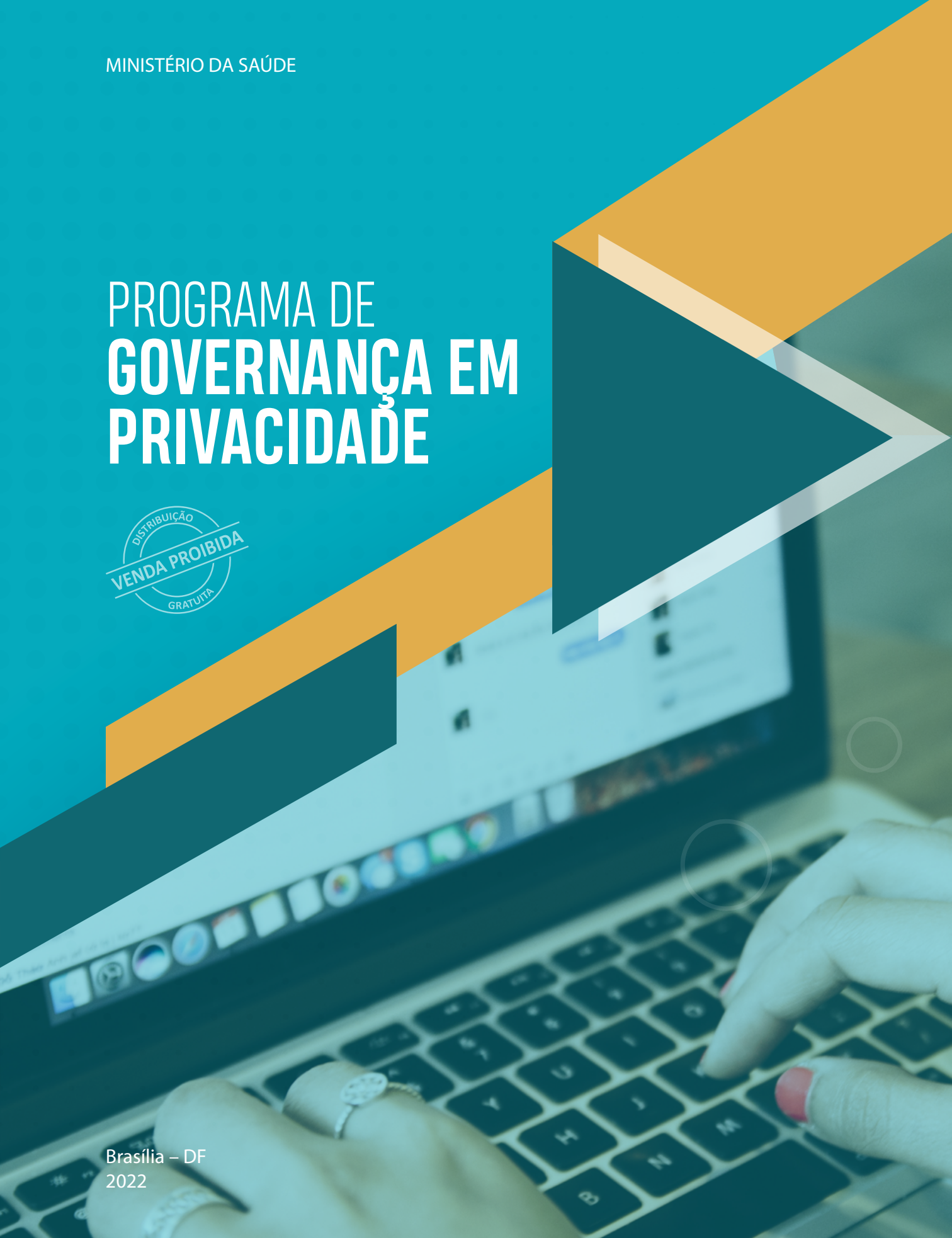
MINISTÉRIO DA SAÚDE

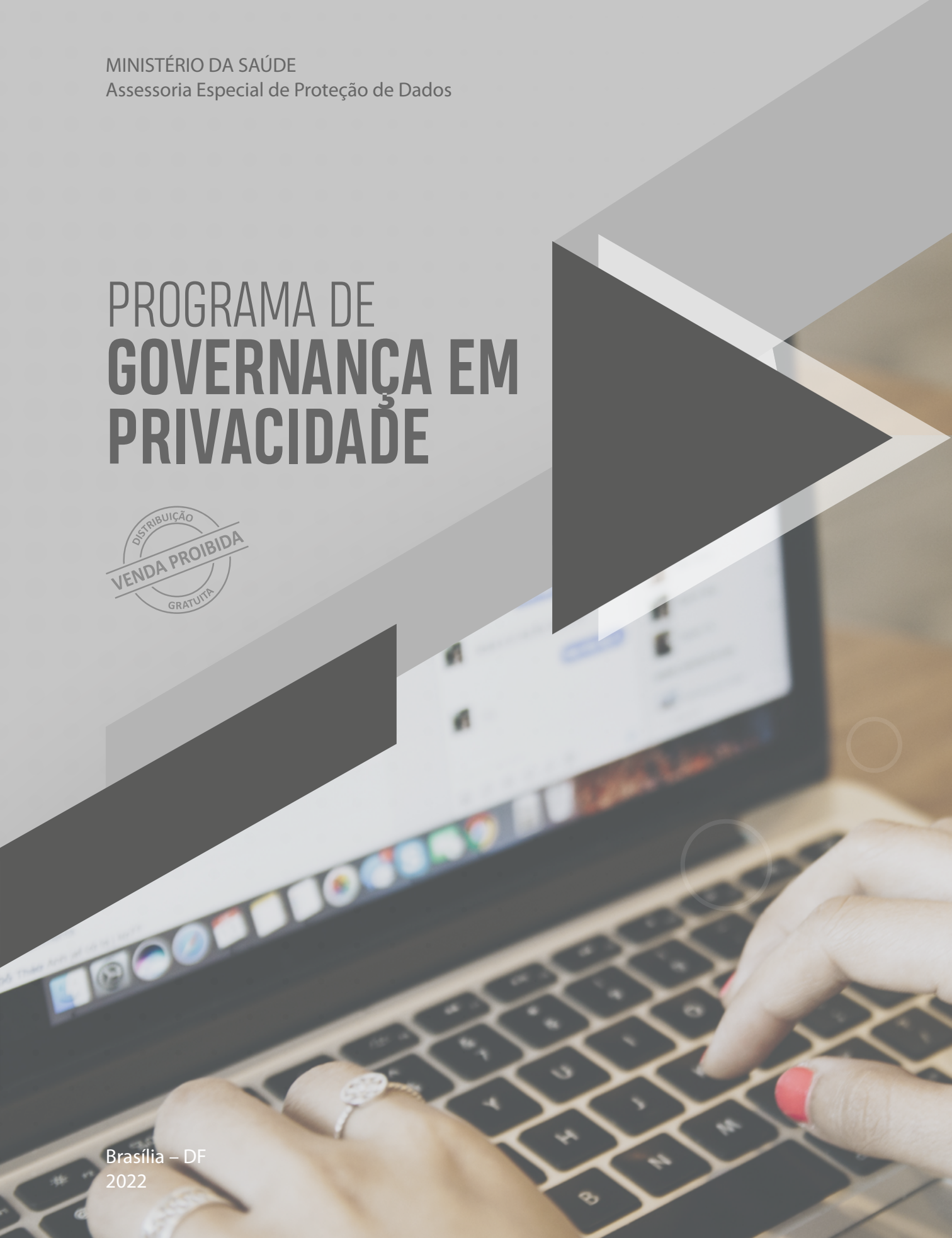
PROGRAMA DE **GOVERNANÇA EM PRIVACIDADE**



