ANVISA
Agência Nacional de Vigilância Sanitária

MODELO DE GOVERNANÇA DE DADOS DA ANVISA

PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

Dez/2023

DIRETOR-PRESIDENTE
Antônio Barra Torres

DIRETORES
Meiruze Sousa Freitas
Daniel Meirelles Fernandes Pereira
Romison Rodrigues Mota
Marcelo Mario Matos Moreira

CHEFE DE GABINETE
Karin Schuck Hemesath Mendes

GERENTE-GERAL DE CONHECIMENTO, INOVAÇÃO E PESQUISA (GGCIP)
Artur Iuri Alves de Sousa

ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS
Reinaldo Tavares Nelli

EQUIPE TÉCNICA
Reinaldo Tavares Nelli
Loiane Alves Vieira

ELABORAÇÃO
Gerência-Geral do Conhecimento, Inovação e Pesquisa (GGCIP)
Equipe de Proteção de Dados Pessoais

ANVISA
Agência Nacional de Vigilância Sanitária

SUMÁRIO

Programa de Governança em Privacidade

O que é? 4

Objetivo 5

Estrutura 6

Etapas 6

Iniciação e Planejamento 6

Nomeação do Encarregado 7

Alinhamento de Expectativas com a Alta Administração 7

Análise da Maturidade – Diagnóstico do Atual Estágio de Adequação à LGPD 8

Análise e adoção de medidas de segurança, inclusive diretrizes e cultura interna 9

Instituição de estrutura organizacional para governança e gestão da proteção de dados pessoais 10

Inventário de Dados Pessoais 10

Levantamento de contratos relacionados a dados pessoais 11

Construção e Execução 12

Políticas e práticas para proteção da privacidade do cidadão 12

Cultura de segurança e proteção de dados e Privacidade desde a Concepção (*Privacy by Design*) 13

Relatório de Impacto à Proteção de Dados Pessoais (RIPD) 14

Política de Privacidade e Política de Segurança da Informação 15

Adequação de cláusulas contratuais 15

Termo de Uso 16

Monitoramento 16

Indicadores de Performance 17

Gestão de Incidentes 17

Análise e Reporte de Resultados 18

REFERÊNCIAS 19

PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

O que é?

A Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), em vigor desde setembro de 2020, dispõe sobre o tratamento de dados pessoais, inclusive em meio digital, por pessoa física ou jurídica de direito público. ou de direito privado, com o objetivo de proteger os direitos fundamentais à liberdade e à vida privada, bem como o livre desenvolvimento da personalidade da pessoa física. A lei estabelece, em seu art. 50, que os responsáveis pelo tratamento, no âmbito das suas competências, para o tratamento de dados pessoais, podem formular regras de boas práticas e de governança que estabelecem as condições de organização e funcionamento, bem como outros procedimentos relacionados com o tratamento de dados pessoais.

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. [...]
>
> § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:
>
> I - **implementar programa de governança em privacidade que, no mínimo:**
>
> a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
>
> b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
>
> c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
>
> d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
>
> e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
>
> f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
>
> g) conte com planos de resposta a incidentes e remediação; e
>
> h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;
>
> II - **demonstrar a efetividade de seu programa de governança em privacidade** quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei. **(grifos nossos)**

Segundo o *Guia de Elaboração de Programa de Governança em Privacidade*, da Secretaria de Governo Digital (SGD/MGI), é importante que se dê destaque aos seus principais atores:

- No papel central, por sua importância, tem-se o **titular do dado**, qualquer pessoa natural, protegida pelo princípio da autodeterminação informativa;
- A seguir, o **controlador**, pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. O controlador pode exercer diretamente o tratamento dos dados. Mas pode, também, designar um operador;
- O **operador** é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Ambos, controlador e operador, recebem a nomeação de "agentes de tratamento";
- O **encarregado** corresponde a uma pessoa natural inequivocamente investida nessa função. Sua incumbência é de fazer a intermediação entre o titular e os agentes de tratamento, mas também entre estes agentes e a Autoridade Nacional de Proteção de Dados - ANPD;
- A **Autoridade Nacional de Proteção de Dados - ANPD** tem a missão de regular o setor de tratamento de dados pessoais. Está autorizada, portanto, a agir em proteção aos princípios e fundamentos da Lei Geral de Proteção de Dados.

