GRUPO I – CLASSE V – Plenário
TC 039.606/2020-1
Natureza: Auditoria.
Órgãos/Entidades: Advocacia-Geral da União; Agência Brasileira de Desenvolvimento Industrial; Agência Brasileira de Inteligência; Agência Brasileira de Promoção de Exportações e Investimentos; e outros.
Representação legal: Juliana Andrade Litaiff (44.123/OAB-DF), Luiza Rocha Jacobsen (46.824/OAB-DF) e outros, representando Serviço Nacional de Aprendizagem do Transporte - Conselho Nacional; Juliana Andrade Litaiff (44.123/OAB-DF), Luiza Rocha Jacobsen (46.824/OAB-DF) e outros, representando Serviço Social do Transporte - Conselho Nacional; Leonardo Andrade Simon, Roberto Parucker e outros, representando Centrais Elétricas do Norte do Brasil S.a.; Cássio Augusto Muniz Borges (91152/OAB-RJ), Francisco de Paula Filho (7.530/OAB-DF) e outros, representando Serviço Social da Indústria - Departamento Nacional; Grazielle Fernandes Pettene, Anna Paula Bottrel Souza (143.502/OAB-RJ), Adriana Diniz de Vasconcellos Guerra (191.390-A/OAB-SP), Saulo Benigno Puttini (42.154/OAB-DF), Pedro Jose de Almeida Ribeiro (163.187/OAB-RJ), Maritisa Mara Gambirasi Carcinoni, Carina Gallardo Rey (132.226/OAB-RJ), Tais Guida Fonseca Guedes (156.097/OAB-RJ), Marcia Aita Almeida (13.539/OAB-DF), Melissa Monte Stephan (118.596/OAB-RJ), Denilson Ribeiro de Sena Nunes (96.320/OAB-RJ), Andre de Castro Oliveira Pereira Braga (201.971/OAB-RJ), Ana Paula Barbosa de Sa (140.352/OAB-RJ), Marcelo Sampaio Vianna Rangel (90.412/OAB-RJ), Rodrigo Sales da Rocha Abreu (155.278/OAB-RJ) e Maria Joana Carneiro de Moraes (158.738/OAB-RJ), representando Banco Nacional de Desenvolvimento Econômico e Social; Leonor Chaves Maia de Sousa (20321/OAB-CE), Arnaldo de Morais Moreira Fernandes Vieira e outros, representando Banco do Nordeste do Brasil S.A..

SUMÁRIO: AUDITORIA. DIAGNÓSTICO DO GRAU DE IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS NA ADMINISTRAÇÃO PÚBLICA FEDERAL. 382 ORGANIZAÇÕES AVALIADAS. NOVE DIMENSÕES: PREPARAÇÃO, CONTEXTO ORGANIZACIONAL, LIDERANÇA, CAPACITAÇÃO, CONFORMIDADE DO TRATAMENTO, DIREITOS DO TITULAR, COMPARTILHAMENTO DE DADOS PESSOAIS, VIOLAÇÃO DE DADOS PESSOAIS E MEDIDAS DE PROTEÇÃO. MAIOR PARTE DAS ORGANIZAÇÕES EM ESTÁGIO INICIAL. ESTRUTURA DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. RECOMENDAÇÕES.

RELATÓRIO

Adoto como parte do relatório a instrução elaborada no âmbito da Secretaria de Fiscalização de Tecnologia da Informação – Sefti (peça 1.049), que contou com o endosso dos dirigentes daquela unidade técnica (peças 1.050 e 1.051):

1. "Introdução

1.1. Deliberação que originou a fiscalização

1. *No âmbito da Estratégia de Fiscalização do TCU em Segurança da Informação (SegInfo) e Segurança Cibernética (SegCiber), constante do Acórdão 4.035/2020-TCU-Plenário (Rel. Min. Vital do Rêgo), foi prevista a realização de 'Auditoria sobre a LGPD' (TC 001.873/2020-2, peça 56, p. 78).*

2. *Esta fiscalização foi autorizada por meio do Acórdão 2.909/2020-TCU-Plenário, de relatoria do Ministro Augusto Nardes (TC 034.479/2020-1, peça 6).*

1.2. Visão geral do objeto

3. *A privacidade é um tema que começou a ganhar relevância em meados de 1890, quando Louis D. Brandeis escreveu um artigo para a revista Harvard Law Review, no qual mencionou que métodos de negócio e invenções recentes daquela época, como a câmera fotográfica, poderiam ameaçar a proteção das pessoas e o direito à privacidade.*

4. *Mais adiante, em 1948, o tema também foi abordado na Declaração Universal dos Direitos Humanos, onde foi descrito, no art. 12, que: 'Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito à proteção da lei'.*

5. *No mesmo sentido, em meados de 1970, com o início da popularização da Tecnologia da Informação (TI) e com o aumento do comércio transfronteiriço europeu, houve a necessidade da adoção de mecanismos que permitissem maior gestão das informações pessoais para garantir que os indivíduos pudessem exercer controle de seus dados sem que houvesse impactos indesejáveis no desenvolvimento econômico. Tal desafio foi tratado, em 1995, por meio da publicação da Diretiva 95/46/CE do Parlamento Europeu, que buscou harmonizar as legislações europeias no que tange ao tratamento de dados pessoais e à livre circulação desses dados.*

6. *No entanto, apesar de se basearem na mesma Diretiva, os países europeus possuíam leis distintas. Diante disso, a União Europeia (EU) publicou, em 2016, o Regulamento Geral de Proteção de Dados (do inglês General Data Protection Regulation – GDPR), que buscou unificar e reforçar a proteção de dados para os indivíduos do continente europeu. Com a publicação da GDPR, o tema privacidade ganhou ainda mais relevância no contexto global. Transações comerciais e as próprias pessoas passaram a demandar mais cuidado com os dados pessoais.*

7. *Seguindo essa tendência, a Lei 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), foi publicada no Brasil. A LGPD, inspirada no GDPR, dispõe sobre o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica, com o intuito de proteger os direitos fundamentais de liberdade e de privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural.*

8. *A LGPD foi promulgada em 14 de agosto de 2018 e, inicialmente, entraria em vigência dezoito meses após a publicação, mas a Medida Provisória (MP) 869/2018 prorrogou esse prazo por mais seis meses. Entretanto, devido à pandemia da Covid-19, foi publicada nova MP (959/2020) que prorrogaria novamente o prazo citado e que levaria a entrada em vigor da legislação para maio de 2021. No entanto, após discussão no Senado, o prazo de 24 meses foi mantido e a Lei passou a vigorar em setembro de 2020, após sanção presidencial.*

9. *Aspectos como o cenário de incertezas quanto ao início de vigência da legislação e a morosidade para a criação da Autoridade Nacional de Proteção de Dados (ANPD) – órgão responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional – contribuíram para que as organizações não estivessem devidamente estruturadas para atender os*

ditames da Lei no início da sua vigência. Ademais, vale destacar que a cultura de proteção de dados no Brasil passou a ser explorada com vigor somente após a publicação da LGPD, enquanto o tema já era debatido com intensidade na Europa desde meados de 1950.

10. *Assim, mesmo após a vigência da LGPD, o Brasil tem sido vítima de graves ataques que resultaram no vazamento de dados pessoais. Dentre esses ataques, pode-se destacar a divulgação pela imprensa do vazamento de dados de mais de 200 milhões de brasileiros ocasionado por falha de segurança em sistema do Ministério da Saúde e o denominado 'megavazamento' que expôs dados de 223 milhões de brasileiros, além de informações de veículos e de CNPJs.*

11. *Os casos supracitados retratam a existência de deficiências relacionadas à cibersegurança no país, o que afeta a privacidade, pois para prover proteção de dados pessoais são necessários investimentos em segurança da informação. A necessidade de aumentar tais investimentos pode ser corroborada pelo fato de o Brasil ter ocupado a 70ª posição no Índice Global de Cibersegurança publicado pela União Internacional de Telecomunicações (UIT) em 2019, ficando atrás de outros países americanos como: Estados Unidos, Canadá, Uruguai, México e Paraguai.*

12. *Ademais, cumpre ressaltar que a segurança da informação é fundamental para a consolidação da proteção de dados pessoais. Todavia, no escopo do levantamento de governança e gestão da segurança da informação e da segurança cibernética na APF, realizado pelo TCU em 2020, foi analisado o índice de gestão de segurança da informação (iGestSegInfo), computado com base nos resultados do levantamento integrado de governança realizado pelo TCU em 2018. Por meio desse índice, verificou-se que apenas 59% das organizações avaliadas implementavam, ainda que de forma parcial, a gestão de segurança da informação: 24% se encontravam no estágio de capacidade aprimorada e 35% no estágio de capacidade intermediária, enquanto 41% ainda se encontravam nos estágios de capacidade inicial ou inexpressiva (TC 001.873/2020-2, peça 46, p. 35-36).*

13. *Diante do exposto, resta clara a necessidade de estimular a implantação da cultura de segurança da informação e de proteção de dados pessoais na Administração Pública Federal (APF), fato que levou o TCU a conduzir esta auditoria, sob a relatoria do ministro Augusto Nardes, para analisar (i) a adequação das organizações públicas federais à LGPD e (ii) a estruturação da ANPD.*

1.3. Objetivo e questões de auditoria

14. *Este trabalho buscou avaliar as ações governamentais e os riscos à proteção de dados pessoais por meio da elaboração de diagnóstico acerca dos controles implementados pelas organizações públicas federais para adequação à LGPD. A fiscalização foi estruturada a partir de três questões de auditoria (**Error! Reference source not found.**):*

14.1. Q1) As organizações se estruturaram para a condução de iniciativas de adequação à LGPD?

14.2. Q2) As organizações implementaram medidas e controles de proteção de dados pessoais para adequação à LGPD?

14.3. Q3) A ANPD e o CNPD (Conselho Nacional de Proteção de Dados) estão estruturados e em operação conforme estabelecido na LGPD?

15. *As duas primeiras questões foram desdobradas em perguntas específicas contempladas em um questionário respondido, de forma online, por 382 organizações públicas federais (**Error! Reference source not found.**).*

16. *A terceira questão gerou outro grupo de perguntas que foram respondidas por meio de reuniões realizadas com membros da ANPD (**Error! Reference source not found.**).*

1.4. Metodologia utilizada

17. *O trabalho foi conduzido em conformidade com as Normas de Auditoria do TCU – NAT (Portaria - TCU 280/2010, alterada pela Portaria - TCU 168/2011) e com o documento 'Padrões de Auditoria de Conformidade' (Portaria - Segecex 26/2009) e está alinhado aos Princípios Fundamentais de Auditoria do Setor Público, conforme tradução da ISSAI 100, disponibilizada no portal do TCU.*

18. *Por se tratar de tema emergente, técnico e complexo, com o intuito de não surpreender os gestores com a condução do trabalho, três meses antes do início da execução da fiscalização (novembro de 2020) foram enviados e-mails às organizações selecionadas para a auditoria para comunicar que o TCU iniciaria, no primeiro trimestre de 2021, trabalho para avaliar a adequação das organizações públicas à LGPD. Além disso, foram divulgadas notícias sobre o trabalho no Portal do TCU e em mídias especializadas, o que contribuiu para a grande adesão de respostas ao questionário eletrônico (100%) e, acredita-se, induziu a adoção das primeiras medidas por várias organizações, devido à expectativa de controle criada.*

19. *O método utilizado para avaliar as organizações foi o de autoavaliação de controles (do inglês Control Self-Assessment – CSA), por meio do qual foi disponibilizado um questionário eletrônico para que os gestores preenchessem as respostas que melhor refletiam a situação das respectivas organizações com relação aos controles relacionados à LGPD. Além de permitir que as organizações verificassem quais controles associados à LGPD foram implementados, as questões também podem ser utilizadas como referência para a condução de futuras iniciativas de adequação.*

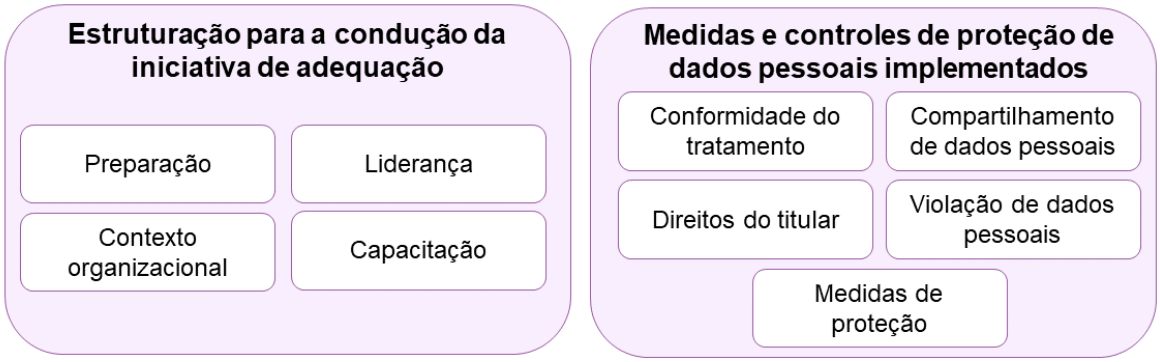
20. *As perguntas do questionário tiveram como referência a própria LGPD e a norma técnica ABNT NBR ISO/IEC 27701:2019 (extensão da ABNT NBR ISO/IEC 27.001 e da ABNT NBR ISO/IEC 27.002 para gestão da privacidade da informação – Requisitos e diretrizes). Também foram consultadas boas práticas oriundas de materiais disponibilizados pelo ICO (Information Commissioner's Office) e pelo CNIL (Commission Nationale de l'Informatique et des Libertés), que são organizações equivalentes à ANPD, a primeira do Reino Unido e a segunda da França, e que são reconhecidas por conduzirem bons trabalhos relacionados à proteção de dados pessoais no continente europeu.*

21. *O questionário (**Error! Reference source not found.**) contemplou 60 questões organizadas em nove dimensões: preparação, contexto organizacional, liderança, capacitação, conformidade do tratamento, direitos do titular, compartilhamento de dados pessoais, violação de dados pessoais e medidas de proteção.*

22. *Ademais, a primeira seção do questionário, identificação do respondente, solicitou dados relacionados à pessoa designada pela organização para responder às perguntas. Tais informações foram úteis para a equipe da fiscalização entrar em contato com os representantes das organizações auditadas para dirimir dúvidas e para prestar esclarecimentos*

23. *As outras dimensões foram elaboradas a partir de duas perspectivas: (i) estruturação para a condução da iniciativa de adequação e (ii) medidas e controles de proteção de dados pessoais implementados, conforme descrito na Figura 1.*

***Figura 1** - Dimensões do questionário*



24. *As questões foram cadastradas na plataforma Lime Survey e distribuídas nas dimensões conforme o Quadro 1. Vale ressaltar que o questionário não contemplou todos os controles possíveis de serem implementados para adequação à LGPD e se limitou a avaliar aspectos que a equipe de auditoria entendeu mais adequados para a realidade das organizações públicas federais no momento atual. Além disso, cumpre frisar que as questões foram validadas por especialistas e pela ANPD, que tiveram a oportunidade de propor modificações.*

Quadro 1 - *Distribuição de questões pelas dimensões do questionário*

Dimensão	***Número de questões***
1. Preparação	*3*
2. Contexto organizacional	*11*
3. Liderança	*13*
4. Capacitação	*4*
5. Conformidade do tratamento	*8*
6. Direitos do titular	*5*
7. Compartilhamento de dados pessoais	*5*
8. Violação de dados pessoais	*6*
9. Medidas de proteção	*5*
Total	*60*

25. *Para responder ao questionário, cada uma das 382 organizações auditadas recebeu um ofício com um link e uma chave de acesso (token) para preencher o questionário online. Por meio da mesma comunicação, as organizações foram notificadas que dúvidas técnicas ou relacionadas à interpretação das questões poderiam ser dirimidas pelo do e-mail auditoria.lgpd@tcu.gov.br.*

26. *Todas as organizações que receberam o ofício responderam ao questionário. No entanto, cumpre fazer uma menção honrosa às organizações de saúde, em especial à Fiocruz, pois se empenharam para enviar as respostas tempestivamente, mesmo diante das dificuldades decorrentes da necessidade de concentrar esforços em atividades diretamente relacionadas ao combate à pandemia.*

27. *Após a expiração do prazo de preenchimento do questionário, as respostas fornecidas pelas organizações foram consolidadas e serviram de insumo para a elaboração do diagnóstico de adequação à LGPD. Outrossim, foi elaborada fórmula matemática para a definição de um indicie criado para avaliar o grau de adequabilidade das organizações, que levou em consideração o atendimento aos controles avaliados em cada uma das dimensões do questionário. Tanto o diagnóstico quanto o índice de adequabilidade são tratados no capítulo 2.*

28. *Por outro lado, as informações utilizadas para a análise da ANPD foram coletadas a partir da exploração de documentos e de entrevistas guiadas por meio de questionário específico (**Error! Reference source not found.**). Os achados decorrentes dessa análise são explorados no capítulo 3.*

1.5. Limitações

29. *Não houve limitações. Todo o planejamento foi cumprido.*

1.6. Volume de recursos fiscalizados

30. *Não se aplica.*

1.7. Benefícios estimados

31. *Pretende-se, com esta fiscalização, contribuir para: (i) a efetividade das práticas governamentais para proteção de dados pessoais; (ii) a conscientização das organizações públicas quanto à necessidade de conduzirem iniciativas para adequação à LGPD; (iii) a produção de conhecimento capaz de auxiliar as organizações na condução dessas iniciativas; (iv) a indução da estruturação da ANPD; e (v) a promoção do acesso dos cidadãos aos direitos estabelecidos na LGPD.*

2. Diagnóstico da adequação das organizações públicas federais à LGPD

32. *Neste capítulo será abordado o diagnóstico que abrange os controles gerais que devem ser implementados pelas organizações públicas federais para adequação à LGPD. Entretanto, vale ressaltar que há questões que abrangem **controles que podem não ser aplicáveis a algumas organizações**, devido ao contexto, ao porte ou aos objetivos institucionais.*

33. *As estatísticas foram geradas a partir das respostas preenchidas pelos gestores por meio do questionário eletrônico disponibilizado às 382 organizações auditadas. Cada seção deste capítulo*

trata uma das dimensões do questionário: preparação, contexto organizacional, liderança, capacitação, conformidade do tratamento, direitos do titular, compartilhamento de dados pessoais, violação de dados pessoais e medidas de proteção.

