Autoridade Nacional de Proteção de Dados
Coordenação-Geral de Fiscalização
Coordenação de Fiscalização

RELATÓRIO DE INSTRUÇÃO Nº 5/2024/FIS/CGF

Brasília, data da assinatura.

RELATÓRIO DE INSTRUÇÃO

SUMÁRIO

1. IDENTIFICAÇÃO

1.1. **Nome/razão social do autuada:** Ministério da Saúde (MS)

1.2. **CPF/CNPJ do autuada:** 00.394.544/0001-85 (0152941)

1.3. **Agente de tratamento:** (X) Controlador ( ) Operador

1.4. **Nome da Encarregada setorial:** Adriana Macedo Marques (Portaria de Pessoal GM/MS nº 953, de 11 de maio de 2023)[1]

1.5. **Nome da Encarregada setorial suplente**: Daniela Barros do Nascimento (Portaria de Pessoal GM/MS nº 953, de 11 de maio de 2023)[2]

1.6. **Contato da Encarregada titular e da Encarregada suplente:** adriana.mmarques@saude.gov.br e daniela.nascimento@saude.gov.br.

2. EMENTA

INCIDENTE DE SEGURANÇA EM ÓRGÃO PÚBLICO. INDISPONIBILIDADE DE ACESSO A DADOS PESSOAIS E A SISTEMAS ESSENCIAIS. DADOS SENSÍVEIS RELATIVOS À SAÚDE. DADOS DE IDOSOS, CRIANÇAS E ADOLESCENTES. AUSÊNCIA DE ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS. AUSÊNCIA DE RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS. CONFIGURAÇÃO DE INFRAÇÕES. ADVERTÊNCIAS. MEDIDAS CORRETIVAS.

1. O incidente de segurança envolveu a indisponibilidade de diversos serviços do Ministério da Saúde, que tratam dados sensíveis relativos à saúde de milhões de brasileiros.

2. Não havia Encarregado pelo tratamento de dados pessoais designado à época. A nomeação somente foi efetivada após a instauração do presente PAS, o que ensejou a aplicação da sanção de advertência por violação ao art. 23, III, LGPD.

3. Os RIPDs solicitados por meio de Medida Preventiva foram parcialmente enviados após a instauração do presente PAS, em sede de Defesa Administrativa, o que ensejou a aplicação da sanção de advertência por infringência ao art. 38, LGPD, cominada com a aplicação de medida corretiva.

4. A comunicação do incidente de segurança à ANPD foi realizada após provocação desta Autoridade, em processo equivocado, o que levou à inclusão do art. 48, LGPD, no Auto de Infração deste PAS. A comunicação do incidente de segurança aos titulares de dados, embora tenha sido efetuada de forma ampla e imediata, somente foi comprovada a esta Autoridade após a instauração do presente PAS. Reconhecida a comunicação à ANPD e aos titulares, afastou-se a infringência do art. 48, LGPD.

5. A resposta à Medida Preventiva foi protocolada em processo diverso. Embora não tenha atendido materialmente aos questionamentos, o documento foi considerado tempestivo. Por isso, afastou-se a incidência do art. 5º do Regulamento de Fiscalização.

6. A razão fundamental do princípio da intranscendência subjetiva da sanção não é aplicável em casos de violações das normas de proteção de dados pessoais cometidas por gestão anterior à atual quando relacionada a mesma pessoa jurídica controladora dos dados pessoais.

7. Há adequação da advertência para infrações graves diante da impossibilidade de outra sanção, em atenção ao princípio da proporcionalidade.

8. A autuada infringiu os arts. 23, III e 38 da LGPD, ensejando a aplicação de 2 (duas) sanções de advertência, cumulada com 2 medidas corretivas para o caso da infringência ao art. 38, LGPD.

3. REFERÊNCIAS

3.1. Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).

3.2. Regimento Interno da Autoridade Nacional de Proteção de Dados, aprovado pela Portaria nº 01, de 08 de março de 2021.

3.3. Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da ANPD, aprovado pela Resolução CD/ANPD nº 1, de 28 de outubro de 2021 – doravante Regulamento de Fiscalização.

3.4. Regulamento de Dosimetria e Aplicação de Sanções Administrativas, aprovado pela Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023 – doravante Regulamento de Dosimetria.

3.5. Processo de Fiscalização (PF) nº 00261.001745/2021-58;

3.6. Processo Administrativo Sancionador (PAS) nº 00261.000456/2022-12;

3.7. Processo de Comunicado de Incidente à ANPD nº 00261.000728/2022-84;

3.8. Formulário CIS (SEI nº 0045645);

3.9. Ofício nº 132/2021/CGF/ANPD/PR (SEI nº 0048902);

3.10. Ofício nº 20/2022/SE/GAB/SE/MS (SEI nº 0048913);

3.11. Ofício nº 2/2022/CGF/ANPD/PR (SEI nº 0048914);

3.12. Aviso 0001/2022 (SEI nº 0048851);

3.13. Nota Técnica nº 18/2022/CGF/ANPD (SEI nº 0048839);

3.14. Despacho Decisório nº 1/2022/CGF/ANPD (SEI nº 0048840);

3.15. Auto de Infração nº 2/2022/CGF/ANPD (SEI nº0048841);

3.16. Ofício nº 70/2022/CGF/ANPD/PR (SEI nº 0048842);

3.17. Ofício nº 418/2022/SE/GAB/SE/MS (SEI nº 0048848);

3.18. Nota Técnica nº 3/2022-CGMA/DEMAS/SE/MS (SEI nº 0048852);

3.19. Portaria GM/MS nº 544 (SEI nº 0048853);

3.20. Portaria DATASUS/SE/MS (SEI nº 0048854);

3.21. Nota Técnica nº 10/2022-COSEGI/CGGOV/DATASUS/SE/MS (SEI nº 0048855);

3.22. Formulário CIS (SEI nº 0048856);

3.23. Anexo RIPD SNT (SEI nº 0048858);

3.24. Anexo RIPD SISREG (SEI nº 0048859);

3.25. Portaria GM/MS nº 3.231 (SEI nº 0048860);

3.26. Despacho COSEGI/CGGOV/DATASUS/SE/MS (SEI nº0048861);

3.27. E-mail MS à Polícia Federal (SEI nº 0048862);

3.28. E-mail MS ao CTIR (3260669) (SEI nº 0048863);

3.29. Nota Oficial Site MS (SEI nº 0048864);

3.30. Nota Técnica nº 5/2022-COSEGI/CGGOV/DATASUS/SE/MS (SEI nº 0048865);

3.31. Portaria GM/MS nº 1.436 (SEI nº 0048888);

3.32. Portaria GM/MS nº 3.362 (SEI nº0048889);

3.33. Portaria GM/MS nº 3.511 (SEI nº 0048891);

3.34. Memória de Reunião (SEI nº 0048894);

3.35. Alegações finais [Ofício nº 26/2024/SEIDIGI/CGOEX/SEIDIGI/MS (SEI nº 0098401) e Nota Técnica nº 3/2024-SEIDIGI/CGOEX/MS (SEI nº 0098402)].

4. SUMÁRIO EXECUTIVO DO PROCESSO

4.1. **Auto de Infração:** 10/03/2022 - Auto de Infração nº 2/2022/CGF/ANPD (SEI nº 0048841).

4.2. **Intimação:** 10/03/2022 – Ofício 70/2022/CGF/ANPD/PR (SEI nº 0048842).

4.3. **Forma da intimação:** (X) Meio eletrônico ( ) Via postal ( ) Pessoal ( ) Comparecimento pessoal ( ) Por edital ( ) Cooperação internacional ( ) Outro meio: contato telefônico.

4.4. **Recibo:** 11/03/2022 – E-mail Confirmação de recebimento (SEI nº 0048845).

4.5. **Dispositivos legais e regulamentares infringidos, nos termos do auto de infração:**

a) Lei Geral de Proteção de Dados Pessoais:

Art. 23, Inciso III – falta de comprovação da indicação do Encarregado pelo Tratamento de Dados Pessoais;

Art. 38 – ausência de envio do Relatório de Impacto à Proteção de Dados pessoais referente a suas operações de tratamento;

Art. 48 – ausência de comunicação à ANPD e ao titular da ocorrência de incidente de segurança que possa acarretar-lhe risco ou dano relevante.

b) Regulamento de Fiscalização:

Art. 5º - não atendimento às requisições da ANPD presentes no Aviso 001/2022.

4.6. **Data da apresentação da defesa:** 23/03/2022. Documentos:

i) Ofício nº 418/2022/SE/GAB/SE/MS (SEI nº0048848);

i i) Nota Técnica nº 3/2022-CGMA/DEMAS/SE/MS (SEI nº 0048852) e anexos.

4.7. **Produção de prova(s) pela autuada:** (X) Não ( ) Sim.

4.8. **Produção de prova(s) pela ANPD:** (X) Não ( ) Sim.

4.9. **Terceiro(s) interessado(s):** (X) Não ( ) Sim.

4.10. **Termo de Ajustamento de Conduta:** (X) Não ( ) Sim.

4.11. **Alegações Finais:** ( ) Não (X) Sim - Alegações Finais - Ofício nº 26/2024/SEIDIGI/CGOEX/SEIDIGI/MS (SEI nº 0098401) e Nota Técnica nº 3/2024-SEIDIGI/CGOEX/MS (SEI nº 0098402).

4.12. **Medidas preventivas aplicadas - art. 32 do Regulamento de Fiscalização:** ( ) Não (X) Sim - Aviso 0001/2022 (SEI nº 0048851).

4.13. **Medidas preventivas aplicadas - art. 26, IV, do Decreto nº 10.474/2020:** (X) Não ( ) Sim.

5. RELATÓRIO

5.1. Conforme disposto no art. 37 do Regulamento de Fiscalização da ANPD, aprovado pela Resolução CD/ANPD nº 1/2021, o processo administrativo sancionador (PAS) destina-se à apuração de infrações à legislação de proteção de dados pessoais que sejam de competência da ANPD, nos termos do artigo 55-J, IV, da LGPD. De acordo com o art. 54 do mencionado regulamento, o Relatório de Instrução subsidiará a decisão de primeira instância, a ser proferida pela Coordenação-Geral de Fiscalização (CGF). Assim, em consonância com os ditames normativos aplicáveis ao caso e demais documentos que constam dos autos, passa-se ao detalhamento dos atos processuais até a presente data, com o objetivo de avaliar os motivos da autuação e os argumentos apresentados pela autuada face à legislação e às normas de proteção de dados.

5.2. Em dezembro de 2021, a ANPD teve conhecimento, por meio de veículos de comunicação, de que sites do ConecteSUS e do Ministério da Saúde teriam supostamente sofrido um ataque *hacker* (SEI nºs 0048899, 0048900 e 0048901), o que teria deixado diversos serviços indisponíveis ao cidadão. Diante dessa informação, e com o intuito de averiguar o ocorrido, esta Coordenação Geral de Fiscalização (CGF) decidiu instaurar o Processo de Fiscalização nº 00261.001745/2021-58.

5.3. Em 10/12/2021, a ANPD enviou o Ofício nº 132/2021/CGF/ANPD/PR (SEI nº 0048902) ao então Secretário Executivo do Ministério da Saúde, no bojo do qual foram solicitados esclarecimentos acerca do suposto ataque, bem como a identificação dos titulares e dados eventualmente afetados, além das medidas adotadas pelo Ministério para mitigar eventuais riscos e danos aos titulares.

5.4. Adicionalmente, o referido ofício informou que, confirmada a indisponibilidade da plataforma - que abriga dados pessoais de saúde de milhões de brasileiros -, haveria incidente de segurança capaz de gerar risco ou dano relevante aos titulares de dados, circunstância que atrai a incidência do art. 48 da LGPD e impõe a obrigação de comunicar o ocorrido não só à ANPD como, também, aos titulares de dados afetados. Por esse motivo, foi solicitado o envio de Comunicação de Incidente de Segurança (CIS) Preliminar, conforme orientações disponíveis em https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis, no prazo recomendado de 2 (dois) dias úteis contados da data de ciência do incidente, assim como a comunicação complementar em até 30 (trinta) dias corridos. Adicionalmente, requereu-se a juntada do relatório de tratamento do incidente e o envio da comprovação da comunicação aos titulares, com conteúdo, forma e data da comunicação. Por fim, foi requerido o encaminhamento do ato de nomeação do Encarregado pelo tratamento de dados pessoais, pois não foram encontradas informações sobre tal identificação no sítio eletrônico do Ministério da Saúde.

5.5. A ANPD também expediu o Ofício nº 133/2021/CGF/ANPD/PR (SEI nº 0048903), endereçado ao Diretor-Geral da Polícia Federal, e o Ofício nº 134/2021/CGF/ANPD/PR (SEI nº 0048904), dirigido ao Secretário-Executivo do Gabinete de Segurança Institucional, também em 10/12/2021, a fim de obter informações sobre a apuração do incidente.

5.6. O Ministério da Saúde (doravante "MS"), por meio do Ofício nº 20/2022/SE/GAB/SE/MS (SEI nº 0048909), em 06/01/2022, informou que "*O incidente de segurança envolveu ataque a* (sic) *conta AWS do Ministério da Saúde, cuja infraestrutura de redes/servidores foi deletada. Nesta infraestrutura de computação em nuvem, estavam alocados os serviços do ConectSUS, Notifica, SIPNI e RNDS, mas não havia evidências de dados vazados ou titulares afetados.*" O MS esclareceu, ainda, que o incidente envolveu ataque com destruição do ambiente, mas que não se tratou de ataque de *ransomware*, não havendo evidências de exfiltração dados. O MS acrescentou que, à época, não existia Encarregado pelo tratamento de dados pessoais nomeado no órgão.