A Figura 1 demonstra a importância central do titular de dados pessoais, frente aos outros atores deste processo:

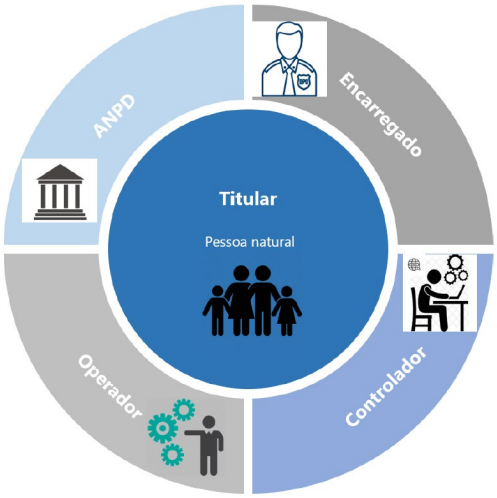

Figura 1: Atores envolvidos com a LGPD
Fonte: Guia para Elaboração do Programa de Governança em Privacidade

Objetivo

Em consonância com a artigo 50 da LGPD, O Programa de Governança em Privacidade da Anvisa (PGP-Anvisa) visa direcionar os aspectos de implementação das regras de proteção de dados e privacidade, além de permitir uma melhoria do nível de maturidade e de conformidade à legislação de proteção de dados pessoais.

Estrutura

Este PGP-Anvisa foi concebido e estruturado com base no ciclo PDCA e composto por 3 etapas (Iniciação e Planejamento; Construção e Execução; Monitoramento), que serão melhor explanadas nos próximos capítulos. Este ciclo fica melhor representando por meio da Figura 2.

Figura 2. Etapas Programa de Gerenciamento de Privacidade – PGP.
Fonte: Guia para Elaboração do Programa de Governança em Privacidade

Etapas

Iniciação e Planejamento

Segundo o *Guia para Elaboração do Programa de Governança em Privacidade*, a etapa de Iniciação e Planejamento deverá cumprir os marcos descritas a seguir:

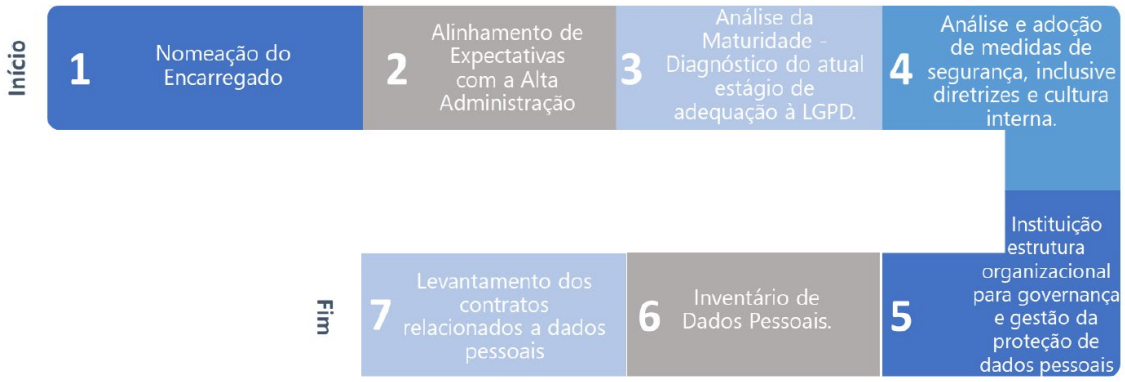

Figura 3. Marcos Iniciação e Planejamento – PGP.
Fonte: Guia para Elaboração do Programa de Governança em Privacidade

Cada um dos marcos apresentados anteriormente será descrito com maior nível de detalhamento nas próximas seções deste documento.

Nomeação do Encarregado

Conforme o artigo 5º, inciso VIII, da Lei Geral de Proteção de Dados (LGPD), o Encarregado é definido como o indivíduo designado pelo controlador e pelo operador para desempenhar o papel de intermediário na comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). O artigo 41 da mesma lei também versa sobre as atividades do Encarregado:

> Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais. [...]
>
> § 2º As atividades do encarregado consistem em:
>
> 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.

A LGPD estabelece que a ANPD poderá estabelecer normas complementares sobre a definição e as atribuições do Encarregado.

O atual Encarregado pelo Tratamento de Dados Pessoais da Anvisa foi nomeado pelo Diretor-Presidente da Agência por meio da Portaria ANVISA nº 207, de 31 de março de 2022, publicado no Boletim de Serviço nº 14/2022.

Os dados do Encarregado estão públicos e acessíveis no sítio eletrônico pelo endereço: https://www.gov.br/anvisa/pt-br/acessoainformacao/tratamento-de-dados-pessoais.

