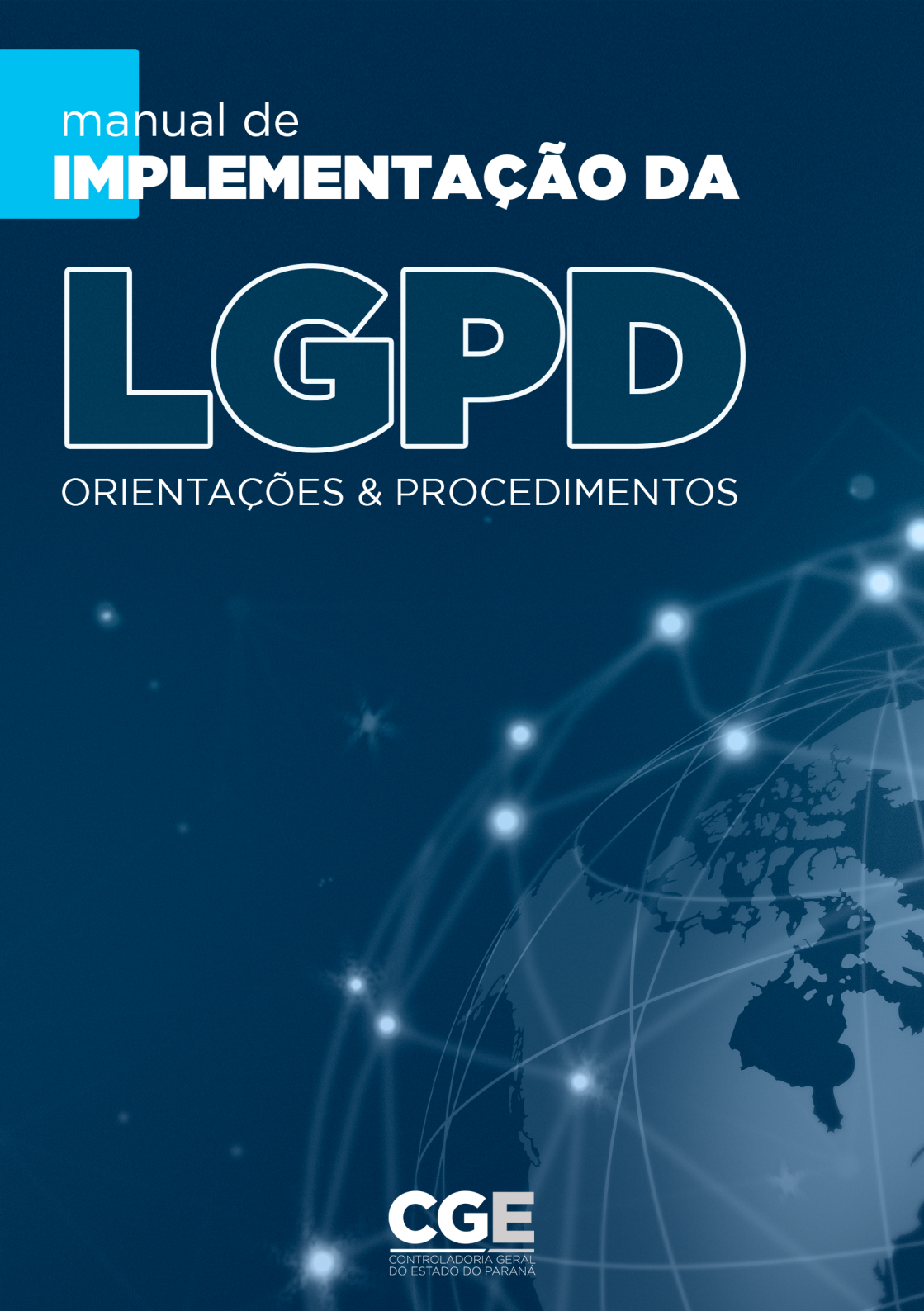
manual de

IMPLEMENTAÇÃO DA LGPD

ORIENTAÇÕES & PROCEDIMENTOS



CGE

CONTROLADORIA GERAL
DO ESTADO DO PARANÁ

GOVERNO DO ESTADO DO PARANÁ

Governador do Estado do Paraná
Carlos Massa Ratinho Junior

Controladora-Geral do Estado do Paraná
Luciana Carla da Silva Azevedo

Elaboração
Assessora Técnica
Mineia Lückfett de Oliveira

Contato:
lgpd@cge.pr.gov.br
mineial@cge.pr.gov.br
(41) 3883-40 47

SUMÁRIO

1 APRESENTAÇÃO

O presente manual tem o objetivo de orientar os agentes públicos quanto aos procedimentos para a implementação da LGPD no âmbito dos órgãos e entidades do Poder Executivo Estadual.