5.7. Diante da resposta do MS, em 13/01/2021, a ANPD enviou o Ofício nº 2/2022/CGF/ANPD/PR (SEI nº 0048914) para esclarecer que tanto o

acesso indevido de terceiros quanto situações acidentais ou ilícitas de destruição, perda ou alteração de dados pessoais constituem incidentes de segurança, razão pela qual deviam ser comunicados nos moldes do art. 48 da LGPD. Também informou-se, na ocasião, que o Ofício nº 20/2022/SE/GAB/SE/MS (SEI nº 0048913) não atendeu material e formalmente aos termos do art. 48 da LGPD.

5.8. Pelos motivos mencionados no ofício supracitado, a ANPD expediu o Aviso 001/2022 (SEI nº 0048917). Este documento indicou o prazo de 30 (trinta) dias para atendimento de suas determinações, contados da data de recebimento.

5.9. Decorrido o prazo estipulado no Aviso, a Coordenação-Geral de Fiscalização (CGF) não identificou qualquer manifestação do MS no processo. Ocorre que, por erro material do regulado, as informações solicitadas foram protocoladas em processo diverso, fato que somente foi conhecido pela CGF após a apresentação da defesa da autuada em sede de Processo Administrativo Sancionador (item 3.4.2 do documento SEI nº 0048852).

5.10. Em vista disso, e desconhecendo a referida manifestação, elaborou-se a Nota Técnica nº 18/2022/CGF/ANPD (SEI nº 0048922), que sugeriu a instauração de Processo Administrativo Sancionador, com base no art. 42 do Regulamento de Fiscalização, por meio da lavratura de Auto de Infração, previsto no art. 46 do mesmo Regulamento[3]. Essa manifestação foi acolhida pelo Despacho Decisório nº 1/2022/CGF/ANPD (SEI nº 0048923), em que o Coordenador-Geral de Fiscalização decidiu pela instauração de Processo Administrativo Sancionador em desfavor do Ministério da Saúde.

5.11. Dessa forma, instaurou-se o presente processo sancionador, SEI/ANPD nº 00261.000456/2022-12, em que foi lavrado o Auto de Infração nº 2/2022/CGF/ANPD (SEI nº0048841). A comunicação ao Ministério se deu por meio do Ofício nº 70/2022/CGF/ANPD/PR (SEI nº 0048842). De acordo com o Auto de Infração, o órgão teria infringido os arts. 23, III; 38 e 48 da LGPD, além do art. 5º do Regulamento de Fiscalização, dispondo do prazo de 10 (dez) dias úteis, a partir da ciência, para apresentar defesa perante a CGF. O e-mail (SEI nº 0048845) atesta o recebimento do referido ofício em 11/03/2022.

5.12. Em 23/03/2022, o MS apresentou tempestivamente sua defesa, por meio do Ofício nº 418/2022/SE/GAB/SE/MS (SEI nº 0048848) e da Nota Técnica 3/2022-CGMA/DEMAS/SE/MS (SEI nº0048852) e anexos, quais sejam:

> I - Portaria GM/MS Nº 544, de 16 de março de 2022 (SEI nº 0048853);
>
> II - Portaria DATASUS, de 22 novembro de 2019 (SEI nº 0048854);

III - Nota Técnica nº 10/2022-COSEGI/CGGOV/DATASUS/SE/MS (SEI nº 0048855);

IV - Formulário de comunicação de incidente à ANPD (SEI nº 0048856);

V - Cópia do e-mail que enviou para a ANPD evidências do incidente (SEI nº 0048857);

VI - RIPD do SNT (SEI nº 0048858);

VII - RIPD do SISREG (SEI nº 0048859);

VIII - Portaria GM/MS nº 3.231, de 22 de novembro de 2021 (SEI nº 0048860);

IX - Despacho COSEGI/CGGOV/DATASUS/SE/MS (SEI nº 0048861);

X - E-mail comunicação do Incidente à Polícia Federal (SEI nº 0048862);

XI - E-mail comunicação do Incidente ao CTIR (SEI nº 0048863); e

XII - Comunicações do Ministério da Saúde à sociedade sobre o incidente ocorrido (SEI nº 0048864).

5.13. Não houve produção de provas conforme o disposto no art. 48 do Regulamento de Fiscalização.

5.14. Em 28/06/2022, o Despacho (SEI nº 0048887) sobrestou o PAS até que fosse publicado o Regulamento de Dosimetria, aprovado pela Resolução CD/ANPD nº 4/2023. O trâmite regular do processo foi retomado em 19/04/2023 pelo Despacho (SEI nº 0048893).

5.15. Em 28/07/2023, foi realizada reunião com o Sr. Rodrigo Otávio Moreira da Cruz, ex-Secretário-Executivo do Ministério da Saúde, a pedido deste, para que apresentasse esclarecimentos quanto ao presente Processo Administrativo Sancionador. A memória da reunião foi registrada no documento SEI nº 0048893.

5.16. Em 30/01/2024, a autuada foi intimada para apresentar alegações finais [Ofício nº 8/2024/FIS/CGF/ANPD (SEI nº 0065805) e Recibo Protocolo MS (SEI nº 0069999)].

5.17. Em 15/02/2024, o MS apresentou tempestivamente as alegações finais [Ofício nº 26/2024/SEIDIGI/CGOEX/SEIDIGI/MS (SEI nº 0098401) e Nota

Técnica nº 3/2024-SEIDIGI/CGOEX/MS (SEI nº 0098402)].

5.18. É o relatório.

6. PRELIMINARES

COMPETÊNCIA

6.1. A Lei nº 13.709/18, Lei Geral de Proteção de Dados (LGPD), art. 5º, I, considera dado pessoal toda "informação relacionada a pessoa natural identificada ou identificável". Ainda, conforme o inciso II do mesmo artigo, é considerado dado pessoal sensível aquele dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. O incidente em questão envolveu ataque à conta AWS (Amazon Web Services) do MS, cuja infraestrutura de redes e servidores foi deletada. Nesta infraestrutura de computação em nuvem, estavam alocados os serviços do (i) CADSUS (Sistema de Cadastro do SUS); (ii) SGOP, que realiza gestão de operadores que podem acessar o CADSUS; (iii) ConecteSUS (sistema de visualização de dados clínicos do próprio usuário); (iv) Notifica (sistema de notificação de casos de Covid); (v) CoronavirusSUS, aplicativo para acompanhamento de informações sobre COVID-19; (vi) SIPNI (Sistema de Informação do Programa Nacional de Imunização); e (vii) RNDS (Rede Nacional de Dados em Saúde), que tratam dados pessoais sensíveis relacionados à saúde de milhões de brasileiros.

6.2. Os dados envolvidos no incidente de segurança aqui tratado são dados pessoais, pois consistem em informação relacionada a pessoa natural identificada ou identificável. Cada um dos sistemas afetados contém uma variedade de dados que se tornaram indisponíveis em virtude do incidente. Por exemplo, com a indisponibilidade do CADSUS, dados pessoais, inclusive sensíveis, deixaram de ser acessados pelos usuários autorizados do sistema, para fins de consulta, inclusão ou alteração (CPF, nome, nome da mãe, nome do pai, sexo, raça/cor, tipo sanguíneo, número de inscrição social (NIS/PIS/PASEP), carteira de identidade, certidões (nascimento, casamento, outras), carteira de trabalho, CNH, passaporte). Com a falha no ConecteSUS, dados como exames clínicos, vacinas, dispensa de medicamentos (alto, médio e baixo custo), fila de transplante e fila para atendimento na rede do SUS de média e alta complexidade ficaram indisponíveis. Com a queda do SIPNI, dados pessoais de cunho clínico, como vacinas aplicadas no usuário, deixaram de ser acessados. Já a indisponibilidade do RNDS impediu o acesso dos usuários a dados como exames, vacinas e prontuário clínico.

6.3. Os elementos colacionados aos autos revelam que a atividade desenvolvida pelo MS configura tratamento de dados pessoais, já que a pasta realizava as mais diversas ações sobre os dados dos usuários, como a coleta, a

produção, a classificação, o armazenamento, o processamento e a utilização desses dados para proporcionar ao cidadão diferentes serviços na área da saúde. Desse modo, resta claro que as operações aqui tratadas se enquadram na previsão do art. 5º, X, da LGPD, que classifica como tratamento "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

6.4. A LGPD ainda define a figura do controlador no art. 5º, VI, como a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais". Tendo em vista que o MS efetua o tratamento de dados pessoais para cadastrar e identificar os titulares em suas plataformas e para operacionalizar os sistemas de informação e suporte de informática para o serviço de saúde do SUS, é patente que a ele competem as decisões referentes ao tratamento de dados pessoais, motivo pelo qual é controlador.

6.5. Ademais, por força do art. 4º, I, do Regulamento de Fiscalização, o MS é considerado agente regulado pela ANPD, haja vista ser um agente de tratamento – no caso, controlador. Cumpre especificar os deveres a que os agentes regulados estão submetidos:

> Art. 5º Os agentes regulados submetem-se à fiscalização da ANPD e têm os seguintes deveres, dentre outros:
>
> I - fornecer cópia de documentos, físicos ou digitais, dados e informações relevantes para a avaliação das atividades de tratamento de dados pessoais, no prazo, local, formato e demais condições estabelecidas pela ANPD;
>
> II - permitir o acesso às instalações, equipamentos, aplicativos, facilidades, sistemas, ferramentas e recursos tecnológicos, documentos, dados e informações de natureza técnica, operacional e outras relevantes para a avaliação das atividades de tratamento de dados pessoais, em seu poder ou em poder de terceiros;
>
> III - possibilitar que a ANPD tenha conhecimento dos sistemas de informação utilizados para tratamento de dados e informações, bem como de sua rastreabilidade, atualização e substituição, disponibilizando os dados e as informações oriundos destes instrumentos;
>
> IV - submeter-se a auditorias realizadas ou determinadas pela ANPD;

> V - manter os documentos físicos ou digitais, os dados e as informações durante os prazos estabelecidos na legislação e em regulamentação específica, bem como durante todo o prazo de tramitação de processos administrativos nos quais sejam necessários; e
>
> VI - disponibilizar, sempre que requisitado, representante apto a oferecer suporte à atuação da ANPD, com conhecimento e autonomia para prestar dados, informações e outros aspectos relativos a seu objeto.

6.6. Uma vez que a atividade realizada pelo MS está inserida nas disposições da LGPD como tratamento de dados pessoais, a competência de atuação da ANPD no presente caso decorre do disposto no art. 5º, XIX da mencionada Lei, já que a Autoridade representa o "órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional". Cabe à ANPD, de acordo com o art. 55-J, "I - zelar pela proteção dos dados pessoais, nos termos da legislação", bem como "IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso" e "XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos".

6.7. No âmbito da ANPD, a CGF é a unidade administrativa responsável por identificar as infrações à LGPD. De acordo com a Portaria nº 1, de 8 de março de 2021 (“Regimento Interno da ANPD”):

> Art. 17. São competências da Coordenação-Geral de Fiscalização, sem prejuízo de outras previstas na Lei nº 13.709, de 2018, no Decreto nº 10.474, de 2020, e na legislação aplicável:
>
> I - fiscalizar e aplicar as sanções previstas no artigo 52 da Lei nº 13.709, de 2018, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
>
> [...]
>
> III - promover ações de fiscalização sobre as ações de tratamento de dados pessoais efetuadas pelos agentes de tratamento, incluído o Poder Público;
>
> [...]
>
> VII - receber as notificações de ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos

titulares e dar o tratamento necessário;

[...]

IX - requisitar aos agentes de tratamento de dados a apresentação de Relatório de Impacto à Proteção de Dados Pessoais;

6.8. O Regulamento de Fiscalização da ANPD, por sua vez, dispõe sobre a estruturação das atividades previstas no art. 17 do Regimento Interno da ANPD. De acordo com o art. 2º do Regulamento, a fiscalização volta-se ao monitoramento, à orientação, à prevenção e à repressão das infrações à LGPD, de sorte a, conforme o art. 3º do mesmo diploma, proteger os direitos dos titulares de dados, promover a implementação da legislação de proteção de dados pessoais e zelar pelo cumprimento das disposições da LGPD.

6.9. Diante das referidas competências, em especial da atividade preventiva, a CGF constatou, na hipótese presente, que haveria risco ou dano relevante aos titulares devido à gravidade do incidente de segurança em questão. Ressalte-se que não apenas o acesso indevido de terceiros a dados pessoais constitui um incidente de segurança. Consoante ao disposto no art. 46, situações acidentais ou ilícitas de destruição, perda ou alteração também constituem incidentes de segurança e devem ser comunicadas nos moldes do art. 48 da LGPD, sempre que possam acarretar risco ou dano relevante aos titulares.