Alinhamento de Expectativas com a Alta Administração

Ainda sobre o artigo 5º da LGPD, nele são delineados os principais atores responsáveis pela conformidade dos órgãos e entidades com as disposições estabelecidas por essa legislação. O quadro abaixo relaciona esses conceitos com o caso concreto da Anvisa:

Atores	Definição (art. 5, LGPD)	Caso concreto
Titular	Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.	Todas as pessoas físicas que possuem dados tratados pela Anvisa.
Controlador	Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.	A Anvisa, como pessoa jurídica de direito público.
Operador	Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.	Servidor, terceirizados, ou colaboradores externos que realizam o tratamento de dados pessoais em nome da Anvisa.
Agentes de tratamento	O controlador e o operador.	Conceitos já mencionados acima.

Encarregado	Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD.	Pessoa indicada formalmente pelo Diretor-Presidente da Anvisa para atuar dentro de rol de atribuições do Encarregado.
Autoridade nacional	Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.	Autoridade Nacional de Proteção de Dados (ANPD).

A presença ativa da alta administração, desempenhando a função de controlador, desempenha um papel crucial na eficácia das iniciativas vinculadas ao cumprimento das responsabilidades estabelecidas pela LGPD. Isso é essencial não apenas para o êxito das atividades conduzidas pelo Encarregado, mas também para seu envolvimento nas decisões estratégicas.

O Decreto nº 10.332, de 28 de abril de 2020, determina a participação do encarregado no Comitê De Governança Digital (CGD) dos órgãos e entidades da administração pública federal direta, autárquica e fundacional.

Desde então, o Encarregado pelo Tratamento de Dados Pessoais da Anvisa integra o Comitê de Governança Digital (CGD), mantendo acesso direto à Alta Administração. Isso permite a coordenação com os demais membros para determinar as fases prioritárias do processo de conformidade com a LGPD.

Análise da Maturidade – Diagnóstico do Atual Estágio de Adequação à LGPD

Nos meses de novembro de 2020 a março de 2021, o Tribunal de Contas da União encaminhou um formulário de autodiagnóstico para 382 órgãos da administração pública federal, inclusive a Anvisa, no sentido de se avaliação o grau de maturidade desses órgãos em relação à implantação da LGPD. O referido diagnóstico, que gerava um score de adequação à LGPD entre 0 e 1, foi encaminhado pela Corte de Contas em outubro de 2022. Na ocasião, a Anvisa apresentou um score de 0,11, classificado como inexpressivo, conforme detalhamento apresentado no quadro abaixo:

Dimensões	Score
Estruturação para condução da iniciativa de adequação	
Preparação	0,25
Contexto organizacional	0,33
Liderança	0,33
Capacitação	0,00
Medidas e controles de proteção de dados pessoais implementados	
Conformidade do tratamento	0,00
Direitos do titular	0,00
Compartilhamento de dados pessoais	0,00
Violação de dados pessoais	0,00
Medidas de proteção	0,10
Score de adequação à LGPD	**0,11**

Ao longo do ano de 2023, a Equipe de Proteção de Dados da GGCIP monitorou mensalmente a evolução deste score, através de um KRT (resultado-chave tático) cuja meta foi estabelecida em

0,35, mediante as ações voltadas à proteção de dados que vêm sendo implementadas na Anvisa. Até o final de novembro/2023, este score já havia atingido a pontuação de **0,40**, superando a meta para a ano corrente.

Outra ação voltada para o diagnóstico de adequação à LGPD foi a preenchimento da Planilha de Autodiagnóstico do Framework de Privacidade e Segurança da Informação, elaborado pela SGD/MGI. Essa ação faz parte do Programa de Privacidade e Segurança da Informação, também da SGD/MGI, que tem como objetivo elevar a maturidade e a resiliência dos órgãos e entidades, em termos de privacidade e segurança da informação, no âmbito do SISP.

A referida planilha apresenta dois índices, *iSeg* e *iPriv*, sendo que o ***iPriv*** (índice de maturidade em privacidade) está diretamente ligado às ações em proteção de dados pessoais. No autodiagnóstico finalizado em outubro de 2023, a aferição das 7 medidas de estruturação básicas e dos 13 controles de privacidade levou ao resultado, para o *iPriv*, de **0,41**, considerado como nível Básico.

Vale ressaltar que, para o próximo Plano de Gestão Anual – PGA 2024, está sendo proposta uma meta de se ampliar o *iPriv* da Anvisa para 0,70, elevando-se a agência para o nível Em Aprimoramento.

Análise e adoção de medidas de segurança, inclusive diretrizes e cultura interna

O artigo 46 da LGPD é enfático em afirmar que "os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais".

A Anvisa publicou em 2018, e vem revisando regularmente, sua *Política de Segurança da Informação e Comunicação (POSIC)*, no intuito de, entre outros aspectos, estabelecer diretrizes para a segurança do todo o ciclo de vida das informações, inclusive dados pessoais, manipuladas pela Agência.