Brasília – DF
2022

MINISTÉRIO DA SAÚDE
Assessoria Especial de Proteção de Dados

PROGRAMA DE **GOVERNANÇA EM PRIVACIDADE**



Brasília – DF
2022

Tiragem: 1ª edição – 2022 – versão eletrônica

Elaboração, distribuição e informações:
MINISTÉRIO DA SAÚDE
Assessoria Especial de Proteção de Dados
Esplanada dos Ministérios, bloco G,
5º andar, sala 521-b
CEP: 70058-900 – Brasília/DF
Tel.: (61) 3315-2862

Departamento de Informática do Sistema Único de Saúde
Esplanada dos Ministérios, Bloco G, Ed. Anexo A,
1º andar, Sala 107
CEP: 70058-900 - Brasília/DF
Tel: (61) 3315-2166

Elaboração de texto:
Daniela Barros do Nascimento
Germano José Avendaño Celin
Graziella Cervo Santana
Juliana de Oliveira Moreira
Letícia de Oliveira Fraga de Aguiar
Marcelo Dias de Sá
Márcio Neves Arbach
Nilton Moreira dos Santos
Victor Alex Begnini
Waldyr Lima Júnior

Editora responsável:
MINISTÉRIO DA SAÚDE
Secretaria-Executiva
Subsecretaria de Assuntos Administrativos
Coordenação-Geral de Documentação e Informação
Coordenação de Gestão Editorial
Esplanada dos Ministérios, bloco G, Edifício Anexo, 3ª andar, sala 374-A
CEP: 70058-900-040 – Brasília/DF
Tels.: (61) 3315-7790 / 3315-7791
E-mail: editora.ms@saude.gov.br

Equipe editorial:
Normalização: Valéria Gameleira da Mota
Revisão textual: Khamila Silva e Tatiane Souza
Design editorial: Marcos Melquíades

Ficha Catalográfica

Brasil. Ministério da Saúde. Assessoria Especial de Proteção de Dados.
Programa de Governança em Privacidade [recurso eletrônico] / Ministério da Saúde, Assessoria Especial de Proteção de Dados. – Brasília : Ministério da Saúde, 2022.
24 p. : il.

Modo de acesso: World Wide Web: http://bvsms.saude.gov.br/bvs/publicacoes/programa_governanca_privacidade.pdf
ISBN 978-65-5993-389-1

1. Governança. 2. Privacidade. 3. Leis sobre a Privacidade. I. Título.

CDU 342.721

Catalogação na fonte – Coordenação-Geral de Documentação e Informação – Editora MS – OS 2022/0542

Título para indexação:
Privacy Governance Program (PGP)

SUMÁRIO

1 PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

1.1 O que é

A Lei n.º 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), vigente desde setembro de 2020, dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural.

A lei estabelece, em seu art. 50, que os controladores, no âmbito de suas competências, pelo tratamento de dados pessoais, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização e funcionamento, assim como demais procedimentos relacionados ao tratamento de dados pessoais.

Diante disso, o Ministério da Saúde (MS), em consonância com seu papel de controlador, por intermédio da Assessoria Especial de Proteção de Dados (AEPD), elaborou este Programa de Governança em Privacidade (PGP/MS). O Programa é um primeiro esforço em busca da adequação do MS aos principais ditames da LGPD.

O acompanhamento das ações do PGP/MS será realizado no âmbito de quatro estruturas de governança do MS: inicialmente pela AEPD, que fará o monitoramento contínuo das ações previstas no Programa, pelo Comitê Executivo de TIC (Cetic/MS) e pelo Comitê de Governança Digital (CGD/MS) e, no que couber, pelo Comitê Interno de Governança (CIG/MS).

O Programa foi elaborado em consonância com o *Guia de Elaboração de Programa de Governança em Privacidade* da Secretaria de Governo Digital do Ministério da Economia (SGD/ME) e está organizado em três tópicos principais, que correspondem às etapas "Iniciação e Planejamento"; "Construção e Execução" e "Monitoramento". As etapas, por sua vez, estão estruturadas em subtópicos que correspondem aos marcos do PGP/MS.

