e Aviso de Privacidade) e seu adendo (sete documentos complementares). Esta peça consolida o raciocínio à luz do conceito de privacy washing — risco que conecta governança documental, conformidade, reputação e legitimidade democrática.

Onde paramos

O artigo principal demonstrou que três instrumentos centrais — Portaria de regulamentação, Política Interna de Privacidade e Aviso de Privacidade — desempenham funções distintas e insubstituíveis no Programa de Governança em Privacidade. Confundir Política Interna (público interno) com Aviso de Privacidade (titular) é equívoco recorrente e juridicamente insustentável.

O adendo ampliou a moldura: ao redor desses três centrais há outros sete documentos típicos — Política de Cookies, Termos de Uso, Termo de Consentimento, PSI, Plano de Resposta a Incidentes, Política de Gestão de Riscos e Política de Contratação de Operadores. Cada um cumpre função específica e nenhum substitui os demais.

Resta a pergunta de fechamento: por que dedicar tanto rigor à articulação correta desse ecossistema? A resposta está em um conceito que dá sentido prático a toda a discussão anterior — o **privacy washing**.

1. O que é privacy washing no setor público

Privacy washing ocorre quando uma organização comunica práticas de proteção de dados mais robustas do que as efetivamente implementadas. É o “greenwashing da privacidade”: a instituição se apresenta como referência, mas não dispõe de controles, processos ou evidências que sustentem o discurso. No setor público, o fenômeno é especialmente grave porque:

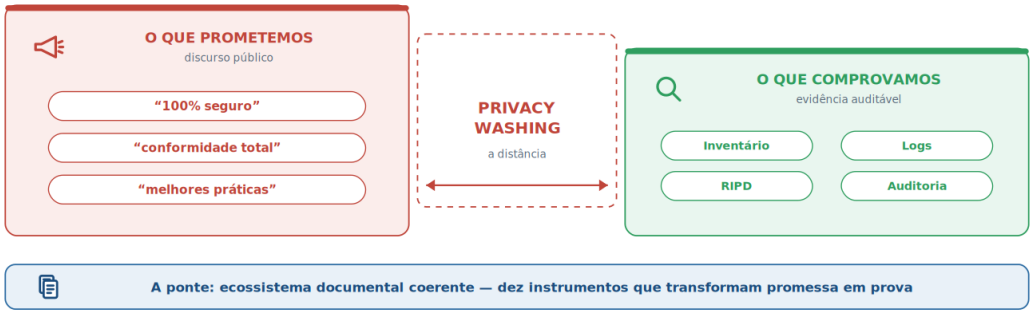
- mina a confiança do cidadão na administração, atacando o pacto simbólico que fundamenta o serviço público;
- expõe a instituição a sanções da ANPD, do Ministério Público, dos Tribunais de Contas e do controle interno;
- cria um abismo entre o discurso institucional e a realidade operacional — o que, descoberto, é juridicamente mais grave do que a ausência originária de discurso.

O VILÃO DESTA SÉRIE: PRIVACY WASHING

Não é apenas marketing exagerado. É risco concreto de conformidade, reputação, segurança e legitimidade. Em órgão público, é também risco democrático — a confiança do cidadão na instituição é o ativo que se perde.

O núcleo do problema é o descompasso entre o que é prometido publicamente e o que pode ser comprovado internamente. É exatamente aqui que o ecossistema documental entra em cena: cada documento, quando existe e está articulado, transforma promessa em compromisso comprovável.

Privacy washing: a distância entre discurso e prática



2. As quatro dimensões do risco institucional

Dentro da instituição, o privacy washing deve ser tratado como risco multidimensional. As quatro dimensões clássicas conversam, cada uma, com instrumentos específicos do PGP.

As quatro dimensões do risco — e o que as contém

2.1. Risco de conformidade / regulatório. Violação de princípios da LGPD (transparência, boa-fé, necessidade, responsabilização, prestação de contas), com possibilidade de sanções da ANPD e de outros órgãos de controle. Mitigado pela existência simultânea de Portaria, Política Interna e Aviso de Privacidade — e pela coerência entre eles.

2.2. Risco reputacional. Promessas não cumpridas são percebidas como enganosas, afetando a imagem institucional e a confiança do cidadão. É a dimensão mais sensível em órgão público, onde a legitimidade depende da percepção de integridade. Mitigada por Avisos verdadeiros, em linguagem clara, validados por evidência interna.

2.3. Risco contratual e de terceiros. Divergências entre o que se promete publicamente, o que está nos contratos com operadores e o que esses operadores fazem na prática.