2.1. Dimensões avaliadas

2.1.1. Preparação

34. *Antes de iniciar o processo de adequação à LGPD, a organização deve adotar medidas para construir um ambiente propício para o sucesso da iniciativa.*

35. *As questões desta seção abordaram aspectos relacionados à identificação e ao planejamento das medidas necessárias à adequação.*

2.1.1.1 Identificação e planejamento das medidas necessárias à adequação à LGPD

36. *A questão 2.1 do questionário buscou avaliar se as organizações conduziram iniciativas para identificar e planejar as medidas necessárias à adequação à LGPD.*

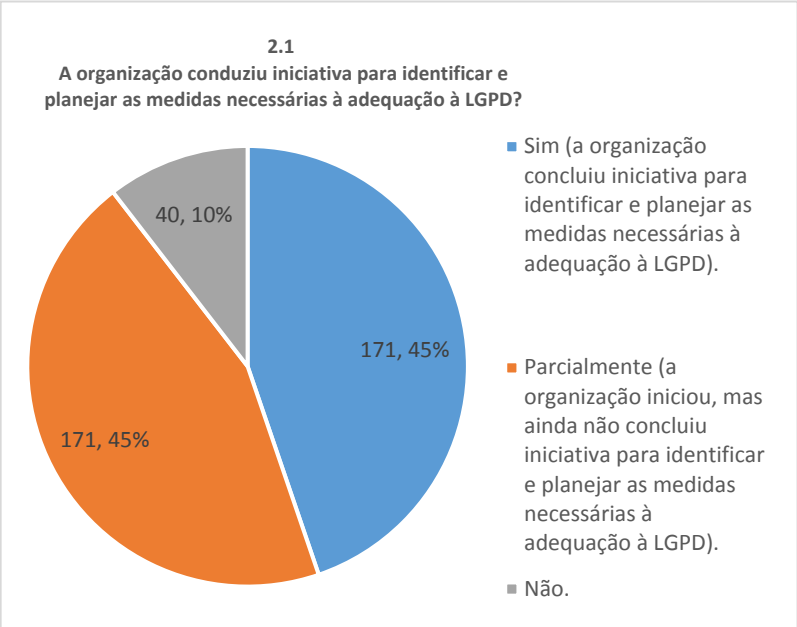
37. *Em consonância com o disposto no art. 50, § 2º, inciso I, da LGPD, o controlador poderá implementar programa de governança em privacidade que seja, entre outros aspectos, adaptado à estrutura, à escala e ao volume das operações, bem como à sensibilidade dos dados pessoais tratados.*

38. *Nesse sentido, é conveniente que as organizações conduzam atividades para identificar e planejar as medidas necessárias à adequação à LGPD, de forma que sejam avaliados aspectos como os requisitos e os riscos inerentes ao projeto de adequação.*

39. *Um exemplo de iniciativa para guiar a definição dessas medidas é a instituição de comitê ou grupo de trabalho que conte com a participação de pessoas pertencentes a diferentes unidades que exercem atividades relevantes para o tratamento de dados pessoais (e.g.: Segurança da Informação, Tecnologia da Informação, Jurídico, Recursos Humanos, Auditoria, Ouvidoria e Área de Negócio/Finalística) para que sejam considerados aspectos inerentes a toda organização. Também é importante que a iniciativa conte com o apoio ou, até mesmo, com a participação direta da alta direção para que receba a devida atenção. O plano de ação é um exemplo de artefato que pode ser produzido por este tipo de iniciativa.*

40. *As respostas à questão 2.1 (Figura 2) demonstram que apenas 45% das organizações concluíram iniciativa de identificação e planejamento das medidas necessárias à adequação.*

Figura 2 - *Condução de iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD*



41. *As organizações que ainda não concluíram este tipo de iniciativa devem tomar as devidas providências, especialmente aquelas que sequer adotaram alguma medida, pois a legislação já está em vigor, bem como a fiscalização exercida pela ANPD e o controle exercido por esta Corte de Contas.*

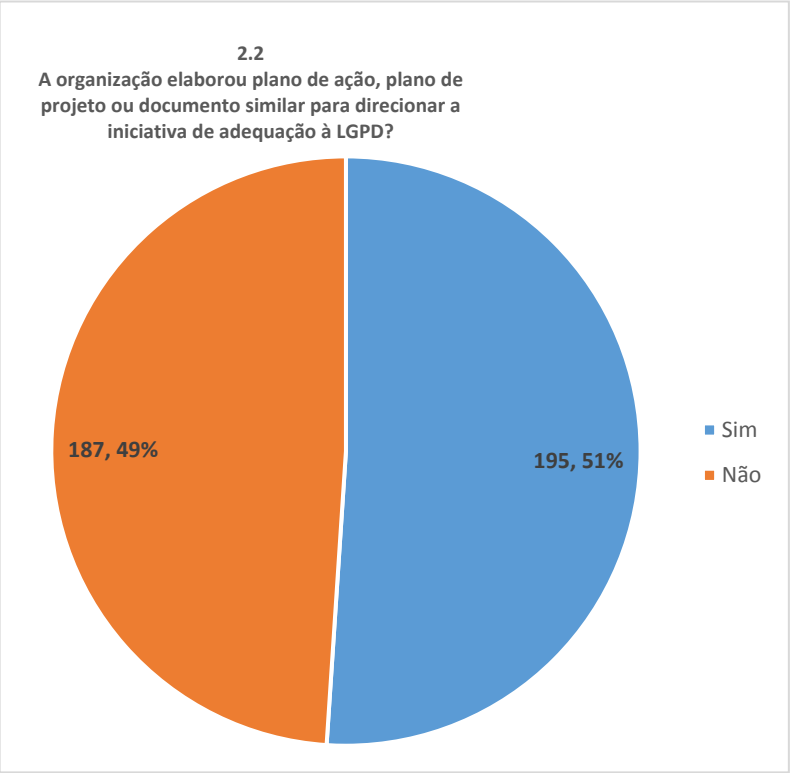
2.1.1.2 <u>Plano de ação</u>

42. *A questão 2.2 do questionário buscou avaliar se as organizações elaboraram plano de ação, plano de projeto ou documento similar para direcionar a iniciativa de adequação à LGPD.*

43. *Em consonância com o disposto no item 5.4.2 da ABNT NBR ISO/IEC 27701:2019, é conveniente que a organização possua informações documentadas relacionadas ao projeto de adequação à LGPD, como: o que será feito, quais recursos serão necessários, quem serão os responsáveis, quando as atividades serão concluídas e como os resultados serão avaliados. Essas informações podem ser consolidadas em um plano de ação, plano de projeto ou documento similar.*

44. *No entanto, as respostas à questão 2.2 (Figura 3) demonstram que quase metade das organizações, 49%, não produziu este tipo de artefato.*

Figura 3 *- Artefato com diretrizes para a iniciativa de adequação*



45. *As organizações que ainda não produziram o plano devem providenciá-lo, pois este é fundamental para guiar os responsáveis na implementação e na implantação de controles para adequação à LGPD.*

46. *Ante o exposto, e considerando que a Secretaria de Governo Digital do Ministério da Economia (SGD/ME) já adotou ações para orientar os órgãos sob sua alçada acerca do assunto, a equipe de auditoria propõe* ***recomendar*** *ao Conselho Nacional de Justiça (CNJ) e ao Conselho Nacional do Ministério Público (CNMP) que, considerando o controle realizado sobre a atuação administrativa das organizações sob suas jurisdições, expeçam orientação quanto ao planejamento das medidas necessárias para adequação à LGPD, considerando as diretrizes estabelecidas no item 5.4.2 da ABNT NBR ISO/IEC 27701:2019.*

2.1.2. Contexto organizacional

47. *Para alcançar os resultados pretendidos pela iniciativa de adequação à LGPD, a organização deve avaliar questões internas e externas.*

48. *As questões desta seção abordaram aspectos relacionados à identificação de normativos correlatos à proteção de dados pessoais que devem ser respeitados pelas organizações, à identificação das partes interessadas e à análise dos dados pessoais tratados e dos processos organizacionais que realizam os tratamentos.*

2.1.2.1 Normativos relacionados ao tratamento de dados pessoais

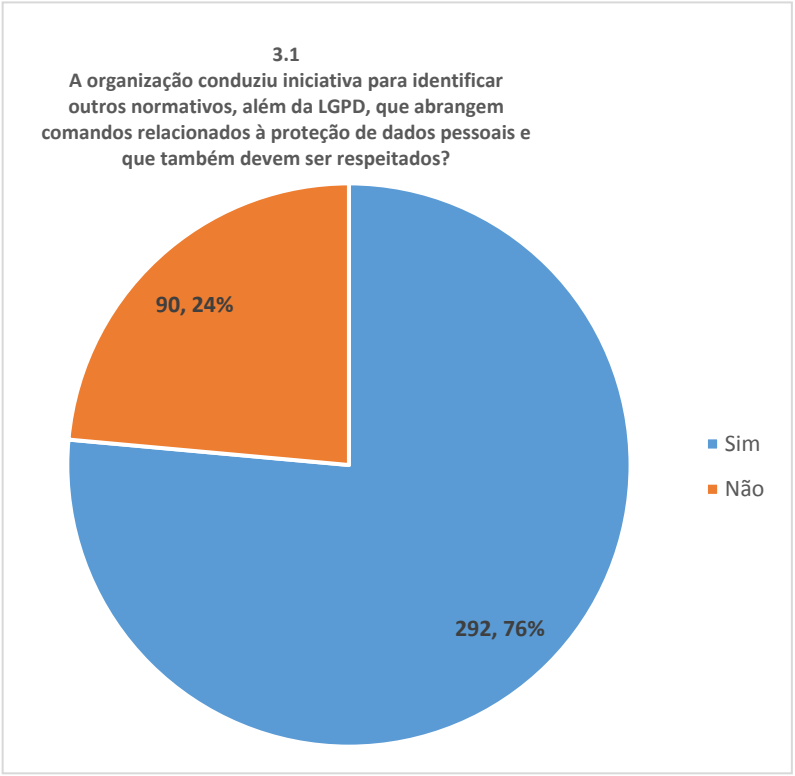
49. *A questão 3.1 do questionário buscou avaliar se as organizações conduziram iniciativa para identificar outros normativos, além da LGPD, que abrangem o tratamento de dados pessoais e que também devem ser respeitados.*

50. *Em consonância com o item 5.2.1 da ABNT NBR ISO/IEC 27701:2019, a organização deve avaliar fatores externos e internos que possam influenciar aspectos relacionados à proteção de dados pessoais, dentre os quais estão as legislações de privacidade. Nesse sentido, vale ressaltar que o arcabouço legal aplicável ao setor público que trata questões relativas à privacidade não se restringe à LGPD. A Constituição Federal, a Lei de Acesso à Informação, o Código de Defesa do Consumidor, a Lei do Cadastro Positivo e a Consolidação das Leis Trabalhistas são exemplos de normas que também*

abrangem comandos relacionados ao tratamento de dados pessoais e que devem ser seguidos por determinadas organizações.

51. *As respostas à questão 3.1 (Figura 4) demonstram que a maioria das organizações, 76%, conduziu iniciativa para identificar esses normativos.*

***Figura 4 -** Identificação de normativos relacionados ao tratamento de dados pessoais, além da LGPD*



52. *A identificação de todos os normativos correlatos ao tratamento de dados pessoais, aplicáveis à organização, é fundamental para evitar que haja retrabalho para adaptar controles já implementados para o cumprimento da LGPD.*

53. *Ante o exposto, a equipe de auditoria propõe **recomendar** à SGD/ME, ao CNJ e ao CNMP que, considerando o controle realizado sobre a atuação administrativa das organizações sob suas jurisdições, expeçam orientação quanto à identificação de normativos correlatos ao tratamento de dados pessoais aplicáveis à organização, considerando as diretrizes estabelecidas no item 5.2.1 da ABNT NBR ISO/IEC 27701:2019.*

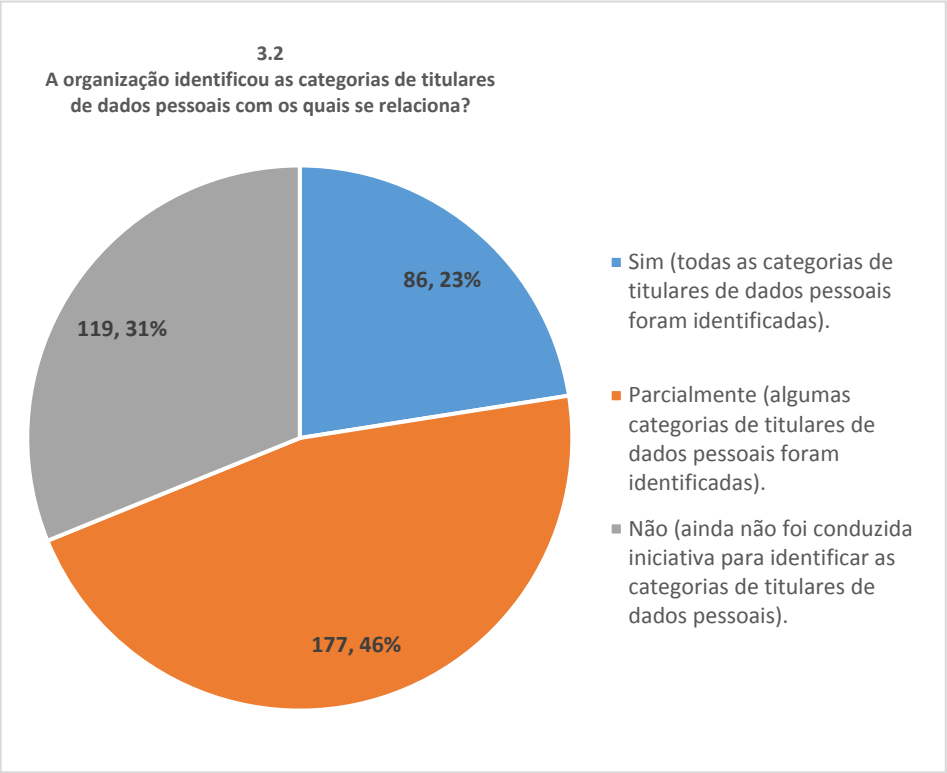
2.1.2.2 Categorias de titulares de dados pessoais

54. *A questão 3.2 do questionário buscou avaliar se as organizações identificaram as categorias de titulares de dados pessoais com os quais se relacionam.*

55. *O titular é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (LGPD, art. 5º, inciso V). Os titulares podem ser enquadrados em diferentes categorias como: cidadão, cliente, servidor público, representante de fornecedor e terceirizado. Ademais, o item 7.2.8 da ABNT NBR ISO/IEC 27701:2019 relata que as organizações devem manter registros de tratamento de dados pessoais que incluam, entre outros aspectos, as categorias dos titulares de dados pessoais.*

56. *A partir das respostas ao questionário, constatou-se que a maioria das organizações, 77% (31% não identificaram e 46% identificaram parcialmente), ainda não identificou todas as categorias de titulares de dados pessoais com os quais mantém relacionamento (Figura 5).*

Figura 5 *- Identificação das categorias de titulares de dados pessoais*



57. *A identificação dessas categorias é importante para auxiliar as organizações a planejarem os controles que serão implementados levando em consideração as diferentes partes interessadas. Por exemplo, organizações que realizam tratamento de dados de crianças e adolescentes devem implementar controles mais rigorosos nos processos que realizam o tratamento destes dados.*

58. *Ante o exposto, e considerando que a SGD/ME já adotou ações para orientar os órgãos sob sua alçada acerca do assunto, a equipe de auditoria propõe* ***recomendar*** *ao CNJ e ao CNMP que orientem as organizações no seu âmbito de atuação quanto à identificação das categorias de titulares de dados pessoais com os quais se relacionam, considerando as diretrizes estabelecidas no item 7.2.8 da ABNT NBR ISO/IEC 27701:2019.*

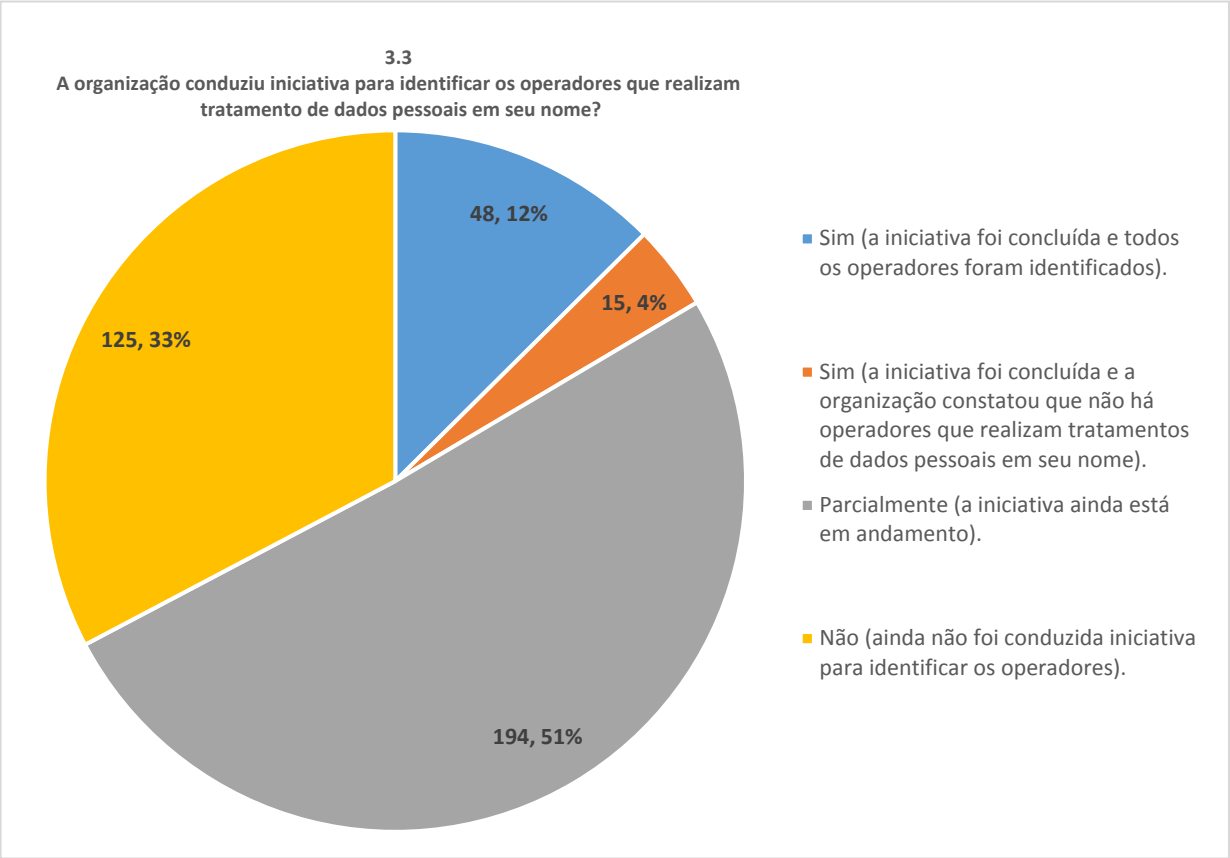
2.1.2.3 Operadores

59. *A questão 3.3 do questionário buscou avaliar se as organizações conduziram iniciativa para verificar se há operadores que realizam tratamento de dados pessoais em seus nomes e identificar esses operadores se for o caso.*

60. *O operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (LGPD, art. 5º, inciso VII). Este, por sua vez, é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (LGPD, art. 5º, inciso VI). Ademais, o item 5.2.2 da ABNT NBR ISO/IEC 27701:2019 relata a importância da identificação das partes interessadas associadas ao tratamento de dados pessoais, dentre as quais está o operador.*

