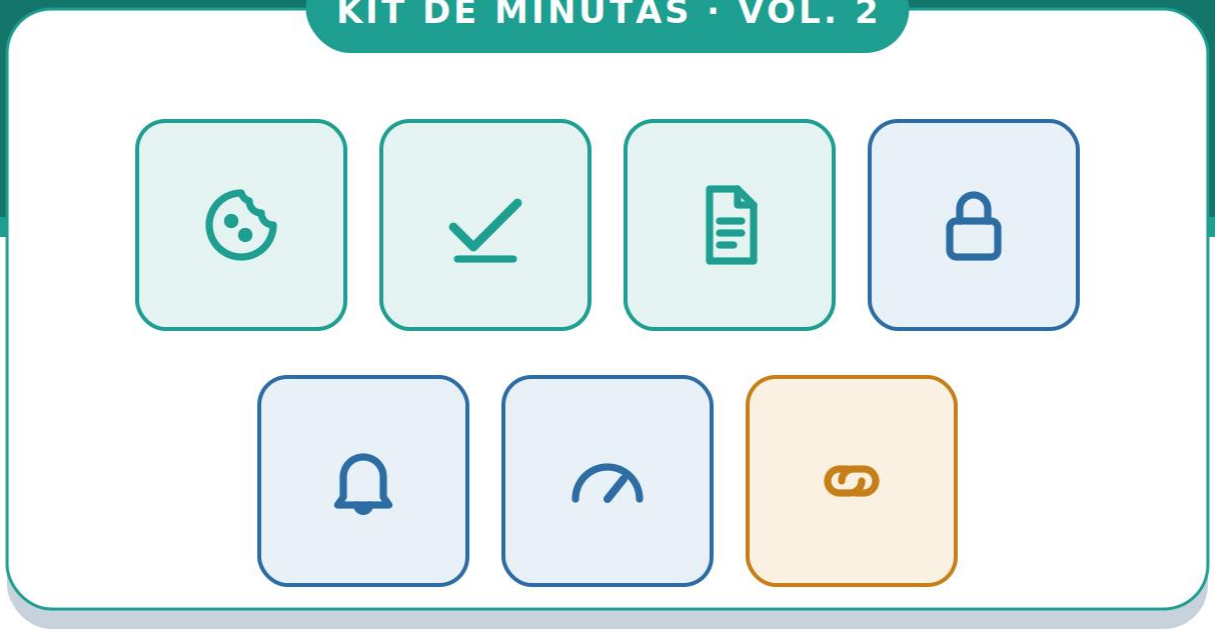
PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

LGPD

PGP
série

KIT DE MINUTAS · VOL. 2



Kit de Minutas — Documentos Complementares

Cookies · Termos de Uso · Consentimento
Segurança · Incidentes · Riscos · Operadores
— os sete que orbitam o núcleo.

Kit de Minutas para Implementação da LGPD

Volume 2 — Documentos Complementares do Programa de Governança em Privacidade

Cookies · Termos de Uso · Termo de Consentimento · Segurança da Informação · Resposta a Incidentes · Gestão de Riscos · Operadores

Continuação do Kit de Minutas (Volume 1: Portaria, Política Interna e Aviso). Reúne os sete documentos que orbitam o núcleo do PGP, conforme o Adendo da série. As convenções de preenchimento são as mesmas do Volume 1.

Os sete complementares em torno do núcleo: teal (titular), azul (sustentação técnica), laranja (cadeia).