6.10. Desse modo, incidentes de segurança envolvem a ocorrência de eventos adversos que comprometam as propriedades de **confidencialidade**, **integridade**, **disponibilidade** e **autenticidade da segurança** de dados pessoais. Assim, incidentes de segurança não se restringem apenas às violações da confidencialidade, uma vez que também abrangem eventos de perda ou de indisponibilidade dados pessoais.[4]

6.11. Esse cenário, portanto, configurou um incidente de segurança com reflexos em dados pessoais, capaz de gerar risco ou dano relevante aos seus titulares e, portanto, de notificação obrigatória à ANPD e aos titulares afetados, nos termos do Art. 48 da LGPD. A autuada deveria, ainda, apresentar as medidas adotadas de modo a mitigar eventuais riscos e danos aos titulares de dados pessoais cujas informações são por ele custodiadas.

6.12. Pelo exposto, à luz da LGPD, fica estabelecida a competência da ANPD no caso concreto, para avaliar, por meio deste Processo Administrativo Sancionador nº 00261.000456/2022-12, a conduta do Ministério da Saúde - controlador de dados e agente regulado - por se tratar de incidente de segurança capaz de gerar risco ou dano relevante aos seus titulares de dados pessoais envolvidos.

OUTRAS QUESTÕES PRELIMINARES

6.13. Quanto à infringência ao art. 5º do Regulamento de Fiscalização, o MS esclareceu que houve equívoco no envio da documentação à ANPD, devido à expressiva demanda de trabalho na resolução do incidente, conforme relatado no Despacho COSEGI/CGGOV/DATASUS/SE/MS (SEI nº 0048861). Isso porque, em paralelo ao tratamento do incidente de segurança e ao atendimento de diversos pedidos de informações, a COSEGI recebeu o processo SEI nº 00261.001702/2021-72, oriundo da ANPD, que solicitava a apuração do suposto vazamento de dados ocorrido no Sistema CADSUS. No momento do recebimento desse novo processo, "o fato de a equipe ser extremamente reduzida e encontrar-se completamente estressada devido a jornadas de trabalho que adentravam madrugadas visando restabelecer todo o ambiente, retornar o serviço para população, e ainda, responder todos os pedidos de esclarecimentos que chegavam", contribuiu para que as informações que estavam sendo formatadas para responder ao processo 00261.001745/2021-58 fossem equivocadamente inseridas no processo 00261.001702/2021-72.

6.14. O órgão afirmou que todas as solicitações realizadas no documento Aviso 0001/2022 (SEI nº 0048851), no processo 00261.001745/2021-58, foram respondidas por meio dos documentos Nota Técnica nº 5/2022-COSEGI/CGGOV/DATASUS/SE/MS (SEI nº 0048865). Anexo Lista de aplicações AWS (SEI nº 0045656), Anexo Defacement MS (SEI nº 0045657), Anexo Evidencias_Incidente_Nuvem (SEI nº 0045658) e Anexo Comunicado PF (SEI nº 0048862). A referida Nota Técnica nº 5/2022-COSEGI/CGGOV/DATASUS/SE/MS foi anexada a esse processo por meio do documento SEI nº 0048865, em que se pode observar a assinatura em 10/02/2022, em respeito ao cumprimento do prazo estabelecido na Medida Preventiva Aviso 0001/2022 (SEI nº 0048851).

6.15. O MS salientou, também, que identificou a ausência da resposta no processo SEI 00261.001745/2021-58 e, ao localizar a resposta em processo similar, imediatamente iniciou a ação corretiva no dia 09/03/2022, com envio das evidências para a ANPD e a produção da Nota Técnica 10/2022-COSEGI/CGGOV/DATASUS/SE/MS (SEI nº 0048855) no mesmo dia. Ressaltou que todas essas ações ocorreram antes do envio do Auto de Infração nº 2/2022/CGF/ANPD (SEI nº 0048841), que foi assinado na data de 10/03/2022, o que, em seu entendimento, demonstra que a regulada já havia identificado o erro material e estava em processo de resolução antes da lavratura do auto de infração.

6.16. É imperioso reconhecer que as alegações do órgão são parcialmente pertinentes. Com efeito, o MS demonstrou expressiva demanda de trabalho para resolução do problema, o que efetivamente pode ter

contribuído para a demora no atendimento às determinações da ANPD. Cumpre salientar que o órgão, instado a se manifestar após a lavratura do auto de infração, apresentou defesa tempestiva acompanhada de vasta documentação, o que contribui para se considerar a boa-fé e correção do comportamento perante a ANPD, circunstância que deve ser reconhecida. Pelo exposto, considerando o erro material constatado e a postura de correção adotada pelo órgão, afasto, de pronto, a verificação da penalidade de não atendimento às requisições da ANPD, consoante ao art. 5º do Regulamento de Fiscalização.

6.17. De todo modo, resta examinar se os elementos apresentados pelo MS em sua defesa são suficientes para afastar a infringência dos outros dispositivos da LGPD indicados no Auto de Infração, quais sejam:

> Art. 23, Inciso III – falta de comprovação da indicação do Encarregado de Dados Pessoais;
>
> Art. 38 – ausência de envio do Relatório de Impacto à Proteção de Dados pessoais referente a suas operações de tratamento.
>
> Art. 48 – ausência de comunicação à ANPD e ao titular da ocorrência de incidente de segurança que possa acarretar-lhe risco ou dano relevante.

6.18. É o que se passa a analisar.

7. ANÁLISE

Circunstâncias da infração e autoria

7.1. De acordo com a instrução do presente processo, o incidente de segurança investigado teve início na noite de 09/12/2021, quando a ETIR/MS (Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais do Ministério da Saúde) identificou o uso abusivo e suspeito de conta ativa de um colaborador do MS, fora do horário de expediente. [redacted]

[redacted]

[ACESSO RESTRITO trechos sombreados são de acesso restrito à autuada – detalhamento do incidente de segurança, de medidas de segurança implementadas em sistema ou de características de funcionamento de sistema – art. 13, II, do Decreto nº 7.724/2012].

7.2. A ETIR identificou que o atacante usou a conta de um colaborador do MS, [redacted], para se autenticar no serviço. Os *logs* do sistema indicaram que, após conseguir a autenticação, a conta de [redacted] iniciou uma sequência de comandos para listar usuários e permissões, aumentando o privilégio da conta [redacted]. Após essa ação, o atacante executou o processo de automação para exclusão em massa dos ativos da infraestrutura em Nuvem do DATASUS. Além disso, os registros DNS foram alterados, direcionando os acessos aos sistemas do Ministério para uma página hospedada fora do Brasil, em Seychelles. Diante da instabilidade da conta do MS e da necessidade de restabelecimento do serviço, dada a criticidade do impacto ao negócio, optou-se por criar novo ambiente virtual para retomar os serviços do Ministério, enquanto o antigo ficou reservado para auditorias. Foram necessários vários dias para que os serviços fossem plenamente restabelecidos. Registre-se que a ETIR/MS concluiu que, apesar de a conta utilizada para violação se tratar de credencial válida, o colaborador em questão não estaria diretamente envolvido no ataque [ACESSO RESTRITO trechos sombreados são de acesso restrito à autuada – detalhamento do incidente de segurança, de medidas de segurança implementadas em sistema ou de características de funcionamento de sistema – art. 13, II, do Decreto nº 7.724/2012].

7.3. Provocado por esta Autoridade, o MS, por meio do Ofício nº20/2022/SE/GAB/SE/MS (SEI nº 0048913), em 06/01/2022, prestou os seguintes esclarecimentos:

> a) O incidente de segurança envolveu ataque a conta AWS do Ministério da Saúde, cuja infraestrutura de redes/servidores foi deletada. Nesta infraestrutura de computação em nuvem, estavam alocados os serviços do ConectSUS, Notifica, SIPNI e RNDS, mas não havia evidências de dados vazados ou titulares afetados. No que toca às medidas para mitigação, o DataSUS exercia o papel de operador do Ministério da Saúde, todavia, até o momento, não existia nomeação de encarregado de dados. Em contrapartida, o DataSUS informou que existiam medidas e controles administrativos, lógicos e físicos para possíveis mitigações.
>
> b) Devido à ausência de nomeação de encarregado, a COSEGI foi orientada pelo Ministério da Economia a comunicar o departamento de Ouvidoria, o que foi feito por meio do Ofício SEI nº 0024388565.
>
> c) Tendo em vista que toda equipe estava alocada na execução de

tarefas para reestabelecimento dos serviços do Ministério da Saúde, optou-se por responder com maiores certezas no prazo de 30 (trinta) dias corridos.

d) Não se tratou de ataque de *ransomware* no incidente, pois envolveu ataque com destruição do ambiente, razão pela qual não havia evidências de exfiltração de dados. Não houve perda de dados e vários serviços como o ConecteSUS, PNI, entre outros, já haviam sido reestabelecidos.

e) Sobre a indicação do encarregado, o Comitê Interno de Governança do Ministério da Saúde, instituído através da Portaria GM/MS nº 870 de 03/05/2021, deliberou durante reunião em 17/12/2021 que o Grupo de Trabalho constituído para implementação da Lei Geral de Proteção de Dados no âmbito do Ministério da Saúde (GT LGPD/MS) procederia com a análise e a indicação até o dia 31/01/2022. Na oportunidade, informou que o GT LGPD/MS era composto por membros de todas as áreas técnicas e estratégicas do Ministério da Saúde, o que viabilizaria a tempestiva indicação.

7.4. Com o avanço das investigações, foi detectado que, em virtude do ataque, milhões de usuários ficaram sem acesso a outros sistemas além dos mencionados no item 7.3 a). Outrossim, foram afetados os sistemas (i) CADSUS (Sistema de Cadastro do SUS); (ii) SGOP, que realiza gestão de operadores que podem acessar o CADSUS; (iii) ConecteSUS (sistema de visualização de dados clínicos do próprio usuário); (iv) NOTIFICA (sistema de notificação de casos de Covid); (v) CoronavirusSUS, aplicativo para acompanhamento de informações sobre COVID-19; (vi) SIPNI (Sistema de Informação do Programa Nacional de Imunização) e (vii) RNDS (Rede Nacional de Dados em Saúde) - Nota Técnica 10/2022-COSEGI/CGGOV/DATASUS/SE/MS, Seção “Dados pessoais e ativos envolvidos” (SEI nº 0048855).

7.5. Diante da resposta do Ministério, a ANPD emitiu o Ofício nº2/2022/CGF/ANPD/PR (SEI nº 0048914), em 13/01/2022, ocasião em que esclareceu que tanto o acesso indevido de terceiros quanto situações acidentais ou ilícitas de destruição, perda ou alteração de dados pessoais constituem incidentes de segurança, razão pela qual deviam ser comunicados nos moldes do art. 48 da LGPD. Em acréscimo, assinalou que o Ofício nº 20/2022/SE/GAB/SE/MS (SEI nº 0048913) não atendeu material e formalmente aos termos do art. 48 da LGPD. Isso porque não teriam sido apresentados (i) a comunicação do incidente de segurança complementar, (ii) a comprovação de comunicação aos titulares, (iii) o relatório de tratamento de incidente e (iv) a indicação de Encarregado.

7.6. Por esse motivo, a ANPD decidiu adotar Medida Preventiva, nos termos do art. 32, II, do Regulamento de Fiscalização, e encaminhou o Aviso 0001/2022 (SEI nº 0048851). O referido Aviso requereu a apresentação de documentos e informações que comprovassem a observância da LGPD no que

concerne (i) à indicação do Encarregado de Dados Pessoais (art. 23, III); (ii) à formalização da comunicação do incidente de segurança à ANPD e aos titulares de dados (art. 48); (iii) ao envio do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) referente às operações de tratamento no caso sob fiscalização (art. 38); e (iv) à 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 (art. 46 e 47). Este documento indicou o prazo de 30 (trinta) dias para atendimento de suas determinações, contados da data de recebimento do Ofício.

7.7. À época, esta CGF não teve acesso às informações prestadas pela regulada tempestivamente, uma vez que, conforme esclarecido anteriormente ([Item 6.13] e [Item 6.14]), o MS, de forma equivocada, protocolou sua manifestação em processo diverso. Em razão disso, e acreditando que o regulado teria deixado de prestar as informações determinadas em sede de Medida Preventiva, a CGF elaborou a Nota Técnica nº 18/2022/CGF/ANPD (SEI nº 0048839), que recomendou a instauração do processo administrativo sancionador para apurar a possível infringência dos seguintes dispositivos:

> **Lei Geral de Proteção de Dados:**
>
> Art. 23, inciso III – falta de comprovação da indicação do encarregado de dados pessoais;
>
> Art. 38 – descumprimento de determinação de envio do relatório de impacto à proteção de dados pessoais referente a suas operações de tratamento;
>
> Art. 48 – descumprimento da obrigação de comunicação do incidente de segurança à ANPD e aos titulares.
>
> **Regulamento de Fiscalização:**
>
> Art. 5º – não atendimento às requisições da ANPD presentes no Aviso 0001/2022 (SEI nº 0048851).

7.8. Por meio do Despacho Decisório nº 1/2022/CGF/ANPD (SEI nº 0048840) o Coordenador-Geral de Fiscalização da ANPD acolheu as razões da Nota Técnica nº 18/2022/CGF/ANPD (SEI nº 0048839) e decidiu pela instauração de processo administrativo sancionador em desfavor do Ministério da Saúde.

7.9. Conforme consignado no [Item 6.16] , em razão do erro material cometido pela autuada, afastou-se a incidência do art. 5º do Regulamento de Fiscalização, não restando caracterizada, portanto, a obstrução à atividade de

fiscalização. No entanto, os elementos colacionados aos autos são suficientes para afirmar que houve um incidente de segurança que impactou vários sistemas do Ministério da Saúde. Embora não tenha acarretado perda, violação ou exfiltração de dados, o incidente provocou a indisponibilidade de diversos serviços essenciais à população, sendo capaz de acarretar risco ou dano relevante aos titulares dos referidos dados, prejudicando milhões de usuários.