61. *Ao consolidar as respostas fornecidas pelas organizações (Figura 6), constatou-se que mais da metade, 51%, não conduziu iniciativa para identificar os operadores.*

Figura 6 *- Condução de iniciativa para identificar os operadores*



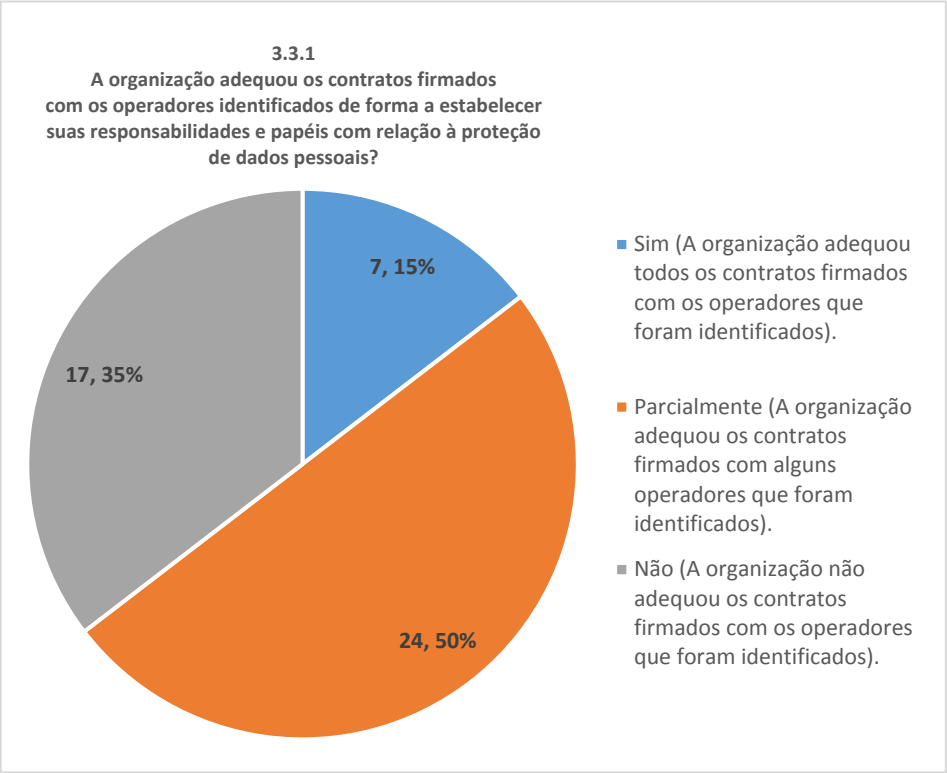
62. *O cenário é preocupante, pois a identificação dos operadores é um ponto chave para a efetividade da proteção dos dados pessoais, uma vez que realizam tratamento de dados em nome das organizações. Além disso, cumpre frisar que o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir obrigações da legislação ou quando não seguirem instruções lícitas do controlador (LGPD, art. 42, §1º, inciso I).*

63. *Ante o exposto, e considerando que a SGD/ME já adotou ações para orientar os órgãos sob sua alçada acerca do assunto, a equipe de auditoria propõe* ***recomendar*** *ao CNJ e ao CNMP que, considerando o controle realizado sobre a atuação administrativa das organizações sob suas jurisdições, expeçam orientação quanto à identificação dos operadores que realizam tratamento de dados pessoais em seus nomes, considerando as diretrizes estabelecidas no item 5.2.2 da ABNT NBR ISO/IEC 27701:2019.*

64. *Assim, para avaliar a efetividade do processo de identificação de operadores, caso a organização informasse que a iniciativa foi concluída e que levou à identificação de todos esses atores, era exibida a subquestão 3.3.1 para avaliar se os contratos firmados com os operadores identificados foram adequados de forma a estabelecer, claramente, os seus papéis e responsabilidades com relação à proteção de dados pessoais, em consonância com o disposto no item 7.2.6 da ISO/IEC 27701:2019.*

65. *As respostas à questão 3.3.1 (Figura 7) demonstram que apenas 15% das organizações adequaram todos os contratos firmados com os operadores identificados.*

***Figura 7** - Adequação dos contratos firmados com os operadores*



66. *A definição dos papeis e responsabilidades é fundamental para dirimir futuros questionamentos judiciais ou extrajudiciais relacionados ao tratamento de dados pessoais. Ademais, pode assegurar que os operadores adotem medidas de segurança, técnicas e administrativas, aptas a proteger os dados que são compartilhados com eles.*

67. *Ante o exposto, a equipe de auditoria propõe **recomendar** à SGD/ME, ao CNJ e ao CNMP que, considerando o controle realizado sobre a atuação administrativa das organizações sob suas jurisdições, expeçam orientação quanto à adequação dos contratos firmados com os operadores de forma a estabelecer, claramente, os papéis e responsabilidades relacionados à proteção de dados pessoais, considerando as diretrizes estabelecidas no item 7.2.6 da ABNT NBR ISO/IEC 27701:2019.*

68. *Apesar das questões exploradas neste tópico se limitarem à análise da identificação de operadores e da adequação dos contratos firmados com eles, percebe-se que as definições do papel de controlador e de operador causam incertezas nos envolvidos em projetos de adequação. Diante disso, e considerando o guia publicado recentemente pela ANPD, alguns aspectos referentes a essas definições serão tratados a seguir.*

69. *Um dos itens que merece destaque é que os agentes de tratamento devem ser definidos para cada operação de tratamento de dados, a partir de uma perspectiva institucional. Embora existam casos de organizações públicas que nomearam, de forma equivocada, pessoa natural vinculada a elas como controlador, o papel deve ser atribuído à própria organização, já que os agentes públicos atuam sob o poder diretivo desta. Ademais, deve-se considerar a Teoria do Órgão, segundo a qual a atuação do servidor deve ser imputada ao órgão que ele representa e não à pessoa física em si.*

70. *Por outro lado, como o agente de tratamento é definido para cada operação de tratamento de dados pessoais, é possível que uma mesma organização seja controladora e operadora, desde que essa definição se dê em diferentes operações de tratamento. No caso de controladores que realizam diretamente tratamento de dados pessoais, seus agentes públicos agem como parte integrante destes e não como operadores.*

71. *Também deve ser destacado o entendimento segundo o qual os órgãos públicos da Administração Direta não são considerados formalmente controladores de dados, sendo esta função atribuída à União, pessoa jurídica de direito público, pois, de acordo com a LGPD, o papel de*

controlador deve ser conferido a uma pessoa natural ou jurídica a quem compete as decisões referentes ao tratamento de dados pessoais.

72. *Conforme a ANPD explicou no guia, embora o controlador nesse caso seja a União, é importante observar que os órgãos públicos exercem, por força do princípio da desconcentração administrativa, atribuições típicas de controlador e devem, portanto, observar as obrigações impostas pela LGPD. Já as entidades da Administração Indireta, que possuem personalidade jurídica própria, seguem o regramento comum de pessoa jurídica estabelecido na LGPD.*

2.1.2.4 Controlador conjunto

73. *A questão 3.4 do questionário buscou analisar se as organizações avaliaram a ocorrência de tratamento de dados pessoais com o envolvimento de controlador conjunto.*

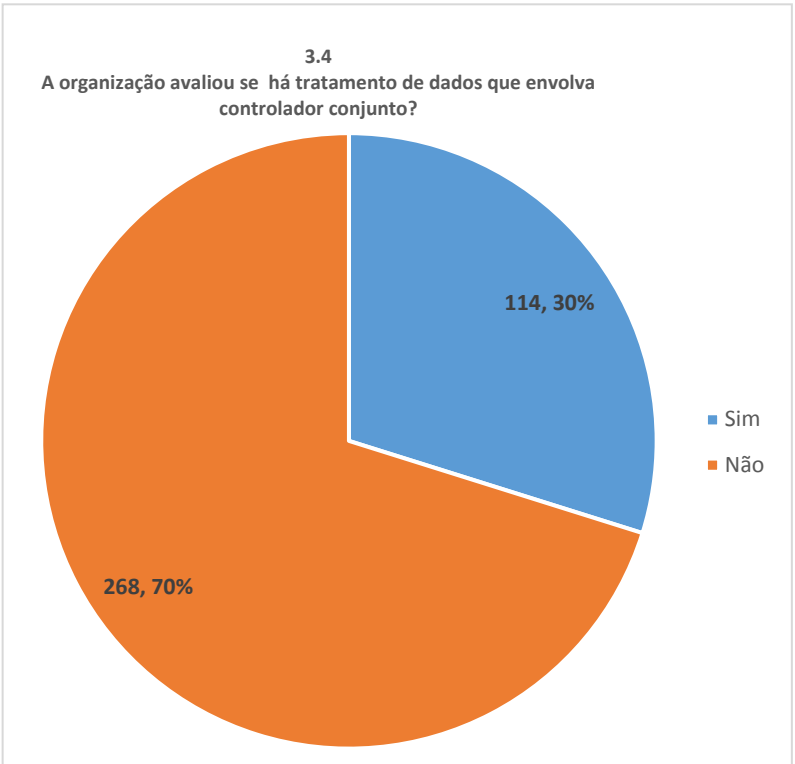
74. *Conforme explorado no tópico anterior, o controlador é a pessoa natural ou jurídica, de direito público ou privado a quem competem as decisões referentes ao tratamento de dados pessoais (LGPD, art. 5º, inciso VI). Por sua vez, de acordo com o item 3.1 da ABNT NBR ISO/IEC 27701:2019, o controlador conjunto é o controlador de dados pessoais que determina os propósitos e as formas de tratamento de dados pessoais em conjunto com outro(s) controlador(es).*

75. *Diferente da lei de proteção de dados europeia, que aborda o tema com mais profundidade, a LGPD explora-o de maneira superficial no art. 42, §1º, inciso II, onde cita que os controladores diretamente envolvidos no tratamento respondem solidariamente em casos de dano ao titular.*

76. *Em seu guia publicado recentemente, a ANPD explica que a existência de controladoria conjunta pode ser avaliada pela observação dos seguintes critérios: (i) mais de um controlador possui poder de decisão sobre o tratamento de dados pessoais; (ii) há interesse mútuo de dois ou mais controladores, com base em finalidades próprias, sobre um mesmo tratamento; e (iii) dois ou mais controladores tomam decisões comuns ou convergentes sobre as finalidades e elementos essenciais do tratamento.*

77. *As respostas fornecidas pelas organizações (Figura 8) demonstram que a maioria, 70%, não avaliou a existência de tratamento de dados com o envolvimento de controlador conjunto.*

***Figura 8** - Avaliação da existência de tratamento de dados com o envolvimento de controlador conjunto*

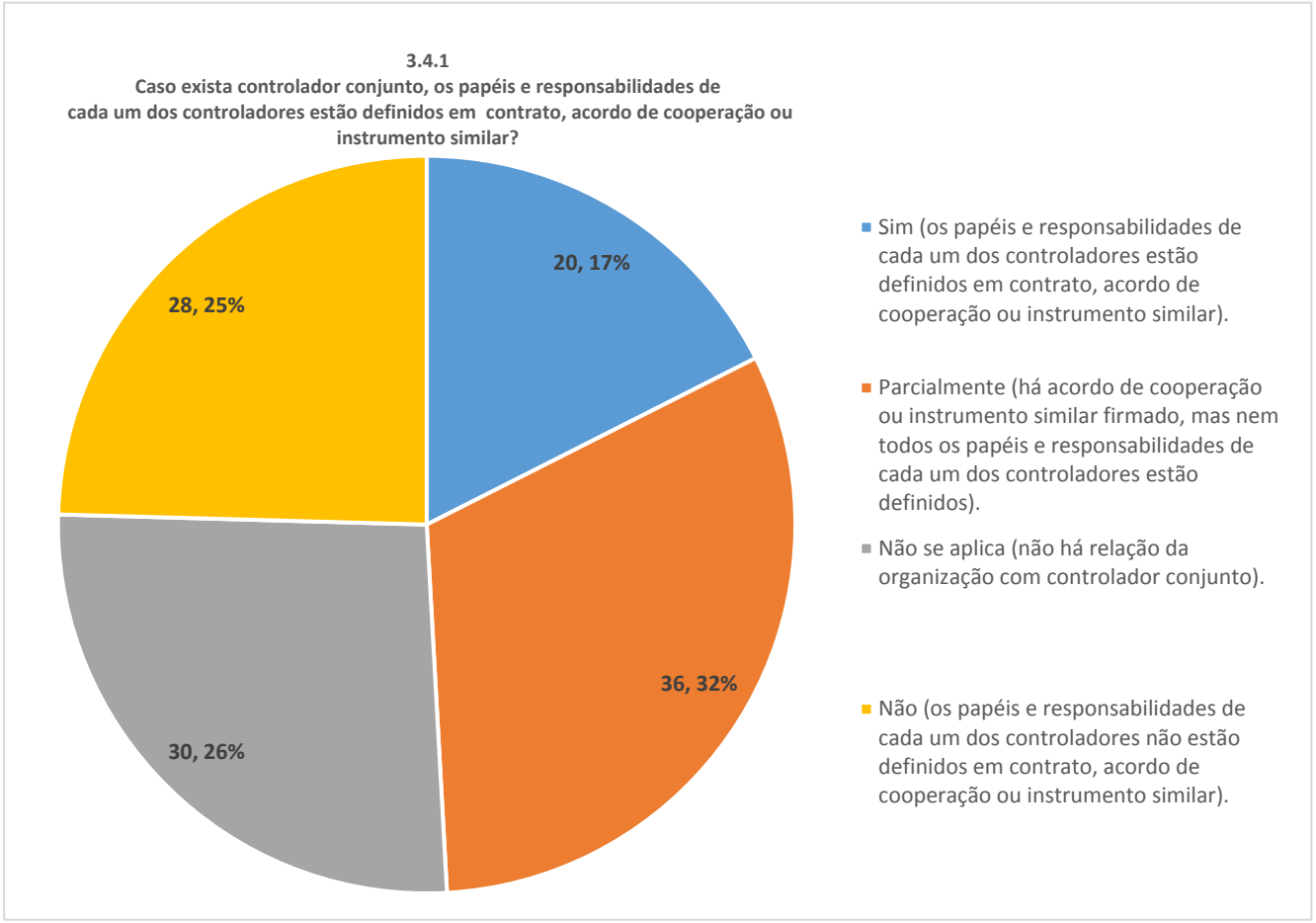


78. *Para melhor avaliar este quesito, caso a organização informasse que avaliou se havia a ocorrência de tratamento de dados pessoais com o envolvimento de controlador conjunto, era exibida*

a subquestão 3.4.1 para averiguar se os papéis e responsabilidades de cada um dos controladores foram definidos em contrato, acordo de cooperação ou instrumento similar, conforme preconiza o item 7.2.7 da ABNT NBR ISO/IEC 27701:2019.

79. *As respostas à questão (Figura 9) mostram que a minoria das organizações que avaliaram a existência de controlador conjunto, 17% (20 de 114), definiu, formalmente, os papeis e responsabilidades de cada um dos controladores conjuntos.*

***Figura 9** - Definição de papéis e responsabilidades de cada um dos controladores em contrato, acordo de cooperação ou instrumento similar*



80. *Diferente da relação controlador-operador, onde há uma delegação de competência, os controladores conjuntos definem, em conjunto, os processos e as finalidades do tratamento. Diante disso, é conveniente que as organizações se atentem para a possibilidade de exercerem o papel de controlador conjunto, o que demanda que o conceito seja analisado com o devido zelo, pois a estrutura de alguns órgãos públicos aparenta envolver essa relação, como, por exemplo, estruturas do Poder Judiciário que abrangem tribunais superiores e regionais.*

81. *Outrossim, a existência de entidades distintas diretamente envolvidas no tratamento de dados pessoais na condição de controlador demanda a adoção de controles consistentes para evitar a materialização de riscos que possam resultar na violação de dados pessoais, bem como na inconsistência de informações armazenadas.*

82. *Ante o exposto, a equipe de auditoria propõe **recomendar** à SGD/ME, ao CNJ e ao CNMP que, considerando o controle realizado sobre a atuação administrativa das organizações sob suas jurisdições, expeçam orientação quanto à avaliação da ocorrência de tratamento de dados pessoais com o envolvimento de controlador conjunto e à definição de papeis e responsabilidades de cada um dos controladores, considerando as diretrizes estabelecidas no item 7.2.7 da ABNT NBR ISO/IEC 27701:2019.*

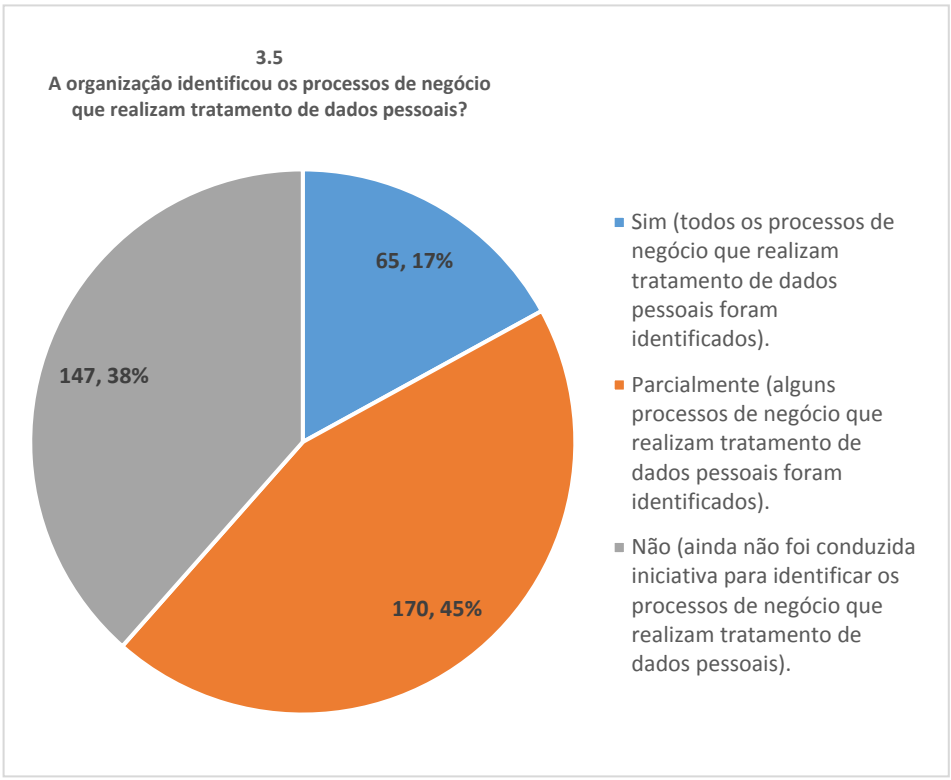
2.1.2.5 Processos que realizam tratamento de dados pessoais

83. *A questão 3.5 do questionário avaliou se as organizações identificaram os processos de negócio que realizam tratamento de dados pessoais.*

84. *O tratamento de dados pessoais envolve toda operação realizada com dados pessoais, como: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (LGPD, art. 5º, inciso X). Ademais, a LGPD é, em regra, aplicável a qualquer operação de tratamento de dados pessoais (LGPD, art. 3º) e o controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizam (LGPD, art. 37), o que denota a importância da identificação dos processos que realizam tais tratamentos.*