Por se tratar de primeira versão, será atualizado periodicamente, de acordo com as necessidades do órgão ou para manter alinhamento com as diretrizes da Autoridade Nacional de Proteção de Dados (ANPD).

1.2 Objetivo

O PGP/MS tem como objetivo orientar a implementação da proteção de dados pessoais e privacidade no MS, em conformidade com os requisitos da LGPD, levando em consideração os aspectos elencados no art. 50, inciso I, da Lei n.° 13.709/2018.

2 ETAPAS DO PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

2.1 Iniciação e Planejamento

Conforme dispõe o *Guia de Elaboração de Programa de Governança em Privacidade* da SGD/ME, esta etapa busca compreender quais as primeiras informações e os dados importantes que devem ser conhecidos para início dos trabalhos de adequação à LGPD.

2.1.1 O Encarregado

Responsável por atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD, o encarregado pelo tratamento de dados pessoais tem as seguintes atribuições:

> I – aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
> II – receber comunicações da autoridade nacional e adotar providências;
> III – orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
> IV – executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares (BRASIL, 2018, art. 41).

Em cumprimento ao art. 41 da LGPD, o MS designou seu encarregado de dados por meio da Portaria GM/MS n.º 3.362, de 25 de agosto de 2022.

Os dados do encarregado são públicos e estão acessíveis no sítio eletrônico pelo link: https://www.in.gov.br/web/dou/-/portaria-gm/ms-n-3.362-de-25-de-agosto-de-2022-425314042.

2.1.2 Alinhamento de Expectativas com a Alta Administração

A Assessoria Especial de Proteção de Dados, em agosto de 2022, deu início a um movimento de disseminação da cultura de proteção de dados e alinhamento dos fluxos de compartilhamento das bases de dados deste Ministério, realizando reuniões com servidores e colaboradores das secretarias finalísticas do MS.

Em reunião do CIG, ocorrida em setembro, que contou com a presença do ministro de Estado da Saúde, Marcelo Queiroga, a AEPD apresentou as ações previstas para adequação do Ministério aos ditames da LGPD, bem como a estrutura deste PGP/MS e o status de realização de cada uma das etapas e marcos do programa, conforme o modelo recomendado pela SGD/ME.

Considerando que o CIG é a instância máxima de governança do MS, conforme disposto no Decreto n.º 9.203, de 22 de novembro de 2017, resta cumprida a etapa de alinhamento de expectativas com a Alta Administração.

Levando em conta que o PGP/MS é um documento em constante revisão e atualização, novos alinhamentos com a Alta Administração serão necessários.

2.1.3 Maturidade da Organização

O grau de maturidade da organização, em relação à adequação aos dispositivos e às exigências da LGPD, pode ser mensurado a partir da resposta do Questionário de Privacidade, oferecido pela SGD/ME. O preenchimento do documento é realizado digitalmente. O questionário considera uma série de questões de autoavaliação organizacional. Ao finalizar o preenchimento, é gerado um índice de maturidade, denominado Indicador de Adequação à LGPD, conforme demonstrado a seguir:

Quadro 1 – Indicador de Adequação à LGPD

Índice	Nível de Adequação
0,00 a 0,29	Inicial
0,30 a 0,49	Básico
0,50 a 0,69	Intermediário
0,70 a 0,89	Em Aprimoramento
0,90 a 1,00	Aprimorado

Fonte: Brasil (2018).

A utilização de indicadores e metas é fundamental para: determinar o progresso no cumprimento dos requisitos de conformidade como a proteção e o controle de dados pessoais; comparar o desempenho em toda a organização; identificar vulnerabilidades e lacunas na política e em sua implementação; aferir grau de segurança e identificar modelos de sucesso.

Para estabelecer uma linha de base inicial, em 2020, foi aplicado no MS o referido questionário. Na ocasião, o resultado foi o seguinte:

Quadro 2 – Diagnóstico Inicial

Dimensão	Índice
Governança	0,2
Conformidade legal e respeito aos princípios	0,29
Transparência e direitos do titular	0,14
Rastreabilidade	0,46
Adequação de contratos e de relações com parceiros	1
Segurança da informação	0,4
Violações de dados	0,1
Índice de Adequação à LGPD (inicial)	0,44 (Básico)

Fonte: SGD/ME.

Numa breve análise, verifica-se que as dimensões de "Governança", "Conformidade legal e respeito aos princípios", "Transparência e direitos do titular", "Adequação de contratos e de relações com parceiros" e "Violação de dados", encontram-se no nível inicial, o que puxa o indicador final também para esse mesmo patamar, ou seja, uma ligeira redução no Índice de Adequação à LGPD, uma vez que este Ministério estava iniciando seu processo de inserção e adoção à LGPD.

Após a criação da AEPD em 2022, repetiu-se o processo de avaliação de maturidade em privacidade de dados e obteve-se o resultado apresentado a seguir:

Quadro 3 – Diagnóstico após avaliação do Núcleo LGPD

Dimensão	Índice
Governança	0,57
Conformidade legal e respeito aos princípios	0,28
Transparência e direitos do titular	0,53
Rastreabilidade	0,5
Adequação de contratos e de relações com parceiros	0,2
Segurança da informação	0,38
Violações de dados	0,48
Índice de Adequação à LGPD	0,42 (Básico)

Fonte: SGD/ME.

Observa-se que, apesar da leve oscilação do índice, em diversas dimensões o MS apresentou aprimoramento, em especial em "Governança"; "Transparência e direitos do titular" e "Violações de dados". A diferença de 0,02 pontos em relação ao primeiro questionário, preenchido em 2020, pode ser explicada pelos contextos institucionais. Se, em 2020, o contexto era de menor maturidade e pouco conhecimento sobre o tema e ter sido preenchido de forma unilateral, o segundo questionário, de 2022, foi respondido com apoio do Departamento de Informática do Sistema Único de Saúde (DataSUS), no âmbito do Núcleo LGPD/DataSUS, e do encarregado pelo tratamento de dados do Ministério da Saúde, em contexto de maior maturidade e conhecimento em relação aos processos de trabalho e sobre a lei, tornando a resposta atual mais precisa e fidedigna à realidade do MS.