7.10. Embora a regulada não tenha se mantido inerte ao Aviso 0001/2022 (SEI nº 0048851), como a CGF julgou no momento da instauração do presente PAS, a manifestação elaborada à época, e protocolada em processo diverso, **tampouco atenderia a todas as requisições da Medida Preventiva**, como se verá a seguir.

7.11. A regulada argumentou, em sede de defesa, por meio da Nota Técnica 3/2022-CGMA/DEMAS/SE/MS (SEI nº 0048852), que:

> (...) todas as solicitações realizadas no documento SEI nº 0024834258 AVISO 01/2022 (processo 00261.001745/2021-58), foram respondidas por meio dos documentos SEI nº 0025268945 (NOTA TÉCNICA Nº 5/2022-COSEGI/CGGOV/DATASUS/SE/MS) 0025106045 (Anexo Lista de aplicações AWS), 0025269609 (Anexo Dafacement MS), 0025269740 (Anexo Evidencias_Incidente_Nuvem) e 0025272984 (Anexo Comunicado PF). A referida NOTA TÉCNICA nº 5/2022 foi anexada à (sic) esse processo, através do documento SEI nº 0025916075, em que pode-se (sic) observar a assinatura em 10 de fevereiro de 2022, dentro do prazo estipulado no SEI nº 0024834258 AVISO 01/2022, em respeito ao cumprimento do prazo estabelecido naquele Ofício.

7.12. Com efeito, a referida Nota Técnica nº 5/2022-COSEGI/CGGOV/DATASUS/SE/MS (SEI nº 0048865) data de 10/02/2022. Entretanto, ao contrário do que afirma a autuada, tal documento, ainda que seja considerado tempestivo, não atendeu a todas as determinações contidas no Aviso. De fato, a Nota Técnica e seus anexos apresentam detalhes sobre o incidente e seus efeitos, bem como acerca das medidas técnicas e administrativas implementadas para enfrentar o problema, demonstrando a observância aos artigos 46 e 47 da LGPD, conforme solicitado no Aviso.

7.13. Entretanto, deve-se destacar que o documento sequer menciona uma previsão quanto à nomeação do Encarregado pelo tratamento de dados pessoais (art. 23, III, da LGPD). Quanto à formalização da comunicação do incidente de segurança à ANPD e aos titulares de dados (art. 48, da LGPD), a Nota Técnica se limitou a informar que "[a] responsabilidade de notificação aos titulares de dados pessoais que foram afetados pelo incidente, por meio de notificação pública e direta não é competência desta Coordenação de Segurança da Informação - COSEGI"; e "Quanto ao Formulário

de comunicação de incidente de segurança com dados pessoais à Autoridade Nacional de Proteção de Dados (ANPD), a documentação está em desenvolvimento pelo Núcleo LGPD do DATASUS". Já no que tange ao envio do RIPD referente às operações de tratamento no caso sob fiscalização (art. 38, da LGPD), a Nota informa que "A elaboração do Relatório de Impacto a Proteção de Dados não é de competência da ETIR/MS, contudo os riscos foram identificados, remediados e implementado (*sic*) ações de melhorias na prevenção de novos incidentes similares ao ocorrido."

7.14. Observa-se, desse modo, que o conteúdo da Nota Técnica nº 5/2022-COSEGI/CGGOV/DATASUS/SE/MS (SEI nº 0048865) mostra-se *insuficiente* para atender a todas as determinações encaminhadas ao MS por meio do Aviso 0001/2022 (SEI nº 0048851). Nesse sentido, nota-se que o controlador (i) não indicou o seu Encarregado pelo tratamento de dados pessoais; (ii) não expediu comunicação aos titulares de dados pessoais potencialmente afetados pelo incidente de segurança; e (iii) não produziu o RIPD referente às operações de tratamento no caso sob fiscalização. **Restam comprovados, assim, os fatos que ensejaram a instauração deste PAS e a autoria por parte da autuada**.

CONDUTA:falta de comprovação da indicação do Encarregado de dados pessoais – art. 23, inciso III, da LGPD

Defesa apresentada pela autuada

7.15. Em sua primeira manifestação à ANPD, em 06/01/2022, por meio do Ofício nº 20/2022/SE/GAB/SE/MS (SEI nº 0048913), o MS informou que, até aquele momento, não havia designação de Encarregado de dados no Ministério. Devido à ausência de nomeação de Encarregado, a COSEGI (Coordenação de Segurança da Informação) foi orientada pelo Ministério da Economia a comunicar o departamento de Ouvidoria. Informou, ainda, que o Comitê Interno de Governança do Ministério da Saúde deliberou, durante reunião em 17/12/2021, que o Grupo de Trabalho constituído para implementação da Lei Geral de Proteção de Dados no âmbito do Ministério da Saúde procederia com a análise e a indicação do Encarregado o até o dia 31/01/2022.

7.16. Diante desse posicionamento, a ANPD, por meio do Ofício nº 2/2022/CGF/ANPD/PR (SEI nº 0048914), de 13/01/2022, ponderou que, apesar de a entrada em vigor da LGPD ter ocorrido em 28/12/2020, até aquele momento o Ministério não havia indicado Encarregado para tratamento de dados pessoais, em claro descumprimento do artigo 41 da LGPD, apesar das comunicações realizadas por esta ANPD em outras ocasiões, desde junho de 2021 (Ofício nº 63/2021/CGF/ANPD/PR, SEI nº 0081924, nos autos do Processo nº 00261.000123/2021-11; Ofício nº 60/2021/CGF/ANPD/PR, SEI nº 0034509, nos autos do Processo nº 00261.000554/2021-79; e Ofício nº

132/2021/CGF/ANPD/PR, SEI nº 0048902, nos autos deste Processo). E, por esse motivo, dentre outros, emitiu o já mencionado Aviso.

7.17. Apenas em 22/03/22, por meio da Nota Técnica 3/2022-CGMA/DEMAS/SE/MS (SEI nº 0048852), já em sede de defesa no presente PAS, a autuada informou a designação de Encarregado pelo tratamento de dados pessoais titular e suplente, por meio da Portaria GM/MS nº 544, de 16 de março de 2022 (SEI nº 0048853). No mesmo documento, a autuada ainda ressaltou que:

> (…) embora não houvesse designação formal do Encarregado até 17/03/2022, o MS já tratava o assunto de proteção de dados pessoais desde 2019, conforme pode ser observado na Portaria DATASUS, de 22 novembro de 2019 (SEI nº 0025949866), que institui o Núcleo LGPD no Departamento de Informática do SUS.

7.18. Em Alegações Finais (SEI nº 0098402), a autuada destacou que, à época dos fatos, muitos conceitos da LGPD ainda não eram completamente compreendidos pelo setor. Alegou que a LGPD possui conteúdo denso, técnico e complexo, tornando desafiadora sua interpretação e a adoção das medidas necessárias para entrada em conformidade. Registrou, inclusive, que a vigência da legislação foi adiada por duas vezes, e que a entrada em vigor das sanções administrativas se deu apenas em 1º de agosto de 2021. Diante disso, o MS alegou que a dificuldade de interpretação das obrigações não decorreu da falta de ações propositivas da pasta, mas, sim, pela própria natureza do tema. Acrescentou à sua argumentação que o Ministério passou por grandes dificuldades no contexto da pandemia do COVID 19. "É cediço que a dimensão da emergência sanitária, o cenário político-cultural e a crise de gerenciamento, com diversas mudanças de Ministros, tornaram ainda maiores os desafios da Pasta em 2020 e 2021".

7.19. Por fim, foi suscitada a necessidade de aplicação do princípio da proporcionalidade em razão da adequação do MS à LGPD, endossada pela implementação de 6 (seis) medidas administrativas relacionadas à proteção de dados pessoais no Ministério da Saúde: (i) criação da Secretaria de Informação e Saúde Digital no Ministério da Saúde; (ii) designação de nova Encarregada de Dados e publicação no sítio eletrônico; (iii) criação de Grupo de Trabalho para tratar especificamente sobre a LGPD; (iv) obtenção de assento para futura composição no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD); (v) realização da 1º Jornada de Proteção de Dados Pessoais no SUS; (vi) adoção de Programa de Privacidade e Segurança da Informação (PPSI) e mais uma medida em andamento, relacionada à (vii) capacitação para servidores das unidades descentralizadas do MS e do SUS, conforme descrito nos tópicos de A) a G) do item 3.9 das Alegações Finais (SEI nº 0098402).

Subsunção do fato ao tipo infracional correspondente

7.20. O art. 23, III, da LGPD estabelece que o tratamento de dados pessoais pelas pessoas jurídicas de direito público deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que, entre outras condições, **seja indicado um Encarregado quando realizarem operações de tratamento de dados pessoais**, nos termos do art. 39 dessa Lei. Este dispositivo, por sua vez, determina que "o operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria". Ou seja, o operador, quando realizando tratamento de dados em nome de determinado controlador, está igualmente obrigado a indicar um Encarregado de dados. Embora, no caso em análise, o MS figure como controlador e não haja outro agente operando o tratamento de dados pessoais em seu nome, o dever de designar um encarregado de dados está presente, conforme dispõe o art. 41 da LGPD.

7.21. Com efeito, o art. 41 estabelece **o dever do controlador de dados de indicar um Encarregado pelo tratamento de dados pessoais e elenca as responsabilidades desse agente**, quais sejam: 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.

7.22. Como visto [Item 7.16], mesmo após mais de um ano da promulgação da LGPD, não havia Encarregado pelo tratamento de dados pessoais designado no Ministério da Saúde, um órgão de governo, controlador, nos termos do art. 5º, VI, da LGPD (item 6.4), incumbido da administração de dezenas de sistemas informáticos essenciais à prestação de serviços de saúde à população, e responsável pelo tratamento dos dados de milhões de cidadãos brasileiros. Embora o Ministério tenha sido alertado por esta ANPD, em outras ocasiões e processos, acerca da necessidade de nomeação de encarregado de dados [Item 7.16], a pasta manteve-se inerte, o que culminou na expedição de Medida Preventiva por esta Autoridade, consubstanciada no Aviso 001/2022 (SEI nº 0048851).

7.23. Em que pese ter havido erro material quando do protocolo da manifestação da regulada em resposta ao referido Aviso, fato é que, nas informações prestadas à época, não havia menção a qualquer previsão para a designação de Encarregado de dados na pasta [Item 7.12]. Com efeito, a nomeação do Encarregado somente ocorreu em 16/03/2022 [Item 7.17] , após lavrado o Auto de Infração nº 2/2022/CGF/ANPD (SEI nº 0048841) e instaurado

o presente PAS, e mais de três meses após o incidente e o envio do Ofício nº 132/2021/CGF/ANPD/PR (SEI nº 0048902), em que a ANPD alertou da obrigação legal de o controlador indicar Encarregado pelo tratamento de dados pessoais [Item 5.3] e [Item 5.4].

7.24. Por todo o exposto, firma-se o entendimento de que, à época do incidente, não havia Encarregado pelo tratamento de dados pessoais designado pelo MS, muito embora a LGPD estivesse vigente há mais de um ano. Some-se a isso o fato de que, mesmo após reiterados alertas desta ANPD, inclusive por meio de Medida Preventiva, o Encarregado de dados somente foi designado depois da instauração deste Processo Administrativo Sancionador. **Resta, dessa forma, caracterizada a violação ao art. 23, III, da LGPD**.

Classificação da infração

7.25. Conforme relatado acima, a autuada incorreu em violação à obrigação estabelecida no art. 23, III, da LGPD. Cabe, então, classificar a infração como leve, média ou grave, conforme indica o art. 8º do Regulamento de Dosimetria:

> Art. 8º As infrações são classificadas, segundo a gravidade e a natureza das infrações e dos direitos pessoais afetados, em:
>
> I - leve;
>
> II - média; ou
>
> III - grave.
>
> § 1º A infração será considerada leve quando não verificada nenhuma das hipóteses relacionadas nos §§ 2º ou 3º deste artigo.
>
> § 2º A infração será considerada média quando puder afetar significativamente interesses e direitos fundamentais dos titulares de dados pessoais, caracterizada nas situações em que a atividade de tratamento puder impedir ou limitar, de maneira significativa, o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação; violação à integridade física; ao direito à imagem e à reputação; fraudes financeiras ou uso indevido de identidade, desde que não seja classificada como grave.
>
> § 3º A infração será considerada grave quando:
>
> I - verificada a hipótese estabelecida no § 2º deste artigo e cumulativamente, pelo menos, uma das seguintes:
>
> a) envolver tratamento de dados pessoais em larga escala, caracterizado quando abranger número significativo de titulares, considerando-se, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica do tratamento realizado;
>
> b) o infrator auferir ou pretender auferir vantagem econômica em decorrência da infração cometida;

> c) a infração implicar risco à vida dos titulares;
>
> d) a infração envolver tratamento de dados sensíveis ou de dados pessoais de crianças, de adolescentes ou de idosos;
>
> e) o infrator realizar tratamento de dados pessoais sem amparo em uma das hipóteses legais previstas na LGPD;
>
> f) o infrator realizar tratamento com efeitos discriminatórios ilícitos ou abusivos; ou
>
> g) verificada a adoção sistemática de práticas irregulares pelo infrator;
>
> II - constituir obstrução à atividade de fiscalização.