85. *No entanto, as respostas fornecidas (Figura 10) mostram que apenas 17% das organizações identificaram todos os processos de negócio que realizam tratamento de dados pessoais.*

***Figura 10** - Identificação dos processos de negócio que realizam tratamento de dados pessoais*



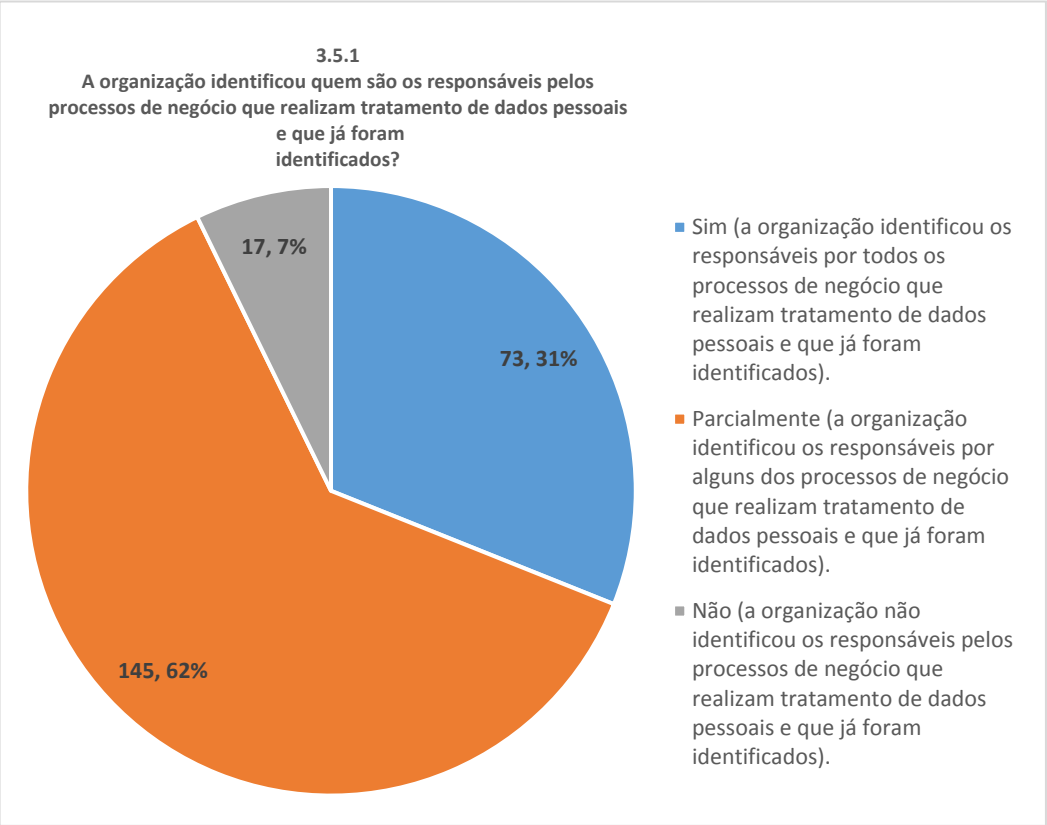
86. *A identificação dos processos que realizam tratamento de dados pessoais é uma das tarefas elementares em um projeto de adequação, pois é a partir dessa identificação que é possível avaliar os riscos inerentes a cada processo e identificar informações relevantes como: o propósito do tratamento, a base legal que justifica esse tratamento e as categorias de titulares de dados envolvidas.*

87. *Ademais, para realizar uma análise consistente dos processos, não basta que estes sejam identificados, é necessário efetuar o mapeamento deles para que sejam detectados outros elementos, como: responsáveis, atividades, atores, dados manipulados e eventuais compartilhamentos de dados.*

88. *Diante disso, caso a organização respondesse que os processos foram identificados em sua totalidade ou parcialmente, a subquestão 3.5.1 era exibida para avaliar se os responsáveis pelos processos que realizam tratamento de dados pessoais foram identificados. Esses responsáveis podem abranger, por exemplo: pessoas, departamentos e operadores.*

89. *No entanto, constatou-se que a maioria das organizações que identificou total ou parcialmente os processos (Figura 10) ainda não identificou os responsáveis por todos os processos que realizam tratamento de dados pessoais, pois 62% identificaram os responsáveis de apenas parte desses processos, enquanto 7% sequer identificou os responsáveis (Figura 11).*

Figura 11 *- Identificação dos responsáveis pelos processos de negócio que realizam tratamento de dados pessoais*



90. *O diagnóstico é preocupante, pois é por meio do mapeamento desses processos que as organizações podem identificar como e por que os dados pessoais são tratados para, posteriormente, analisar os riscos inerentes ao tratamento de dados pessoais.*

91. *Ante o exposto, e considerando que a SGD/ME já adotou ações para orientar os órgãos sob sua alçada acerca do assunto, a equipe de auditoria propõe* ***recomendar*** *ao CNJ e ao CNMP que, considerando o controle realizado sobre a atuação administrativa das organizações sob suas jurisdições, expeçam orientação quanto à identificação dos processos de negócio que realizam tratamento de dados pessoais, bem como dos respectivos responsáveis, considerando o disposto nos arts. 3º, 5º, inciso X, e 37 da LGPD e as diretrizes estabelecidas no item 7.2.8 da ABNT NBR ISO/IEC 27701:2019.*

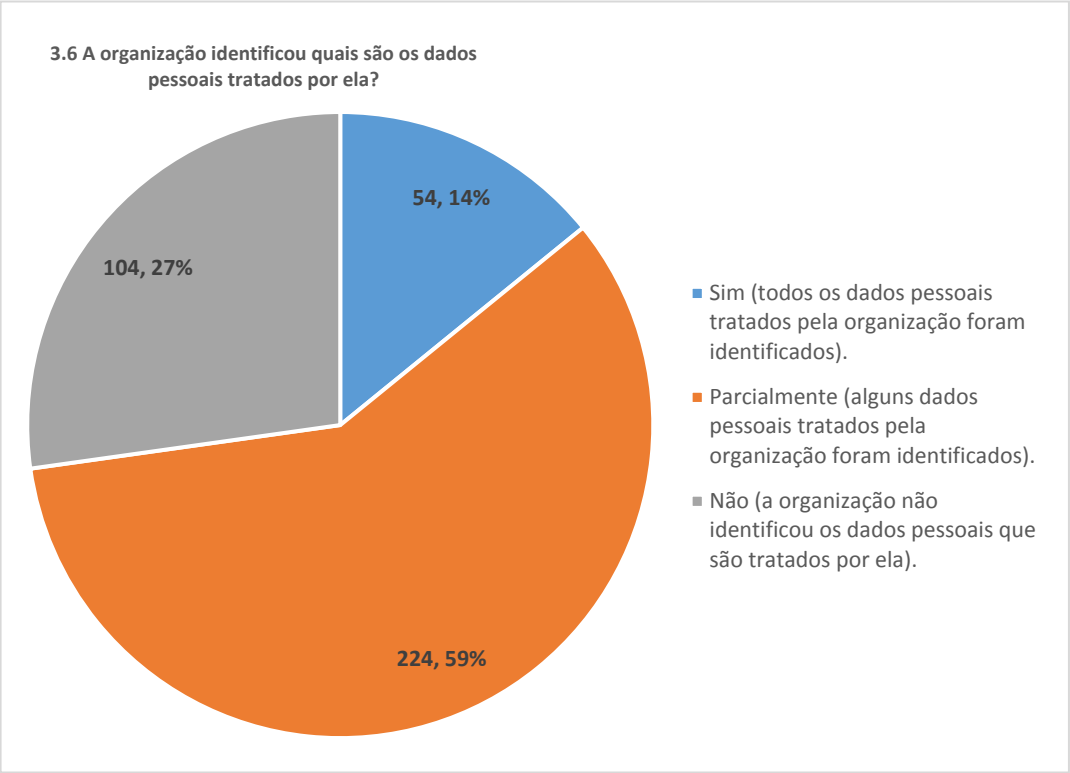
2.1.2.6 <u>Dados pessoais tratados</u>

92. *A questão 3.6 do questionário avaliou se as organizações identificaram os dados pessoais que são tratados por elas.*

93. *O dado pessoal é uma informação relacionada à pessoa natural identificada ou identificável (LGPD, art. 5º, inciso I), como: nome, número do documento de identidade, data de nascimento e endereço residencial. Obviamente, para prover a proteção de dados pessoais, é necessário saber quais desses dados são tratados pela organização. Ademais, a identificação dos dados pessoais é fundamental para viabilizar a manutenção do registro das operações de tratamento (LGPD, art. 37)*

94. *Todavia, as respostas ao questionário (Figura 12) demonstram que a minoria das organizações, 14%, identificou todos os dados pessoais que tratam.*

Figura 12 *- Identificação dos dados pessoais tratados pelas organizações*

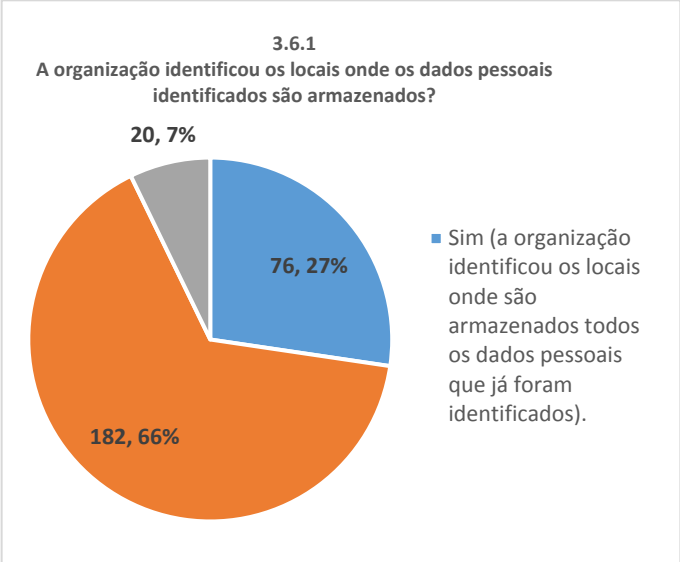


95. *Não basta saber quais dados pessoais são tratados pela organização, é necessário saber onde se encontram. Os dados pessoais podem ser armazenados em diferentes dispositivos, como: ativos de TI (e.g.: servidores de banco de dados, nuvem, dispositivo USB, storage e fita de backup) e arquivos físico (armários e pastas). Ademais, é importante que as organizações identifiquem o endereço onde os dados se encontram. Essas informações são úteis para a análise de riscos.*

96. *Diante disso, caso a organização respondesse que os dados foram identificados em sua totalidade ou parcialmente, era exibida a subquestão 3.6.1 para avaliar se foram identificados os locais onde esses dados são armazenados.*

97. *No entanto, constatou-se que apenas 27% dessas organizações identificaram os locais onde todos os dados pessoais são hospedados (Figura 13).*

Figura 13 *- Local onde os dados pessoais identificados são armazenados*



98. *No mesmo sentido do tópico anterior, o diagnóstico é preocupante, pois a identificação dos dados pessoais, bem como de sua localização, é necessária para a análise de riscos associados à*

privacidade. Além disso, a identificação desses dados, em conjunto com a dos processos que os manipulam, é fundamental para avaliar se as atividades de tratamento respeitam os princípios elencados no art. 6º da LGPD.

99. *Ante o exposto, e considerando que a SGD/ME já adotou ações para orientar os órgãos sob sua alçada acerca do assunto, a equipe de auditoria propõe* ***recomendar*** *ao CNJ e ao CNMP que, considerando o controle realizado sobre a atuação administrativa das organizações sob suas jurisdições, expeçam orientação quanto à identificação dos dados pessoais que são tratados por elas, bem como dos locais de armazenamento desses dados, considerando o disposto nos arts. 5º, inciso I, e 37 da LGPD e as diretrizes estabelecidas no item 7.2.8 da ABNT NBR ISO/IEC 27701:2019.*

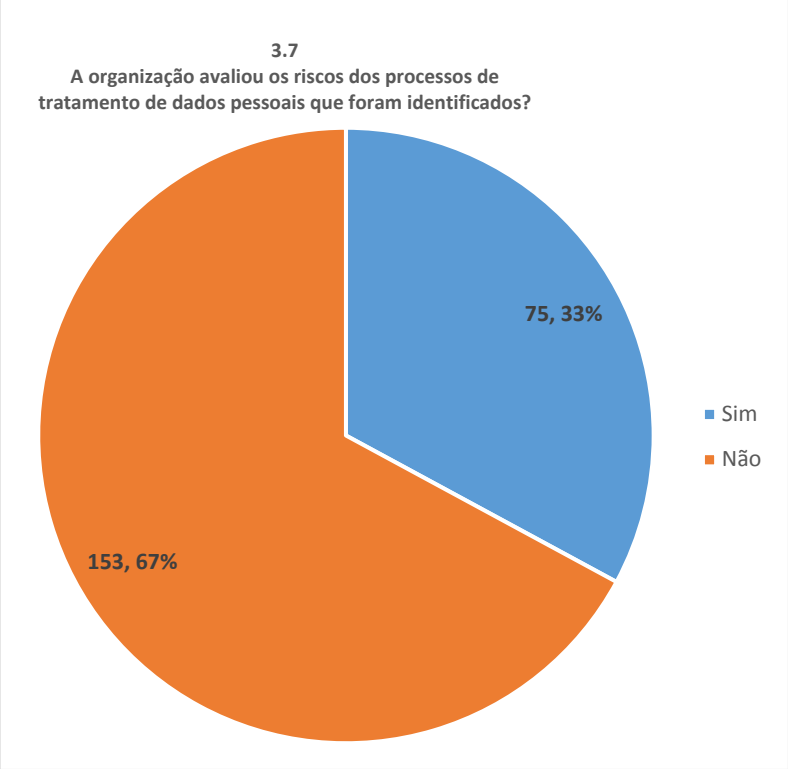
2.1.2.7 Riscos dos processos de tratamento de dados pessoais

100. *A questão 3.7 do questionário buscou apreciar se as organizações avaliaram os riscos inerentes aos processos de tratamento de dados pessoais. Esta questão foi exibida apenas para organizações que identificaram os processos organizacionais que realizam tratamento de dados pessoais (questão 3.5) e os respectivos dados pessoais (questão 3.6), de maneira integral ou parcial.*

101. *Em consonância com o disposto no art. 50, §2º, alínea 'd' da LGPD e no item 5.4.1.2 da ABNT NBR ISO/IEC 27701:2019, os riscos associados aos processos que realizam tratamento de dados pessoais devem ser avaliados para direcionar a definição de quais processos serão priorizados no projeto de adequação à LGPD.*

102. *No entanto, constatou-se que apenas 33% das organizações que responderam esta questão fizeram a análise de riscos (Figura 14).*

Figura 14 *- Avaliação dos riscos associados aos processos de tratamento de dados pessoais*



103. *Este diagnóstico retrata a ausência da cultura de gestão de riscos na APF. Ademais, cumpre frisar que a análise de riscos não deve ocorrer apenas durante o projeto de adequação, é algo que deve ser realizado continuamente. Por fim, é importante que a organização considere tanto as consequências que podem ocorrer para ela própria como para os titulares de dados pessoais caso os riscos se materializem.*

104. *Ante o exposto, e considerando que a SGD/ME já adotou ações para orientar os órgãos sob sua alçada acerca do assunto, a equipe de auditoria propõe* ***recomendar*** *ao CNJ e ao CNMP que,*

considerando o controle realizado sobre a atuação administrativa das organizações sob suas jurisdições, expeçam orientação quanto à avaliação de riscos relacionados aos processos de tratamento de dados pessoais, considerando o disposto no art. 50, §2º, alínea 'd', da LGPD e as diretrizes estabelecidas no item 5.4.1.2 da ABNT NBR ISO/IEC 27701:2019.

2.1.3. Liderança

105. *A alta direção deve demonstrar liderança e comprometimento com a iniciativa de adequação à LGPD. Além disso, a existência e a elaboração de políticas relacionadas à proteção de dados pessoais e a nomeação de um encarregado que tenha autonomia para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD são fundamentais para o processo de adequação.*

106. *As questões desta seção são relacionadas à nomeação do encarregado e à existência de políticas que buscam assegurar a segurança das informações e a proteção dos dados pessoais.*

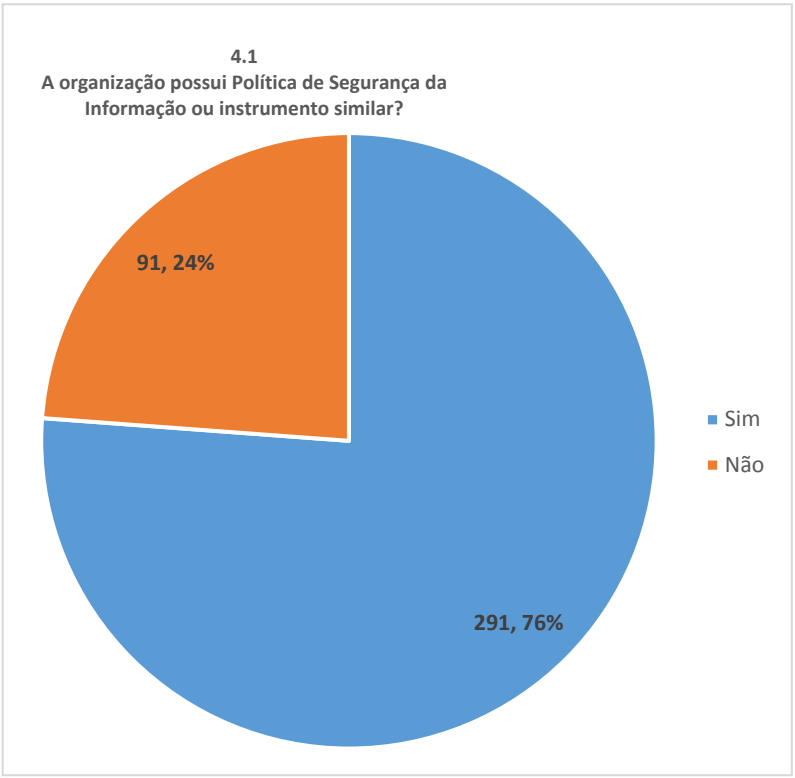
2.1.3.1 Política de Segurança da Informação

107. *A questão 4.1 do questionário buscou avaliar se as organizações possuíam Política de Segurança da informação ou instrumento similar.*

108. *Em consonância com o disposto no item 6.2.1.1 da ABNT NBR ISO/IEC 27701:2019, uma Política de Segurança da Informação estabelece a abordagem da organização para gerenciar os objetivos de segurança da informação. Tal política deve ser aprovada pela alta direção e estar de acordo com os requisitos de negócio e com leis e regulamentações aplicáveis.*

109. *As respostas ao questionário (Figura 15) demonstram que 24% das organizações não possuem Política de Segurança da Informação ou instrumento similar.*

***Figura 15** - Existência de Política de Segurança da Informação*



110. *O resultado é alarmante, pois, mesmo abrangendo a minoria, a análise do número por outra perspectiva leva à conclusão de que cerca de uma em cada quatro organizações não possui a política, o que é grave, pois a segurança da informação é um dos pilares que viabilizam a proteção de dados pessoais.*

111. *Por fim, cumpre ressaltar que a primeira versão da ABNT ISO/IEC 27002 – norma internacional projetada para as organizações usarem como referência na seleção de controles para implementação de um sistema de gestão de segurança da informação – foi publicada em 2005. Desde*

então, o tema ganhou relevância, tanto que o TCU, nos levantamentos de governança realizados a partir de 2007, tem questionado as organizações públicas federais quanto à necessidade de adotarem práticas de gestão de segurança da informação, o que inclui a elaboração da Política de Segurança da Informação.