Em tratativas com a SGD/ME, acerca dos possíveis impactos decorrentes da diminuição do Índice de Adequação à LGPD, foi esclarecido pela Gerência de Relacionamento, que o Diagnóstico de Privacidade tem como objetivo direcionar as ações do próprio órgão, por exemplo, priorização de assuntos ou outras necessidades, ou seja, não restando quaisquer desdobramentos acerca da diminuição do referido índice.

Dessa forma, é importante a realização de um novo diagnóstico organizacional em 2023, uma vez que o objetivo ao final deste 1º ciclo é que o MS possa atingir o nível intermediário de adequação à LGPD. Esses resultados serão norteadores para adoção de providências visando à adequação do órgão aos ditames da LGPD, com a expectativa de alcançar, até 31 de dezembro de 2023, a Meta de 0,69 relativa ao Índice de Adequação à LGPD (intermediário).

2.1.4 Medidas de Segurança

As medidas de segurança adotadas pelo DataSUS estão definidas pela Política de Segurança da Informação e Comunicação (Posic) do MS, a qual contém os Procedimentos Operacionais de Segurança em Tecnologia da Informação.

A segurança da informação é constantemente revista e aprimorada com a adoção de novas medidas. Uma das abordagens adotadas pelo DataSUS atualmente é garantir que os dados estejam protegidos durante todo o seu tratamento (desde a coleta até o descarte). Nesse processo, são utilizados diversos sistemas, tecnologias e ferramentas para permitir a criptografia e o controle de acesso de forma integrada.

Os controles de segurança consistem em um conjunto amplo de medidas, visando minimizar os riscos presentes nos ativos de informação. Eles são baseados na norma de segurança aceita internacionalmente (ISO 27001/27002 e a extensão 27701) e nas especificações de segurança impostas pelos Instrumentos Normativos de Processo e aprovados pela Diretoria-Executiva.

2.1.5 Estrutura Organizacional para Governança e Gestão da Proteção de Dados Pessoais

A inviolabilidade à intimidade e à vida privada são direitos assegurados constitucionalmente no Brasil (Constituição da República Federativa do Brasil, art. 5º, inciso X). A proteção de dados pessoais no Brasil, inclusive em meios digitais, é regida pela Lei n.º 13.709, de 2018, LGPD, que regula atividades de tratamento de dados pessoais.

Frente à importância e aos níveis de complexidade das temáticas que envolvem a Gestão e a Governança de Dados, o MS redefiniu sua estrutura organizacional com vistas à constituição de política e diretrizes de Governança de Dados, tendo como propósitos: descrever procedimentos, regramentos, protocolos técnicos para subsidiar a tomada de decisão dos comitês de governança do órgão, bem como garantir agilidade, segurança e qualidade nas produções a serem geradas no monitoramento e na avaliação no âmbito do Sistema Único de Saúde (SUS).

Nesse sentido, a partir da publicação do Decreto n.º 11.098, de 20 de junho de 2022, que aprovou a nova estrutura regimental do MS, foi criada a Assessoria Especial de Proteção de Dados.

A instituição da AEPD permitiu ao MS contar com uma estrutura especializada na implementação, na supervisão, na avaliação e no monitoramento de adequação à LGPD no âmbito da saúde pública. A criação da Assessoria, inédita entre os órgãos ministeriais, evidencia os esforços deste Ministério em relação à proteção de dados pessoais e traz à sua estrutura de gestão e de governança de dados maior robustez.

A forma como os dados pessoais são tratados no SUS exige procedimentos, estruturas e recursos condizentes com o setor de saúde, em razão de sua complexidade. A criação de uma assessoria especializada, ligada ao Gabinete do Ministro, evidencia a preocupação do MS com a privacidade e proteção de dados da saúde, alinhando-se, inclusive, com as boas práticas de Governança de Dados de países que compõem a Organização para Cooperação e Desenvolvimento Econômico (OCDE).

São atribuições da AEPD:

> I – supervisionar as atividades relacionadas à proteção de dados pessoais no âmbito do Ministério;
> II – assessorar diretamente o Ministro de Estado e a alta administração em assuntos relacionados à proteção de dados pessoais;
> III – elaborar diretrizes, coordenar, supervisionar, avaliar e monitorar a implementação da Lei n.º 13.709, de 14 de agosto de 2018, no âmbito do Ministério;
> IV – propor e avaliar ações que visem à adequação das atividades de tratamento de dados pessoais aos regulamentos e às normas vigentes;
> V – propor, coordenar e supervisionar iniciativas que qualifiquem atividades e processos relacionados ao tratamento de dados pessoais;
> VI – analisar e avaliar comunicações, reclamações e solicitações dos titulares de dados pessoais, com a prestação de esclarecimentos ou com a adoção de providências necessárias;
> VII – receber comunicações e promover a interlocução do Ministério com a Autoridade Nacional de Proteção de Dados; e
> VIII – propor, coordenar e avaliar ações de gestão de riscos estratégicos relacionados à proteção de dados pessoais, com a emissão de opiniões e pareceres quando necessário. (BRASIL, 2022).

A atuação da Assessoria busca a conformidade do órgão com os requisitos mínimos de proteção de dados pessoais definidos pela LGPD. Na tarefa, orienta as Secretarias do MS acerca da temática e conta com o suporte do DataSUS e do Departamento de Monitoramento e Avaliação do Sistema Único de Saúde (Demas), órgãos integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (Sisp) no MS.

A estruturação da AEPD, assim como suas competências, foi matéria de avaliação pela SGD/ME, por meio da Nota Técnica SEI n.º 31902/2022/ME, a qual avaliou a necessidade do DataSUS e do Demas prestarem suporte às atividades finalísticas da AEPD, em especial, no que diz respeito aos processos e às atividades que envolvam recursos de tecnologia da informação. O intuito é auxiliar a AEPD no exercício de suas atribuições, para que assim possa ser mantida a boa governança de Tecnologia da Informação e Comunicação (TIC) no âmbito do MS e, consequentemente, no Sisp, de forma a: padronizar os processos, os sistemas de suporte e infraestrutura; e evitar a sobreposição de atribuições e descoordenação de atividades.