NOTA DE REDAÇÃO *Modelos de referência, não documentos prontos. Adapte cada um à realidade da instituição e submeta ao Encarregado (DPO) e à assessoria jurídica antes de publicar ou aprovar. Campos [EM AZUL] preenchem-se; notas amarelas apagam-se na versão final.*

GRUPO A · VOLTADOS AO TITULAR (PÚBLICO EXTERNO)

MINUTA 4 · EXTERNO

Política de Cookies

Instrumento externo, complementar ao Aviso — linguagem clara, com banner e painel de preferências

NOTA DE REDAÇÃO *Complementa o Aviso de Privacidade (não o substitui). Cookies não estritamente necessários exigem consentimento prévio, livre e granular; fechar o banner no "X" não equivale a consentir, e não pode haver caixas pré-marcadas (Guia da ANPD sobre cookies).*

POLÍTICA DE COOKIES — [NOME DO ÓRGÃO]

Última atualização: [DATA] · Versão [Nº]

1. O que são cookies

Cookies são pequenos arquivos que um site guarda no seu dispositivo para lembrar informações sobre a sua visita. Usamos também tecnologias semelhantes, como pixels e armazenamento local.

2. Por que utilizamos

Usamos cookies para manter o portal funcionando, lembrar suas preferências e, com o seu consentimento, entender como o site é utilizado para melhorá-lo.

3. Categorias que utilizamos

Categoria	Para que serve	Precisa do seu consentimento?
Estritamente necessários	Permitem o funcionamento básico e seguro do portal.	Não
Funcionais / preferências	Lembram escolhas como idioma e acessibilidade.	Sim, quando não essenciais
Analíticos / desempenho	Medem o uso do site de forma agregada para melhorá-lo.	Sim
Publicidade / terceiros	[Se aplicável] medem campanhas ou integram serviços externos.	Sim

4. Como você gerencia seus cookies

Na primeira visita, exibimos um **banner** para você aceitar, recusar ou personalizar os cookies não essenciais. A qualquer momento, você pode rever suas escolhas no nosso **painel de preferências** [INSERIR LINK/ACESSO] ou nas configurações do seu navegador.

5. Consentimento e revogação

O consentimento para cookies não essenciais é livre e específico por categoria, e pode ser **revogado a qualquer momento** com a mesma facilidade com que foi concedido. A recusa não impede o uso dos serviços essenciais do portal.

6. Atualizações

Esta Política pode ser atualizada para refletir mudanças técnicas ou normativas; a data e a versão constam no topo. Para o tratamento de dados em geral, consulte o nosso [Aviso de Privacidade — INSERIR LINK].

MINUTA 5 · EXTERNO

Termos de Uso

Instrumento externo de natureza contratual — disciplina o uso do serviço (não é instrumento da LGPD)

> **NOTA DE REDAÇÃO** *Regula como o serviço pode ser usado, não o tratamento de dados — este vai para o Aviso de Privacidade. Evite cláusulas que "absorvam" a função informativa do Aviso. Base: Marco Civil da Internet, CDC (quando cabível) e regramentos próprios.*

TERMOS DE USO — [NOME DO SERVIÇO/PORTAL]

[NOME DO ÓRGÃO] · Vigência a partir de [DATA] · Versão [Nº]

1. Objeto e aceitação. Estes Termos regem o uso do [SERVIÇO/PORTAL] disponibilizado por [NOME DO ÓRGÃO]. Ao acessar ou utilizar o serviço, o usuário declara que leu e concorda com estes Termos.

2. Definições. Consideram-se: **usuário**, a pessoa que acessa o serviço; **serviço**, as funcionalidades oferecidas no [PORTAL/APLICATIVO]; **conta**, o cadastro de acesso, quando existente.

3. Cadastro e acesso. [Se houver cadastro:] o usuário compromete-se a fornecer informações verídicas e a manter a confidencialidade de suas credenciais, responsabilizando-se pelos acessos realizados.

4. Regras de uso e conduta. O usuário compromete-se a utilizar o serviço de forma lícita, sendo vedado:

I – violar a lei, direitos de terceiros ou estes Termos;

II – tentar obter acesso não autorizado a sistemas ou dados;

III – inserir conteúdo ilícito, ofensivo ou que comprometa a segurança.

5. Propriedade intelectual. O conteúdo e os elementos do serviço pertencem a [NOME DO ÓRGÃO] ou a seus licenciadores, vedado o uso não autorizado.