Coberta pela Política de Contratação de Operadores, pela due diligence de fornecedores e pela auditoria contratual periódica.

2.4. Risco operacional e de segurança. Declarações de “privacy by design”, “criptografia” e “controle de acesso rigoroso” não suportadas por controles reais. Criam falsa sensação de segurança e aumentam a probabilidade de incidentes. Coberta pela PSI, pelo Plano de Resposta a Incidentes e pela Política de Gestão de Riscos.

3. O ecossistema documental como antídoto

A tese que conecta o artigo principal, o adendo e este fecho é a seguinte: cada documento do PGP, quando existe, está atualizado e é coerente com os demais, fecha uma porta específica de privacy washing. Cada documento ausente, genérico ou desconectado abre uma porta nova.

Documento do PGP	Risco de privacy washing se ausente ou fraco	Evidência que ele fornece (antídoto)
Portaria de regulamentação	“Temos governança LGPD” sem ato instituidor — pura declaração simbólica.	Ato publicado em diário oficial criando Comitê, designando Encarregado e fixando prazos.
Política Interna de Privacidade	Declara princípios (privacy by design, minimização) sem norma que os imponha aos servidores.	Documento aprovado pela alta direção, com sanções internas e responsabilidades funcionais.
Aviso de Privacidade	“Zelamos pelos seus dados” sem informar finalidades, bases legais ou direitos.	Documento público claro com todos os elementos do art. 9º, camadas e contato do DPO.
Política de Cookies	Banner “protegemos sua privacidade” enquanto cookies de terceiros rastreiam sem consentimento.	Política específica + banner com toggles por categoria + painel permanente de preferências.
Termos de Uso	Cláusulas vagas que confundem regras de uso com tratamento de dados.	Contrato de uso claro, separado e coerente com o Aviso de Privacidade.
Termo de Consentimento	“Você é o dono dos seus dados” sem registro auditável de consentimentos válidos.	Consentimento granular, livre, informado e revogável, com trilha de auditoria por finalidade.
Política de Segurança (PSI)	Aviso menciona “criptografia” e “controles rigorosos” sem PSI que os imponha.	Controles técnicos formalizados (ISO 27001/27002), auditáveis interna e externamente.
Plano de Resposta a Incidentes	“Temos processos para incidentes” sem fluxo nem prazo para notificar ANPD/titular.	Procedimento com fases, papéis, prazos (3 dias úteis à ANPD) e templates de comunicação.
Política de Gestão de Riscos	Aviso menciona “avaliação de riscos” sem metodologia nem matriz aplicada.	Metodologia formal (ISO 31000/27005) com matriz P×I, base para RIPDs auditáveis.
Política de Contratação de Operadores	“Selecionamos parceiros com cuidado” sem due diligence nem cláusulas LGPD.	Régua de avaliação + cláusulas obrigatórias + monitoramento contínuo + plano de saída.

Leitura crítica: uma instituição que publica apenas o Aviso — sem Política Interna, PSI, Plano de Incidentes ou Política de Operadores — está, por construção, em risco elevado de privacy washing. Promete ao titular um nível de proteção que os documentos internos não sustentam. A LGPD, lida com o conceito de privacy washing, exige consistência entre as camadas — não apenas a publicação isolada do documento externo.

4. Cinco dimensões de diagnóstico

Para tratar o privacy washing de forma estruturada, o diagnóstico passa por cinco dimensões objetivas.

Dimensão de risco	Foco da avaliação	Sinais de privacy washing
Discurso vs. prática	Compara declarações públicas (Aviso, campanhas, relatórios) com evidências internas (Inventário, RIPDs, contratos, logs).	Política copiada de template; promessas sem inventário; termos técnicos sem comprovação.
Regulatório	Sensibilidade dos dados tratados, conformidade demonstrável à LGPD, histórico de reclamações.	Ausência de Inventário, ROPA, RIPD; bases legais não documentadas; canais de direitos não publicados.
Reputacional	Visibilidade institucional, dependência da confiança pública, evolução de reclamações em canais oficiais.	Comunicação promissora sem respaldo; campanhas “LGPD compliant” sem evidências; reclamações crescentes.
Contratual e de terceiros	Alinhamento entre cláusulas contratuais e práticas reais dos operadores; existência de due diligence.	Contratos pré-LGPD sem aditivo; ausência de avaliação de fornecedores; alegações sem certificações.
Operacional e de segurança	Implementação efetiva de controles, minimização, retenção, criptografia, gestão de acessos.	Discurso de “privacy by design” sem PSI; sem Plano de Incidentes; logs ausentes; sem testes.

