PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

LGPD

PGP
série

ADENDO

O Ecossistema Documental do Programa de Governança em Privacidade

Onde entram Cookies, Termos de Uso, Consentimento, Segurança, Incidentes, Riscos e Operadores.

O ecossistema documental do Programa de Governança em Privacidade

Para além dos três instrumentos centrais — onde entram Cookies, Termos de Uso, Consentimento, Segurança, Incidentes, Riscos e Operadores.

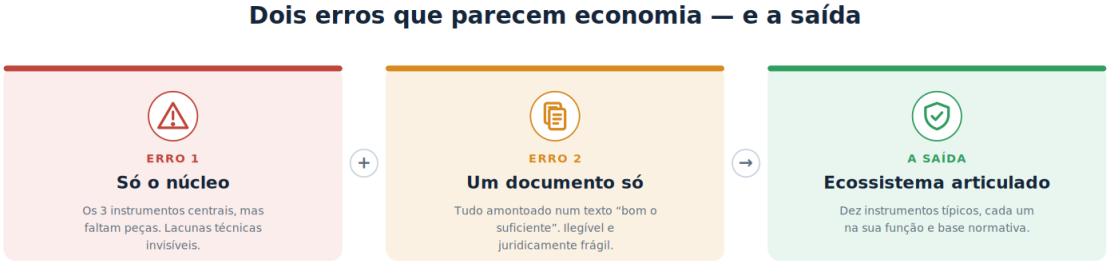
Complemento à análise sobre Portaria de regulamentação, Política Interna de Privacidade e Aviso de Privacidade — com a distinção em relação aos sete documentos que orbitam o núcleo do Programa.

Por que este adendo existe — e o erro que ele evita

O artigo principal analisou os três instrumentos centrais do Programa de Governança em Privacidade (PGP), insubstituíveis entre si:

- **a Portaria de regulamentação da LGPD** — ato instituinte, voltado ao público interno;
- **a Política Interna de Privacidade** — ato normativo estruturante, voltado ao público interno;
- **o Aviso de Privacidade** — instrumento de transparência ativa, voltado ao titular.

Aqui é onde mora a próxima armadilha. Dominar esses três pode dar a sensação de "missão cumprida" — mas eles **não esgotam** o ecossistema documental de uma instituição madura. Ao redor do núcleo existem outros sete documentos que se relacionam com a LGPD em graus diferentes e que costumam ser confundidos com os centrais. Dois atalhos parecem economizar esforço e, na prática, cobram caro:



A PREMISSA DO ADENDO

Cada documento desempenha função própria. Nenhum substitui os três instrumentos centrais; e nenhum dos três centrais substitui os documentos complementares. Confusão entre eles é, novamente, ausência de qualificação técnica.

Este adendo descreve cada um dos sete, fixa suas finalidades específicas e oferece um quadro comparativo final. Comece pelo mapa: o núcleo no centro, os complementares em órbita, codificados por cor conforme o público e a camada a que pertencem.

Teal: documentos voltados ao titular. Azul: sustentação técnica interna. Laranja: extensão à cadeia de terceiros.

1. Política de Cookies

O que é. Documento externo, voltado ao usuário/titular, dedicado especificamente às tecnologias de rastreamento utilizadas no portal: cookies, pixels, SDKs, web beacons, fingerprinting, armazenamento local. Detalha quais tecnologias são usadas, em quais categorias se enquadram (estritamente necessárias, funcionais, analíticas, publicitárias/de terceiros), por quanto tempo persistem e quem é o destinatário.

Função primária. Cumprir a obrigação informativa específica detalhada no Guia Orientativo da ANPD sobre Cookies e Tecnologias de Rastreamento, viabilizando o consentimento granular do titular para cookies não estritamente necessários — e a revogação igualmente granular a qualquer tempo.

Apoia-se em duas peças técnicas:

- **Banner de cookies** — primeira camada, exibida na entrada do portal.
- **Painel de preferências** — segunda camada, com toggles por categoria, acessível permanentemente.