6. Disponibilidade e responsabilidades. O serviço é oferecido conforme disponibilidade, podendo sofrer interrupções para manutenção. [Adaptar as limitações de responsabilidade ao regime jurídico da instituição.]

7. Suspensão e encerramento. O acesso poderá ser suspenso ou encerrado em caso de descumprimento destes Termos, observado o devido processo.

8. Proteção de dados pessoais. O tratamento de dados pessoais decorrente do uso do serviço é descrito no **Aviso de Privacidade** [INSERIR LINK], que integra estes Termos para esse fim específico.

9. Alterações. Estes Termos podem ser alterados; a versão vigente e sua data constam no topo. O uso continuado após alterações implica concordância.

10. Legislação e foro. Aplica-se a legislação brasileira, elegendo-se o foro de [COMARCA/SEÇÃO JUDICIÁRIA], salvo competência legal diversa.

MINUTA 6 · EXTERNO

Termo de Consentimento

Instrumento externo específico — usado apenas quando a base legal é o consentimento (um por finalidade)

NOTA DE REDAÇÃO *Use somente quando o consentimento for a base legal adequada — no setor público é exceção. Deve ser granular (um Termo por finalidade), livre, informado e revogável. Consentimento genérico ou em bloco é vedado.*

TERMO DE CONSENTIMENTO PARA TRATAMENTO DE DADOS PESSOAIS

Finalidade: **[DESCREVER A FINALIDADE ESPECÍFICA]**

Controlador: [NOME DO ÓRGÃO], CNPJ [Nº], com sede em [ENDEREÇO]. Contato do Encarregado: [E-MAIL].

Finalidade do tratamento: seus dados serão tratados exclusivamente para [DESCREVER A FINALIDADE], não sendo usados para finalidades incompatíveis.

Dados tratados: [LISTAR OS DADOS ESPECÍFICOS — ex.: nome, e-mail, telefone].

Base legal: consentimento do titular, nos termos do art. 7º, I [ou art. 11, I, se dado sensível] da LGPD.

Prazo de tratamento: os dados serão tratados por [PRAZO/EVENTO] e, depois, eliminados ou anonimizados.

Compartilhamento: [Se houver, indicar com quem e por quê; caso contrário, declarar que não há compartilhamento para esta finalidade.]

Revogação e direitos: você pode revogar este consentimento a qualquer momento pelo canal [INDICAR], sem afetar a licitude do tratamento anterior à revogação, e exercer os direitos do art. 18 da LGPD.

Consequências de não consentir: [DESCREVER o que ocorre caso o titular não consinta — ex.: impossibilidade de participar da ação específica, sem prejuízo do acesso aos serviços essenciais].

DECLARAÇÃO DE ACEITE

☐ Li e concordo com o tratamento dos meus dados pessoais para a finalidade acima descrita.

Nome: **[NOME DO TITULAR]** CPF: **[Nº]**

Data: **[DATA]** Assinatura / registro eletrônico de aceite: **[_____]**

GRUPO B · SUSTENTAÇÃO TÉCNICA INTERNA

MINUTA 7 · INTERNO

Política de Segurança da Informação (PSI)

Ato normativo interno — cobre toda a informação institucional, não apenas dados pessoais

NOTA DE REDAÇÃO *A Política Interna de Privacidade remete a esta PSI quanto aos controles técnicos. Referencie as normas adotadas (ABNT NBR ISO/IEC 27001 e 27002; em órgãos federais, IN do GSI/PR).*

[NOME DO ÓRGÃO] — POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Aprovada por [INSTÂNCIA] em [DATA] · Versão [Nº]

Capítulo I — Objeto e abrangência

Art. 1º Esta Política estabelece princípios, diretrizes e controles para preservar a confidencialidade, a integridade e a disponibilidade das informações de [NOME DO ÓRGÃO].

Art. 2º Aplica-se a todos os agentes que acessem informações ou recursos da instituição, em qualquer suporte.