Ainda, quanto ao estabelecimento de diretrizes, essas especificamente voltadas à temática da proteção de dados, a Portaria nº 1.184/2023, que trata da *Política de Proteção de Dados Pessoais* na Anvisa, apresenta um capítulo direcionado às medidas de proteção dos dados pessoais (artigos 25 a 28) e outro tratando de segurança e boas práticas (artigos 32 e 33).

O artigo 33 da Política de Proteção de Dados Pessoais enfatiza ainda, em seu parágrafo 3º, a importância de promover a cultura de proteção de dados:

> § 3º As boas práticas adotadas de proteção de dados pessoais e a governança implantada deverão ser objeto de campanhas informativas na esfera interna da Anvisa e em seu sítio eletrônico, visando a disseminar cultura protetiva, com conscientização e sensibilização dos interessados.

Outra ação voltada à cultura de segurança é a divulgação interna, para todos os servidores e colaboradores, de pílulas semanais de conhecimento sobre o tema privacidade e proteção de dados. Isso é realizado pela Equipe de Proteção de Dados da GGCIP deste novembro de 2023.

Instituição de estrutura organizacional para governança e gestão da proteção de dados pessoais

Em 23 de junho de 2023, foi publicada a Portaria ANVISA nº 673/2022, que alterou a Portaria nº 60, de 24 de janeiro de 2022, que instituiu a *Política de Governança Organizacional* da Anvisa. Em seu artigo 22, foram acrescidas algumas competências ao Comitê de Governança Digital (CGD) da Anvisa, entre elas a preocupação com as iniciativas para as atividades relacionadas a proteção de dados pessoais:

> Art. 1º Alterar os arts. 20, 21 e 22 da Portaria n° 60, de 24 de janeiro de 2022, publicada no DOU de 26 de janeiro de 2022, Seção 1, pág. 92, que passam a vigorar com a seguinte redação:
>
> "[...]
>
> Art. 22. Compete ao CGD: [...]
>
> IX - monitorar a implementação da Lei Geral de Proteção de Dados - LGPD e estabelecer Programa de Governança em Privacidade e Segurança;
>
> [...] "(NR)

Ainda, sobre o CGD, cabe reforçar a participação do Encarregado no comitê como membro titular, mesmo antes da alteração promovida pela Portaria ANVISA nº 673/2022.

Corroborando com essa ação, a Portaria ANVISA nº 1.184/2023 (Política de Proteção de Dados Pessoais da Anvisa), disciplina sobre a competência de vários atores internos sobre esta temática. No ato normativo em questão, ficam evidenciadas as atribuições relacionadas à governança da proteção de dados pessoais, por parte do CGD:

> Portaria ANVISA nº 1.184/2023
>
> Art. 35. Compete ao Comitê de Governança Digital da Anvisa:
>
> I - aprovar as alterações na Política de Proteção de Dados Pessoais da Anvisa; e
>
> II - aprovar o plano de trabalho do Comitê de Governança Digital referente às atividades de proteção de dados pessoais. [...]
>
> Art. 38. Os assuntos referentes à proteção de dados pessoais serão submetidos ao Comitê de Governança Digital da Anvisa, e deverão observar as suas regras e estrutura de governança, ressalvadas as competências específicas do Encarregado.

A Anvisa poderá ainda criar uma unidade organizacional específica para realizar a gestão, em nível operacional, das atividades voltadas à privacidade e proteção dos dados pessoais.

Inventário de Dados Pessoais

Conforme estabelecido pelo artigo 37 da LGPD, o Inventário de Dados Pessoais (IDP) refere-se ao registro das atividades de tratamento de dados pessoais conduzidas pelo órgão. Esse inventário deve detalhar informações como:

- atores envolvidos (agentes de tratamento e o Encarregado);
- finalidade (o que a instituição faz com o dado pessoal);
- ciclo de vida do dado pessoal (coleta, retenção, processamento, compartilhamento e eliminação);

- hipótese de tratamento;
- 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; e
- medidas de segurança atualmente adotadas.

Para auxiliar o alcance deste objetivo, a SGD/MGI criou uma ferramenta, em forma de planilha eletrônica, e um guia para elaboração do inventário. Esse material encontra-se disponível em https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-e-modelos.

Em junho de 2021, foi realizado um levantamento de informações, baseado dos processos da cadeia de valor da Anvisa, no sentido de se caminhar para a obtenção de uma primeira versão do IDP da agência. Atualmente, a Equipe de Proteção de Dados Pessoais da GGCIP está trabalhando na análise das informações coletadas nessa atividade pretérita, transcrevendo-as para o padrão sugerido pelo *template* criado pela SGD, com o objetivo de se publicar essa primeira versão do inventário. Está previsto para o ano de 2024 a atualização de todo o Inventário de Dados Pessoais da Anvisa, com base na nova cadeia de valor, e com uma maior amplitude de informações sobre os dados pessoais tratados pela agência.