7.26. O art. 23, III, da LGPD determina que seja indicado um Encarregado de dados quando o tratamento de dados pessoais for realizado pessoas jurídicas de direito público, para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público. Por sua vez, o art. 41 atribui ao controlador de dados o dever de indicar Encarregado pelo tratamento de dados pessoais, e elenca as responsabilidades desse agente de tratamento.

7.27. No caso em análise, restou evidente que a ausência de indicação de Encarregado pelo tratamento de dados dificultou a comunicação com a ANPD e prejudicou o cumprimento de determinações e providências estabelecidas pela Autoridade, de forma tempestiva e apropriada.

7.28. Com efeito, segundo relatado pela autuada no Despacho COSEGI/CGGOV/DATASUS/SE/MS (SEI nº 0048861), já em sede de Defesa Administrativa:

> 5. Devido à dimensão do incidente, a ação imediata da COSEGI, após a confirmação do ataque, foi notificar ainda na madrugada do dia 10 de dezembro de 2021, a ocorrência do incidente, evidenciados nos documentos SEI nº 0025920949 e 0025917218. Essa ação imediata está alinhado (sic) coma Norma de Tratamento e Resposta à Incidente do Ministério da Saúde e teve como objetivo subsidiar de informações as autoridades competentes, Departamento de Polícia Federal - DPF e Gabinete de Segurança Institucional - GSI para o processo de investigação do crime cibernético e transparência no ocorrido, ficando demonstrada a preocupação dessa área com a comunicação com autoridades competentes.
>
> 6. Até aquela época, havia-se o entendimento na equipe de que a ANPD seria notificada quando houvesse acesso não autorizado a dados sensíveis e/ou pessoais. Essa interpretação foi corrigida e ajustada após alinhamento com a própria ANPD, onde essa coordenação já ajustou os processos internos, incluindo a ANPD no rol de autoridades competentes comunicadas quando ocorrido incidentes de segurança.

7.29. Ou seja, à época dos fatos, mesmo após um ano da promulgação da LGPD, a autuada desconhecia conceitos basilares relativos a incidentes de segurança capazes de gerar risco ou dano relevante aos titulares, e sequer considerava a ANPD no rol de autoridades que deveriam ser informadas nessas situações, mesmo sendo esta autarquia o órgão que detém a competência de zelar proteção dos dados pessoais (art. 55-J, I, LGPD). Diante desse cenário, mesmo que o incidente envolvesse o acesso não autorizado a dados sensíveis e/ou pessoais, ainda assim a comunicação com esta Autoridade restaria prejudicada, pois fato é que a Pasta não possuía Encarregado pelo tratamento de dados pessoais.

7.30. Para além da atribuição de receber as comunicações da Autoridade e adotar providências, como visto [Item 7.21], o Encarregado é também responsável por receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar as providências necessárias, além de orientar os funcionários da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.

7.31. Embora a infração em análise não se confunda com o incidente propriamente, que resultou na indisponibilidade de serviços essenciais à população, depreende-se que a ausência de Encarregado de dados enquadra-se na hipótese estabelecida no § 2º do art. 8º do Regulamento de Dosimetria, uma vez que tal infração foi capaz de afetar significativamente interesses e direitos fundamentais dos titulares de dados pessoais, "caracterizada nas situações em que a atividade de tratamento puder impedir ou limitar, de maneira significativa, o exercício de direitos ou a utilização de um serviço (...). Logo, **a infração ao art. 23, III ora analisada se enquadra nos requisitos do art. 8º, §2º, do Regulamento de Dosimetria, atendendo ao critério para ser classificada como média.**

7.32. Ademais, verifica-se que a infração atende, cumulativamente ao § 2º, as alíneas a) e d) do § 3º, I. Isso porque o tratamento de dados pessoais realizado pelo MS e afetado pelo incidente de segurança é claramente em larga escala, pois abrangeu todos os titulares de dados cadastrados em diversos sistemas, como ConecteSUS e CADSUS. Registre-se que, somente neste último, o MS informou que mais de 300 milhões de cadastros foram afetados, pois o sistema atende não somente pessoas naturais, mas também estabelecimentos de saúde (SEI nº 0048855, fl. 10). Além disso, tendo em vista a abrangência do incidente, é seguro concluir que este também envolveu tratamento de dados pessoais de crianças, de adolescentes e de idosos, assim como dados pessoais sensíveis, vez que diversos dados referentes a saúde dos titulares ficaram indisponíveis, bem como dados sobre origem racial ou étnica. Essas características elevam o grau de classificação da infração que, por esse motivo, **passa a ser considerada como grave, segundo art. 8º, §3º, I, "a" e "d", do Regulamento de Dosimetria**.

Definição do tipo de sanção administrativa

7.33. Para a definição do tipo de sanção adequada, o art. 10, II, do Regulamento de Dosimetria, indica ser aplicável multa simples quando a infração for classificada como grave[5]. No entanto, o art. 52, §3º, da LGPD, ao estabelecer as sanções que podem ser impostas a entidade ou a órgãos públicos, afasta, por omissão, a possibilidade de aplicação de multa ou de multa diária a esses agentes de tratamento. Por outro lado, o Regulamento de Dosimetria define, em seu art. 9º, que a advertência somente pode ser aplicada quando a infração for leve ou média, ou quando houver necessidade de imposição de medida corretiva.

7.34. No presente caso, não há que se falar em medida corretiva, uma vez que a designação do Encarregado pelo tratamento de dados no Ministério da Saúde foi formalizada em 16/03/2022, após a instauração do presente processo. Após algumas revogações, cabe registrar que a atual encarregada de dados foi designada pela Portaria GM/MS nº 953, de 11 de maio de 2023 (SEI nº 0095578).

7.35. Muito embora a infração em tela seja grave, as outras sanções previstas na LGPD (no caso, os incisos IV, V e VI do art. 52) tampouco são adequadas para o caso, em função do interesse público que justifica a necessidade do tratamento dos dados pessoais. Em razão, portanto, de seu caráter residual, deve ser aplicada a sanção de advertência no caso em apreço, mesmo diante de infração classificada como grave, em linha com decisões precedentes desta Autoridade [Relatório de Instrução nº 2/2024/FIS/CGF/ANPD (SEI nº 0057714) e Relatório de Instrução nº 4 /2024/FIS/CGF/ANPD (SEI nº 0136258)].

7.36. A esse respeito, importante ressaltar que o Regulamento de Dosimetria objetivou afastar a advertência quando sanção mais séria deveria ser aplicada. No entanto, diante da impossibilidade ou da inadequação de outra sanção, impedir a aplicação da advertência resultaria em uma infração grave quedar sem sanção alguma. Tal solução seria contrária ao sistema de dosimetria instituído pela ANPD e violaria frontalmente o princípio da proporcionalidade, parâmetro basilar na aplicação de sanções, conforme estabelece o art. 52, §1º, XI, da LGPD.

7.37. Embora tenha sua análise relativizada no presente processo, vez que não será aplicada a sanção de multa, as circunstâncias atenuantes e agravantes serão registradas, a fim de reconhecer a sua existência no caso concreto. Em que pese a constatação do equívoco cometido pela autuada ao protocolar sua resposta ao Aviso 0001/2022 (SEI nº 0048851) em processo diverso [Item 6.16], a manifestação não atendeu materialmente à determinação para designar Encarregado pelo tratamento de dados no órgão

[Item 7.12]. Identifica-se, portanto, a ocorrência de uma circunstância agravante, nos termos do art. 32, §2º, II, do Regulamento de Fiscalização. Por outro lado, houve a *cessação da infração* com a designação do Encarregado pelo tratamento de dados, após a instauração do PAS e antes da decisão de primeira instância [Item 7.17], o que demonstra a adoção de medida corretiva pelo controlador com o objetivo de sanar a conduta ilícita, ainda que tal fato tenha ocorrido de forma extemporânea. A autuada, ademais, não se furtou a reconhecer a falha, e buscou corrigi-la durante o trâmite do processo administrativo sancionador, o que proporcionou um diálogo mais efetivo e responsivo junto à ANPD.

7.38. **Fica, portanto, cominada a sanção de advertência para a infração ao art. 23, III.**

CONDUTA: não comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares – art. 48 da LGPD

Defesa apresentada pela autuada

7.39. Em sua primeira manifestação à ANPD, em 06/01/2022, por meio do Ofício nº 20/2022/SE/GAB/SE/MS (SEI nº 0048913), o MS prestou alguns esclarecimentos acerca do incidente de segurança, como as circunstâncias e a dinâmica do ataque, os sistemas afetados e as medidas de segurança adotadas. No entanto, quanto ao envio da Comunicação de Incidente de Segurança (CIS) Preliminar, solicitado por meio do Ofício nº 132/2021/CGF/ANPD/PR (SEI nº 0048902), a regulada limitou-se a responder que, devido ao fato de toda a equipe estar alocada na execução de tarefas para o reestabelecimento dos serviços, a COSEGI optaria por responder, com maiores certezas, em 30 dias corridos. Ademais, em que pese o mesmo ofício da CGF ter ressaltado que o art. 48 da LGPD impõe a obrigação de comunicar o incidente não só à ANPD, como também aos titulares de dados afetados, e ainda ter solicitado a comprovação de tal comunicação, na primeira interlocução com esta Autoridade, não houve qualquer manifestação do MS nesse sentido.

7.40. Diante desse posicionamento, a ANPD, por meio do Ofício nº 22/2022/CGF/ANPD/PR (SEI nº 0048914), de 13/01/2022, alertou que o ataque, por ter provocado a indisponibilidade de sistemas que tratam dados pessoais sensíveis relacionados à saúde de milhões de brasileiros, configurou um incidente de segurança capaz de gerar risco ou dano relevante aos seus titulares e, portanto, de notificação obrigatória à ANPD e aos titulares afetados, nos termos do art. 48 da LGPD. Ademais, a Autoridade ressaltou que a manifestação apresentada (item7.39) não atendeu material e formalmente aos termos do art. 48 da LGPD, conforme solicitado no Ofício nº

132/2021/CGF/ANPD/PR, e repisou que não houve apresentação da Comunicação do Incidente de Segurança e da comprovação de comunicação aos titulares. Consequentemente, por esse motivo, dentre outros, emitiu o já mencionado Aviso.

7.41. Já em sede de Defesa Administrativa no presente PAS, protocolada em 22/03/2022, a autuada, por meio da Nota Técnica nº 3/2022-CGMA/DEMAS/SE/MS (SEI nº 0048852), ponderou que, imediatamente após o incidente, os analistas e técnicos ficaram dedicados ao restabelecimento do ambiente afetado, para que os serviços pudessem ser disponibilizados à população com a maior brevidade possível. De acordo com o relatado, a ação imediata da COSEGI foi notificar, ainda na madrugada do dia 10 de dezembro de 2021, a ocorrência do incidente ao Departamento de Polícia Federal - DPF e ao Gabinete de Segurança Institucional - GSI para colaborar com transparência no processo de investigação do crime cibernético, o que demonstraria a preocupação dessa área com a comunicação junto às autoridades competentes. Ainda segundo a Pasta, até aquele momento, prevalecia o entendimento de que a ANPD somente deveria ser notificada em caso de acesso não autorizado a dados pessoais.

7.42. A autuada também destacou o equívoco ocorrido na época, quando a resposta aos questionamentos do Ofício nº 22/2022/CGF/ANPD/PR (SEI nº 0048914) foi protocolada em outro processo, por causa da expressiva demanda de trabalho devido ao ataque, e repisou a boa-fé em enviar as evidências do incidente logo que constatado o erro. A defesa também apresentou o Formulário de Comunicado à ANPD (SEI nº 0048856) e a Nota Técnica nº 10/2022-COSEGI/CGGOV/DATASUS/SE/MS (SEI nº 0048855), abordando as informações essenciais coletadas para tratamento do incidente ocorrido no ambiente do DATASUS, por meio da ETIR/MS. As evidências descritas na referida nota técnica foram encaminhas por e-mail e protocoladas no Processo de CIS (SEI nº 00261.000728/2022-84).

7.43. No que se refere à comunicação aos titulares, por entender que o impacto ao cidadão foi a indisponibilidade dos serviços sustentados pelo ambiente tecnológico objeto do incidente, o Ministério da Saúde optou por realizar várias comunicações públicas sobre o ocorrido, conforme demonstrado no documento Nota Oficial Site MS (SEI nº 0048864);

7.44. Em Alegações Finais (SEI nº 0098402), o MS destacou os elementos apresentados que demonstrariam seu compromisso com notificações a autoridades competentes, e que a Pasta teria realizado todos os esforços para responder à ANPD dentro dos prazos estipulados. Aduziu, ainda, que, devido à equipe reduzida e à sobrecarga de trabalho com esforços para restabelecimento da infraestrutura informática, somadas às diversas requisições de informação, o documento foi inserido no processo incorreto,

mas que, percebido o erro, iniciou imediatamente as providências para envio do relatório atualizado para a ANPD. Acrescentou que, após o envio da defesa, foi anexado ao processo de CIS o Formulário de Comunicação de Incidente Complementar (SEI nº 0045653), em 06/04/2022, nos termos requeridos pela ANPD.

7.45. Soma-se a isso o fato de que o Ministério passou por grandes dificuldades no contexto da pandemia do COVID 19. "É cediço que a dimensão da emergência sanitária, o cenário político-cultural e a crise de gerenciamento, com diversas mudanças de Ministros, tornaram ainda maiores os desafios da Pasta em 2020 e 2021".