Relação com os instrumentos centrais. É instrumento autônomo, mas complementar ao Aviso de Privacidade. O Aviso descreve o tratamento de dados em geral; a Política de Cookies trata especificamente da camada técnica de rastreamento. Não se substituem: o portal precisa de ambos.

2. Termos de Uso

O que é. Documento externo, de natureza contratual, que estabelece as regras de uso de um serviço digital da instituição — portal, aplicativo, protocolo eletrônico, plataforma de

inscrições. Define direitos e deveres do usuário, hipóteses de suspensão, regras de conduta, propriedade intelectual, limitações de responsabilidade e foro.

Função primária. Disciplinar a relação jurídica entre a instituição e quem usa o serviço — no setor público, é frequentemente equiparado ao "regulamento de uso" do serviço digital. Não é, em si, um instrumento da LGPD.

Base normativa principal. Código de Defesa do Consumidor (Lei nº 8.078/1990) nas relações cabíveis, Marco Civil da Internet (Lei nº 12.965/2014), Lei de Acesso à Informação (Lei nº 12.527/2011) e regramentos administrativos próprios.

Relação com a LGPD. Tangencial. Pode conter cláusulas sobre dados pessoais, mas o tratamento de dados é matéria do Aviso de Privacidade, não dos Termos. A confusão mais comum — e mais grave — é redigir Termos de Uso que "absorvam" a função informativa do Aviso. Resultado: nem os Termos cumprem seu papel contratual com clareza, nem o art. 9º da LGPD é satisfeito.

Os Termos de Uso dizem como o serviço pode ser utilizado. O Aviso de Privacidade diz o que é feito com os dados de quem o utiliza.

3. Termo de Consentimento

O que é. Documento externo, específico para situações em que a base legal do tratamento é o consentimento do titular (art. 7º, I e art. 11, I da LGPD). Materializa o ato de consentir em forma documental — textual, eletrônico (com registro auditável de aceite) ou multimídia.

Função primária. Coletar consentimento livre, informado, inequívoco e para finalidade específica, com todos os requisitos do art. 8º da LGPD: identificação do controlador, finalidade exata, dados envolvidos, prazo, possibilidade de revogação e consequências da recusa.

Característica essencial. Cada Termo de Consentimento é granular — um por finalidade. Consentimento genérico, omnibus ou em bloco é vedado pela LGPD. Comunicação opcional, pesquisa de satisfação, coleta analítica não essencial, vinculação a programa específico — cada caso requer Termo próprio, revogável com a mesma facilidade com que foi concedido (art. 8º, §5º).

Relação com os instrumentos centrais. Não substitui o Aviso. O Aviso descreve todo o tratamento da instituição (em diversas bases legais); o Termo de Consentimento é a peça concreta usada quando a base eleita é o consentimento. Em órgão público, a maior parte dos tratamentos se ampara em outras bases (obrigação legal, políticas públicas, exercício regular de direitos), e o consentimento é exceção — mas, quando usado, exige Termo formal.

4. Política de Segurança da Informação (PSI)

O que é. Documento normativo interno que estabelece princípios, diretrizes e controles para preservar a confidencialidade, integridade e disponibilidade da informação institucional — toda a informação, não apenas dados pessoais. Articula-se em sub-normas: gestão de

acessos, classificação da informação, uso aceitável, backup e continuidade, criptografia, gestão de fornecedores, segurança física e em desenvolvimento.

Função primária. Proteger os ativos informacionais da instituição. É a base normativa interna para que o art. 46 da LGPD (medidas de segurança técnicas e administrativas) saia do papel e seja operado por equipes técnicas, com responsabilidades claras.

Base normativa principal. ABNT NBR ISO/IEC 27001 (sistema de gestão da segurança da informação) e 27002 (controles); em órgãos federais, Instruções Normativas do GSI/PR; em estaduais e municipais, normas próprias adaptadas a esse referencial.

Relação com os instrumentos centrais. Não substitui a Política Interna de Privacidade, embora se interpenetrem. A Política Interna é específica para dados pessoais e LGPD; a PSI cobre toda a informação corporativa (inclusive a que não é dado pessoal). Em organizações maduras, a Política Interna remete à PSI quanto aos controles técnicos, evitando duplicação.