Levantamento de contratos relacionados a dados pessoais

A LGPD reforça, em alguns de seus artigos, a importância do compartilhamento de dados pessoais ser precedidos de instrumentos jurídicos que o suporte. Os contratos normalmente são os mecanismos que mais figuram para direcionar a relação entre o órgão e o entre privado.

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...]
>
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; [...]
>
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
>
> [...]
>
> Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.
>
> § 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto: [...]
>
> IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; [...] (grifos nossos)

A Anvisa, por meio da liderança da GECOP/GGGAF, vem estabelecendo uma frente de trabalho com vistas à adequação dos contratos celebrados pela agência à LGPD, conforme pode ser verificado no SEI º 25351.905248/2023-12. Os modelos de contratos utilizados seguem o padrão

disponibilizado pela Advocacia-Geral da União (AGU), de modo a se manterem mais compatíveis com a iniciativa em questão.

Como os contratos novos já estão passando por processo interno de verificação de aderência à LGPD, em uma próxima etapa, a Agência deverá avançar para a análise dos contratos já celebrados anteriormente à reestruturação dos processos, no sentido de se alcançar a completude da adequação desses instrumentos.

Construção e Execução

Para a etapa de Construção e Execução, o *Guia para Elaboração do Programa de Governança em Privacidade* apresenta um modelo baseado nos seguintes marcos:

Figura 4. Etapas Construção e Execução – PGP.
Fonte: Guia para Elaboração do Programa de Governança em Privacidade

Adiante, serão detalhados cada um desses seis marcos mencionados e como eles estão sendo e serão abordados pela Anvisa.

Políticas e práticas para proteção da privacidade do cidadão

No artigo 50 da LGPD, que versa especificamente sobre o estabelecimento de um programa de governança em privacidade, são apresentadas características para esses instrumentos, entre elas, a existência de políticas e a criação de uma relação de confiança com os titulares de dados.

> § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:
>
> I - implementar programa de governança em privacidade que, no mínimo: [...]
>
> d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
>
> e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

Neste sentido, a Anvisa publicou a sua *Política de Proteção de Dados Pessoais* (Portaria ANVISA nº 1.184/2023, já mencionada outras vezes nesse documento) com artigos específicos voltados aos direitos dos titulares de dados (artigo 19), ao atendimento aos titulares de dados (artigos 20, 21 e 22) e a medidas de proteção dos dados pessoais (artigos 25, 26, 27 e 28).

Outras políticas, como a de privacidade e da segurança da informação, bem como os artefatos voltada ao gerenciamento de incidentes com dados pessoais, serão objeto de maior detalhamento no 4º marco (Política de Privacidade e Política de Segurança da Informação) desta etapa de Construção e Execução.

Cultura de segurança e proteção de dados e Privacidade desde a Concepção (*Privacy by Design*)

Para além de estabelecer um programa de proteção de dados pessoais, o verdadeiro desafio reside em fomentar uma cultura voltada à salvaguarda dessas informações. Nesse contexto, busca-se que cada indivíduo compreenda e contribua ativamente para o aperfeiçoamento contínuo e prática da privacidade como um direito fundamental.

Cada colaborador da Anvisa é instado a agir de maneira consciente e construtiva, compreendendo os conceitos de privacidade e proteção de dados pessoais. Isso inclui o entendimento dos tipos de dados pessoais processados pela Agência e a consciência do papel da Anvisa na proteção de cada uma dessas informações.

No sentido de promover esta cultura protetiva, está apresentada no Plano de Desenvolvimento de Pessoas (PDP) 2024 uma competência transversal voltada ao aprendizado e aperfeiçoamento dos servidores acerca da LGPD, capacitando-os para identificar requisitos legais, papéis e responsabilidades relativos aos processos e as medidas de segurança para tratar e proteger dados pessoais.

Outra importante prática sugerida é a capacitação de novos servidores e colaboradores no momento do ingresso na Agência. Essa capacitação poderá ser oferecida por meio de cartilhas dedicadas à prática da segurança da informação, apresentando-se aspectos normativos e operacionais. Uma sugestão de temas a serem abordados seriam normativos internos, proteção de e-mail, cuidados na navegação *web*, proteção contra *phishing*, manuseio de documentos físicos/digitais, cuidados com o login e senha, entre outros.