112. *Destaca-se que, por meio do emblemático Acórdão 1.233/2012, de relatoria do Ministro Aroldo Cedraz, o Plenário do TCU recomendou ao CNJ e ao CNMP que, dentre outras medidas, orientassem os entes sob suas jurisdições na implementação dos seguintes controles de segurança da informação: nomeação de responsável pela segurança da informação na organização, criação de comitê para coordenar os assuntos de segurança da informação, definição de processo de gestão de riscos de segurança da informação, estabelecimento de política de segurança da informação, definição de processo de elaboração de inventário de ativos e definição de processo de classificação da informação (itens 9.13.9 e 9.15.12). Por meio do mesmo acórdão, o Plenário recomendou ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR) que orientasse os órgãos e entidades sob sua jurisdição que a implantação dos controles gerais de segurança da informação positivados em suas normas não é faculdade, mas obrigação da alta administração, e a não implantação, sem justificativa, é passível da aplicação de multa pelo TCU (item 9.8.2).*

113. *Recentemente, no âmbito do Poder Executivo Federal, o Decreto 9.637/2018 – que instituiu a Política Nacional de Segurança da Informação (PNSI) – determinou, em seu art. 15, inciso II, que compete aos órgãos e às entidades da administração pública federal 'elaborar sua política de segurança da informação e as normas internas de segurança da informação, observadas as normas de segurança da informação editadas pelo Gabinete de Segurança Institucional da Presidência da República'. Nesse sentido, destaca-se a Instrução Normativa GSI/PR 1/2020 que, em seu art. 9º, estabeleceu a obrigatoriedade a todos os órgãos e entidades da administração pública federal de possuírem uma Política de Segurança da Informação.*

114. *No mesmo sentido, a Resolução CNJ 396/2021 – que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário – determinou, em seu art. 19, inciso II, que compete à alta administração de cada órgão 'elaborar a Política de Segurança da Informação e normas internas correlatas ao tema, observadas as normas de segurança da informação editadas pelo CNJ'. Já a Resolução CNMP 156/2016 – que instituiu a Política de Segurança Institucional e o Sistema Nacional de Segurança Institucional do Ministério Público (SNS/MP) – determinou, em seu art. 22, inciso III, que cabe às instituições que compõem SNS/MP 'instituir política e plano de segurança institucional, planos de segurança orgânica [incluindo a segurança da informação] e normas e procedimentos necessários à execução de tais planos (...)'.*

115. *Diante do exposto, a equipe de auditoria propõe* ***dar ciência*** *às 91 organizações que informaram, por meio de resposta ao questionário, que não possuem Política de Segurança da Informação, ou instrumento similar, que a ausência do referido documento afronta o disposto nos normativos de referência.*

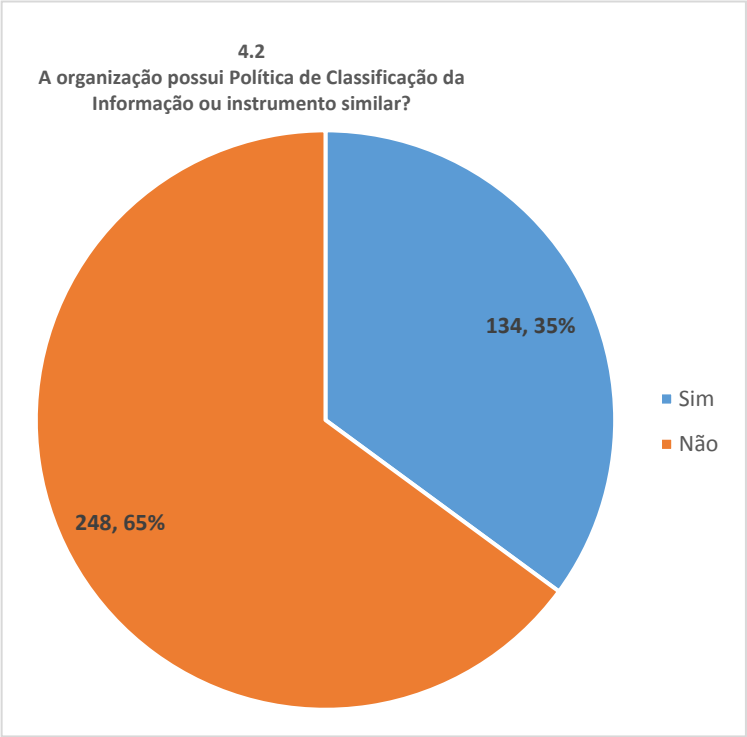
2.1.3.2 <u>Política de Classificação da Informação</u>

116. *A questão 4.2 do questionário buscou avaliar se as organizações possuíam Política de Classificação da Informação ou instrumento similar.*

117. *Em consonância com o disposto no item 6.5.2 da ABNT NBR ISO/IEC 27701:2019, uma Política de Classificação da Informação deve fornecer diretrizes para assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância. O tema também é abordado em outros normativos como a Lei de Acesso à Informação, Lei 12.527/2011, que explora, no art. 24, a classificação da informação quanto ao grau de sigilo.*

118. *No entanto, as respostas do questionário (Figura 16) demonstram que apenas 35% das organizações possuem Política de Classificação da Informação.*

Figura 16 *- Existência de Política de Classificação da Informação*

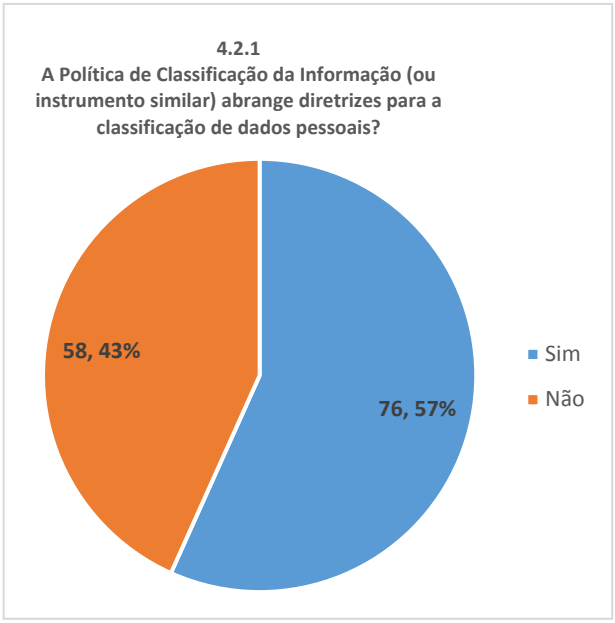


119. *Semelhante ao citado no capítulo anterior, a Política de Classificação da Informação é mencionada desde a primeira versão da norma ABNT ISO/IEC 27002 e deveria ser contemplada em mais organizações.*

120. *Vale ressaltar que o questionamento quanto à existência da política em questão se deu pelo fato de a classificação da informação ser importante para a proteção de dados pessoais, pois viabiliza que estes sejam identificados e tratados adequadamente (item 6.5.2 da ABNT NBR ISO/IEC 27701:2019). Diante disso, caso a organização respondesse que possuía Política de Classificação da Informação, era exibida a subquestão 4.2.1 para avaliar se a referida política abrangia diretrizes para a classificação de dados pessoais.*

121. *As respostas (Figura 17) demonstram que a maioria das organizações que possui Política de Classificação da Informação, 57%, providenciou a adequação da política para contemplar diretrizes para a classificação de dados pessoais.*

Figura 17 *- Diretrizes para a identificação de dados pessoais na Política de Classificação da Informação*



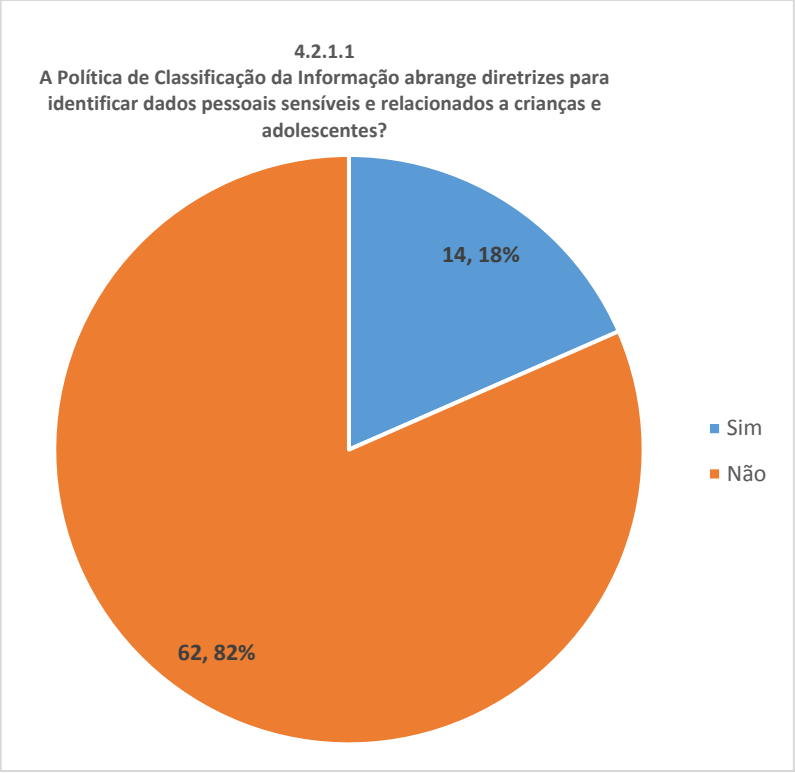
122. *As organizações que ainda não atualizaram a política para contemplar a classificação de dados pessoais devem providenciar tal alteração.*

123. *Ainda quanto à classificação da informação, a LGPD demanda que sejam adotados cuidados específicos para o tratamento de dados pessoais sensíveis, que abrangem dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (LGPD, art. 5º, inciso II, e art. 11). O mesmo ocorre com o tratamento de dados pessoais de crianças e adolescentes (LGPD, art. 14).*

124. *Diante disso, caso a organização afirmasse que a Política de Classificação da Informação abrangia a classificação de dados pessoais, era exibida outra subquestão, 4.2.1.1, para avaliar se a política abrangia diretrizes para a classificação de dados pessoais sensíveis e de crianças e adolescentes.*

125. *No entanto, constatou-se que apenas 18% das organizações que responderam esta questão contemplaram diretrizes para classificação desses dados (Figura 18).*

Figura 18 *- Existência de diretrizes para identificação de dados pessoais sensíveis e de crianças e de adolescentes na Política de Classificação da Informação*



126. *Como os dados pessoais sensíveis e de crianças e adolescentes demandam a adoção de controles mais rigorosos, as organizações precisam contemplar diretrizes para a identificação desses dados na Política de Classificação da Informação.*

127. *Por fim, apesar de o foco desta fiscalização ser na avaliação de aspectos ligados à LGPD, cumpre ressaltar que a referida política não deve focar apenas em dados pessoais, é necessário que as organizações tenham a política também para justificar a não divulgação de outras informações, uma vez que a publicidade é a regra e que o sigilo deve ser amparado por justificativas plausíveis. Do mesmo modo, a inexistência de uma política consistente pode potencializar o risco de divulgação de informações sensíveis, que não deveriam ser divulgadas.*

128. *Ante o exposto, a equipe de auditoria propõe* ***recomendar*** *à SGD/ME, ao CNJ e ao CNMP que, considerando o controle realizado sobre a atuação administrativa das organizações sob suas jurisdições, expeçam orientação quanto à elaboração de Política de Classificação da Informação que*

considere a classificação de dados pessoais, considerando o disposto nos arts. 5º, inciso II, 11 e 14 da LGPD e no art. 31, § 1º, da Lei 12.527/2011, bem como as diretrizes estabelecidas no item 6.5.2 da ABNT NBR ISO/IEC 27701:2019.

2.1.3.3 Política de Proteção de Dados Pessoais

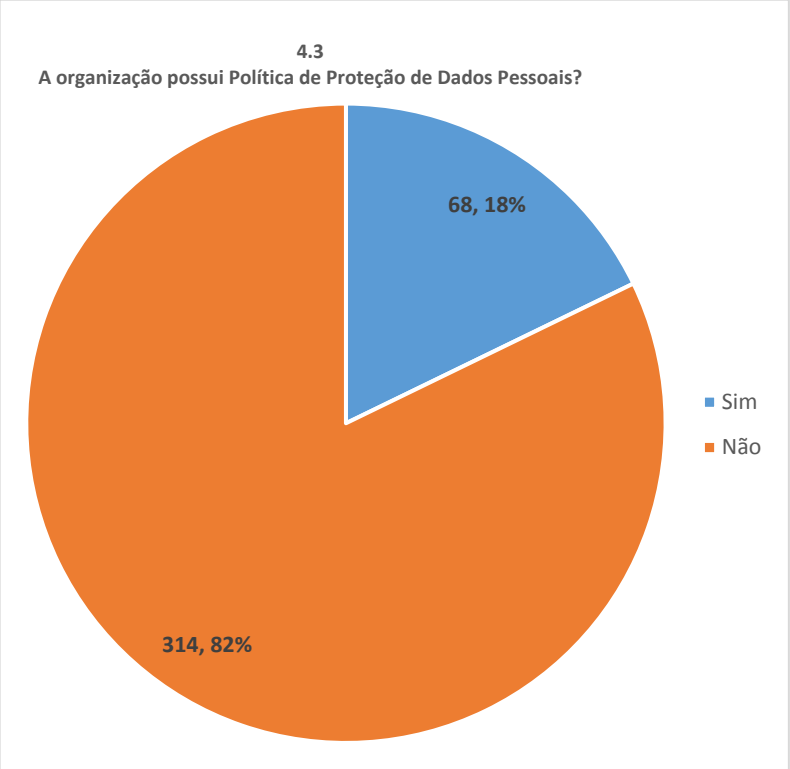
129. *A questão 4.3 do questionário buscou avaliar se as organizações possuíam Política de Proteção de Dados Pessoais ou instrumento similar.*

130. *A Política de Proteção de Dados Pessoais deve estar alinhada com a Política de Segurança da Informação e com a Política de Classificação da Informação e deve fornecer diretrizes para assegurar que as organizações alcancem a conformidade com os normativos de proteção de dados pessoais (item 6.2.1.1 da ABNT NBR ISO/IEC 27701:2019).*

131. *Cumpre ressaltar que a Política de Proteção de Dados Pessoais não se confunde com a Política de Privacidade. A primeira é voltada para o público interno da organização enquanto a segunda é direcionada ao público externo.*

132. *As respostas fornecidas pelas organizações (Figura 19) mostram que apenas 18% das organizações possuem Política de Proteção de Dados Pessoais ou documento similar.*

***Figura 19** - Existência de Política de Proteção de Dados Pessoais*



133. *É importante que as organizações instituam uma Política de Proteção de Dados Pessoais para estabelecer diretrizes e para demonstrar o seu comprometimento no que tange ao cumprimento dos regulamentos de proteção de dados pessoais. Ademais, essas diretrizes podem ser definidas e publicadas em um documento específico ou acrescentadas no texto da Política de Segurança da Informação.*

134. *Ante o exposto, a equipe de auditoria propõe **recomendar** à SGD/ME, ao CNJ e ao CNMP que, considerando o controle realizado sobre a atuação administrativa das organizações sob suas jurisdições, expeçam orientação quanto à elaboração de Política de Proteção de Dados Pessoais, considerando as diretrizes estabelecidas no item 6.2.1.1 da ABNT NBR ISO/IEC 27701:2019.*

2.1.3.4 Encarregado

135. *A questão 4.4 do questionário avaliou se as organizações nomearam o encarregado pelo tratamento de dados pessoais. Vale ressaltar que, no caso do papel do encarregado, deve ser nomeada*

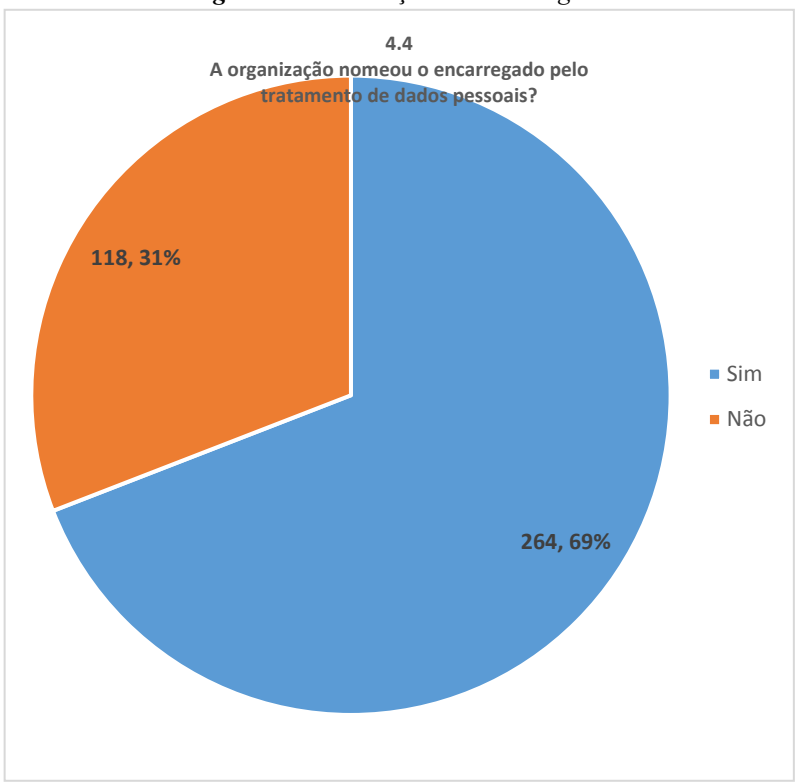
uma pessoa responsável pelo cargo, diferentemente do papel do controlador, que deve ser a própria organização.