5. Plano de Resposta a Incidentes de Segurança

O que é. Documento operacional interno — não normativo, mas procedimental — que define o passo a passo quando um incidente de segurança é detectado. Cobre as fases típicas: preparação, identificação, contenção, erradicação, recuperação e lições aprendidas.

Função primária. Garantir resposta tempestiva, coordenada e auditável a incidentes. Para fins de LGPD, operacionalizar o dever de comunicação à ANPD e ao titular previsto no art. 48 quando o incidente puder acarretar risco ou dano relevante.

Conteúdo típico:

- Definição clara do que constitui incidente (com gradações de severidade).
- Papéis e responsabilidades (CSIRT/equipe de resposta, Encarregado, Comitê, alta direção).
- Fluxo de escalonamento e prazos internos.
- Critérios para comunicação à ANPD e ao titular.
- Templates de comunicação ao titular e à ANPD.
- Registro de evidências e cadeia de custódia.

O PRAZO QUE NÃO PODE FALHAR

A Resolução CD/ANPD nº 15/2024 (Regulamento de Comunicação de Incidente de Segurança) fixa a comunicação à ANPD e aos titulares em até 3 dias úteis, contados de quando o controlador toma conhecimento de que o incidente afetou dados pessoais. Os registros devem ser guardados por, no mínimo, 5 anos.

Base normativa principal. ABNT NBR ISO/IEC 27035 (gestão de incidentes); orientações do CERT.br; e a Resolução CD/ANPD nº 15/2024 sobre comunicação de incidentes.

Relação com os instrumentos centrais. Não substitui a PSI nem a Política Interna de Privacidade. É instrumento de execução — assume que as políticas existem e descreve como agir quando algo dá errado.

6. Política de Gestão de Riscos de Segurança e Privacidade

O que é. Documento normativo interno que estabelece a metodologia de identificação, análise, avaliação, tratamento, monitoramento e comunicação de riscos de segurança da informação e proteção de dados. Define matriz de probabilidade × impacto, escala de severidade, apetite ao risco e ciclo de revisão.

Função primária. Garantir que decisões sobre proteção de dados e segurança sejam tomadas com base em análise estruturada de risco, e não em intuição. Subsidia diretamente o Relatório de Impacto à Proteção de Dados (RIPD), previsto no art. 38 da LGPD, e a priorização de ações no Plano de Ação institucional.

Base normativa principal. ABNT NBR ISO 31000 (gestão de riscos — diretrizes), ABNT NBR ISO/IEC 27005 (riscos de segurança da informação), NIST Risk Management Framework e — em órgãos federais — normas do TCU e da CGU sobre gestão de riscos.

Relação com os instrumentos centrais. Complementa a Política Interna de Privacidade ao oferecer a metodologia técnica para a avaliação de risco do tratamento. É o que permite que a privacy by design (princípio declarado na Política Interna) seja efetivamente aplicada em decisões concretas de projeto e contratação.

7. Política de Contratação e Gestão de Operadores

O que é. Documento normativo interno que disciplina como a instituição contrata e mantém relação com agentes operadores (art. 5º, VII da LGPD) — terceiros que tratam dados pessoais em seu nome: empresas de tecnologia, hospedagem em nuvem, telefonia, plataformas de comunicação, digitalização documental, entre outros.

Função primária. Estender a governança em privacidade para toda a cadeia de tratamento, evitando que dados escapem do controle institucional por relações contratuais frouxas. Operacionaliza o art. 39 da LGPD (responsabilidade do operador) e a corresponsabilidade do controlador prevista nos arts. 42 e 44.

Conteúdo típico:

- Régua de avaliação de maturidade do operador antes da contratação (cyber + LGPD).
- Cláusulas LGPD obrigatórias em contratos novos (instruções documentadas, segurança, sigilo, suboperadores, atendimento a titulares, notificação de incidentes, devolução/eliminação ao fim do contrato).
- Régua de adequação para contratos pré-LGPD (termo aditivo).
- Monitoramento contínuo (auditorias, relatórios, evidências).
- Plano de saída e portabilidade de dados.