Sobre o paradigma da Privacidade desde a Concepção (Privacy by Design), faz-se referência ao *Guia de Boas Práticas – LGPD*, da SGD/MGI, onde são apresentados 7 princípios fundamentais descritos pela Dra. Ann Cavoukian, a serem aplicados para que se alcance sucesso na busca por este modelo de privacidade:

- Proativo, e não reativo; preventivo, e não corretivo;
- Privacidade deve ser o padrão dos sistemas de TI ou práticas de negócio;
- Privacidade incorporada ao projeto (design);
- Funcionalidade total;
- Segurança e proteção de ponta a ponta durante o ciclo de vida de tratamento dos dados;
- Visibilidade e Transparência; e
- Respeito pela privacidade do usuário.

Para implementação de um modelo de privacidade desde a concepção, principalmente no que tange a questão dos dados pessoais, a Anvisa, como custodiante dessas informações, deverá buscar meios de revisitar seus processos de negócio, os sistemas que os suportam e o ciclo de vida de tratamento dos seus dados, de modo a observar a aplicação dos princípios supramencionados.

Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

Segundo o *Guia de Boas Práticas – LGPD*:

> O **Relatório de Impacto à Proteção dos Dados Pessoais (RIPD)** representa documento fundamental a fim de demonstrar que o controlador realizou uma avaliação dos riscos nas operações de tratamento de dados pessoais que são coletados, tratados, usados, compartilhados e quais medidas são adotadas para mitigação dos riscos que possam afetar as liberdades civis e direitos fundamentais dos titulares desses dados.

O RIPD é uma importante forma de verificação de conformidade no tratamento de dados pessoais, que auxilia inclusive na documentação do processo de tratamento. A Figura 5 apresenta as etapas para se elaborar o referido Relatório de Impacto.

Figura 5. Etapas da Elaboração de um RPID.
Fonte: Guia de Boas Práticas – LGPD

A LGPD, em seu artigo 38, descreve as principais informações a constarem quando da elaboração do RIPD.

> Art. 38. A autoridade nacional 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. Observado 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 das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

A Anvisa deverá, ao longo de 2024, trabalhar na elaboração dos Relatórios de Impacto à Proteção de Dados Pessoais daqueles processos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD. Essa análise será conduzida de forma conjunta entre o Encarregado e as áreas técnicas da Agência.

Política de Privacidade e Política de Segurança da Informação

Segundo o *Guia de Elaboração de Termo de Uso e Política de Privacidade*:

> A **Política de Privacidade** cumpre, fundamentalmente, o dever de transparência disposto como princípio na LGPD, tendo como objetivo descrever ao titular dos dados pessoais, os procedimentos e processos adotados no tratamento de dados pessoais realizado pelo serviço, bem como informá-lo sobre as medidas de proteção de dados pessoais adotadas. (grifos nossos)

A Política de Privacidade deve ser um documento que observa os princípios da transparência e da publicidade e, por este motivo, deve ser características como:

- apresentar linguagem clara e simples;
- demonstrar precisão nas informações sobre o tratamento de dados pessoais;
- estar disponível em endereço de fácil acesso;
- orientar o usuário sobre como se manifestar quanto ao tratamento;
- ser alvo de atualização constante.

Com base no *Guia de Elaboração de Termo de Uso e Política de Privacidade*, da SGD/MGI, a Anvisa deverá elaborar o seu modelo de política de privacidade, com o fito de melhorar a sua comunicação externa, com o titular de dados. Esse documento deverá servir como base para a elaboração da política de privacidade para cada serviço (ou grupo de serviços) da agência.

Quanto à segurança da informação, como já mencionado na etapa de Iniciação e Planejamento, a Anvisa dispõe de uma Política de Segurança de Informação e Comunicação (POSIC), publicada por meio da Portaria ANVISA nº 72, de 26 de janeiro de 2023, que vêm sendo revisada regularmente com a orientação do Comitê de Governança Digital (CGD). À medida que as ações voltadas a proteção de dados pessoais avançarem no âmbito da agência, a revisão de pontos pertinentes da POSIC deverá ocorrer, de formar a manter sempre compatíveis as duas frentes de trabalho: segurança da informação e proteção de dados.

Adequação de cláusulas contratuais

Os contratos celebrados com entes públicas devem cumprir as normas de segurança e proteção de dados pessoais conforme estipulado pela LGPD. Nesse sentido, foram delineadas diretrizes que orientam a adequação dos contratos aos requisitos legais estabelecidos.

Atualmente, essas diretrizes estão postas por meio do Parecer n.º 00004/2022/CNMLC/CGU/AGU, elaborado pela Câmara Nacional de Modelos de Licitações e

Contratos Administrativos, da Consultoria-Geral da União. O documento apresenta importantes conclusões sobre a aplicação da LGPD no âmbito de Licitações e Contratos e pode ser consultado através do SEI 2722166.