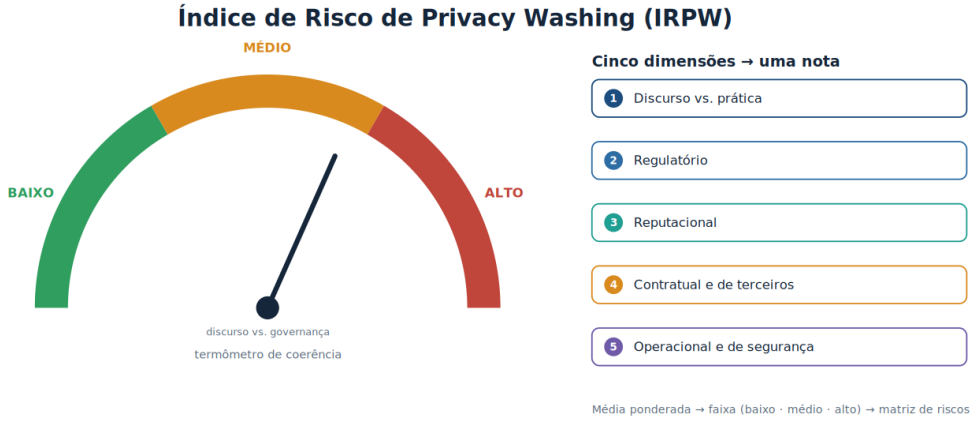
A pergunta-âncora que percorre as cinco dimensões é simples e devastadora quando aplicada com honestidade:

O que prometemos publicamente × o que conseguimos comprovar com documento, log, auditoria ou evidência verificável?

Quando a resposta é “prometemos mais do que comprovamos”, há privacy washing — mesmo que involuntário, mesmo que de boa-fé, mesmo que oriundo de campanha de comunicação mal calibrada.

5. Índice de Risco de Privacy Washing (IRPW)

Para consolidar o diagnóstico em um instrumento de gestão, propõe-se um Índice de Risco de Privacy Washing (IRPW) — KPI/KRI institucional que traduz avaliações qualitativas em um indicador numérico, tornando visível um risco que, sem instrumentação, tende a ser difuso e intangível.



Como o IRPW funciona:

- Atribui-se nota (por exemplo, de 1 a 5) a cada uma das cinco dimensões de diagnóstico.
- Calcula-se média ponderada — algumas dimensões podem ter maior peso (tipicamente “discurso vs. prática” e “regulatório”).
- Classifica-se o resultado em faixas (baixo · médio · alto), orientando a priorização de recursos.
- Integra-se o IRPW à matriz corporativa de riscos e aos relatórios periódicos enviados à alta gestão.

Por que adotar. O IRPW funciona como termômetro de coerência. Detecta — antes da ANPD ou da imprensa — quando o discurso institucional cresce mais rápido do que a governança interna, e permite à alta direção decidir, com base em dado e não em intuição, onde investir esforço de mitigação. Sem IRPW, o risco existe, mas é invisível; com ele, vira um número que aparece em relatório, em ata, em reunião de comitê — e que cobra atenção.

6. Sinais de alto risco de privacy washing

Há sinais típicos que, isolados ou combinados, indicam alta probabilidade de privacy washing. Um profissional qualificado deve mapeá-los proativamente:

- Comunicação institucional mais sofisticada que a governança interna documentada.
- Política de Privacidade copiada de modelo genérico, sem decisões reais da instituição.
- Aviso de Privacidade publicado sem inventário de dados atualizado que o sustente.
- Ausência de evidências para os controles anunciados (sem PSI, sem Plano de Incidentes, sem logs).
- Promessas exageradas de segurança e proteção sem base técnica auditável.
- Confiança excessiva em fornecedores e operadores sem due diligence nem cláusulas LGPD.
- Falta de alinhamento entre comunicação, TI, jurídico e Encarregado/DPO.
- Termos técnicos (anonimização, criptografia ponta a ponta, minimização) usados sem definição precisa nem prática correspondente.
- Histórico crescente de reclamações de privacidade — sem revisão correspondente da política e das práticas.

7. Frases proibidas — o vocabulário do privacy washing

SE NÃO PUDER COMPROVAR, NÃO PUBLIQUE

Certas formulações são, em si mesmas, sinais de privacy washing. Devem ser banidas da comunicação institucional sempre que não houver documento, log ou auditoria que as sustente.