Relação com os instrumentos centrais. Estende a Política Interna de Privacidade para fora dos muros institucionais. O Aviso de Privacidade, por sua vez, deve refletir a existência desses operadores, mencionando categorias de compartilhamento (art. 9º, V da LGPD).

Quadro comparativo geral

O quadro abaixo consolida, em uma única visão, todos os documentos analisados — os três instrumentos centrais do artigo principal e os sete complementares deste adendo.

Documento	Público	Função primária	Base normativa	Vínculo com a LGPD
Portaria de regulamentação	Interno	Instituir Comitê, designar Encarregado, fixar cronograma	Poder normativo do dirigente	Cria estrutura para cumprir a LGPD
Política Interna de Privacidade	Interno	Princípios, diretrizes, regras e sanções internas	Res. CD/ANPD 20/2024	Operacionaliza a LGPD internamente
Aviso de Privacidade	Externo	Informar ao titular sobre o tratamento de dados	Art. 9º LGPD	Cumpre a transparência ativa do art. 9º
Política de Cookies	Externo	Informar e coletar consentimento sobre rastreamento	Guia ANPD de Cookies	Detalha consentimento (art. 7º I) na web
Termos de Uso	Externo	Contratualizar regras de uso do serviço digital	CDC; Marco Civil	Tangencia a LGPD; não é instrumento dela
Termo de Consentimento	Externo	Coletar consentimento específico do titular	Art. 8º LGPD	Materializa a base legal do art. 7º I
Política de Segurança (PSI)	Interno	Controles de confidencialidade, integridade e disponibilidade	ISO 27001-27002; GSI/PR	Atende ao art. 46 (segurança)
Plano de Resposta a Incidentes	Interno	Detecção, contenção e comunicação de incidentes	ISO 27035; Res. ANPD 15/2024	Operacionaliza o art. 48 (notificação)
Política de Gestão de Riscos	Interno	Metodologia de identificação e tratamento de riscos	ISO 31000 e 27005	Subsidia o RIPD (art. 38)
Política de Contratação de Operadores	Interno (efeitos externos)	Avaliar e gerir operadores terceirizados	Arts. 5º VII e 39 LGPD	Estende a governança a toda a cadeia

A leitura do quadro evidencia três fatos:

- **Quatro documentos são externos** (Aviso, Cookies, Termos de Uso e Termo de Consentimento). Todos os demais são internos.
- **Cada documento ancora-se em base normativa específica.** Nenhum é “genérico”. A LGPD é referência transversal, mas Termos de Uso, PSI e gestão de riscos têm bases próprias (Marco Civil, ISO 27001, ISO 31000).
- **Os três centrais são insuficientes isoladamente.** Uma instituição só com eles cumpre o núcleo da LGPD, mas opera sem as ferramentas de segurança, incidentes, risco e cadeia de terceiros que dão sustentação técnica ao programa.

Foco: os três documentos externos que convivem no portal

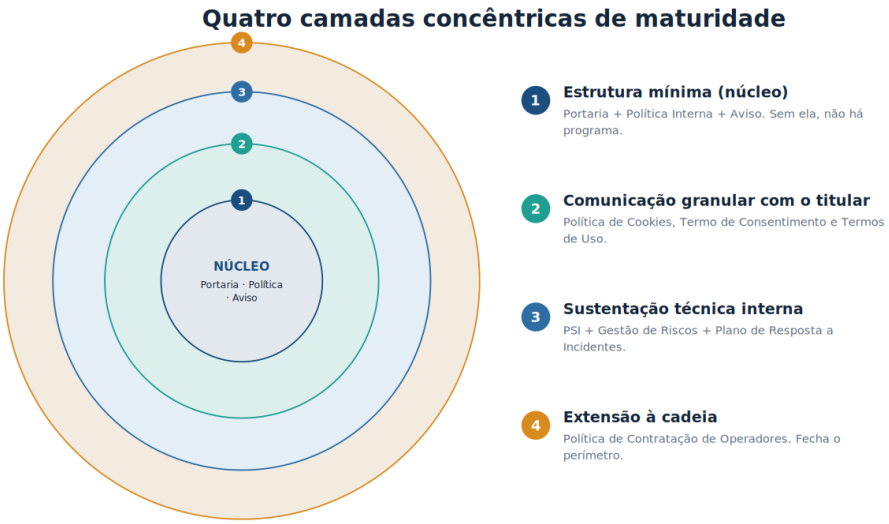
Há confusão frequente entre os documentos externos que coexistem no portal — Aviso de Privacidade, Política de Cookies e Termo de Consentimento. Todos comunicam com o titular, mas cumprem funções distintas.