Tais orientações são fundamentais não só para garantir a correta aplicabilidade da lei, mas também para evitar a violação dos direitos do titular de dados em relação ao tratamento de dados pessoais efetuado pelo Estado.

As recomendações para a implementação da LGPD estão baseadas no conjunto de normas legais relacionadas ao tema, bem como nos materiais disponibilizados pelo Governo Federal.

2 COMITÊ GESTOR DE PROTEÇÃO DE DADOS PESSOAIS - CGPDP

O Comitê Gestor de Proteção de Dados Pessoais - CGPDP tem a finalidade de dar auxílio no cumprimento da Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), bem como do Decreto Estadual nº 6.474/2020 (Regulamenta a aplicação da LGPD no âmbito da Administração Pública Estadual direta, autárquica e fundacional do Poder Executivo do Estado do Paraná).

Este Comitê é formado por equipe multidisciplinar, composta de servidores da alta gestão, tecnologia da informação, setor jurídico, encarregado de dados, entre outras áreas afins que possam contribuir para o desenvolvimento de um plano de ação adequado e eficiente para implementação da LGPD.

É recomendável que CGPDP esteja sujeito, ao menos, às seguintes atribuições:

avaliar os mecanismos de tratamento e proteção dos dados existentes e propor políticas, estratégias e metas para a conformidade do órgão ou entidade com as disposições da Lei n. 13.709, de 14 de agosto de 2018;

formular princípios e diretrizes para a gestão de dados pessoais;

supervisionar a execução dos planos, dos projetos e das ações aprovados para viabilizar a implantação das diretrizes previstas na Lei n. 13.709, de 14 de agosto de 2018;

prestar orientações sobre o tratamento e a proteção de dados pessoais, de acordo com as diretrizes estabelecidas na Lei n. 13.709, de 14 de agosto de 2018 e nas normas internas;

propor e monitorar a adoção de medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;

promover o intercâmbio de informações sobre a proteção de dados pessoais com outros órgãos.

3 PLANO DE AÇÃO PROCESSOS E DETALHAMENTOS DA IMPLEMENTAÇÃO

O Plano de Ação elenca as principais atividades que deverão ser executadas pelo órgão ou entidade para o cumprimento das exigências da Lei Geral de Proteção de Dados.

Considerando as atribuições da Controladoria-Geral do Estado, elencadas no art. 5º do Decreto Estadual nº 6.474/2020, em especial no inciso I, o qual estabelece que compete à CGE orientar os encarregados de dados dos órgãos e entidades quanto a implementação da LGPD, sugere-se o modelo a seguir, que poderá sofrer adequações, conforme especificidades:

PROCESSOS	DETALHAMENTO
1. Diagnósticos: 1.1. Da cultura organizacional; 1.2.Da governança de dados	Aplicação de questionário aos servidores para verificar a percepção e o conhecimento dos mesmos a respeito da LGPD; Aplicação de questionário ao gestor da pasta para verificar quais as práticas atuais aplicadas e em qual estágio o órgão se encontra.
2. Mapeamento de Dados Pessoais	Catalogar todo o fluxo de dados pessoais, objeto das operações de tratamento
3. Levantamento de Riscos	Procedimento para ajudar a planejar as ações preventivas tomadas por parte do órgão; Deverá abranger todos os envolvidos no processo de tratamento de dados (controlador e operador). *ISO 27001 *Necessidade de atualização periódica
4. Criação de Política de Privacidade de Dados	A Política de Privacidade de Dados é um documento informativo que descreve ao titular a forma, os processos e os procedimentos adotados no tratamento dos dados pessoais e as medidas de privacidade empregadas.
5. Adaptação de documentos	Revisão de contratos e demais documentos (impressos e digitais) para atender ao disposto nas normas pertinentes à LGPD.
6. Termo de Compromisso e Confidencialidade	Termo de Compromisso e Confidencialidade a ser exigido daqueles que tenham acesso a dados pessoais no âmbito do órgão ou entidade.
7. Política de Segurança da Informação	A Política de Segurança da Informação é o conjunto de princípios e diretrizes que têm a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados, informações e conhecimentos que compõem o ativo da informação do órgão ou entidade.
8. Plano de Resposta a Incidentes e Privacidade	**a**.conferir clareza sobre o fluxo de procedimentos adequados e responsáveis no caso de incidentes; **b.** preservar a reputação e imagem do órgão ou entidade; **c.** assegurar respostas rápidas, efetivas e coordenadas; **d.** quantificar e monitorar desempenho; **e.** evoluir continuamente com as lições aprendidas.