✗ “Garantimos proteção total dos seus dados.”

✗ “Seus dados estão 100% seguros conosco.”

✗ “Não compartilhamos dados com terceiros.” — quando, de fato, há operadores envolvidos.

✗ “Adotamos as melhores práticas do mercado.” — genérico, não auditável.

✗ “Estamos em total conformidade com a LGPD.” — sem evidências documentais.

✗ “Usamos criptografia de ponta a ponta.” — sem PSI que a exija e logs que a comprovem.

Comprove tudo o que comunica. Se não puder provar, não divulgue.

8. Checklist anti-privacy-washing

DIAGNÓSTICO OBJETIVO DA EXPOSIÇÃO

Cada item respondido com “não” ou “parcialmente” é um vetor concreto de privacy washing. Cada “sim, com evidência documental” é um documento ou processo do PGP funcionando como deveria.

✓ Toda promessa pública pode ser comprovada por evidência interna (documento, log, auditoria)?

✓ O Aviso de Privacidade reflete o que está no Inventário, RIPDs e ROPAs — e vice-versa?

✓ Os princípios da Política Interna (privacy by design, minimização, segurança) estão implementados pela PSI, Plano de Incidentes e Gestão de Riscos?

✓ As cláusulas LGPD nos contratos com operadores são compatíveis com o que se promete ao titular?

✓ Termos técnicos usados na comunicação pública têm definição precisa e prática real correspondente?

✓ Campanhas de comunicação foram validadas por DPO, jurídico, TI e comunicação antes de publicar?

✓ Existe Painel de Privacidade funcional para revogação de consentimento tão fácil quanto a concessão?

✓ Há IRPW calculado e revisado periodicamente, integrado à matriz corporativa de riscos?

✓ Auditorias periódicas testam a coerência entre o que se declara e o que se opera?

✓ Existe processo formal de revisão e correção de declarações públicas quando uma lacuna é identificada?

9. Plano de mitigação em três fases

Quando o diagnóstico aponta risco médio ou alto, o plano de ação articula-se em três fases coordenadas.

Fase 1 — Mitigação e correção imediata

- Revisar e, se necessário, reescrever declarações públicas que não possam ser comprovadas pelos controles internos atuais.
- Fortalecer processos em áreas sensíveis (dados de crianças, saúde, dados sensíveis, transferência internacional).
- Estruturar o monitoramento da percepção pública e canais ágeis de resposta a reclamações.
- Estabelecer programa de auditoria e due diligence de privacidade para operadores críticos.
- Validar, via auditoria interna, a aplicação real dos princípios da Política Interna (minimização, retenção, segurança).

Fase 2 — Aprimoramento cultural e de governança

- Garantir que a Política Interna reflita decisões reais de gestão, não modelos genéricos.
- Assegurar DPO/Encarregado atuante, com comitê funcional, métricas e planos de ação publicizados.
- Incorporar privacidade como critério de sucesso em OKRs/KPIs estratégicos — com poder real de rejeitar ou adaptar projetos que contrariem princípios declarados.
- Capacitar continuamente servidores e operadores quanto às práticas reais (não apenas teóricas) do PGP.

Fase 3 — Integração à governança e monitoramento contínuo

- Inserir o IRPW na matriz corporativa de riscos da instituição.
- Incluir a análise de risco de privacy washing nos relatórios periódicos de conformidade à alta gestão.
- Usar o IRPW como etapa padrão na due diligence de novos produtos, serviços e fornecedores.
- Realizar auditorias periódicas focadas na consistência entre promessas e práticas — não apenas na existência documental.

10. O profissional qualificado como antídoto definitivo

Ao longo da série, uma figura emerge como elemento decisivo: o profissional qualificado em LGPD. É quem articula o ecossistema documental, garante coerência entre as camadas e

protege a instituição do privacy washing. As competências exigidas, agora consolidadas, são:

- **Domínio conceitual** — distinguir com precisão os dez instrumentos típicos e saber o que cada um faz e o que nenhum substitui.
- **Domínio técnico** — conhecer as técnicas de entrega ao titular (camadas, just-in-time, painel), as normas ABNT (ISO 27001/27002/27005/27035, 31000), as Resoluções da ANPD (4/2023, 15/2024, 18/2024, 19/2024, 20/2024) e os Guias Orientativos.
- **Visão de risco** — operar IRPW, matriz P×I, apetite ao risco, due diligence e KPI/KRI de privacidade; traduzir LGPD em linguagem de gestão estratégica.
- **Sensibilidade comunicacional** — traduzir governança interna em comunicação clara ao titular, reconhecer frases proibidas e validar campanhas antes da publicação.
- **Cultura de evidência** — exigir que tudo o que se publica seja comprovável por documento, log ou auditoria; não autorizar promessa institucional sem base sustentável.