Conforme citado no marco de levantamento de contratos relacionados a dados pessoais (etapa de Iniciação e Planejamento), a Anvisa vem seguindo as observações da AGU, tanto em relação ao parecer supramencionado como na utilização das minutas disponibilizadas pelo órgão. O foco atual tem estado sobre os novos contratos e, posteriormente, a Agência deverá avançar para a adequação dos contratos já celebrados e ainda vigentes.

Termo de Uso

Em definição apresentada pelo *Guia de Elaboração de Termo de Uso e Política de Privacidade*, o Termo de Uso é uma modalidade de contrato de adesão no qual as cláusulas são unilateralmente estipuladas pelo fornecedor do serviço, sem que o usuário tenha a capacidade de discutir ou modificar significativamente seu conteúdo. Esse contrato é formalizado entre o provedor do serviço e o usuário, delineando os direitos e responsabilidades de ambas as partes.

Assim como a Política de Privacidade, o Termo de Uso, para garantir o seu objetivo de informar o titular de dados pessoais, precisa ser escrito em linguagem simples e objetiva, ser preciso ao apresentar informações sobre o(s) serviço(s), passar por atualização constante e, por fim, estar facilmente disponível ao titular.

Baseando-se ainda no *Guia de Elaboração de Termo de Uso e Política de Privacidade*, a Anvisa deverá elaborar o seu modelo padrão de Termo de Uso. Cumpre salientar que, diferentemente de uma política de privacidade, o documento em questão deve destacar as regras e condições aplicáveis ao(s) serviço(s). É neste momento, ao tomar ciência dessas regras, que o usuário final (titular de dados) deve aceitar e concordar com o termo.

Entendendo que a Anvisa possui vários serviços disponíveis ao usuário, das mais diferentes naturezas e que cumprem diversas finalidades, a agência deve zelar para que cada um desses serviços (ou grupo de serviços) mantenha o seu Termo de Uso, com base no modelo a ser elaborado, porém cuidando para que as especificidades de cada contexto sejam contempladas.

Monitoramento

À medida que as etapas anteriores trataram de diagnosticar, planejar e implementar ações voltadas à governança em privacidade, sempre estruturando-se na LGPD, a última etapa consiste no monitoramento dessas ações, seja observando-se os indicadores ou mesmo realizado a gestão de incidentes com dados pessoais.

Para a etapa de Monitoramento, o Guia para Elaboração do Programa de Governança em Privacidade descreve os seguintes marcos:

Figura 6. Etapas Monitoramento – PGP
Fonte: Guia para Elaboração do Programa de Governança em Privacidade, adaptado para a Anvisa

Indicadores de Performance

Os Indicadores de Performance (Key Performance Indicator – KPIs) são medidas quantificáveis usadas pelas instituições para rastrear e avaliar o sucesso de uma determinada atividade, iniciativa ou processo. No contexto do PGP-Anvisa, a análise regular dos principais indicadores de desempenho permitirá à agência verificar lacunas no programa de gerenciamento de privacidade assim como averiguar o status de outras iniciativas de privacidade.

Inicialmente, propõe-se adotar os Indicadores de Performance listados a seguir, observando-se a recomendação da SGD/MGI:

- Monitoramento e acompanhamento do número de incidentes de violação de dados pessoais e/ou vazamento de dados pessoais;
- iPriv (índice de maturidade em Privacidade): obtido através da ferramenta de autodiagnóstico do *Framework de Privacidade e Segurança da Informação*;
- Índice de serviços com dados pessoais inventariados: número de serviços com dados pessoais inventariados/número de serviços com dados pessoais do órgão*100;
- Índice de conscientização em proteção de dados: quantidade de treinamentos realizados / quantidade de treinamentos previstos * 100.

É importante observar que a lista acima traz o indicador *iPriv*, em lugar dos Resultados do diagnóstico de adequação à LGPD. Tal medida foi adotada pois, desde a publicação da Portaria nº 852/2023 (Programa de Privacidade e Segurança da Informação do Governo Federal), a SGD regulamentou o uso do Framework de Privacidade e Segurança da Informação para os órgãos do SISP.

Gestão de Incidentes

A *Guia de Resposta a Incidentes de Segurança*, editado pela SGD, apresenta o seguinte conceito sobre incidentes de segurança com dados pessoais:

> 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 em 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.

Os incidentes de segurança não se limitam apenas a violações da confidencialidade; eles também englobam eventos que resultam na perda ou indisponibilidade de dados pessoais. Exemplos desses incidentes incluem o sequestro de dados (*ransomware*), acesso não autorizado a informações armazenadas em sistemas computacionais e a divulgação não intencional de dados dos titulares.

Se detectado o risco ou dano relevante ao titular de dados pessoais, conforme o exposto no artigo 48 da LGPD, o incidente deverá ser comunicado à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares de dados envolvidos.