3.1
DIAGNÓSTICOS
3.1.1
DA CULTURA ORGANIZACIONAL

A adequação dos órgãos e entidades estaduais no âmbito do Poder Executivo em relação à Lei Geral de Proteção de Dados está diretamente relacionada a uma transformação cultural das instituições, de modo que sejam atingidos todos os níveis, desde o estratégico até o operacional.

Essa mudança cultural envolve: (i) refletir sobre a privacidade dos dados pessoais do cidadão em todas as fases que envolvem o tratamento; e (ii) desenvolver ações de conscientização dos agentes públicos, no sentido de incorporar o respeito à privacidade dos dados pessoais nas atividades institucionais cotidianas.

Nesse contexto, o diagnóstico da cultura organizacional tem como principal objetivo, identificar o nível de percepção dos agentes públicos em relação à LGPD, orientar o encarregado de dados e os órgãos e entidades do Poder Executivo Estadual, conforme as suas necessidades específicas, e promover melhoramentos em relação ao tratamento de dados.

É relevante que essa pesquisa seja feita de forma ampla, de modo a atingir um número expressivo de agentes públicos, para que a partir da análise sobre a percepção e o conhecimento dessas pessoas sobre a proteção de dados pessoais, seja possível identificar a necessidade de ampliação da conscientização em relação ao assunto.

A referida avaliação poderá ser realizada por meio do questionário sugerido no Anexo I deste Manual.

3.2.1
DA GOVERNANÇA DE DADOS

Tão importante quanto a conscientização dos servidores em relação à proteção de dados, é a governança desses, realizada mediante a análise do planejamento, gestão e controle do uso dos mesmos.

A avaliação desses aspectos pode ser efetuada por meio do de questionário próprio (Anexo II), a ser preenchido pelos gestores, com o objetivo de mensurar quais são as práticas atuais, determinando em qual estágio o órgão ou entidade se encontra, antes de avançar nas mudanças necessárias para adequação à LGPD, por intermédio de estratégias futuras.

Ressalta-se a importância da realização periódica dessa avaliação, com a finalidade de acompanhar a evolução e a necessidade de eventuais melhorias, fundamentais à governança do tratamento.

3.2 MAPEAMENTO DE DADOS PESSOAIS

Mapeamento de dados pessoais é uma atividade de catalogação de todo o fluxo de dados pessoais, que são objeto das operações de tratamento. Recomenda-se que as informações obtidas sejam mantidas em sistemas eletrônicos, facilitando a tomada de decisões e a manutenção de registros.

Esse levantamento pode ser realizado mediante o preenchimento de planilhas, conforme modelo sugerido: **Planilha para Mapeamento de Dados**.

3.3 LEVANTAMENTO DE RISCOS

O levantamento de riscos tem como objetivo mitigá-los, por meio do controle e da redução desses, até que, em algum momento, eles sejam extintos. Trata-se de um procedimento que ajuda a planejar as ações preventivas tomadas por parte dos órgãos ou entidades estaduais.

Para que essa análise ocorra de forma satisfatória, todos os envolvidos no processo de tratamento de dados devem participar desse levantamento.
Considerando que o resultado é utilizado como um indicador que informa o nível dos riscos, a fim de obter um diagnóstico da situação, deve ser periodicamente revisitado e atualizado.

3.4
POLÍTICA DE PRIVACIDADE DE DADOS

A Política de Privacidade de Dados é um documento a ser elaborado pelo órgão ou entidade que explicita as práticas e processos adotados referentes ao tratamento de dados pessoais, assim como as medidas de privacidade adotadas.

Visa demonstrar credibilidade e transparência aos titulares e atender às normas previstas na LGPD.