Cabe destacar que o DataSUS e o Demas compõem, com o Comitê Executivo de Tecnologia da Informação e Comunicação (Cetic/MS), o Comitê de Governança Digital (CGD/MS) e o Comitê Gestor de Saúde Digital (CGSD), a estrutura organizacional para a governança e gestão da proteção de dados pessoais no âmbito deste Ministério.

O Cetic/MS, de natureza consultiva e deliberativa e de caráter permanente, atua como colegiado técnico que presta apoio às decisões do CGD/MS. Este, de natureza deliberativa e caráter permanente, abarca responsabilidades estratégicas e executivas, tais como: avaliação de propostas de políticas, diretrizes, objetivos e estratégias de TIC. O CGSD/MS é instância colegiada tripartite e ocupa-se da governança da Política Nacional de Informação e Informática em Saúde (PNIIS) e da Estratégia de Saúde Digital para o Brasil 2020-2028 (ESD28). Os três colegiados, de acordo com suas competências, atuam como instâncias internas de apoio à governança nos temas de privacidade, de proteção de dados pessoais e no cumprimento das disposições da LGPD.

2.1.6 Inventário de Dados Pessoais

O Inventário de Dados Pessoais (IDP) tem como objetivo principal documentar o tratamento de dados pessoais realizados pela instituição, em alinhamento ao previsto no art. 37 da LGPD. Consiste em fazer um balanço do que o MS faz com os dados pessoais disponíveis em seus sistemas, identificando os agentes de tratamento, quais dados pessoais são tratados, onde estão armazenados e que operações são realizadas com eles.

De uma forma geral, esse registro mantido pelo IDP descreve informações em relação ao tratamento de dados pessoais realizado pelo MS:

- Atores envolvidos (agentes de tratamento e o encarregado).
- Finalidade (o que a instituição faz com o dado pessoal).
- Hipótese (arts. 7º e 11 da LGPD).
- Previsão legal.
- Dados pessoais tratados pela instituição.
- Categoria dos titulares dos dados pessoais.
- Tempo de retenção dos dados pessoais.
- Instituições com as quais os dados pessoais são compartilhados.
- Transferência internacional de dados (art. 33 LGPD).
- Medidas de segurança atualmente adotadas.

O IDP é um importante documento de governança de dados pessoais e de subsídio para avaliação de impacto à proteção de dados pessoais, com vistas a verificar a conformidade do MS no que se refere ao preconizado pela LGPD.

O modelo de Inventário de Dados Pessoais adotado pelo MS é o proposto pela SGD/ME. O MS elaborou, com o apoio técnico da SGD/ME, dois IDPs até o momento. Com base no mapeamento de sistemas mais atualizado, o MS possui mais de 300 sistemas catalogados, contando, nesse rol, sistemas legados e sistemas que não tratam dados pessoais sensíveis. Também há que considerar a existência de sistemas cuja gestão cabe a outra unidade da Federação, ficando sob a responsabilidade do MS o armazenamento dos dados.

2.2 Construção e Execução

2.2.1 Políticas e práticas para proteção da privacidade do cidadão

A Política de Privacidade é um documento interno dirigido a funcionários e eventuais terceiros que forneçam produtos e serviços para a instituição (contratados). Esse documento deve informar como os dados pessoais serão tratados, armazenados e transmitidos para atender às necessidades organizacionais e às legislações aplicáveis, definindo todos os aspectos relativos à proteção de dados, incluindo a elaboração de Avisos de Privacidade para serviços digitais do MS, conforme o caso.

A Política de Privacidade deve ser considerada por toda a instituição – do mais alto nível de governança institucional até as equipes operacionais. Deve ser compreensível, acessível a todos os funcionários, abrangente, conciso, orientado para a prática, mensurável e testável.

Seus principais componentes são:

- Objetivo: por que a política existe e as metas a serem alcançadas.
- Escopo: que recursos (pessoas, processos e tecnologias) a política protege.
- Responsabilidades: quais os responsáveis por cada atividade relacionada à proteção de dados, incluindo líderes, gerentes, demais funcionários e terceiros.
- Conformidade: estrutura para garantir a adequação às normas aplicáveis, incluindo políticas e procedimentos complementares (ex.: política de controle de acesso) e regime de sanções disciplinares por desrespeito à política de privacidade.

No caso do MS, tanto a equipe de servidores públicos, comissionados e terceirizados como toda e qualquer organização que venha a prestar serviços ou fornecer produtos, mediante licitação ou contratação direta, estarão sujeitas à Política de Privacidade ministerial e às devidas práticas de proteção ao cidadão.

2.2.2 Cultura de segurança e proteção de dados

Para que um Programa de Governança em Privacidade seja corretamente implementado, é essencial que toda a instituição esteja bem alinhada. A melhor forma de fazer isso é a partir de programas de treinamento e conscientização do corpo funcional.

Campanhas de treinamento e comunicação devem informar leis e políticas aplicáveis e as consequências por violá-las, identificar possíveis violações, explicar como abordar reclamações e incluir procedimentos de denúncia.

Com relação ao MS, enquanto conhecimentos gerais sobre a Política de Privacidade devem ser comunicados a todas as equipes, algumas funções podem necessitar de capacitações específicas e mais especializadas, a saber:

- A Gestão de Pessoas deve ser informada sobre procedimentos administrativos para tratar dados pessoais do corpo funcional durante todo o ciclo de vida dos dados.
- A Tecnologia da Informação deve ser capacitada para a implementação de medidas técnicas de segurança que protejam os dados pessoais tratados no âmbito da instituição.
- A Ouvidoria deve ser preparada para receber solicitações e reclamações de titulares de dados, com respeito a seus direitos e eventuais vazamentos de dados.
- A Comunicação Social deve compreender bem o Programa de Governança em Privacidade para que possa traduzi-lo em campanhas de conscientização para o resto do corpo funcional.