Capítulo II — Princípios

Art. 3º A segurança da informação orienta-se pelos princípios de confidencialidade, integridade, disponibilidade, autenticidade e legalidade.

Capítulo III — Diretrizes

Art. 4º São diretrizes mínimas:

I – gestão de acessos pelo princípio do menor privilégio e da necessidade de conhecer;

II – classificação da informação conforme sensibilidade e criticidade;

III – uso aceitável dos recursos de tecnologia;

IV – cópias de segurança (backup) e continuidade dos serviços;

V – uso de criptografia para dados em trânsito e em repouso, quando aplicável;

VI – gestão de segurança junto a fornecedores e operadores;

VII – segurança física e do ambiente;

VIII – desenvolvimento seguro e registros (logs) de eventos relevantes.

Capítulo IV — Responsabilidades, conformidade e disposições finais

Art. 5º As responsabilidades de gestão e operação da segurança serão definidas em normas complementares, sob coordenação de [ÁREA RESPONSÁVEL].

Art. 6º Esta Política observa as referências [ABNT NBR ISO/IEC 27001 e 27002; IN GSI/PR, quando aplicável] e será revisada a cada [Nº] meses.

Art. 7º O descumprimento sujeita o agente às sanções cabíveis, observado o devido processo. Esta Política entra em vigor na data de sua publicação.

MINUTA 8 · INTERNO

Plano de Resposta a Incidentes de Segurança

Documento operacional interno — define o passo a passo quando algo dá errado

NOTA DE REDAÇÃO *Documento procedimental (não normativo): assume que a PSI e a Política Interna existem. O prazo de comunicação à ANPD e aos titulares é de até 3 dias úteis e os registros devem ser guardados por, no mínimo, 5 anos (Resolução CD/ANPD nº 15/2024). Referência técnica: ABNT NBR ISO/IEC 27035.*

[NOME DO ÓRGÃO] — PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA

Versão [Nº] · Aprovado em [DATA]

1. Objetivo

Estabelecer procedimento tempestivo, coordenado e auditável de resposta a incidentes de segurança que possam afetar informações e dados pessoais.

2. Definições e severidade

Considera-se **incidente** qualquer evento que comprometa a confidencialidade, integridade ou disponibilidade da informação. Os incidentes serão classificados em níveis de severidade [ex.: baixa, média, alta e crítica], conforme impacto e abrangência.

3. Equipe e papéis

A resposta é conduzida pela equipe de resposta a incidentes (CSIRT/[ÁREA]), com participação do Encarregado, do Comitê Gestor, da alta direção e da área de comunicação, com responsabilidades definidas para cada fase.

4. Fases da resposta

- **Preparação** — manter recursos, contatos e treinamentos prontos.
- **Identificação** — detectar, registrar e classificar o incidente.
- **Contenção** — limitar a propagação e o impacto.
- **Erradicação** — remover a causa e as vulnerabilidades exploradas.
- **Recuperação** — restabelecer os serviços com segurança.
- **Lições aprendidas** — registrar causas e melhorias.

5. Comunicação à ANPD e aos titulares

Quando o incidente puder acarretar risco ou dano relevante, a comunicação à ANPD e aos titulares afetados será feita em até **3 (três) dias úteis**, contados do conhecimento de que o incidente afetou dados pessoais, com o conteúdo mínimo exigido. Os registros do incidente serão mantidos por, no mínimo, **5 (cinco) anos** (art. 48 da LGPD; Resolução CD/ANPD nº 15/2024).

6. Registro, evidências e revisão

Todas as ações e evidências serão registradas com preservação da cadeia de custódia. O Plano será testado e revisado periodicamente, ao menos a cada [Nº] meses.