Em relação ao seu conteúdo, recomenda-se que contenha, no mínimo as seguintes informações:

OBJETO DA POLÍTICA	Escopo Princípios Definições
NORMAS PARA O TRATAMENTO DE DADOS PESSOAIS	Referências Legais e Normativas Bases para Tratamento de Dados Pessoais Tratamento dos Dados Pessoais Tratamento de Dados Pessoais Sensíveis Direitos dos Titulares Deveres para Uso Adequado de Dados Pessoais Relações com Terceiros Prazos de Conservação dos Dados Pessoais Uso e Trânsito de Documentos Físicos Uso de Mídias, Dispositivos Móveis e Aplicativos Do Compartilhamento de Dados
AGENTES DE TRATAMENTO	Controlador Operador Encarregado
DISPOSIÇÕES FINAIS	Diretrizes de Implementação Complementação, Revisão e Vigência

3.5
ADAPTAÇÃO DE DOCUMENTOS

Esta etapa do processo de implementação se refere a revisão de contratos, termos de cooperação, convênios e outros instrumentos congêneres, físicos ou digitais, a fim de incluir deveres e obrigações às partes contratantes, pertinentes ao direito constitucional à proteção de dados pessoais.

Neste contexto, a Procuradoria-Geral do Estado, por meio da Resolução nº 160/2022 – PGE, publicou a Minuta Padronizada de Termo Aditivo, para Implementação do Direito Constitucional à Proteção dos Dados nos contratos firmados com a Administração Pública.

3.6
TERMO DE COMPROMISSO E CONFIDENCIALIDADE

É um documento aplicável àqueles que tenham acesso a dados pessoais no âmbito do órgão ou entidade. Tem como escopo efetuar o tratamento de dados pessoais confidencialmente, não podendo ser divulgados a terceiros não autorizados, salvo quando explicitamente forem classificados como públicos, sendo disponíveis, conforme as regras de sigilo.

3.7
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação é um documento que tem por objetivo promover o gerenciamento da segurança da informação, estabelecendo regras e padrões de proteção. Busca ainda manter a confidencialidade e o sigilo das informações classificadas como tal, e evitar incidentes de segurança, como vazamentos, perdas, alterações ou acessos indevidos.

Para a criação de uma política adequada é recomendável que sejam observadas as seguintes etapas:

a) Compreenda as necessidades de segurança da informação do órgão ou entidade: a primeira etapa é entender as necessidades de segurança da informação do órgão ou entidade, incluindo os dados e informações sensíveis que precisam ser protegidos.

b) Identifique as ameaças: é essencial identificar as ameaças mais comuns que podem afetar a segurança da informação, como vírus, invasões de hackers e erros humanos.

c) Elabore sua política de segurança da informação: com base nas necessidades de segurança e nas ameaças identificadas, é hora de elaborar sua PSI. A política deve incluir medidas para garantir a confidencialidade, integridade e disponibilidade das informações.

d) Implemente as medidas de segurança: após a elaboração da política, é hora de implementar as medidas de segurança, incluindo a autenticação de usuários, criptografia de dados, controle de acesso a sistemas e dados, backups regulares, verificações de integridade de arquivos, proteção contra vírus, alta disponibilidade, entre outras medidas.

e) Treinamento: é imprescindível que todos os agentes públicos estejam cientes da política de segurança da informação e saibam como aplicá-la.

3.8 PLANO DE RESPOSTA A INCIDENTES E PRIVACIDADE

De acordo com a Autoridade Nacional de Proteção de Dados (ANPD), um incidente de segurança com dados pessoais é qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

A LGPD determina que os agentes de tratamento de dados pessoais (Controlador e Operador) devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Diversas ferramentas e técnicas podem ser utilizadas para mitigar os riscos e efeitos de incidentes de segurança, como por exemplo, senhas fortes, anonimização ou pseudonimização dos dados, criptografia, minimização dos dados coletados, atualização constante dos aplicativos, ferramentas técnicas de segurança, dentre outros.

O vazamento de dados pessoais, um dos mais conhecidos incidentes de segurança, ocorre quando dados são indevidamente acessados, coletados e divulgados ou repassados a terceiros. O dano ao titular pode ser das mais diversas naturezas, como fraudes, tentativas de golpes, uso indevido dos dados, venda dos dados, etc.

O Plano de Resposta a Incidentes de Segurança e Privacidade é essencialmente um processo que descreve a forma como o órgão ou entidade vai responder às situações de emergência e exceção.