136. *O encarregado é a pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares de dados pessoais e a ANPD (LGPD, art. 5º, inciso VIII). O termo DPO (do inglês Data Protection Officer) é comumente utilizado para se referir ao encarregado.*

137. *Em consonância com o disposto na IN SGD/ME 117/2020, art. 1º, §1º, inciso I, convém que o encarregado detenha, além de sólidos conhecimentos da LGPD, conhecimentos relativos a temas associados à legislação como: Direito, Governança Corporativa, Gestão de Riscos, Tecnologia da Informação e Segurança da Informação.*

138. *As respostas do questionário (Figura 20) demonstram que a maioria das organizações, 69%, nomeou o encarregado.*

***Figura 20** - Nomeação do encarregado*



139. *Todavia, não basta nomear o encarregado, é conveniente que a nomeação seja publicada em veículo de comunicação oficial como o Diário Oficial da União (DOU). No mesmo sentido, a LGPD, no § 1º do art. 41, determina que a identidade e as informações de contato (e.g.: e-mail e telefone) do encarregado sejam divulgadas publicamente, preferencialmente no sítio eletrônico da organização. Diante do exposto, caso a organização respondesse que nomeou o encarregado, eram exibidas as subquestões 4.4.1 – para avaliar se a nomeação foi publicada em veículo de comunicação oficial – e 4.4.3 – para verificar se as identidades e as informações de contato do encarregado foram divulgadas na internet.*

140. *A partir da análise das respostas (Figura 21), constata-se que a maioria, 75%, das organizações que nomeou o encarregado providenciou a publicação da nomeação em meio de comunicação oficial. O mesmo ocorreu com a divulgação da identidade e das informações de contato na internet (Figura 22), onde 67% dessas organizações informaram que realizaram tal divulgação.*

Figura 21 *- Publicação da nomeação do encarregado em veículo de comunicação oficial*

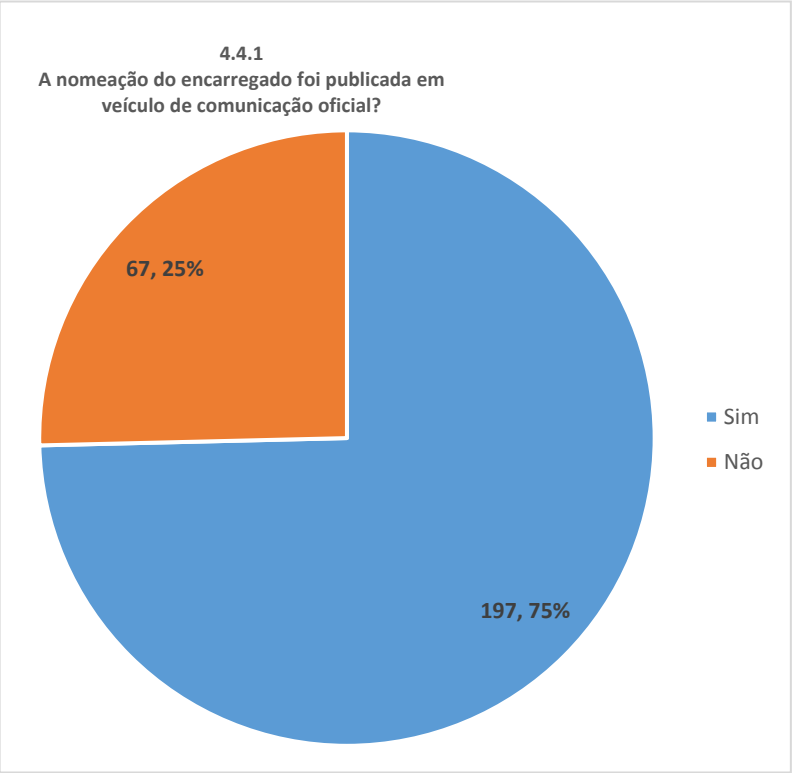
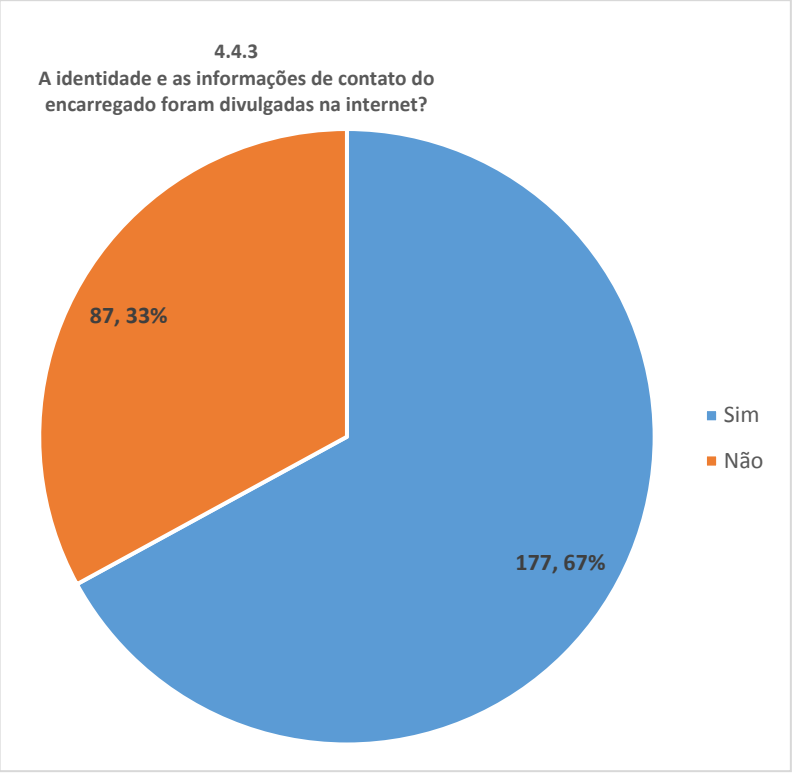


Figura 22 *- Divulgação de informações do encarregado na internet*

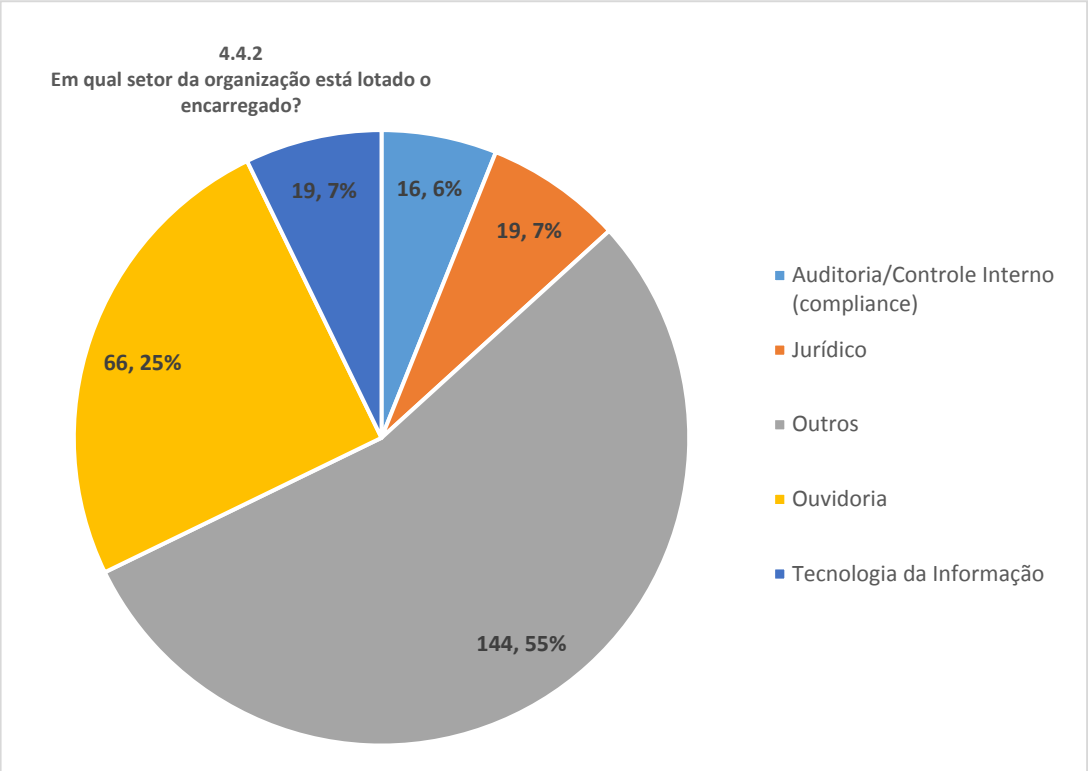


141. *Por fim, caso a organização informasse que designou o encarregado, também foi exibida a subquestão 4.4.2 para verificar em qual setor estaria lotada a pessoa designada. Esse questionamento foi realizado porque, conforme descrito no item 6.3.1.1 da ABNT NBR ISO/IEC 27701:2019, o encarregado deve ser independente e ter liberdade para reportar ao nível gerencial apropriado para assegurar a efetiva gestão de riscos de privacidade. Além disso, em consonância com o disposto na IN SGD/ME 117/2020, art. 1º, inciso II, é recomendável que o encarregado não faça parte de um setor no*

qual possa haver conflito de interesses, pois, em caso de vazamento de dados pessoais podem ser omitidas, propositalmente, informações relevantes.

142. *As respostas ao questionário (Figura 23) mostram que boa parte dos encarregados, 25%, está lotada na Ouvidoria. Os setores de Tecnologia da Informação (TI), Jurídico e Auditoria/Controle Interno obtiveram percentual aproximado de 7%.*

***Figura 23** - Lotação do encarregado*



143. *A nomeação do encarregado pertencente à Ouvidoria pode ocorrer porque o setor já possui estrutura consistente para atendimento de requisições externas, o que tende a facilitar a implementação de controles associados aos direitos dos titulares. No entanto, pode haver casos em que a Ouvidoria não possui acesso direto ao nível de gestão apropriado para assegurar a gestão de riscos de privacidade. O mesmo pode ocorrer com outros setores.*

144. *Assim, não é sem motivo que a IN SGD/ME 117/2020 é clara ao informar, no art. 1º, inciso II, que o encarregado não deve se encontrar lotado em unidades de TI ou ser gestor de sistemas de informação.*

145. *Em suma, é importante que o encarregado tenha independência e acesso à alta administração. Diante disso, é recomendável que as organizações avaliem se o encarregado possui as características citadas para providenciarem os devidos ajustes.*

146. *Ademais, cumpre frisar que na legislação europeia o papel do encarregado possui mais atribuições do que o disposto na lei brasileira. No entanto, o papel é relevante para o sucesso das iniciativas de adequação e para estimular a implantação da cultura de proteção de dados nas organizações.*

147. *É importante mencionar também que, no âmbito do setor privado, existem situações em que organizações tem optado por contratar o encarregado de proteção de dados como um serviço (DPO as a service), terceirizando a atividade para empresas desempenharem a função, prática que deve ser vista com cautela pelo poder público devido ao papel estratégico a ela atribuído pela legislação.*

148. *Em seu guia publicado recentemente**Error! Bookmark not defined.**, a ANPD explica a definição de encarregado pelo tratamento de dados e suas atribuições conforme a LGPD, mas não orienta sobre os perfis e requisitos profissionais desejáveis e nem sobre os locais apropriados de lotação do*

encarregado, o que ainda pode ser feito por meio de norma complementar, conforme possibilita o art. 41, § 3º, da LGPD.

149. *Diante do exposto, a equipe de auditoria propõe* ***recomendar*** *à ANPD que oriente as organizações públicas quanto às responsabilidades, aos perfis e requisitos profissionais desejáveis, bem como sobre os locais apropriados de lotação do encarregado no normativo relacionado ao tema que está previsto na agenda regulatória da instituição, em consonância com o disposto no art. 41, § 3º, da Lei 13.709/2018.*

2.1.4. Capacitação

150. *A organização deve conduzir iniciativas para conscientizar e capacitar os colaboradores em proteção de dados pessoais.*

151. *A conscientização é importante para que os colaboradores conheçam as políticas organizacionais relacionadas à proteção de dados pessoais e para que reconheçam como suas ações são relevantes para a preservação da privacidade dos titulares.*

152. *As ações de capacitação devem considerar diferentes níveis de envolvimento dos colaboradores no tema, de forma que aqueles que ocupam funções com responsabilidades essenciais, relacionadas à proteção de dados pessoais, recebam treinamento diferenciado, além do nível básico fornecido aos demais.*

153. *Nesta seção foram abordadas questões para avaliar o planejamento e a realização de ações de conscientização e de capacitação.*

2.1.4.1 Plano de Capacitação

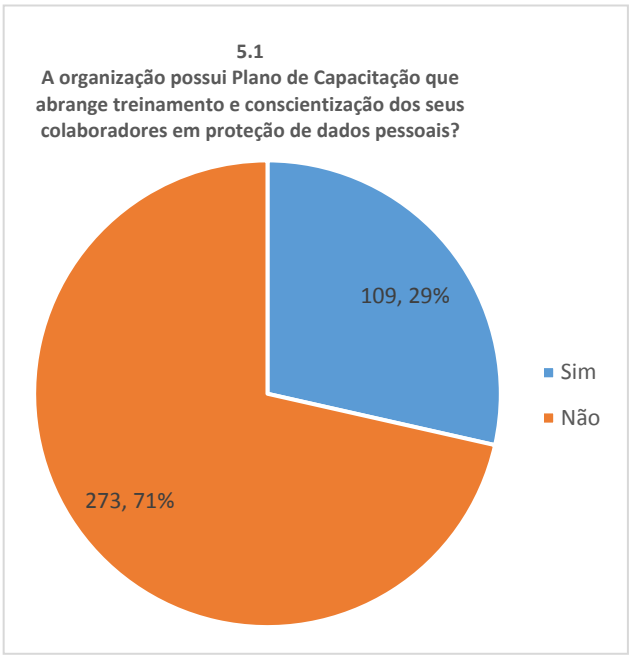
154. *A questão 5.1 do questionário buscou verificar se as organizações elaboraram Plano de Capacitação para direcionar o treinamento e a conscientização dos colaboradores em proteção de dados pessoais.*

155. *Em consonância com o disposto no item 5.5.2 da ABNT NBR ISO/IEC 27701:2019, é conveniente que cada organização elabore um plano de capacitação para determinar as competências necessárias para os recursos humanos envolvidos em atividades que realizam o tratamento de dados pessoais. O referido plano deve mapear as lacunas de conhecimento associadas ao tema, bem como planejar ações de treinamento para redução dessas lacunas.*

156. *Além do foco voltado para as pessoas diretamente envolvidas em atividades de tratamento de dados pessoais, é coerente que recursos humanos que não estão diretamente ligados a esse tipo de atividade sejam conscientizados quanto à importância do tema e dos impactos que podem ser causados em casos de violação de dados pessoais, conforme relatado no item 5.5.3 da ABNT NBR ISO/IEC 27701:2019. Diante do exposto, conclui-se que o plano de capacitação deve contemplar ações de treinamento e de conscientização. No entanto, nada impede que a organização elabore planos apartados: um para treinamento e outro para conscientização.*

157. *As respostas à questão 5.1 (Figura 24) demonstram que a minoria das organizações, 29%, possui Plano de Capacitação que abrange a proteção de dados pessoais.*

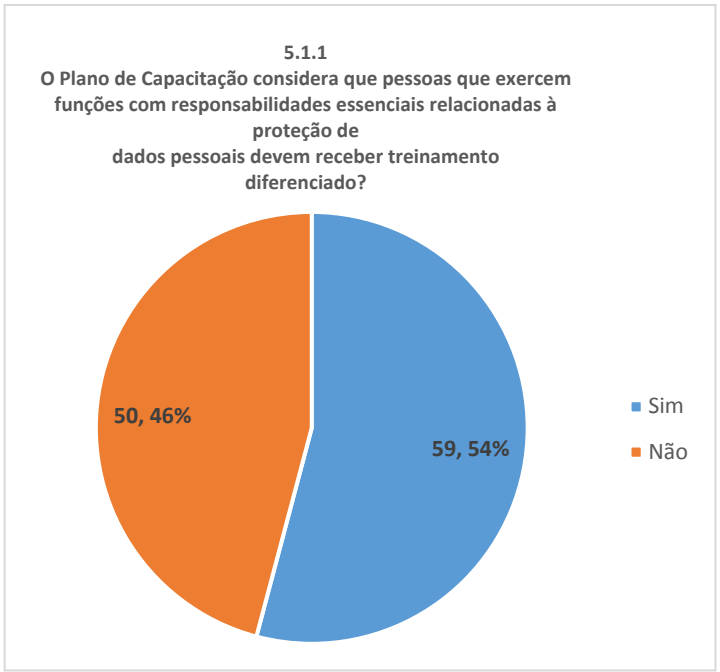
Figura 24 *- Existência de plano de capacitação*



158. *O resultado é preocupante, pois a LGPD é uma legislação técnica e complexa, que exige estudo para que as organizações adquiram maturidade no tema. Para que a maturidade seja alcançada, é fundamental que os colaboradores sejam treinados e conscientizados em proteção de dados pessoais.*

159. *No mesmo sentido, para averiguar a qualidade dos planos de capacitação que foram elaborados, caso a organização afirmasse ter produzido o artefato, era exibida a subquestão 5.1.1 para avaliar se o plano considerava que pessoas que exercem funções com responsabilidades essenciais relacionadas à proteção de dados pessoais deveriam receber treinamento diferenciado. No entanto, constatou-se que quase metade das organizações que elaboraram o plano, 46%, não consideraram essa necessidade (Figura 25).*

Figura 25 *- Consideração de treinamento diferenciado para pessoas que exercem funções relevantes para a proteção de dados pessoais*



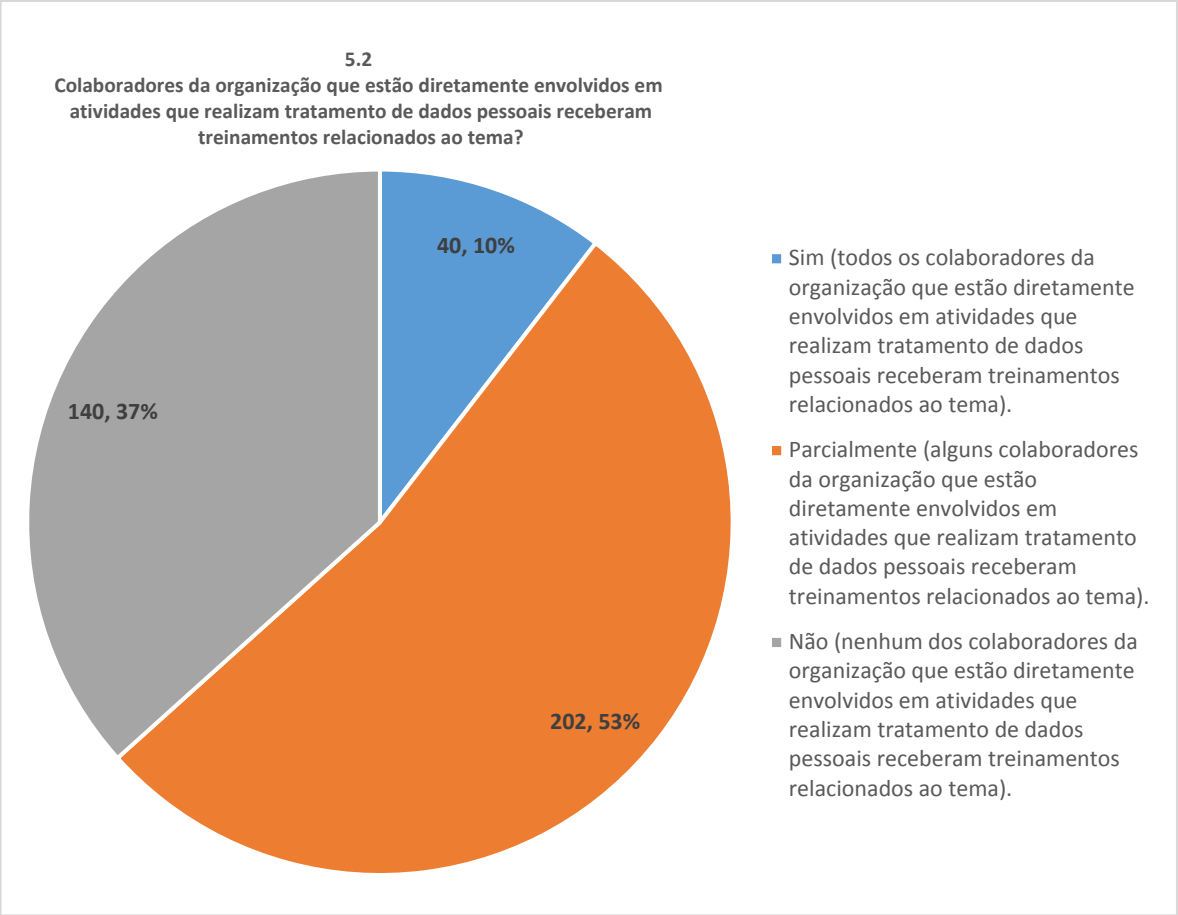
160. *O resultado demonstra a necessidade de as organizações planejarem, com cuidado, o treinamento e a conscientização dos seus colaboradores.*