Métodos de treinamento e conscientização podem variar e incluem cursos de capacitação presenciais, e-learning, reuniões de equipe, boletins informativos, e-mails, pôsteres, folhetos, slogan e informações no portal eletrônico. Complementarmente, podem ser realizados treinamentos conduzidos por representantes internos ou externos à instituição.

As campanhas de conscientização poderão ser continuamente desenvolvidas pela área de Comunicação Social do MS, com apoio da Assessoria Especial de Proteção de Dados e do DataSUS, para desenvolver a cultura da privacidade dentro da instituição. Dessa maneira, prevê a adoção de tais práticas como ação contínua.

2.2.3 Privacidade desde a Concepção – *privacy by design*

Conforme o *Guia de Boas Práticas (LGPD)* da SGD/ME, o conceito de Privacidade desde a Concepção (PdC) significa que a privacidade e a proteção de dados devem ser consideradas desde a concepção e perdurar por todo o ciclo de vida do projeto, sistema, serviço, produto ou processo.

Esse paradigma ressalta ao menos três valores: (i) a proatividade, ao se incluir a privacidade como parte dos requisitos de engenharia do sistema; (ii) a incorporação de controles de privacidade, que serão auditados e avaliados continuamente, e (iii) o respeito aos titulares de dados, a partir do uso de controles transparentes, permitindo que indivíduos exerçam seus direitos. Alguns exemplos de medidas técnicas e organizacionais *privacy by design* incluem:

- Uso de criptografia para proteção de bases de dados e meios de comunicação.
- Anonimização e pseudoanonimização de bases de dados.
- Controle de acesso baseado em funções.
- Mecanismo de respostas a requisições e reclamações dos titulares de dados.
- Plano de respostas a incidentes e remediação de segurança e privacidade.
- Segurança física.
- Políticas de privacidade para aquisição de produtos/serviços.
- Políticas de gerenciamento da segurança da informação.
- Política de retenção e eliminação de dados pessoais.

2.2.4 Relatório de Impacto à Proteção de Dados Pessoais – Ripd

Conforme art. 5º, inciso XVII, da LGPD, considera-se **Relatório de Impacto à Proteção de Dados Pessoais** documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

O art. 38, parágrafo único, da LGPD declara que a ANPD poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial. Parágrafo único. E observando o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança.

O art. 32 da LGPD preconiza que a ANPD poderá solicitar aos agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

Ao elaborar o Ripd, o Ministério realiza avaliação da conformidade de suas operações de tratamento de dados em relação ao previsto pela LGPD, propiciando que sejam tomadas as medidas necessárias para a proteção dos dados pessoais e para assegurar os direitos dos titulares desses dados.

Além disso, evidencia que o MS está aderente ao princípio da responsabilização e à prestação de contas (LGPD art. 6º, X), ao demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais.

A orientação da SGD é para que o Ripd seja publicado em versão resumida, contemplando o fornecimento das informações sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dos tratamentos de dados pessoais.

De acordo com a SGD/ME, o Ripd deve ser elaborado antes do órgão iniciar o tratamento de dados pessoais, preferencialmente, na fase inicial do programa, projeto ou serviço que tem o propósito de usar esses dados.

Conforme o art. 38, parágrafo único (LGPD):

> (...) o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

A SGD/ME disponibiliza uma ferramenta para avaliação dos riscos de segurança e privacidade, e o resultado do relatório será a base para o preenchimento e a construção do Ripd do MS. Essa ferramenta pode ser acessada pelo seguinte link: https://limesurvey.sgd.nuvem.gov.br/index.php/856128.

2.2.5 Medidas e Política de Segurança da Informação e Política de Privacidade

Parte das medidas de segurança adotadas pelo DataSUS são:

- Regras de firewall de redes para filtro de pacotes e bloqueio de portas de acesso.
- Firewall de aplicação web para proteção contra-ataques como falsificação de solicitação entre *sites*, *cross-site-scripting* (XSS), inclusão de arquivos e *SQL Injection*. Sendo uma defesa de protocolo da camada 7 (no modelo *OSI*).

- Software de proteção antivírus e antimalware para servidores.
- Rotinas de proteção de dados.
- Segurança das comunicações, com a utilização de protocolos de comunicação seguros – como TLS/HTTPS – e aplicativos com criptografia fim a fim.
- Processo de Gerenciamento de Vulnerabilidade, no qual as atividades são gerenciadas em três ciclos: detecção, remediação e monitoramento. Cada atividade é composta por uma lista de ações a serem realizadas.
- Processo de Gestão de Continuidade do Negócio que identifica ameaças potenciais para a organização e os possíveis impactos nas operações de negócio, fornecendo uma estrutura capaz de responder efetivamente e salvaguardar os interesses da organização.
- Processo de Gestão de Acessos que busca garantir o uso de serviços a usuários autorizados e, ao mesmo tempo, prevenir que usuários não autorizados tenham acesso a esses serviços. Além disso, as concessões deverão ser aplicadas respeitando o princípio de privilégios mínimos e apenas pela duração de tempo necessário. O processo é implementado para decidir quem deverá ter direitos de acesso sobre os ativos de TI.
- Contrato de acordo de nível de serviço (*Service Level Agreement* – SLA) para os serviços de nuvem, que contemplam a segurança dos dados armazenados e o uso de autenticação com múltiplos fatores, para acesso aos serviços e dados pessoais que estão na nuvem.
- Processo de resposta e remediação a incidentes de segurança.
- Processo de Conscientização e Treinamento de segurança da informação para todos os colaboradores do Ministério.