7.46. Por fim, a autuada também suscitou a observância, pela ANPD, de uma atuação responsiva, conforme previsto no Regulamento de Fiscalização e no Regulamento de Dosimetria, além da ponderação do princípio da proporcionalidade, diante das medidas adotadas pela Pasta, de forma a afastar a aplicação da sanção no caso.

Análise dos fatos à luz da defesa

7.47. O art. 48 da LGPD determina que cabe ao controlador comunicar à ANPD e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Nos termos do §1º do mencionado artigo, a comunicação deverá ser feita em prazo razoável. Ainda que a regulamentação do prazo para a comunicação do incidente estivesse pendente à época dos fatos, o §2º do art. 48 da LGPD confere à ANPD o poder de determinar ao controlador providências para a salvaguarda dos direitos dos titulares, tais como medidas para reverter ou mitigar os efeitos do incidente e a ampla divulgação do fato em meios de comunicação.

7.48. No caso em comento, a autuada notificou o incidente ao DPF (SEI nº 0048862) e ao GSI imediatamente após o ocorrido (SEI nº 0048863). Entretanto, o MS alega que o entendimento à época era de que a ANPD somente deveria ser notificada em caso de acesso não autorizado a dados pessoais. No dia seguinte ao ataque, por meio do Ofício nº 132/2021/CGF/ANPD/PR (SEI nº 0048902), a ANPD informou da necessidade de comunicação do incidente à Autoridade e aos titulares, nos termos do art. 48 da LGPD. Solicitou-se que o envio da Comunicação de Incidente de Segurança (CIS) Preliminar fosse realizado no prazo recomendado de 2 (dois) dias úteis, contados da data de ciência do incidente. E facultou que as informações não disponíveis no momento fossem encaminhadas no prazo de até 30 dias corridos, por meio de comunicação complementar.

7.49. Em sua resposta, datada de 06/01/2022 (SEI nº 0048913), o MS trouxe informações elaboradas pelo Departamento de Informática do Sistema Único de Saúde - DATASUS/SE/MS e pela COSEGI. Embora não tenha utilizado o formulário padrão e seguido as instruções fornecidas pelo site da ANPD

[conforme instruído em ofício (SEI nº 0048902)], o MS apresentou informações preliminares acerca das circunstâncias do incidente sofrido, esclarecendo, por exemplo, que não se tratava de um ataque de *ransomware*, e que não havia evidências de violação ou exfiltração de dados. Ainda, o MS informou que havia adotado medidas e controles administrativos, lógicos e físicos para restabelecer os sistemas e mitigar novos incidentes, mas não forneceu maiores detalhes. Argumentou que, em razão da alocação de toda a equipe nas tarefas para a retomada dos sistemas, responderia com "maiores certezas" em 30 dias corridos (SEI nº 0048913).

7.50. Diante da lacuna de informações, em 13/01/2022 (E-mail SEI nº 0048919), e, portanto, transcorridos mais de 30 dias do incidente, a ANPD enviou novo ofício (SEI nº 0048914) acompanhado do Aviso 001/2022 (SEI nº 0048851). Isso porque, conforme mencionado anteriormente [Item 5.7], a manifestação do MS (SEI nº 0048913) não atendeu material e formalmente aos termos do art. 48 da LGPD: não houve apresentação da Comunicação do Incidente de Segurança e da comprovação de comunicação aos titulares, tampouco foi apresentado o relatório de tratamento de incidente com evidências técnicas acerca da ocorrência ou não da extração ou perda de dados pessoais. A referida Medida Preventiva estabeleceu o prazo de trinta dias, a contar da data do recebimento pelo MS, para que as determinações contidas no documento fossem cumpridas.

7.51. Conforme mencionado anteriormente [Item 6.13], a manifestação do MS em resposta ao Aviso apenas foi conhecida em 23/03/2022, com a apresentação da Defesa Administrativa [Nota Técnica 3/2022-CGMA/DEMAS/SE/MS (SEI nº 0048852) e anexos]. De acordo com a peça, as determinações do Aviso foram respondidas por meio dos documentos Nota Técnica nº 5/2022-COSEGI/CGGOV/DATASUS/SE/MS (SEI nº 0048865), Anexo Lista de aplicações AWS, Anexo Defacement MS, (Anexo_Evidencias_Incidente_Nuvem) e Anexo Comunicado PF.

7.52. Embora as informações não tenham sido prestadas no formato indicado pela CGF, por meio de formulário apropriado, é necessário reconhecer que os documentos apresentados continham o detalhamento requerido acerca do incidente de segurança. Com efeito, a Nota Técnica nº 5/2022-COSEGI/CGGOV/DATASUS/SE/MS (SEI nº 0048865), assinada em 10/02/2022 e, portanto, antes da instauração deste PAS, traz informações abrangentes acerca do ataque sofrido. O documento descreve detalhadamente o incidente, relata as causas, as ações provocadas pela conta suspeita, os sistemas e dados pessoais afetados, os riscos identificados, as medidas de contenção adotadas, as medidas de segurança, técnicas e administrativas tomadas, além das oportunidades de melhoria identificadas. Adicionalmente, os anexos trazem evidências técnicas e relatórios que analisam os logs dos dispositivos, identificando as atividades suspeitas. Além

disso, cabe registrar que, após a instauração deste processo administrativo sancionatório, os formulários de comunicação de incidente de segurança com dados pessoais à ANPD, parcial e complementar, foram juntados ao processo de CIS (SEI nº 0045645 e 0045651, respectivamente). Também vale dizer que a defesa juntou a Nota Técnica 10/2022-COSEGI/CGGOV/DATASUS/SE/MS (SEI nº 0048855), que complementou as informações da Nota Técnica nº 5, apresentada anteriormente.

7.53. Diante desse contexto, é imperioso admitir que, caso a CGF tivesse tomado conhecimento desses documentos à época em que foram produzidos e protocolados em outro processo, provavelmente o Auto de Infração que originou o presente PAS não apontaria, como possível violação, a falta de notificação à ANPD acerca do incidente. Por outro lado, **os documentos então apresentados [Item 7.51] não fazem qualquer alusão à comunicação dos titulares de dados afetados.** Com efeito, a referida Nota Técnica nº 5/2022-COSEGI/CGGOV/DATASUS/SE/MS (SEI nº 0048865) apenas menciona, no item 4.6, que "A responsabilidade de notificação aos titulares de dados pessoais que foram afetados pelo incidente, por meio de notificação pública e direta não é competência desta Coordenação de Segurança da Informação - COSEGI". Ou seja, ainda que se considerasse atendida a obrigação contida no Aviso acerca da obrigatoriedade de notificação do incidente de segurança à ANPD, o fato de a regulada não ter apresentado comprovação de que os titulares de dados teriam sido igualmente informados, nos termos do art. 48 da LGPD, não afastaria a instauração do presente PAS com base na possível infringência desse artigo.

7.54. Entretanto, com a apresentação da defesa da autuada, por meio de Nota Técnica e anexos [Item 7.51], restou claro que a comunicação aos titulares foi efetuada amplamente, embora a regulada tenha juntado elementos comprobatórios dessa comunicação apenas nesse momento processual. Com efeito, o anexo Nota Oficial Site MS (SEI nº 0048864) apresenta uma sequência de comunicados oficiais à população, iniciados às 8h50min do dia 10/12/2021, portanto horas após o ataque, esclarecendo as circunstâncias do incidente, os sistemas afetados, as alternativas disponíveis para acessar os serviços, bem como atualizações sobre a retomada das plataformas informáticas. Os comunicados foram disponibilizados não somente no site do ministério, mas também veiculados em outros canais oficiais da Pasta, como Youtube e Instagram, ampliando o alcance da informação.

7.55. Em que pesem os comunicados não mencionarem todos os elementos estabelecidos pelo art. 48, §1º, da LGPD, entende-se que, em razão da natureza do incidente, que implicou a indisponibilidade de serviços, e não o vazamento, a violação ou a exfiltração de dados pessoais, não houve prejuízo aos usuários. Isso porque a comunicação ao titular se presta,

sobretudo, para que este possa adotar as devidas precauções e salvaguardas em relação aos dados afetados, evitando, por exemplo, fraudes e outras ações delituosas. No caso em tela, não foram identificados riscos em relação aos dados pessoais, que foram integralmente recuperados sem que houvesse qualquer acesso indevido. Registre-se, de todo modo, que tal fato não torna o incidente menos gravoso.

7.56. Do exposto, tendo em vista que a regulada (i) elaborou Nota Técnica com os esclarecimentos sobre o incidente, apresentando as informações requeridas no Formulário de CIS, o que não foi conhecido pela ANPD à época devido ao erro material já relatado e (ii) comunicou amplamente o incidente aos titulares afetados, por meio de múltiplos canais da Pasta, **fica afastada, assim, a infração ao art. 48 da LGPD**.

CONDUTA: não apresentar RIPD após solicitação da ANPD - art. 38 da LGPD

Defesa apresentada pela autuada

7.57. Conforme mencionado, por meio do Ofício nº 2/2022/CGF/ANPD/PR (SEI nº 0048914), de 13/01/2022, a ANPD ponderou que as informações prestadas pelo MS, até aquele momento, acerca do incidente ora analisado não haviam atendido material e formalmente o requisitado no Ofício nº 132/2021/CGF/ANPD/PR (SEI nº 0048902). Por esse motivo, a Autoridade emitiu o Aviso 0001/2022 (SEI nº 0048851), solicitando, dentre outras providências, a apresentação do "Relatório de impacto à proteção de dados pessoais, inclusive caso envolva dados sensíveis, referente a suas operações de tratamento no caso sob fiscalização", conforme disposto no art. 38 da LGPD.

7.58. Em sua Defesa Administrativa (SEI nº 0048852, item 3.4.2), a autuada alegou que todas as determinações contidas no referido Aviso foram atendidas por meio da Nota Técnica nº 5/2022-COSEGI/CGGOV/DATASUS/SE/MS e anexos (Despacho COSEGI, SEI nº 0048882, item 10).

7.59. A Defesa relatou, ainda, que o MS tem dedicado esforços para elaboração dos RIPDs referentes a seus sistemas, e que isso poderia ser constatado da leitura da Nota Técnica nº 10/2022-COSEGI/CGGOV/DATASUS/SE/MS (SEI nº 0048855), que complementou as informações relativas ao incidente de segurança inicialmente apresentadas por meio da Nota Técnica nº 5 referenciada acima. O documento destaca que a elaboração dos RIPDs estaria prevista no contexto do Plano de Transformação Digital, firmado com a então Secretaria de Governo Digital do Ministério da Economia – SGD/ME. Acrescentou que, com o apoio da SGD/ME, foram elaborados os RIPDs para os sistemas SNT (SEI nº 0048858) e SISREG (SEI nº 0048859), e que o objetivo seria implementar as ações também nos demais

sistemas considerados críticos no Ministério da Saúde.

7.60. Segundo a Nota Técnica nº 10 (SEI nº 0048855, fl. 14 e 15):

> O DATASUS enquanto órgão do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP, tem participado de discussões e seguido as orientações dispostas no Guia de Boas Práticas da LGPD, para implementação na Administração Pública Federal, divulgado pela Secretaria de Governo Digital do Ministério da Economia. Além disso, atualmente está em andamento no DATASUS, a repactuação do Plano de Transformação Digital entre o MS com a SEME/PR e SGD/ME, Processo SEI 25000.146333/2021-48, relacionado ao Eixo - Segurança e Privacidade de Dados nos sistemas onde o objetivo é implementar as ações dos seis sistemas considerados críticos no Ministério da Saúde, a saber: SISREG, SNT, SIVEP-Gripe, e-SUS Notifica, HEMOVIDA e e-SUS AF, conforme detalhamento disposto abaixo:

EIXO – SEGURANÇA E PRIVACIDADE DE DADOS		
AÇÕES	**SECRETARIA/DIRETORIA**	**SITUAÇÃO**
SISREG Inventário de dados; Termos de Uso / Política de Privacidade; Gestão de Riscos e Implementação de Controles; Relatório de Impacto.	SGD / DATASUS	Abril/2022
SNT Inventário de dados; Termos de Uso / Política de Privacidade; Gestão de Riscos e Implementação de Controles; Relatório de Impacto.	SGD / DATASUS	Abril/2022
SIVEP-Gripe Inventário de dados; Termos de Uso / Política de Privacidade; Gestão de Riscos e Implementação de Controles; Relatório de Impacto.	SGD / DATASUS	Dezembro/2022
e-SUS Notifica Inventário de dados; Termos de Uso / Política de Privacidade; Gestão de Riscos e Implementação de Controles; Relatório de Impacto.	SGD / DATASUS	Dezembro/2022
HEMOVIDA Inventário de dados; Termos de Uso / Política de Privacidade; Gestão de Riscos e Implementação de Controles;	SGD / DATASUS	Dezembro/2022

Relatório de Impacto.		
e-SUS AF Inventário de dados; Termos de Uso / Política de Privacidade; Gestão de Riscos e Implementação de Controles; Relatório de Impacto.	SGD / DATASUS	Dezembro/2022

7.61. Ou seja, além dos dois RIPDs já apresentados, o planejamento previa a elaboração dos RIPDs referentes a mais quatro sistemas considerados críticos pelo MS até dezembro de 2022.