Está em fase final de elaboração, por meio da liderança da COSED/GEOTI/GGTIN, o documento que apresenta a Política de Tratamento de Incidentes de Segurança Cibernética (PTISC/Anvisa). A política em questão, que tem o objetivo de assegurar o alinhamento das práticas de tratamento de incidentes com as estratégias de negócio da Agência, já conta com procedimentos de resposta para o caso de incidentes com dado pessoal.

Quanto à comunicação com a autoridade nacional nos casos específicos mencionados, a Agência deverá elaborar um Plano de Comunicação à ANPD que torne mais ágil e uniforme o fluxo de informações e auxilie na mitigação de novos incidentes.

Análise e Reporte de Resultados

A análise e divulgação dos resultados são igualmente recomendadas durante a etapa de monitoramento, com o propósito de evidenciar o valor do PGP-Anvisa para a alta administração. Ao destacar o progresso das iniciativas e os resultados alcançados, assim como enfatizar o papel da privacidade em benefício do cidadão, é possível consolidar e fortalecer a cultura de proteção dos dados.

No sentido de coordenar as atividades de análise e reporte de resultados, o Encarregado tem um importante papel. Ele atua gerenciando o estabelecimento das métricas que permitirão o acompanhamento e a verificação de efetividade do PGP-Anvisa e realizando a divulgação dos resultados para toda a agência.

Para facilitar a comunicação desses resultados, é recomendado à Anvisa, ainda por meio do Encarregado de Dados, que se estabeleça um rito de elaboração de relatórios periódicos sobre o PGP-Anvisa que facilite a visualização e compreensão dos resultados, além do fornecimento de informações à ANPD, quando se fizer necessário.

REFERÊNCIAS

ANVISA. Agência Nacional de Vigilância Sanitária. Tratamento de Dados Pessoais. Brasília: ANVISA, [2023]. Disponível em: https://www.gov.br/anvisa/pt-br/acessoainformacao/tratamento-de-dados-pessoais. Acesso em 15 out. 2023.

ANVISA. Agência Nacional de Vigilância Sanitária. Portaria nº 60, de 24 de janeiro de 2022. Institui a Política de Governança Organizacional da Agência Nacional de Vigilância Sanitária. Brasília: ANVISA, [2022]. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-pt-n-60-de-24-de-janeiro-de-2022-376057065. Acesso em: 16 out. 2023.

ANVISA. Agência Nacional de Vigilância Sanitária. Portaria nº 1.184, de 17 de outubro de 2023. Institui a Política de Proteção de Dados Pessoais da Agência Nacional de Vigilância Sanitária. Brasília: ANVISA, [2023]. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-1.184-de-17-de-outubro-de-2023-517296997. Acesso em: 01 dez. 2023.

ANVISA. Agência Nacional de Vigilância Sanitária. Portaria nº 72, de 26 de janeiro de 2023. Institui a Política de Segurança da Informação e Comunicações (POSIC) da Agência Nacional de Vigilância Sanitária. Brasília: ANVISA, [2023]. Disponível em: https://anvisabr.sharepoint.com/:b:/r/sites/COSED/Documentos%20Partilhados/MANUAIS%20e%20TUTORIAIS/posic%20-out-23.pdf?csf=1&web=1&e=bxshvt. Acesso em: 01 dez. 2023.

BRASIL. Presidência da República. Secretaria-Geral. Lei n.° 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: PR, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 3 out. 2023.

BRASIL. Ministério da Economia. Secretaria de Governo Digital. Guia de Boas Práticas - Lei Geral de Proteção de Dados (LGPD). Brasília, DF: ME, 2020. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_programa_governanca_privacidade.pdf. Acesso em: 2 nov. 2023.

BRASIL. Ministério da Gestão e Inovação em Serviços Públicos. Secretaria de Governo Digital. Privacidade e Segurança. Guias e Modelos. Brasília, DF: ME, 2021. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-e-modelos Acesso em: 7 nov. 2023.

BRASIL. Ministério da Gestão e Inovação em Serviços Públicos. Secretaria de Governo Digital. Guia de Elaboração de Programa de Governança em Privacidade - Lei Geral de Proteção de Dados (LGPD). Brasília, DF: MGI, 2023. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_programa_governanca_privacidade.pdf. Acesso em: 7 nov. 2023.

BRASIL. Presidência da República. Secretaria-Geral. Decreto nº 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: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10332.htm. Acesso em: 3 out. 2023.

BRASIL. Ministério da Gestão e Inovação em Serviços Públicos. Secretaria de Governo Digital. Guia de Elaboração de Termo de Uso e Política de Privacidade. Brasília, DF: MGI, 2023. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_termo_uso_politica_privacidade.pdf. Acesso em: 25 nov. 2023.