Quanto aos incidentes de segurança, destacam-se os esforços da AEPD, em conjunto com o DataSUS, para elaboração de um Plano de Resposta a Incidentes de Segurança e Privacidade, contemplando: a padronização de procedimentos para apuração de ocorrências; a definição de critérios de relevância para notificação à Autoridade Nacional de Proteção de Dados; e o estabelecimento de fluxo de comunicação entre o encarregado pelo tratamento de dados e a Coordenação de Segurança da Informação, do DataSUS.

2.2.6 Adequação Cláusulas Contratuais

Os contratos firmados com o poder público deverão atender às exigências de segurança e à proteção de dados pessoais, conforme estabelecido na LGPD. Para tanto,

foram traçadas algumas diretrizes que orientam a adequação contratual aos moldes legais exigidos.

O Parecer n.º 00004/2022/CNMLC/CGU/AGU, elaborado no âmbito da Câmara Nacional de Modelos de Licitações e Contratos Administrativos, da Consultoria-Geral da União aborda a aplicação da Lei Geral de Proteção de Dados em Licitações e Contratos e tem a seguinte conclusão:

- A contratação do serviço de armazenamento de dados em nuvem é lícita, prevista de forma expressa no ordenamento vigente e se encontra incorporada à prática de gestão de TIC do governo federal.
- No que se refere à transferência internacional de dados pessoais, a contratação é possível nas hipóteses do art. 33 da LGPD, atentando-se para o fato de que pontuais incisos ainda aguardam regulamentação por parte da ANPD e de que a transferência para empresas privadas necessita observar o art. 26 da LGPD.
- Enquanto não é editada essa regulamentação, em especial no que se refere às contratações públicas, recomenda-se inserção de cláusula genérica nas minutas contratuais que eventualmente possam exigir transferência internacional nos termos sugeridos na fundamentação anterior.
- Caso a própria Administração necessite efetuar transferência internacional de dados, também deverá observar essas hipóteses restritas do art. 33 da LGPD, bem como o art. 26 dessa lei.
- A contratação de suboperador de dados é, em princípio, lícita, pois não há vedação na legislação vigente.
- Respondem, de forma solidária, todos os agentes de tratamento pelos danos eventualmente causados.
- Recomenda-se que haja inclusão de cláusula para tratar do tema dos impactos da LGPD nas subcontratações.
- Pode ser exigida declaração da contratada de que seu pessoal cumpre adequadamente a LGPD.
- Entende-se possível a exigência de uma declaração que dê conta da adaptação da licitante ou contratada aos termos da LGPD, inclusive no que se refere ao conhecimento necessário dos empregados para o cumprimento dos deveres da lei.
- É possível que a Administração realize diligências para aferir o cumprimento da LGPD pela licitante ou pela contratada.
- É recomendável inclusão de disposições específicas no termo de referência ou no projeto básico para abordar as questões tratadas, podendo-se adotar, como sugestão.

- Com relação às minutas, recomenda-se supressão de números de documentos pessoais, notadamente nos contratos, bem como de exigência de atestados antecedentes criminais, uma vez que a possibilidade dessa exigência é excepcional.
- Admite-se que a Administração continue exigindo comprovação de exames admissionais e demissionais, devendo tal documentação ser guardada apenas enquanto não prescritas as obrigações trabalhistas correlatas e somente para a finalidade de comprovar o cumprimento dessas obrigações.
- Quanto ao dado pessoal do endereço, que somente foi localizado na minuta de contrato de locação, é recomendável que seja suprimido quando o locador for pessoa natural, uma vez que a divulgação desse instrumento poderia expor indevidamente esse dado. Nesse caso, tal dado deverá ser arquivado em local à parte, uma vez que a Administração poderá necessitar dele para eventual contato com o locador, inclusive para eventual citação ou intimação em processos judiciais ou administrativos.
- Quando exigido documento pessoal para fins de identificação de pessoa responsável por realizar vistoria em procedimento licitatório, é recomendável que no termo de vistoria conste consentimento da pessoa para que seu nome e documento fiquem no processo e que possam ser acessados por terceiros, ante a natureza pública do processo.

A Advocacia-Geral da União (AGU) sugere que se insira nas minutas o que segue:

I. inserção na relação de obrigações de eventuais contratadas do dever de manter a Administração contratante informada de toda a cadeia de circulação dos dados pessoais compartilhados;
II. inserção de cláusula no contrato com operador de dados, no sentido da imediata e precisa comunicação ao controlador sobre eventual contratação de suboperadores.

Assim, as adequações dos instrumentos contratuais no âmbito do MS serão realizadas conforme as orientações da Câmara Nacional de Modelos de Licitações e Contratos Administrativos, da Consultoria-Geral da União, nos moldes do Parecer n.º 00004/2022/CNMLC/CGU/AGU, até que novas orientações sejam expedidas pela AGU ou pela Autoridade Nacional de Proteção de Dados.

2.2.7 Termo de Uso

O Termo de Uso informa as regras que o usuário está sujeito ao utilizar o serviço disponibilizado pelo MS, enquanto a Política de Privacidade origina-se da responsabilidade

de que os agentes de tratamento de dados sejam transparentes com o titular de dados pessoais e informem como as atividades de tratamento de tais dados atendem ao princípio da transparência, disposto no art. 6º da LGPD.

Deve ser salientado que as informações necessitam ser fornecidas com exatidão, clareza e relevância, garantindo que os termos sejam constantemente atualizados e mantendo a fidedignidade das informações acerca do tratamento de dados pessoais realizado pela instituição. É importante que o Termo de Uso e a Política de Privacidade sejam disponibilizados em local de destaque de forma a facilitar o acesso do usuário/titular às informações sobre o serviço e tratamento dos dados pessoais.

O Termo de Uso e a Política de Privacidade podem ser consolidados em um documento único ou constar em documentos separados. A depender da conveniência e do contexto do serviço prestado, deve-se avaliar a melhor forma de apresentá-los ao cidadão.