Pela potencial gravidade, a resposta deve ser rápida e confiável, ao mesmo tempo resguardando evidências forenses que podem ajudar a prevenir novos incidentes e atendendo as exigências legais de comunicação e transparência. Para o processo funcionar e ser estabelecido é pré-requisito a preparação prévia e contínua, atendendo os seguintes itens:

a) conferir clareza sobre o fluxo de procedimentos adequados e responsáveis no caso de incidentes;

b) preservar a reputação e imagem do órgão ou entidade;

c) assegurar respostas rápidas, efetivas e coordenadas;

d) quantificar e monitorar desempenho;

e) evoluir continuamente com as lições aprendidas.

4 DESIGNAÇÃO DO ENCARREGADO DE DADOS

É a pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares de dados e a Autoridade Nacional de Proteção de dados – ANPD, conforme previsto no inciso VIII, do art. 5º da LGPD.
De acordo com o inciso III, do art. 23 da LGPD, as pessoas jurídicas de direito público, quando realizarem operações de tratamento de dados pessoais, deverão indicar um encarregado.

Em nível de Estado, é feita no âmbito de cada órgão ou entidade da Administração Pública, conforme inciso I do art. 8º do Decreto Estadual nº 6474/2020, e deve ser comunicada, mediante ofício, via e-protocolo, à Controladoria-Geral do Estado (Resolução CGE nº 13/2021).

5 CURSOS E CAPACITAÇÕES

É imprescindível que os agentes públicos conheçam as regras estabelecidas na LGPD, particularmente àqueles que trabalham diretamente com dados pessoais. Esse alinhamento garante que todos estejam a par das mudanças, afastando eventuais irregularidades.

Nesse contexto, a CGE-PR vem desenvolvendo um conjunto de ações, que envolvem cursos e capacitações, visando disseminar informações e orientações aos servidores do Estado sobre a LGPD, a fim de nortear a implementação da Lei no âmbito do Poder Executivo Estadual, além de alertar quanto à importância da observância das normas legais pertinentes, entre os quais destacamos:

WEBINAR 01
Das Controladorias-Gerais Do Estado E Da União: Lei Geral De Proteção De Dados (LGPD)
Realizado Em 25/03/2021;

WEBINAR 02
LGPD - decreto 6.474/2020 No poder executivo paranaense realizado em 31/03/2021;

WEBINAR 03
LGPD - Perguntas e respostas (PGE, cge e cgu)
realizado em 16/04/2021;

LEI GERAL DE PROTEÇÃO DE DADOS
LGPD na administração pública – Por Rodrigo Pironti
Realizado em 22/04/2021.

LEI GERAL DE PROTEÇÃO DE DADOS E A ADMINISTRAÇÃO PÚBLICA
Cursos Permanentes/2024 - Modalidade On-line

6 ANEXOS

ANEXO I
DIAGNÓSTICO - CULTURA ORGANIZACIONAL

Este diagnóstico inicial procura identificar o conhecimento dos servidores, sobre a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018.
São 10 (dez) perguntas e não há identificação das pessoas.
Prazo para resposta: xx/xx/xxxx
*Obrigatório

1. Insira sua unidade/setor: *
_____

2. Você já participou de capacitação sobre a Lei Geral de Proteção de Dados dentro ou fora do órgão? *
☐ Palestra
☐ Seminário
☐ Curso (Presencial ou EaD)
☐ Leitura de textos e documentos
☐ Não possuo capacitação no assunto
☐ Outro:

3. Você sabe o que são dados pessoais? *
☐ Sim
☐ Não

4. Em seu trabalho no órgão, você realiza alguma atividade que envolve dados pessoais? *
☐ Sim
☐ Não
☐ Não sei

5. Por quais meios você trabalha com dados pessoais? *
☐ Sistemas
☐ Planilhas Eletrônicas
☐ Documentos Eletrônicos
☐ Documentos Físicos
☐ Não sei dizer se trabalho com dados pessoais no dia a dia
☐ Outro:

6. Dos fluxos que fazem parte do seu trabalho no órgão, em quais você faz uso de dados pessoais? *
☐ Distribuição
☐ Requisição de informações
☐ Análise jurídica
☐ Requerimentos diversos
☐ Solicitação de cumprimento de decisões
☐ Não sei informar
☐ Outro:

7. Por quais meios você recebe as solicitações para trabalhar com dados pessoais no órgão? *
☐ E-mail
☐ Físico
☐ Telefone
☐ Não sei responder
☐ Outro:

8. Há alguma orientação a respeito do tratamento dos dados pessoais que instruem as solicitações ou requerimentos? *
☐ Sim
☐ Não
☐ Não é necessária orientação, pois o uso da informação é institucional
☐ Outro:

9. Somente os dados pessoais estritamente necessários são acessados? *
☐ Sim
☐ Não
☐ Não sei informar

10. Deseja fazer alguma consideração sobre o assunto Proteção de Dados?
☐ Sim
☐ Não

Se sim, descreva:

ANEXO II

DIAGNÓSTICO – GOVERNANÇA DA DADOS

A – GOVERNANÇA:

1. As partes envolvidas com a implementação da LGPD realizaram a leitura do Guia de Boas Práticas sobre a Lei Geral de Proteção de Dados (LGPD) produzido pela Secretaria de Governo Digital?
☐ Sim
☐ Não
☐ Parcialmente

2. O órgão já realizou um planejamento do seu Programa Institucional de Privacidade de Dados?
☐ Sim
☐ Não
☐ Parcialmente

3. O órgão desenvolveu um plano de comunicação interno do Programa Institucional de Privacidade de Dados?
☐ Sim
☐ Não
☐ Parcialmente

4.O órgão já realizou a indicação de um encarregado com conhecimento e experiência suficientes e autonomia para implementar a LGPD?
☐ Sim
☐ Não
☐ Parcialmente

5. O órgão disponibilizou para o encarregado os recursos necessários para implementação da LGPD e acesso direto à alta administração?
☐ Sim
☐ Não
☐ Parcialmente

6. O órgão designou os líderes responsáveis por cada frente de atuação no tratamento dos dados?
☐ Sim
☐ Não
☐ Parcialmente

7. Foram definidos indicadores que serão utilizados para medir os resultados do Programa Institucional de Privacidade de Dados?
☐ Sim
☐ Não
☐ Parcialmente

8. O órgão elaborou Relatório de Impacto à Privacidade de Dados Pessoais - RIPD?
☐ Sim
☐ Não
☐ Parcialmente

9. O RIPD foi elaborado com base nas orientações da seção 2.5 e Anexo I do Guia de Boas Práticas LGPD?
☐ Sim
☐ Não
☐ Parcialmente

10. A(s) área(s) envolvidas com tratamento de dados participou(aram) de algum treinamento relacionado com o tema de proteção de dados pessoais?
☐ Sim
☐ Não
☐ Parcialmente

B- CONFORMIDADE LEGAL E RESPEITO AOS PRINCÍPIOS:

11. O órgão, dentro dos limites de suas competências legais, implementou ações para não tratar e coletar de forma inadequada ou excessiva os dados pessoais dos cidadãos e tratar a mínima quantidade de dados necessários para atingir a finalidade legal desejada?
☐ Sim
☐ Não
☐ Parcialmente

12. O órgão realizou um mapeamento entre os dados processados e a competência legal/finalidade para a qual eles são necessários?
☐ Sim
☐ Não
☐ Parcialmente

13. O órgão estabeleceu procedimento ou metodologia para verificar se os princípios da LGPD estão sendo respeitados durante o desenvolvimento de serviços que tratarão dados pessoais desde a fase de concepção do produto ou do serviço até a sua execução (Privacy by Design)?
☐ Sim
☐ Não
☐ Parcialmente

14. Os princípios da LGPD são aplicados a todo tratamento de dados pessoais realizados pelo órgão, tanto para clientes dos serviços públicos fornecidos quanto servidores, funcionários e/ou colaboradores da instituição?
☐ Sim
☐ Não
☐ Parcialmente

15. O órgão conscientizou a(s) área(s) envolvida(s) com tratamento de dados pessoais que a administração pública pode efetuar o tratamento de dados pessoais no exercício de suas competências legais ou execução de políticas públicas para entrega de serviços públicos e que nesses casos não precisará colher o consentimento do titular dos dados?
☐ Sim
☐ Não
☐ Parcialmente

16. O órgão ao efetuar o tratamento de dados pessoais no exercício de suas competências legais ou execução de políticas públicas dá publicidade sobre a finalidade e a forma como o dado será tratado?
☐ Sim
☐ Não
☐ Parcialmente