Sem esse profissional — ou com ele em posição subalterna, sem autonomia, sem orçamento, sem voz no comitê — o programa tende a se reduzir a aparência. Documentos existem, mas não conversam. O Aviso é publicado, mas não tem lastro. A Política Interna é aprovada, mas não opera. Slogans circulam, mas evidências não. É o terreno fértil do privacy washing institucional.

11. Conclusão geral da série

O artigo principal estabeleceu que Portaria, Política Interna e Aviso de Privacidade são três instrumentos centrais distintos, com destinatários, naturezas e funções próprias — e que confundi-los é descumprir a LGPD.

O adendo ampliou a moldura, mostrando que sete outros documentos típicos compõem o ecossistema completo do PGP, cada um com função específica e nenhum substituível.

Este fecho final demonstrou que essa arquitetura documental, quando articulada com integridade e coerência, é o antídoto direto contra o privacy washing — risco que combina conformidade, reputação, contratos, segurança e legitimidade democrática.

> *A LGPD não se cumpre com discurso. Cumpre-se com estrutura documental coerente, governança ativa, evidência auditável e profissional qualificado que articule tudo isso.*

Instituições públicas que entendem essa equação investem em todos os dez instrumentos, cultivam profissionais qualificados, adotam o IRPW como instrumento de governança e cuidam para que cada palavra publicada ao cidadão tenha lastro interno auditável. Em troca, recebem o que a LGPD se propõe a entregar: confiança real, conformidade demonstrável, proteção concreta dos direitos dos titulares e legitimidade democrática preservada.

A PRIVACIDADE COMO INTEGRIDADE INSTITUCIONAL

A privacidade no setor público não é obrigação legal a cumprir formalmente. É elemento central de integridade e de serviço público responsável — e exige discurso e prática alinhados, do primeiro ato instituidor ao último contrato com

> operador. Esse alinhamento é o que separa o programa autêntico do privacy washing maquiado de conformidade.

Fecho Final · Encerramento da série Programa de Governança em Privacidade

Artigo principal → Adendo → Fecho Final · três documentos · uma única tese de coerência institucional

Sobre o autor

Durval Senna da Silva

Auditor de Controle Externo — Tribunal de Contas do Estado do Espírito Santo (TCE-ES)

Coordenador do Comitê Executivo de Proteção de Dados Pessoais e da Ouvidoria do TCE-ES

durval.senna@tcees.tc.br

Servidor público desde 1984, com atuação em diversos setores do TCE-ES — Gerência de Recursos Humanos, Coordenação do Núcleo de Controle de Documentos e Secretaria de Tecnologia da Informação —, atualmente como um dos Coordenadores da Ouvidoria do Tribunal.

Formado em Economia, com pós-graduação em Gestão de RH, em Gestão Pública e em Lei Geral de Proteção de Dados (LGPD). Certificado em Ouvidorias Públicas; em NPS – Net Promoter Score 2.0 (Track.Co); em Proteção de Dados Pessoais pela Data Privacy Brasil (parceira oficial da IAPP – International Association of Privacy Professionals); como Profissional de Privacidade de Dados (LGPD) e Gestor de Privacidade pela TIExames; CDPA – Certified Data Privacy Auditor; e com formação em DPO pela PUC-Campinas.

Atualmente coordena a Ouvidoria do TCE-ES e o Comitê Executivo de Proteção de Dados Pessoais do Tribunal de Contas do Espírito Santo.

PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

LGPD

PGP
série

A série completa

Este documento faz parte de uma série de cinco peças complementares.

1. **Artigo principal**
   Regulamentação · Política Interna · Aviso

2. **Adendo**
   O ecossistema documental — 7 complementares

3. **Fecho Final** — VOCÊ ESTÁ AQUI
   Privacy Washing no Setor Público

4. **Kit de Minutas · Vol. 1**
   Minutas dos 3 instrumentos centrais

5. **Kit de Minutas · Vol. 2**
   Minutas dos 7 documentos complementares

Material de apoio para a implementação da LGPD em instituições públicas.

Durval Senna da Silva

Auditor de Controle Externo · Coordenador do Comitê de Proteção de Dados — TCE-ES

durval.senna@tcees.tc.br