Aspecto	Aviso de Privacidade	Política de Cookies	Termo de Consentimento
Função	Informar de modo geral o tratamento	Detalhar o rastreamento no portal	Coletar consentimento específico
Escopo	Toda a relação titular ↔ instituição	Restrito à web (cookies/SDKs)	Restrito a uma finalidade
Coleta consentimento?	Não — apenas informa	Sim — cookies não essenciais	Sim — é o próprio ato de consentir
Suporte típico	Página + camadas + just-in-time	Banner + painel de preferências	Formulário + registro auditável
Base legal LGPD	Art. 9º (informação)	Art. 7º I + Guia ANPD	Art. 7º I + art. 8º (requisitos)
Revogação	Não aplicável	Pelo painel de cookies	Pelo Painel de Privacidade

Na prática: um portal maduro tem Aviso de Privacidade no rodapé permanente, Política de Cookies com banner na entrada e painel de preferências, e Termos de Consentimento específicos para cada finalidade que exija essa base legal. Nenhum substitui o outro.

Como tudo se articula: quatro camadas concêntricas

A maturidade do Programa de Governança em Privacidade pode ser lida como camadas concêntricas — cada uma pressupõe a anterior.



Camada 1 — Estrutura mínima (núcleo). Portaria + Política Interna + Aviso de Privacidade. Sem essa camada, não há programa.

Camada 2 — Comunicação granular com o titular. Política de Cookies, Termos de Consentimento e (quando aplicável) Termos de Uso. Detalham aspectos específicos da relação titular ↔ instituição.

Camada 3 — Sustentação técnica interna. PSI + Gestão de Riscos + Plano de Resposta a Incidentes. Garantem que a Política Interna tenha estrutura técnica para ser executada — não apenas declarada.

Camada 4 — Extensão da governança à cadeia. Política de Contratação de Operadores. Estende toda a estrutura acima aos terceiros que tratam dados em nome da instituição, fechando o perímetro de responsabilidade.

Cada camada pressupõe a anterior. Pular camadas ou misturar funções não economiza esforço — gera retrabalho, exposição sancionatória e perda de confiança.

Fecho do adendo: o mapa completo é a vantagem

O artigo principal demonstrou que Portaria, Política Interna e Aviso não se substituem entre si. Este adendo amplia a moldura: nem mesmo esses três, juntos, esgotam o ecossistema documental de uma instituição madura.

A LGPD ancora um programa que exige articulação técnica entre dez instrumentos típicos — **quatro voltados ao titular** (Aviso, Cookies, Termos de Uso, Termo de Consentimento) e **seis voltados ao público interno e contratual** (Portaria, Política Interna, PSI, Plano de Incidentes, Gestão de Riscos, Contratação de Operadores). Cada um cumpre função específica, ancora-se em base normativa própria e produz efeitos distintos.

A VANTAGEM DE QUEM ENXERGA O MAPA INTEIRO

Mapear essa estrutura, identificar lacunas e articular consistência entre os documentos é, novamente, qualificação técnica — não algo que se improvisa. Instituições que reconhecem essa complexidade desde o início economizam tempo, recursos e exposição. As que tentam cumprir a LGPD com um único documento “bom o suficiente” descobrem, em fiscalização, que “bom o suficiente” é, juridicamente, insuficiente.

Adendo ao artigo principal — Programa de Governança em Privacidade

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** — VOCÊ ESTÁ AQUI
   O ecossistema documental — 7 complementares

3. **Fecho Final**
   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