17. O órgão adota sistemas e procedimentos para cumprir o direito de retificação de informações do titular do dado?
☐ Sim
☐ Não
☐ Parcialmente

C- TRANSPARÊNCIA E DIREITOS DO TITULAR

18. A identidade e as informações de contato do encarregado foram divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador?
☐ Sim
☐ Não
☐ Parcialmente

19. O órgão comunica internamente os objetivos do Programa Institucional de Privacidade de Dados?
☐ Sim
☐ Não
☐ Parcialmente

20. O órgão elaborou uma Política de privacidade para cada serviço de forma a informar os direitos dos titulares de dados e revisou as Políticas de Privacidade já existentes?
☐ Sim
☐ Não
☐ Parcialmente

21. As Políticas de Privacidade dos serviços são elaboradas em linguagem simples e acessível?
☐ Sim
☐ Não
☐ Parcialmente

D – RASTREABILIDADE

22. O órgão já realizou um inventário dos serviços que tratam dados pessoais?
☐ Sim
☐ Não
☐ Parcialmente

23. O órgão já realizou uma classificação dos dados tratados entre dados pessoais e dados pessoais sensíveis?
☐ Sim
☐ Não
☐ Parcialmente

24. O órgão mantém rastreabilidade dos dados do titular seja em formato eletrônico ou físico (papel)?
☐ Sim
☐ Não
☐ Parcialmente

E - ADEQUAÇÃO DE CONTRATOS E DE RELAÇÕES COM PARCEIROS

25. O órgão já realizou uma adequação dos instrumentos convocatórios que estão sendo elaborados?
☐ Sim
☐ Não
☐ Parcialmente

26. O órgão já realizou uma revisão dos contratos em vigência para adequá-los à Lei Geral de Proteção de Dados?
☐ Sim
☐ Não
☐ Parcialmente

F – SEGURANÇA DA INFORMAÇÃO

27. O órgão efetivamente implementou os controles de segurança para os riscos identificados no Relatório de Impacto à Proteção dos Dados Pessoais?
☐ Sim
☐ Não
☐ Parcialmente

28. O órgão instituiu uma equipe que realiza o monitoramento das vulnerabilidades técnicas dos serviços que tratam dados pessoais?
☐ Sim
☐ Não
☐ Parcialmente

29. O órgão gera evidências para comprovar que tomou medidas de segurança para proteger os dados pessoais contra ameaças externas e internas?
☐ Sim
☐ Não
☐ Parcialmente

30. Medidas de segurança são planejadas desde a fase de concepção do produto ou do serviço até a sua execução (Security by Design)?
☐ Sim
☐ Não
☐ Parcialmente

G- VIOLAÇÃO DE DADOS

31. O órgão estabeleceu um processo de comunicação das possíveis violações de dados pessoais?
☐ Sim
☐ Não
☐ Parcialmente

32. O órgão realiza uma gestão de incidentes para tratar possíveis violações dos dados de forma efetiva?
☐ Sim
☐ Não
☐ Parcialmente

33. O órgão fornece um canal para recebimento de denúncias e de alertas de ocorrências de irregularidades, como denúncias de possíveis vazamento de dados e falhas de segurança?
☐ Sim
☐ Não
☐ Parcialmente

REFERÊNCIAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 14 maio 2021.

GOVERNO FEDERAL. **Guias operacionais para adequação à LGPD.** 11 abr. 2019. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de--dados/guias-operacionais-para-adequacao-a-lgpd>. Acesso em: 17 abr. 2021.

GOVERNO FEDERAL. **Guia de boas práticas:** Lei Geral de Proteção de Dados (LGPD). 10 abr. 2020. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-boas-praticas--lei-geral-de-protecao-de-dados-lgpd>. Acesso em: 27 abr. 2021.

PARANÁ. Decreto nº 6.474, de 14 de dezembro de 2020. Regulamenta a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), no âmbito da Administração Pública Estadual direta, autárquica e fundacional do Poder Executivo do Estado do Paraná. Disponível em: <https://www.legislacao.pr.gov.br/legislacao/pesquisarAto.do?action=exibir&codAto=244066&indice=1&totalRegistros=7&dt=18.4.2021.10.54.41.988>. Acesso em: 14 maio 2021.

CGE

CONTROLADORIA GERAL
DO ESTADO DO PARANÁ