MINUTA 9 · INTERNO

Política de Gestão de Riscos de Segurança e Privacidade

Ato normativo interno — a metodologia que sustenta decisões e o RIPD

NOTA DE REDAÇÃO *É o que permite operacionalizar o privacy by design declarado na Política Interna e subsidiar o Relatório de Impacto (RIPD, art. 38). Referências: ABNT NBR ISO 31000 e ISO/IEC 27005; em órgãos federais, normas do TCU e da CGU.*

[NOME DO ÓRGÃO] — POLÍTICA DE GESTÃO DE RISCOS DE SEGURANÇA E PRIVACIDADE

Aprovada por [INSTÂNCIA] em [DATA] · Versão [Nº]

Capítulo I — Objeto e escopo

Art. 1º Esta Política define a metodologia de gestão de riscos relacionados à segurança da informação e à proteção de dados pessoais de [NOME DO ÓRGÃO].

Capítulo II — Metodologia

Art. 2º O processo de gestão de riscos compreende as etapas de identificação, análise, avaliação, tratamento, monitoramento e comunicação.

Art. 3º A avaliação utilizará matriz de **probabilidade × impacto**, com escala de severidade [ex.: baixo, médio, alto, crítico] e definição do **apetite ao risco** da instituição.

Capítulo III — Tratamento e integração

Art. 4º O tratamento poderá mitigar, transferir, evitar ou aceitar o risco, de forma justificada e documentada.

Art. 5º Os resultados subsidiarão os Relatórios de Impacto à Proteção de Dados (RIPD) e a priorização de ações do Programa, integrando-se à matriz corporativa de riscos.

Capítulo IV — Responsabilidades e revisão

Art. 6º As responsabilidades de cada instância serão definidas em normas complementares, sob coordenação de [ÁREA]. Esta Política observa as referências ABNT NBR ISO 31000 e ISO/IEC 27005 e será revisada a cada [Nº] meses.

GRUPO C · EXTENSÃO À CADEIA DE TERCEIROS

MINUTA 10 · INTERNO (EFEITOS CONTRATUAIS)

Política de Contratação e Gestão de Operadores

Ato normativo interno que estende a governança a quem trata dados em nome da instituição

NOTA DE REDAÇÃO *Fecha o perímetro de responsabilidade. As categorias de compartilhamento com operadores devem aparecer também no Aviso de Privacidade (art. 9º, V). Base: arts. 5º, VII; 39; 42 e 44 da LGPD.*

[NOME DO ÓRGÃO] — POLÍTICA DE CONTRATAÇÃO E GESTÃO DE OPERADORES

Aprovada por [INSTÂNCIA] em [DATA] · Versão [Nº]

Capítulo I — Objeto e escopo

Art. 1º Esta Política disciplina a contratação e a gestão de operadores — terceiros que tratam dados pessoais em nome de [NOME DO ÓRGÃO] (art. 5º, VII da LGPD).

Capítulo II — Avaliação prévia (due diligence)

Art. 2º Antes da contratação, o operador será avaliado quanto à maturidade em segurança e proteção de dados, mediante [questionário/régua de avaliação], proporcionalmente ao risco do tratamento.

Capítulo III — Cláusulas obrigatórias

Art. 3º Os contratos conterão, no mínimo, cláusulas que obriguem o operador a:

I – tratar os dados somente conforme instruções documentadas do controlador;

II – adotar medidas de segurança compatíveis com o art. 46 da LGPD;

III – manter sigilo e capacitar seus colaboradores;

IV – contratar suboperadores apenas com autorização prévia;

V – apoiar o atendimento aos titulares e às requisições da ANPD;

VI – notificar incidentes ao controlador em [PRAZO] horas;

VII – devolver ou eliminar os dados ao término do contrato.

Capítulo IV — Contratos anteriores, monitoramento e saída

Art. 4º Os contratos firmados antes da vigência da LGPD serão adequados por termo aditivo.

Art. 5º Os operadores serão monitorados de forma contínua (auditorias, relatórios e evidências), e cada relação preverá plano de saída e portabilidade dos dados.

Art. 6º As responsabilidades de gestão serão definidas em normas complementares. Esta Política será revisada a cada [Nº] meses e entra em vigor na data de sua publicação.

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**
   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
   VOCÊ ESTÁ AQUI

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