2.1.4.2 Treinamento de colaboradores envolvidos em atividades que realizam tratamento de dados pessoais

161. *A questão 5.2 buscou avaliar se as pessoas diretamente envolvidas em atividades que realizam tratamento de dados pessoais já participaram de treinamentos relacionados ao tema.*

162. *As respostas (Figura 26) demonstram que apenas 10% das organizações treinaram todos os colaboradores diretamente envolvidos em atividades que realizam tratamento de dados pessoais.*

***Figura 26** - Treinamento de colaboradores diretamente envolvidos no tratamento de dados pessoais*



163. *Como a LGPD está em vigência há quase um ano, os colaboradores diretamente envolvidos em atividades que realizam tratamento de pessoais já deveriam ter participado de treinamentos correlatos ao tema.*

164. *Ante o exposto, a equipe de auditoria propõe **recomendar** à SGD/ME, ao CNJ e ao CNMP que, considerando o controle realizado sobre a atuação administrativa das organizações sob suas jurisdições, expeçam orientação quanto à elaboração de Plano de Capacitação que considere a realização de treinamento e conscientização dos colaboradores em proteção de dados pessoais, considerando as diretrizes estabelecidas nos itens 5.5.2 e 5.5.3 da ABNT NBR ISO/IEC 27701:2019.*

2.1.5. Conformidade do tratamento

165. *A organização deve ser capaz de provar que os tratamentos de dados pessoais que realiza são lícitos. Para isso, deve demonstrar que os princípios estabelecidos pela LGPD são seguidos e que os tratamentos são fundamentados em, ao menos, uma das bases legais descritas na legislação.*

166. *Nesta seção são abordadas questões para avaliar se os tratamentos estão em conformidade com alguns dos princípios e se estão fundamentados em alguma base legal. Também foi avaliado se a organização possui registro para documentar detalhes das atividades de tratamento.*

2.1.5.1 Finalidades das atividades de tratamento de dados pessoais

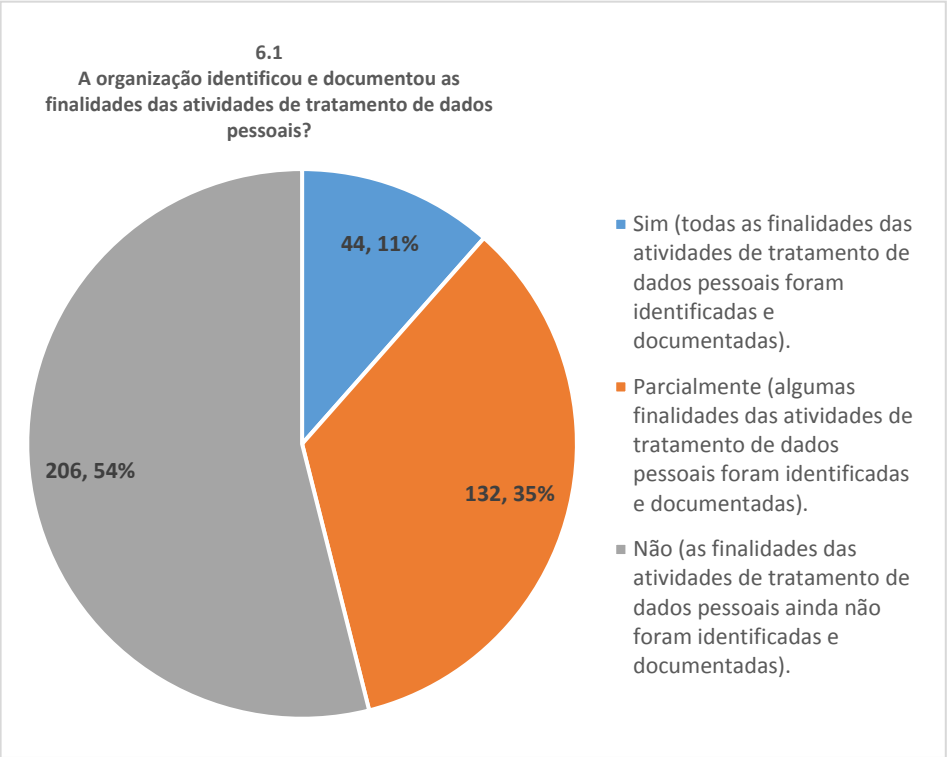
167. *A questão 6.1 do questionário buscou verificar se as organizações identificaram e documentaram as finalidades das atividades de tratamento de dados pessoais.*

168. *Dentre os princípios que as atividades de tratamento de dados pessoais devem observar, destaca-se o da finalidade, que se caracteriza pela realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível (LGPD, art. 6º, inciso I).*

169. *No mesmo sentido, o item 7.2.1 da ABNT NBR ISO/IEC 27701:2019 recomenda que a organização identifique e documente os propósitos específicos para o tratamento dos dados pessoais, bem como assegure que os titulares entendam esses propósitos.*

170. *Entretanto, as respostas à questão 6.1 (Figura 27) mostraram que somente 11% das organizações identificaram e documentaram todas as finalidades das atividades de tratamento de dados pessoais.*

***Figura 27** - Identificação e documentação das atividades de tratamento de dados pessoais*



171. *Ante o exposto, e considerando que a SGD/ME já adotou ações para orientar os órgãos sob sua alçada acerca do assunto, a equipe de auditoria propõe **recomendar** ao CNJ e ao CNMP que, considerando o controle realizado sobre a atuação administrativa das organizações sob suas jurisdições, expeçam orientação quanto à identificação e à documentação das finalidades das atividades de tratamento de dados pessoais, considerando o disposto no art. 6º, inciso I, da LGPD e as diretrizes estabelecidas no item 7.2.1 da ABNT NBR ISO/IEC 27701:2019.*

172. *Ademais, caso a organização informasse que identificou parte ou a totalidade das finalidades das atividades de tratamento de dados pessoais, eram exibidas as subquestões 6.1.1 e 6.1.2. A primeira para verificar se as organizações avaliaram se coletam apenas os dados estritamente necessários para cumprir com as finalidades de tratamento de dados pessoais (LGPD, art. 6º, incisos II e III; e item 7.4.1 da ABNT NBR ISO/IEC 27701:2019). A segunda para avaliar se as organizações analisaram se os dados pessoais são retidos (armazenados) durante o tempo estritamente necessário para cumprir com as mesmas finalidades (item 7.4.7 da ABNT NBR ISO/IEC 27701:2019).*

173. *Entretanto, a maioria das organizações que respondeu à questão 6.1.1, 51%, não avaliou se coleta apenas os dados estritamente necessários para cumprir com as finalidades (Figura 28). Ao passo que 61% dessas organizações não avaliaram se os dados pessoais são retidos (armazenados) durante o tempo estritamente necessário para cumprir com as finalidades elencadas (Figura 29).*

Figura 28 *- Avaliação quanto à coleta de dados estritamente necessários às finalidades de tratamento*

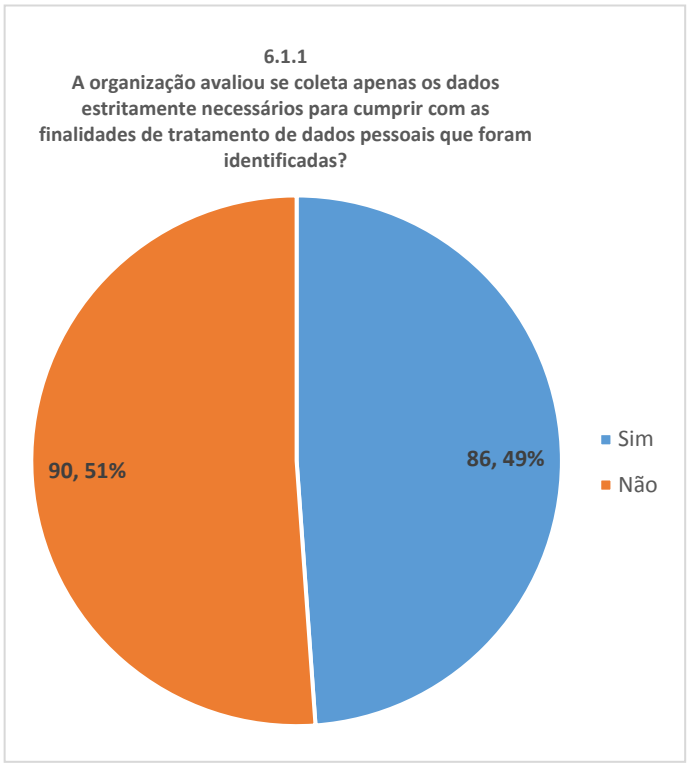
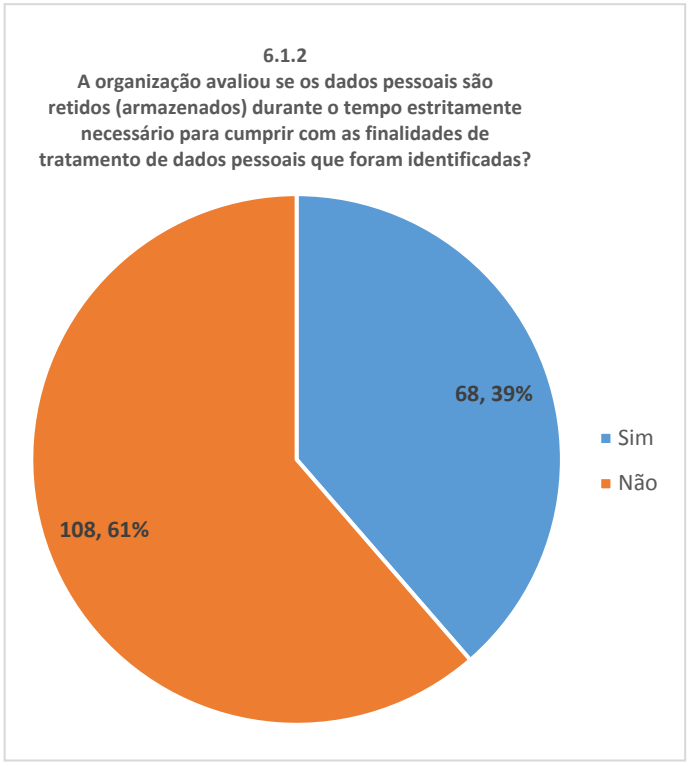


Figura 29 *- Avaliação quanto ao tempo em que os dados pessoais são retidos*



174. *As respostas às questões exploradas neste tópico demonstram a necessidade de as organizações avaliarem e definirem as finalidades dos processos de tratamento de dados pessoais. A coleta de dados pessoais estritamente necessários para cumprir com as finalidades merece atenção especial, pois é comum que as organizações coletem dados desnecessários. Ademais, quanto ao tempo de guarda de registros, vale ressaltar que, conforme descrito no art. 40 da LGPD, a ANPD poderá dispor sobre o assunto.*

175. *Ante o exposto, e considerando que a SGD/ME já adotou ações para orientar os órgãos sob sua alçada acerca do assunto, a equipe de auditoria propõe* ***recomendar*** *ao CNJ e ao CNMP que, considerando o controle realizado sobre a atuação administrativa das organizações sob suas jurisdições, expeçam orientação quanto à necessidade de avaliar se coletam apenas os dados estritamente necessários para as finalidades de tratamento de dados pessoais e se os dados são retidos durante o tempo estritamente necessário às mesmas necessidades, considerando o disposto no art. 6º, incisos II e III, da LGPD e as diretrizes estabelecidas nos itens 7.4.1 e 7.4.7 da ABNT NBR ISO/IEC 27701:2019.*

2.1.5.2 Bases legais

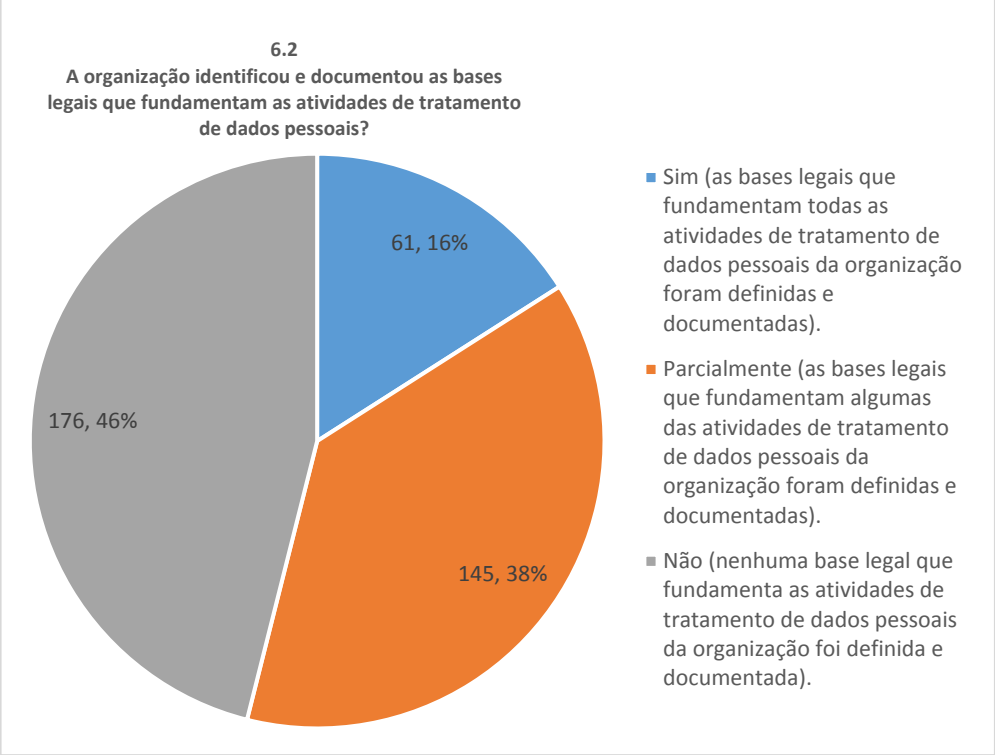
176. *A questão 6.2 do questionário buscou avaliar se as organizações identificaram e documentaram as bases legais que fundamentam as atividades de tratamento de dados pessoais.*

177. *Na LGPD, a bases legais estão definidas no art. 7º, que relaciona dez hipóteses nas quais tratamento de dados pessoais poderá ser realizado: mediante o fornecimento de consentimento pelo titular; para o cumprimento de obrigação legal ou regulatória pelo controlador; pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas; para a realização de estudos por órgão de pesquisa; quando necessário para a execução de contrato; para o exercício regular de direitos em processo judicial, administrativo ou arbitral; para a proteção da vida ou da incolumidade física do titular ou de terceiro; para a tutela da saúde; quando necessário para atender aos interesses legítimos do controlador ou de terceiro; e para a proteção do crédito.*

178. *Sob a mesma perspectiva, o item 7.2.2 da ABNT NBR ISO/IEC 27701:2019 recomenda que a organização determine, documente e esteja em compliance com a base legal pertinente para o tratamento de dados, para os propósitos identificados.*

179. *Entretanto, as respostas à questão 6.2 (Figura 30) mostraram que quase metade das organizações, 46%, afirmou que nenhuma base legal que fundamenta as atividades de tratamento de dados pessoais foi identificada e documentada.*

Figura 30 *- Identificação e documentação das bases legais*



180. *As respostas às questões exploradas neste tópico demonstram a necessidade de as organizações fundamentarem as atividades de tratamento de dados pessoais em bases legais. Além disso, vale ressaltar que a legislação não impede que uma atividade de tratamento seja fundamentada em mais de uma base legal.*

181. *Ademais, cumpre destacar que as organizações públicas devem se atentar ao art. 23 da LGPD ao analisar as bases legais, pois o referido artigo cita que o tratamento de dados por organizações públicas deve ser realizado para atendimento da finalidade pública, na persecução do interesse público, com o intuito de executar as competências legais ou cumprir as atribuições legais do serviço público.*

182. *Ante o exposto, e considerando que a SGD/ME já adotou ações para orientar os órgãos sob sua alçada acerca do assunto, a equipe de auditoria propõe* ***recomendar*** *ao CNJ e ao CNMP que, considerando o controle realizado sobre a atuação administrativa das organizações sob suas jurisdições, expeçam orientação quanto à identificação e à documentação das bases legais que fundamentam as atividades de tratamento de dados pessoais, considerando o disposto nos arts. 7º e 23 da LGPD e as diretrizes estabelecidas no item 7.2.2 da ABNT NBR ISO/IEC 27701:2019.*

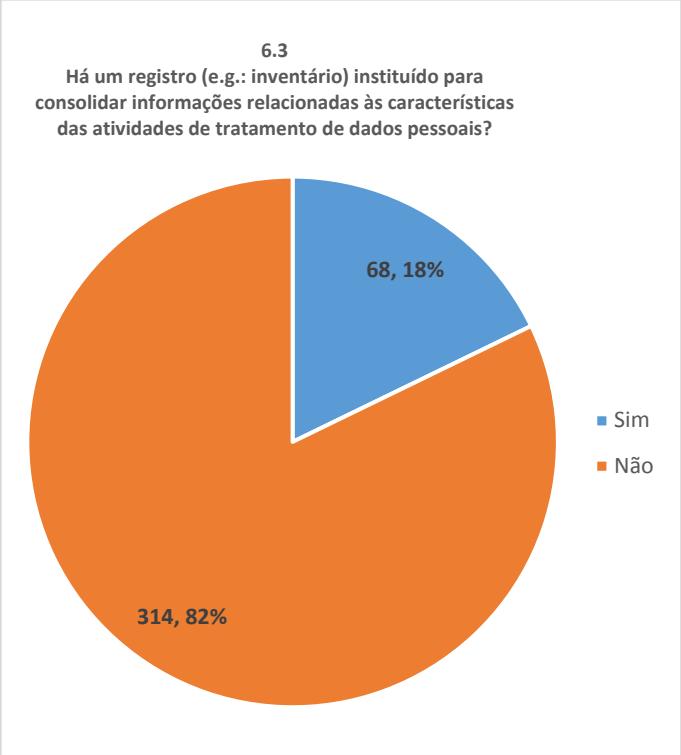
2.1.5.3 Registro das operações de tratamento de dados pessoais

183. *A questão 6.3 do questionário buscou verificar se as organizações possuem um registro (e.g.: inventário) instituído para consolidar informações relacionadas às características das atividades de tratamento de dados pessoais.*

184. *De acordo com o art. 37 da LGPD, o controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem. Outrossim, o item 7.2.8 da ABNT NBR ISO/IEC 27701:2019 cita que é conveniente que a organização mantenha, de maneira segura, os registros necessários ao suporte às suas obrigações para o tratamento de dados pessoais e que uma maneira de manter os registros de tratamento de dados pessoais é por meio de um inventário, que pode contemplar informações como: tipo de tratamento, propósitos para o tratamento, descrição das categorias de dados pessoais, descrição das categorias de titulares e descrição geral das medidas de segurança adotadas.*

185. *Todavia, as respostas à questão 6.3 mostraram que 82% das organizações não possuem um registro instituído para consolidar informações relacionadas às características das atividades de tratamento de dados pessoais (Figura 31).*

Figura 31 *- Registro de informações sobre as características das atividades de tratamento de dados pessoais*



186. *Diante desse diagnóstico, vale destacar a existência do Guia de Elaboração de Inventário de Dados Pessoais da Secretaria de Governo Digital (SGD) do Ministério da Economia (ME), que*

abrange diretrizes para a elaboração de inventário de dados pessoais, material que pode auxiliar as organizações a instituírem o registro supracitado.