O MS adotará como modelo padrão para seus serviços, o Termo de Uso e Política de Privacidade sugeridos pela SGD/ME. Disponível no seguinte link: *https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd*

2.3 Monitoramento

O monitoramento será implementado após a consolidação do Programa de Governança em Privacidade no âmbito da saúde, visando mensurar o grau de conformidade com a LGPD e garantir o aprimoramento do Programa, com base nos seguintes marcos: Indicadores de Performance e Plano de Resposta a Incidentes de Privacidade e Segurança.

2.3.1 Indicadores de Performance

Os Indicadores de Performance ou *Key Performance Indicator* (KPI) são utilizados para quantificar os resultados alcançados em um determinado período. Os Indicadores de Performance também contribuem para orientar melhorias e a evolução do grau de maturidade do PGP/MS.

No momento, serão adotados os seguintes indicadores recomendados pela SGD/ME:

- Monitoramento e acompanhamento do número de incidentes de violação de dados pessoais e/ou vazamento de dados pessoais.
- Resultados do Diagnóstico de Adequação à LGPD – índice de adequação.
- Índice de serviços com dados pessoais inventariados: número de serviços com dados pessoais inventariados/número de serviços com dados pessoais do órgão*100.

2.3.2 Plano de Resposta a Incidentes de Privacidade e Segurança

Os incidentes de segurança podem acarretar risco ou dano relevante aos titulares, portanto, em conformidade com o disposto no art. 48 da LGPD, o controlador deverá comunicar à ANPD e ao titular dos dados a eventual ocorrência. Diante disso, foram adotadas estratégias para dar cumprimento à previsão legal:

- Construção de um fluxograma específico para o tratamento adequado dos incidentes.
- Definição da forma, conteúdo e canal da comunicação aos titulares, atendendo aos princípios da transparência e da publicidade.

REFERÊNCIAS

BRASIL. **Decreto n.º 11.098, de 20 de junho 28 de 2022**. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Ministério da Saúde e remaneja e transforma cargos em comissão e funções de confiança. Brasília, DF: Imprensa Nacional, 2022. Disponível em: https://www.in.gov.br/web/dou/-/decreto-n-11.098-de-20-de-junho-de-2022-408904817. Acesso em: 3 nov. 2022.

BRASIL. Ministério da Economia. Secretaria de Governo Digital. **Guia de Elaboração de Programa de Governança em Privacidade - Lei Geral de Proteção de Dados (LGPD)**. Brasília, DF: ME, 2020. Disponivel em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_governanca_privacidade.pdf. Acesso em: 1 nov. 2022.

BRASIL. Presidência da República. Secretaria-Geral. **Lei n.° 13.709, de 14 de agosto de 2018**. Brasília, DF: PR, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 nov. 2022.

BIBLIOGRAFIAS

BRASIL. Ministério da Economia. Secretaria de Governo Digital. **Instrução Normativa n.º 1, de 4 de abril de 2019**. Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal. Brasília, DF: ME, 2019. Disponível em: https://www.gov.br/governodigital/pt-br/contratacoes/instrucao-normativa-sgd-me-no-1-de-4-de-abril-de-2019. Acesso em: 1 nov. 2022.

BRASIL. Ministério da Economia. Secretaria de Governo Digital. **Portaria n.º 778, de 4 de abril de 2019**. Dispõe sobre a implantação da Governança de Tecnologia da Informação e Comunicação nos órgãos e entidades pertencentes ao Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal. Brasília, DF: ME, 2019. Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/70268218. Acesso em: 2 nov. 2022.

BRASIL. Ministério da Saúde. **Portaria GM/MS n.º 3.295, de 17 de agosto de 2022**. Institui o Comitê de Governança Digital no âmbito do Ministério da Saúde. Brasília, DF: MS, 2022. Disponível em: https://brasilsus.com.br/wp-content/uploads/2022/08/portaria3295.pdf. Acesso em: 1 nov. 2022.

BRASIL. Ministério da Saúde. **Portaria GM/MS n.º 307, de 22 de fevereiro de 2021**. Aprova o Planejamento Estratégico do Ministério da Saúde para o período de 2020-2023, e dá outras providências. Brasilia, DF: MS, 2021. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/gm/2021/prt0307_23_02_2021.html. Acesso em: 1 nov. 2022.

BRASIL. Ministério da Saúde. **Portaria GM/MS n.º 870, de 3 de maio de 2021**. Institui o Comitê Interno de Governança do Ministério da Saúde – CIG. 2022.-MS. Brasília, DF: MS,2021. Disponível em: https://brasilsus.com.br/wp-content/uploads/2021/05/portaria870.pdf. Acesso em: 9 nov.

BRASIL. Ministério da Saúde. **Portaria MS n.º 1.966, de 17 de julho de 2018**. Institui a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) no MS. Brasília, DF: MS, 2018.

BRASIL. Ministério da Saúde. **Portaria MS n.º 271, de 27 de janeiro de 2017**. Aprova a Política de Segurança da Informação e Comunicações do Ministério da Sáude. Brasília, DF: MS, 2017. Disponíel em: https://bvsms.saude.gov.br/bvs/saudelegis/gm/2017/prt0271_27_01_2017.html. Acesso em: 1 nov. 2022.

BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. **Portaria n.º 107, de 2 de maio de 2018**. Aprova a versão revisada da Estratégia de Governança Digital da Administração Pública Federal para o período 2016 - 2019. Brasília, DF: MP, 2018. Disponível em: https://www.gov.br/economia/pt-br/assuntos/patrimonio-da-uniao/legislacao/arquivos-anteriores/portariasold/portarias-da-spu/arquivos/2018/portaria-no-107.pdf/view. Acesso em: 2 nov. 2022.

BRASIL. Presidência da República. Secretaria-Geral. **Decreto n.º 10.332, de 28 de abril de 2020**. Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências. Brasília, DF: PR, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10332.htm. Acesso em: 1 nov. 2022.

DISQUE SAÚDE 136

Biblioteca Virtual em Saúde do Ministério da Saúde
bvsms.saude.gov.br

SUS

MINISTÉRIO DA SAÚDE

Governo Federal