7.62. Em Alegações Finais (SEI nº 0098401), a autuada retomou as informações prestadas em sede de Defesa Administrativa, reiterando o compromisso de implementar os relatórios referentes aos sistemas mais críticos do MS, no contexto do Plano de Transformação Digital firmado com a Secretaria de Governo Digital do Ministério da Economia – SGD/ME. Destacou a instituição do Grupo de Trabalho para Implementação da LGPD (GTLGPD), que, dentre as entregas, prevê a formulação de um plano de ação para implementação da LGPD na Pasta e a discussão das diretrizes para elaboração dos RIPDs. Por fim, enumerou as medidas implementadas pelo MS que demonstrariam o compromisso da nova gestão com a temática da LGPD, e suscitou a aplicação do princípio da proporcionalidade.

Subsunção do fato ao tipo infracional correspondente

7.63. O art. 38 da LGPD prevê a possibilidade de a ANPD *requisitar* relatório de impacto à proteção de dados pessoais (RIPD) aos regulados. Nos termos do art. 5º, XVII, da LGPD, o RIPD é o documento elaborado pelo 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. Este documento foi expressamente solicitado por esta CGF no Aviso 0001/2022 (SEI nº 0048851). Ainda, conforme consignado no item 5.16 da Nota Técnica nº 18/2022/CGF/ANPD (SEI nº 0048839), a determinação de confecção do RIPD pela ANPD advém da necessidade de compreensão do processo de tratamento de dados efetuado pelo órgão. Note-se que, à época da emissão do Aviso e da elaboração da Nota Técnica 18, esta CGF não tinha conhecimento da totalidade dos sistemas que teriam sido impactados pelo ataque, uma vez que a notificação completa do incidente somente ocorreu por ocasião da Defesa Administrativa. No entanto, a requisição contida no Aviso estabelece que deveria ser apresentado o RIPD referente a **suas operações de tratamento no caso sob fiscalização, ou seja, todos os sistemas afetados pelo incidente em tela.**

7.64. Inicialmente, é preciso esclarecer que, embora a autuada alegue

que todas as determinações contidas no Aviso 001/2022 foram atendidas por meio da Nota Técnica nº 5/2022-COSEGI/CGGOV/DATASUS/SE/MS e anexos (Despacho COSEGI, SEI nº 0048882, item 10) tais documentos não apresentaram quaisquer RIPDs. Na realidade, a mencionada Nota Técnica alegou que:

> (...) A elaboração do Relatório de Impacto à Proteção de Dados não é de competência da ETIR/MS, contudo, os riscos foram identificados, remediados e implementado (sic) ações de melhorias na prevenção de novos incidentes similares ao ocorrido. (SEI nº 0048865 fl. 4)

7.65. Apenas em 22/03/2022, já em sede de Defesa Administrativa no presente PAS, a autuada apresentou os RIPDs relativos aos sistemas SNT e SISREG, além do cronograma para elaboração dos relatórios pertinentes aos demais sistemas considerados mais críticos pelo MS, no contexto do Plano de Transformação Digital [Item 7.59] e [Item 7.60].

7.66. Já em Alegações Finais (SEI nº 0098401), a autuada se ateve a retomar os resultados já apresentados em sede de Defesa, sustentou o modelo de fiscalização responsiva e aduziu a aplicação do princípio da proporcionalidade, tendo em vista as medidas adotadas e os compromissos assumidos para adequação da Pasta à LGPD. Ou seja, embora o cronograma apresentado pela autuada tenha previsto a elaboração dos RIPDs relativos aos sistemas SIVEP-Gripe, e-SUS Notifica, HEMOVIDA, e-SUS AF para dezembro de 2022 [Item 7.60], não houve, até o momento, a apresentação dos referidos documentos.

7.67. Destaque-se que, conforme o referido Aviso, a regulada deveria apresentar Relatório de Impacto à Proteção de Dados Pessoais referente **a suas operações de tratamento no caso sob fiscalização**. Como se sabe, o processo em tela derivou de um incidente de segurança que afetou uma série de sistemas ou operações de tratamento da autuada. Isto posto, **a apresentação dos RIPDs referentes apenas aos sistemas SNT e SISREG não atende às determinações desta ANPD**, sobretudo considerando-se o cronograma apresentado, que previa a conclusão dos trabalhos em dezembro de 2022 [Item 7.60].

7.68. **Diante do exposto, resta caracterizada a infração ao art. 38 da LGPD, em razão da não apresentação de todos os RIPDs pertinentes após solicitação da ANPD**. Para além dos RIPDs dos sistemas SNT e SISREG, enviados em sede de Defesa Administrativa, resta à autuada apresentar os relatórios referentes aos sistemas SIVEP-Gripe, e-SUS Notifica, HEMOVIDA, e-SUS AF, bem como aqueles que concernem aos sistemas CADSUS, SGOP, SIPNI, NOTIFICA, RNDS, CONECTESUS e CORONAVIRUSUS, afetados pelo incidente.

Classificação da infração

7.69. Conforme relatado acima, a autuada incorreu em violação ao disposto no art. 38 da LGPD. Necessário, então, classificar a infração como leve, média ou grave, conforme indica o art. 8º do Regulamento de Dosimetria [Item 7.25].

7.70. Cabe repisar que a infração em análise não se confunde com o incidente propriamente, que resultou na indisponibilidade de sistemas informáticos, impedindo o exercício de direitos e a utilização de serviços essenciais à população. Sendo assim, no presente caso, não há indícios de que a infração em si – a não apresentação do RIPD – tenha afetado significativamente os interesses e direitos fundamentais dos titulares de dados, prejudicado ou agravado a situação desses titulares. Portanto, não se verifica, no caso em tela, a condição estabelecida no art. 8º, § 2º para que a infração seja considerada grave, posto que seria necessário constatar essa hipótese cumulativamente com ao menos uma das demais hipóteses elencadas no art. 8º, § 3º, I.

7.71. No que tange às hipóteses do art. 8º, 3º, I do Regulamento de Dosimetria tampouco é possível constatar que a infração cometida atende aos requisitos de quaisquer alíneas, uma vez que a produção do Relatório em si não se confunde com o incidente e, portanto, não contempla tratamento de dados pessoais. Adicionalmente, no caso concreto, a não apresentação do RIPD é infração autônoma e não obstruiu a atividade de fiscalização por não ter impedido a apuração do incidente de segurança, dessa forma, não se verifica, igualmente, a hipótese do art. 8º, 3º, II do Regulamento de Dosimetria.

7.72. Diante disso, conclui-se que a infração atende ao disposto no art. 8º, § 1º, "A infração será considerada leve quando não verificada nenhuma das hipóteses relacionadas nos §§ 2º ou 3º deste artigo".

7.73. **Isto posto, a infração ao art. 38 da LGPD, no presente caso, fica configurada como leve.**

Definição do tipo de sanção administrativa

7.74. Para a definição do tipo de sanção adequada, o art. 10º, I, do Regulamento de Dosimetria indica ser aplicável multa simples quando "o infrator não tenha atendido as medidas preventivas ou corretivas a ele impostas, dentro dos prazos estabelecidos, quando aplicável". Como visto, ainda que tenha ocorrido um equívoco no protocolo da resposta ao Aviso 0001/2022 (SEI nº 0048851) (Medida Preventiva), tal manifestação não contemplou a apresentação dos RIPDs relativos ao tratamento de dados efetuado pela regulada e afetados pelo incidente, verificando-se, portanto, a condição do art. 10º, I. No entanto, o art. 52, §3º, da LGPD, ao estabelecer as sanções que podem ser impostas a entidade ou a órgãos públicos, afasta, por

omissão, a possibilidade de aplicação de multa ou de multa diária a esses agentes de tratamento. Vale registrar, também, que a aplicação das sanções previstas nas Seções VIII, IX, X, XI e XII do Regulamento de Dosimetria não são adequadas, em razão do interesse público que justifica o tratamento de dados.

7.75. Por outro lado, o Regulamento de Dosimetria define, em seu art. 9º, que a advertência pode ser aplicada quando a infração for leve ou média, ou quando houver necessidade de imposição de medida corretiva. Essa hipótese se aplica à presente infração, tendo em vista a classificação da gravidade como leve e a necessidade de determinar à autuada que apresente os RIPDs cuja elaboração foi prevista no Plano de Transformação Digital, com conclusão estimada para dezembro de 2022 [Item 7.60], em atenção ao disposto no art. 38 da LGPD.

7.76. Em que pese a constatação do equívoco cometido pela autuada ao protocolar sua resposta ao Aviso 0001/2022 (SEI nº 0048851) em processo diverso [Item 6.16], a manifestação não atendeu materialmente à determinação para apresentar o RIPD referente ao tratamento de dados efetuado [Item 7.12]. Identifica-se, portanto, a ocorrência de uma circunstância agravante, nos termos do art. 32, §2º, II, do Regulamento de Fiscalização. Por outro lado, a infração foi parcialmente cessada com a apresentação do RIPD para dois dos sistemas críticos, e a apresentação de cronograma para conclusão dos demais, de forma célere, após a instauração do PAS e antes da decisão de primeira instância [Item 7.65], o que demonstra a adoção de medida corretiva pelo controlador com o objetivo de sanar a conduta ilícita e de implementar procedimentos internos voltados ao tratamento seguro e adequado de dados, em consonância com a LGPD. A autuada não se furtou a reconhecer a falha, e buscou corrigi-la durante o trâmite do processo administrativo sancionador, o que proporcionou um diálogo mais efetivo e responsivo junto à ANPD.

7.77. **Aplica-se, portanto, a sanção de advertência, cumulada com medida corretiva.**

Definição da medida corretiva

7.78. Tendo em vista o relatado acima, impõe-se as seguintes medidas corretivas:

> a) Apresentar, **no prazo de 10 (dez) dias úteis da data de intimação da decisão do Despacho Decisório**, o Relatório de Impacto de Proteção de Dados dos sistemas considerados críticos pelo Ministério da Saúde, conforme apresentado na alínea e), do item 3.1, da Nota Técnica nº 10/2022-COSEGI/CGGOV/DATASUS/SE/MS (SEI nº 0048855): SIVEP-Gripe, e-SUS Notifica, HEMOVIDA, e-SUS AF, cuja previsão de

conclusão, segundo o cronograma divulgado pela autuada, seria dezembro de 2022.

b) Apresentar, **no prazo de 10 (dez) dias úteis da data de intimação da decisão do Despacho Decisório**, o Relatório de Impacto de Proteção de Dados dos demais sistemas afetados pelo incidente de segurança que originou o presente Processo Administrativo Sancionador – caso ainda estejam operacionais -, conforme apresentado no item 3.1 da Nota Técnica nº 10/2022-COSEGI/CGGOV/DATASUS/SE/MS (SEI nº 0048855), e item 7.68 deste Relatório de Instrução: CADSUS, SGOP, SIPNI, NOTIFICA, RNDS, CONECTESUS e CORONAVIRUSUS.

c) Alternativamente, caso os RIPDs mencionados nas alíneas a) e b) acima não tenham sido concluídos até a presente decisão, apresentar, **no prazo de 10 (dez) dias úteis da data de intimação da decisão do Despacho Decisório,** cronograma de elaboração dos documentos para cada um dos sistemas. O prazo de cumprimento de todas as etapas previstas no cronograma não deverá ultrapassar 180 (cento e oitenta) dias, contados da data de intimação do Despacho Decisório.

DA INAPLICABILIDADE DA PRESERVAÇÃO REPUTACIONAL DO ÓRGÃO; DO PRINCÍPIO DA INTRANSCENDÊNCIA SUBJETIVA PARA O AFASTAMENTO DAS SANÇÕES E DO PRINCÍPIO DA PROPORCIONALIDADE NA APLICAÇÃO DAS SANÇÕES

7.79. A aplicação das sanções indicadas nos tópicos anteriores decorre da própria leitura do art. 52, da LGPD, ao sujeitar os agentes de tratamento aos tipos de sanções discriminadas no referido artigo, quando verificadas infrações cometidas às normas da LGPD. No caso presente, foram esclarecidos todos os fatos e evidências que levaram à conclusão das violações ao art. 23, II e ao art. 38, da LGPD.

7.80. Por outro lado, reconheceu-se que a aparente inércia da autuada, que poderia ensejar uma sanção por violação do art. 5º do Regulamento de Fiscalização, não passou de mero erro material. Além disso, afastou-se a infringência do art. 48, uma vez constatada a comunicação do incidente de segurança à ANPD, ainda que tardiamente e sem o uso de formulário próprio; e a ampla comunicação do incidente para os titulares em geral, mesmo que a comprovação de tal publicização tenha ocorrido apenas por ocasião da Defesa Administrativa.

7.81. Para além disso, não se vislumbra viável, como requerido pelo MS, o afastamento de sanções que recaem sobre condutas violadoras às

previsões da LGPD sob o argumento de que o infrator poderá suportar efeitos reputacionais negativos. Conforme já demonstrado por esta Autoridade em decisão anterior relativa à autuada (Relatório de Instrução nº 4/2024/FIS/CGF, SEI nº 0136258, Processo 00261.001882/2022-73), além de as sanções apresentarem seus vieses preventivo, educativo, repressivo e dissuasório, no presente caso, os efeitos das sanções cumuladas com as medidas corretivas sobrepujam o efeito reputacional negativo para o autuada. Isso porque as sanções visam estimular a observância ao princípio da responsabilização e prestação de contas (art. 6º, X, da LGPD), bem como propiciar o exercício da autodeterminação informativa dos titulares (art. 2º, II, da LGPD), elementos pilares do direito à proteção de dados pessoais.

7.82. Na realidade, a aplicação da sanção e o consequente reconhecimento da ocorrência das infrações pelo Ministério da Saúde são uma oportunidade para que a autuada demonstre as medidas de adequação técnicas e administrativas adotadas (ou em curso) posteriormente ao incidente, o que poderá causar o efeito oposto ao suscitado.

7.83. De forma complementar a todos os argumentos expostos, tampouco aplica-se, no caso em concreto, a razão fundamental do princípio da intranscendência subjetiva, como arguido pela autuada. Conforme assentado no precedente citado [Item 7.81], cabe destacar que o referido princípio foi aplicado pelo Supremo Tribunal Federal (STF) e pelo Superior Tribunal de Justiça (STJ) em contextos diversos da presente hipótese, importando em medidas restritivas a recursos financeiros/participações em convênios, entre outras consequências decorrentes da inscrição de ente federativo em cadastros de inadimplentes[6].

7.84. Ademais, conforme indicado em precedente desta Autoridade (item 7.81), o recente entendimento do STF[7] é de que tampouco tal previsão deve ser acolhida em casos de mudança de gestão governamental. Destaque-se que, no voto proferido pelo Ministro Gilmar Mendes no julgamento da ACO 2745/DF, foi ressaltado que a aplicação do princípio da intranscendência subjetiva tratar-se-ia de hipótese antirrepublicana e incoerente ao Estado de Direito.

7.85. Importa mencionar que o posicionamento recente do STF escora o entendimento desta Autoridade na medida em que a responsabilidade das infrações recai sobre a pessoa jurídica na qualidade de **controladora dos dados pessoais**, **não sobre as "pessoas naturais que integram a pessoa jurídica e cujos atos expressam a atuação desta",** como explicitado no Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, publicado em abril de 2022[8]. Desta forma, no âmbito de competência da ANPD, neste caso, cabe a esta Autoridade aplicar sanções à pessoa jurídica considerada como controladora, o Ministério da Saúde, não à

gestão ou gestores do Ministério quando da ocorrência da infração.

7.86. Com efeito, a relação jurídica do controlador com o titular não termina, necessariamente, com a mera alteração de gestão governamental. Entendimento diverso pressuporia que os direitos dos titulares de dados fossem restringidos a cada troca de governo. Não foram demonstradas, no caso em concreto, e em razão das sanções a serem aplicadas, restrições que pudessem prejudicar a execução de políticas públicas, como outrora suscitados em julgados dos referidos Tribunais Superiores. Ao contrário, conforme supracitado [Item 7.82], há efeitos benéficos aos titulares de dados, que decorrerem da postura do autuada frente às determinações exaradas durante o processo de fiscalização prévio e presente sancionador.

7.87. Alinhado a isso, a garantia da persecução do interesse público e da finalidade pública também foram preservados no caso, ao contrário do que faz crer o autuada ao afirmar que a aplicação da sanção em 2024 por infração ocorrida em 2021, em "outro Governo", não seria razoável, violando-se o art. 39, VI, do Regulamento de Fiscalização. Isso porque a interpretação dos dispositivos deve considerar a observância do interesse público primário sobre o interesse público secundário. Conforme suscitado no Relatório de Instrução nº 01/2024/CGF/ANPD (SEI nº 0053354), e reiterado no Relatório de Instrução nº 4/2024/FIS/CGF (SEI nº 0136258), esta CGF já esclareceu que o interesse público primário, como interesse de toda a sociedade, é o próprio parâmetro para a ponderação, em oposição ao interesse público secundário, interesse este último que o autuada pretende proteger ao defender o afastamento da sanção tendo em vista o transcurso do tempo, a potencial desconfiança da população e a mudança de gestão governamental.

7.88. Diante do exposto, não há que se falar em inaplicabilidade das sanções à pessoa jurídica do MS, em razão de i) potenciais efeitos reputacionais à autuada e ii) atos praticados por gestão diversa da presente, tendo em vista que não foram suscitados argumentos e provas capazes de afastar a autoria e materialidade do autuada das violações ao art. 23, III e ao art. 38, da LGPD.

7.89. Por fim, não se pode, tampouco, afastar a aplicação das sanções com base no princípio da proporcionalidade no exercício da atividade fiscalizatória responsiva, conforme suscitado pela autuada em suas Alegações Finais (SEI nº 0098401), sobretudo quando a própria aplicação das sanções já considerou a observância do princípio da proporcionalidade.

7.90. Conforme prevê o Regulamento de Fiscalização, a atuação responsiva da Autoridade considera a postura dos agentes regulados e os riscos identificados para a adoção de medidas proporcionais – dentre elas, a aplicação de sanções.

7.91. Quanto à postura da autuada, percebe-se que este falhou em colaborar com a Autoridade, na medida em que as demandas do regulador não foram atendidas a contento e, portanto, escalaram gradualmente para instrumentos mais interventivos. Em que pese o equívoco cometido no protocolo da resposta ao Aviso, foi possível constatar que essa manifestação não atendeu integralmente ao requerido, o que levaria, de toda forma, à instauração do presente PAS - que concluiu pela configuração das infrações ao art. 23, III e at. 38.

7.92. No que tange aos riscos identificados, restou evidente que a ausência de Encarregado pelo tratamento de dados pessoais designado pelo controlador prejudicou a interlocução com esta Autoridade e dificultou a obtenção de informações na completude necessária e de forma célere. Tanto que o formulário de CIS no formato requerido somente foi protocolado em 23/03/2022, e a comprovação da comunicação com o titular somente foi apresentada por ocasião da Defesa Administrativa. Já a ausência dos RIPDs prejudicou a adequada avaliação da Autoridade – e do próprio controlador - acerca dos processos de tratamento de dados pessoais envolvidos, bem como dos riscos associados. Consequentemente, não se pôde avaliar a adequação das medidas, salvaguardas e mecanismos de mitigação de riscos que poderiam ser adotados em caso de incidente de segurança.

7.93. Dito isso, entende-se que **a gravidade das infrações constatadas é proporcional à aplicação da sanção de advertência, frise-se, a mais branda dentre as previstas no art. 52, da LGPD**. Este posicionamento já foi explicitado, inclusive, na Análise de Impacto Regulatório que precedeu o Regulamento de Dosimetria - Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023.

ADOÇÃO DE MEDIDAS PARA ADEQUAÇÃO À LGPD

7.94. Conforme indicado na Nota Técnica 10/2022-COSEGI/CGGOV/DATASUS/SE/MS (SEI nº 0048855), que acompanhava a Defesa Administrativa, o MS informou ter implementado diversas medidas para corrigir a falha e retomar os serviços à população. Também foram identificadas e endereçadas várias oportunidades de melhoria com o intuito de evitar novas falhas. Além disso, há diversas ações de planejamento e governança em curso, com o objetivo de ajustar todas as políticas e ações de segurança da informação à LGPD, a fim de mitigar as ocorrências de incidentes como o ora analisado.

7.95. Ademais, em Alegações Finais (SEI nº 0098402), a autuada informou que foram implementadas seis medidas administrativas relacionadas à proteção de dados na Pasta (i) criação da Secretaria de Informação e Saúde Digital no Ministério da Saúde; ii) designação de nova Encarregada de Dados e publicação no sítio eletrônico; iii) criação de Grupo de Trabalho para tratar especificamente sobre a LGPD; iv) obtenção de assento

para futura composição no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD); v) realização da 1º Jornada de Proteção de Dados Pessoais no SUS, vi) adoção do Programa de Privacidade e Segurança da Informação (PPSI), e que mais uma medida estaria em andamento, relacionada à capacitação para servidores das unidades descentralizadas do MS e do SUS, conforme descrito nos tópicos de A) a G) do item 3.9 das Alegações Finais (SEI nº 0098402).

7.96. Reconhecendo-se os esforços empreendidos pela autuada para mitigar as falhas e retomar os serviços à população, o empenho do órgão para manter um Encarregado de dados designado e para elaborar os RIPDs dos sistemas críticos, bem como as providências já adotadas e em andamento quanto a mecanismos administrativos e técnicos; consideram-se ausentes a conveniência e oportunidade de encaminhar notícia ao órgão de controle interno da autuada para apuração de eventual falta funcional, nos termos do art. 55-J, XXII, da LGPD.

8. CONCLUSÃO

8.1. Ante o exposto, considerando que o conjunto probatório nos autos demonstra a autoria e a materialidade dos fatos descritos, e que estes correspondem às infrações tipificadas pelos enquadramentos indicados no Auto de Infração nº 8/2022/CGF/ANPD (SEI nº 0050494) - afastadas as infrações ao art. 5º do Regulamento de Fiscalização e ao art. 48 da LGPD -, conclui-se pelas seguintes recomendações:

8.1.1. Por violação ao art. 23, III, da LGPD, a aplicação da sanção de ADVERTÊNCIA ao Ministério da Saúde, sem a imposição de medida corretiva, nos termos dos itens [Item 7.33] a [Item 7.38] deste Relatório de Instrução.

8.1.2. Por violação ao art. 38 da LGPD, a aplicação da sanção de ADVERTÊNCIA ao Ministério da Saúde, com a imposição de duas medidas corretivas (com a possibilidade de adoção de uma medida corretiva alternativa) nos termos dos itens [Item 7.74] a [Item 7.78] deste Relatório de Instrução.

8.2. Por fim, é importante registrar que a classificação das infrações, a definição das sanções, inclusos parâmetros e critérios, e a adoção de medidas corretivas restringem-se às circunstâncias deste caso em concreto. Tais decisões não vinculam, naturalmente, a análise e o posicionamento da CGF em futuros processos sancionadores.

9. ENCAMINHAMENTOS

9.1. O presente Relatório de Instrução deve ser encaminhado ao Coordenador-Geral de Fiscalização para decisão, de acordo com art. 55 do Regulamento de Fiscalização.

9.2. Após proferida a decisão, a autuada deverá ser intimado para cumprimento da sanção e/ou apresentação de recurso, em até 10 dias úteis, em consonância com o art. 58 do Regulamento de Fiscalização.

9.3. A decisão deve ser publicada no DOU, segundo o art. 55 do Regulamento de Fiscalização.

9.4. Após trânsito em julgado, este Processo Administrativo Sancionador deverá ser encaminhado para a fase de cumprimento da decisão para acompanhamento das obrigações de fazer determinadas.

À consideração superior.

ULLIANA CERVIGNI MARTINELLI
Servidora em Exercício Descentralizado

De acordo. Encaminhe-se.

JORGE ANDRÉ FERREIRA FONTELLES DE LIMA
Coordenador de Fiscalização

_____

[1] Conforme publicizado no site do Ministério da Saúde e colacionado aos autos (SEI nº 0098402). Disponível em: https://www.gov.br/saude/pt-br/acesso-a-informacao/lgpd/encarregado-pelo-tratamento-de-dados-pessoais. Acesso em 29/10/2024.

[2] Conforme publicizado no site do Ministério da Saúde e colacionado aos autos (SEI nº 0098402). Disponível em: https://www.gov.br/saude/pt-br/acesso-a-informacao/lgpd/encarregado-pelo-tratamento-de-dados-pessoais. Acesso em 29/10/2024.

[3] É importante registrar que, embora o MS tenha protocolado uma resposta ao Aviso tempestivamente, mas em processo equivocado, ela, por si só, não seria suficiente para endereçar todos os pontos levantados na Medida Preventiva. Por esse motivo, ressalta-se que o presente Processo Administrativo Sancionador seria instaurado de toda maneira, em função de outras irregularidades que não foram sanadas no Processo de Fiscalização anterior, conforme será abordado em maiores detalhes ao longo do presente Relatório de Instrução.

[4] Disponível em https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Acessado em 23/09/2024.

[5] Art. 10. A ANPD aplicará a sanção de multa simples quando: I - o infrator não tenha atendido as medidas preventivas ou corretivas a ele impostas, dentro dos prazos estabelecidos, quando aplicável; II - a infração for

classificada como grave;

[6] Os julgados colacionados pela autuada, inclusive, referem-se a casos desta situação (itens 3.37 e 3.38 das Alegações Finais [SEI nº 0098399]).

[7] Vide: STF, DJ 16 mar. 2022, ACO 3090 AGR/DF, Voto do Rel. Min. Roberto Barroso; STF, DJ 01 out. 2020, ACO 3402/DF, Rel. Min. Alexandre de Moraes; STF, DJ 17 set. 2020, ACO 3083/DF, Rel. Min. Ricardo Lewandowski.

[8] Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf. Acesso em 30 abr. 2024.

Documento assinado eletronicamente por **Ulliana Cervigni Martinelli**, **Servidor(a) em Exercício Descentralizado-ANPD**, em 30/10/2024, às 17:48, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Jorge André Ferreira Fontelles de Lima**, **Coordenador(a)**, em 30/10/2024, às 17:49, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://anpd-super.mj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0152934** e o código CRC **61CA6163**.

SCN Quadra 06, Conjunto A, Ed. Venâncio 3000, Bloco A, 9º andar, - Bairro Asa Norte, Brasília/DF, CEP 70716-900
Telefone: (61) 2025-8168 - https://www.gov.br/anpd/pt-br

Referência: Caso responda a este documento, indicar expressamente o Processo nº 00261.000456/2022-12

SEI nº 0152934