187. *Ante o exposto, e considerando que a SGD/ME já adotou ações para orientar os órgãos sob sua alçada acerca do assunto, a equipe de auditoria propõe* ***recomendar*** *ao CNJ e ao CNMP que, considerando o controle realizado sobre a atuação administrativa das organizações sob suas jurisdições, expeçam orientação quanto à manutenção de registro das operações de tratamento de dados pessoais, considerando o disposto no art. 37 da LGPD e as diretrizes estabelecidas no item 7.2.8 da ABNT NBR ISO/IEC 27701:2019.*

2.1.5.4 Relatório de impacto à proteção de dados pessoais

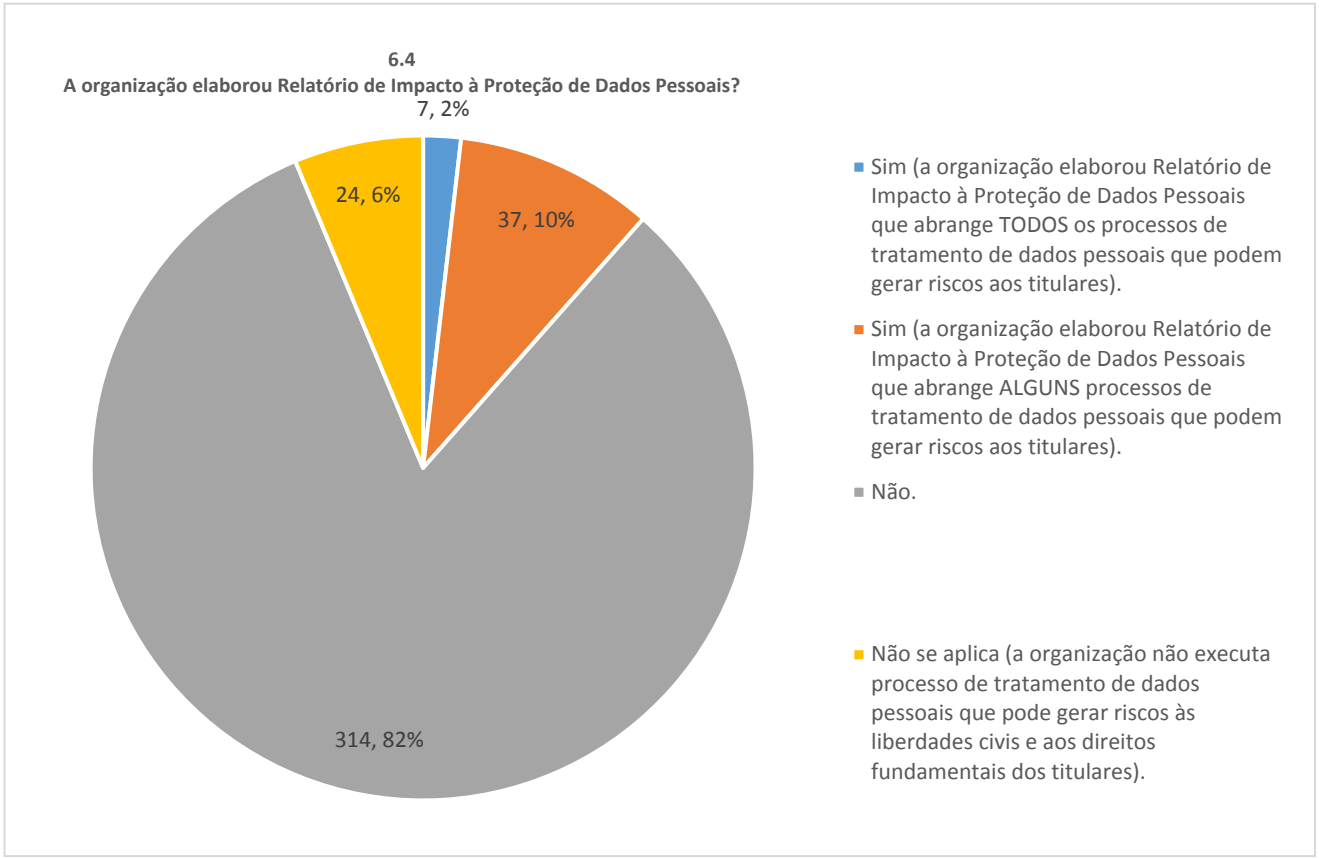
188. *A questão 6.4 do questionário buscou verificar se as organizações elaboraram relatório de impacto à proteção de dados pessoais (RIPD).*

189. *O art. 5º, inciso XVII, da LGPD define que o RIPD é uma documentação do controlador que contempla a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais dos titulares, bem como medidas para mitigação desses riscos.*

190. *No mesmo sentido, o item 7.2.5 da ABNT NBR ISO/IEC 27701:2019 recomenda que os riscos gerados pelo tratamento de dados pessoais sejam analisados por meio de uma avaliação de impacto de privacidade, que considere elementos como: tipos de dados pessoais tratados, local de armazenamento desses dados e para onde os dados podem ser transferidos.*

191. *Contudo, as respostas à questão 6.4 (Figura 32) mostraram que somente 2% das organizações elaboram RIPD que abrange todos os processos de tratamento de dados pessoais que podem gerar riscos aos titulares.*

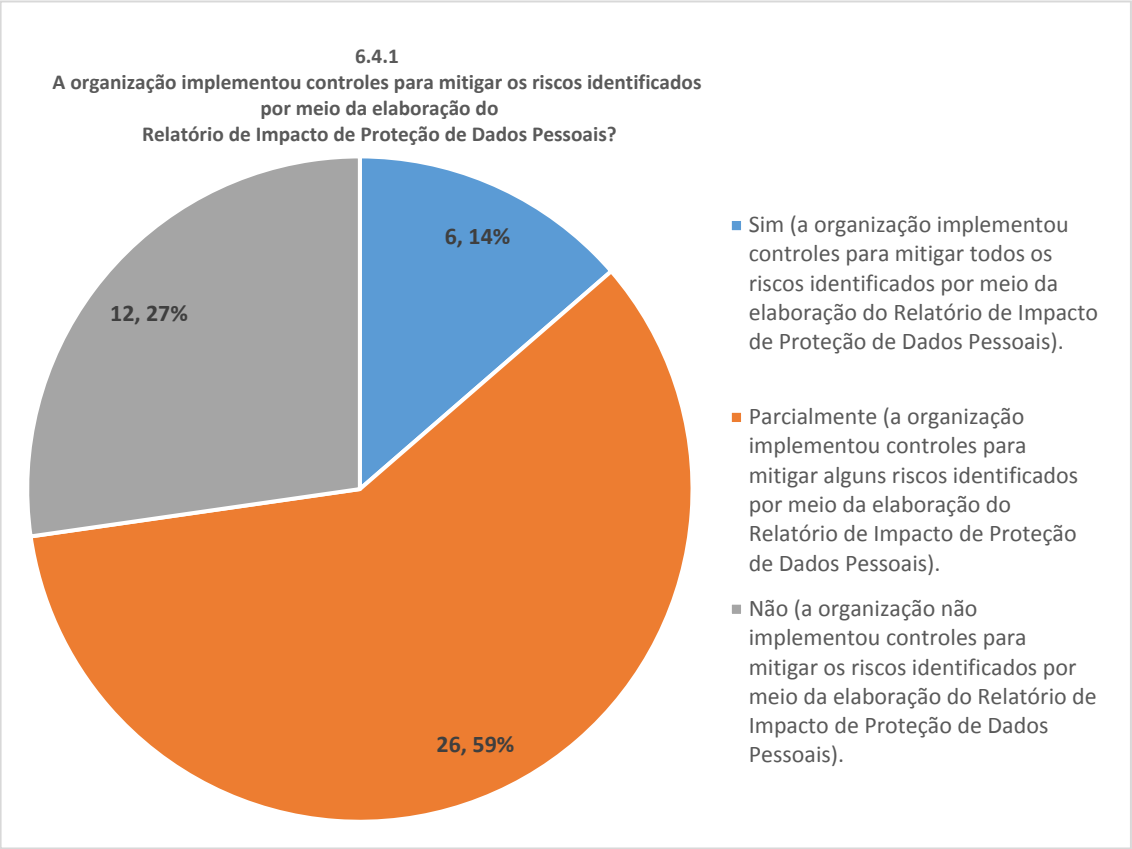
Figura 32 *- Relatório de impacto à proteção de dados pessoais*



192. *Ademais, caso a organização informasse que elaborou o RIPD, era exibida a subquestão questão 6.4.1 para verificar se foram implementados controles para mitigar os riscos identificados por meio da elaboração do artefato. No entanto, as repostas mostraram (Figura 33) que apenas 14% das*

organizações que elaboraram o RIPD implementaram os controles supracitados para todos os riscos identificados.

***Figura 33** - Implementação de controles identificados por meio do RIPD*



193. *O cenário encontrado corrobora com a ideia de que as organizações públicas não possuem a cultura de gestão de riscos. Porém, vale destacar que a elaboração do RIPD ainda deverá ser regulamentada pela ANPD (LGPD, art. 55-J, inciso XIII) e que a SGD/ME já realizou oficina e disponibilizou guia, template e estudo de caso para auxiliar os órgãos do SISP na elaboração do artefato.*

194. *Cumpre frisar que o RIPD pode ser considerado um instrumento auxiliar da gestão de riscos. A título de exemplo, cita-se o RIPD elaborado pelo Banco Central, no qual escreveu que 'dispõe de diferentes sistemas de controles internos, que variam de acordo com a natureza do dado pessoal, para mitigar eventuais riscos de falha na proteção de dados pessoais', mas que, apesar do elevado grau de maturidade de sua gestão de riscos, 'não se pode garantir a eliminação total dos riscos que, em caso de materialização, causariam impacto à privacidade dos dados pessoais existentes na instituição' (peça 998, p. 6).*

195. *Por fim, embora a publicação do RIPD na internet possa ser considerada uma boa prática de transparência, as organizações devem ter cuidado para omitirem eventuais trechos do documento que exponham vulnerabilidades com potencial de serem exploradas por atores mal-intencionados.*

196. *Ante o exposto, e considerando que a SGD/ME já adotou ações para orientar os órgãos sob sua alçada acerca do assunto, a equipe de auditoria propõe **recomendar** ao CNJ e ao CNMP que, considerando o controle realizado sobre a atuação administrativa das organizações sob suas jurisdições, expeçam orientação quanto à elaboração do RIPD e de implementar controles para mitigar os riscos identificados, considerando o disposto no art. 5º, inciso XVII, da LGPD e as diretrizes estabelecidas no item 7.2.5 da ABNT NBR ISO/IEC 27701:2019.*

2.1.6. <u>Direitos do titular</u>

197. *A organização deve assegurar que os titulares tenham acesso às informações relacionadas ao tratamento de seus dados pessoais. Para isso, deve publicar, de maneira clara e concisa, informações*

relativas ao tratamento desses dados. A organização também deve estar preparada para atender os direitos dos titulares que são elencados na LGPD.

198. *Nesta seção são abordadas questões relacionadas à elaboração da política de privacidade e ao atendimento dos direitos dos titulares.*

2.1.6.1 Política de Privacidade

199. *A questão 7.1 do questionário buscou avaliar se as organizações possuem Política de Privacidade ou instrumento similar. Cumpre ressaltar que o termo Política de Privacidade foi utilizado com o mesmo sentido de Aviso de Privacidade.*

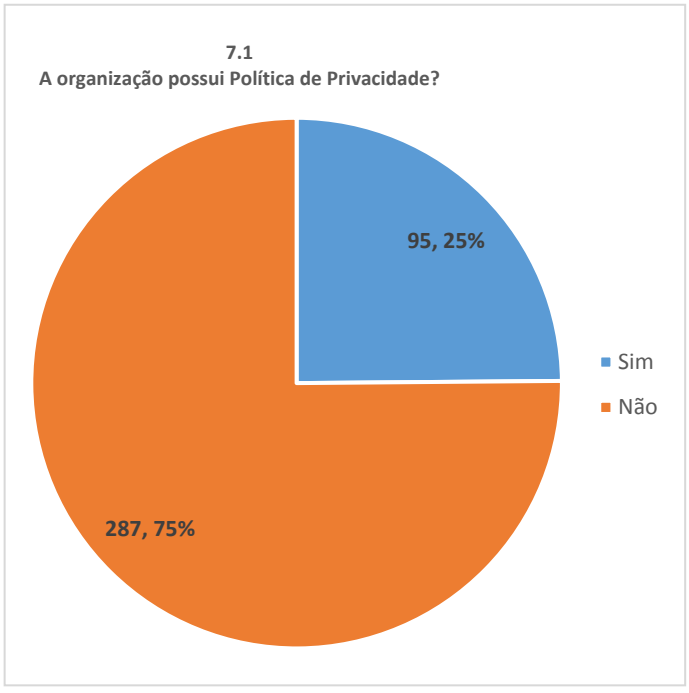
200. *O art. 6º da LGPD enumera, além da boa-fé, dez princípios que as atividades de tratamento de dados pessoais devem observar. Dentre os quais se destacam: o livre acesso, que representa a garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais (inciso IV); e a transparência, que representa a garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento (inciso VI).*

201. *No mesmo sentido, o art. 9º assegura que o titular tem direito ao acesso facilitado às seguintes informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva: a finalidade específica do tratamento; a forma e a duração do tratamento; a identificação e os dados de contato do controlador; o uso compartilhado de dados; as responsabilidades dos agentes que realizam os tratamentos; e os direitos do titular.*

202. *Ademais, os itens 7.3.2 e 7.3.3 da ABNT NBR ISO/IEC 27701:2019 recomendam que a organização determine, documente e forneça aos titulares de dados pessoais, de forma clara e facilmente acessível, informações que identifiquem o controlador de dados pessoais e que descrevam o tratamento de seus dados pessoais. Também é mencionado que as informações devem ser fornecidas em tempo hábil e de forma concisa, completa, transparente, inteligível e facilmente acessível, usando uma linguagem curta e clara, apropriada ao público-alvo. Convém que essas informações sejam reunidas em um documento que deverá ser endereçado aos usuários de seus serviços e sistemas.*

203. *Entretanto, a partir das respostas à questão 7.1, foi constatado que 75% das organizações ainda não elaboraram o artefato (Figura 34), o que demonstra que não é dada a devida transparência ao titular de como os seus dados pessoais são tratados.*

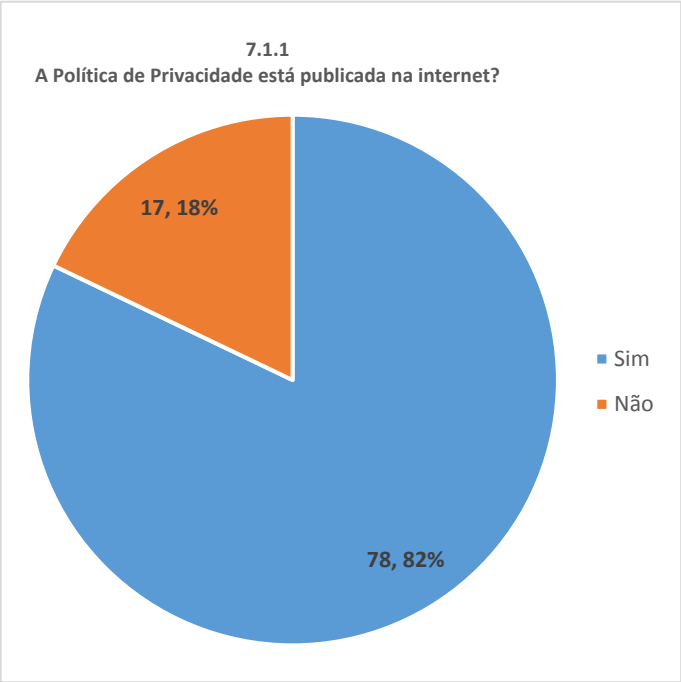
***Figura 34** - Política de privacidade*



204. *Além disso, de acordo com o inciso I do art. 23 da LGPD, o Poder Público deve informar as hipóteses em que, no exercício de suas competências, realiza o tratamento de dados pessoais, fornecendo informações sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos.*

205. *Dessa forma, caso a organização informasse que possuía Política de Privacidade ou documento similar, era exibida a subquestão questão 7.1.1 (Figura 35) para verificar se o artefato estava publicado na internet. As repostas mostraram que a maioria, 82%, providenciou a publicação.*

***Figura 35** - Publicação da política de privacidade na internet*



206. *Diante do exposto, fica evidente que a maioria das organizações não comunica, de maneira clara e concisa, informações relativas ao tratamento de dados pessoais.*

207. *Ante o exposto, a equipe de auditoria propõe **recomendar** à SGD/ME, ao CNJ e ao CNMP que, considerando o controle realizado sobre a atuação administrativa das organizações sob suas jurisdições, expeçam orientação quanto à elaboração de Política de Privacidade, considerando o disposto nos arts. 6º, incisos IV e VI, 9º e 23, inciso I, da LGPD e as diretrizes estabelecidas nos itens 7.3.2 e 7.3.3 da ABNT NBR ISO/IEC 27701:2019.*

2.1.6.2 <u>Mecanismos para atender os direitos dos titulares</u>

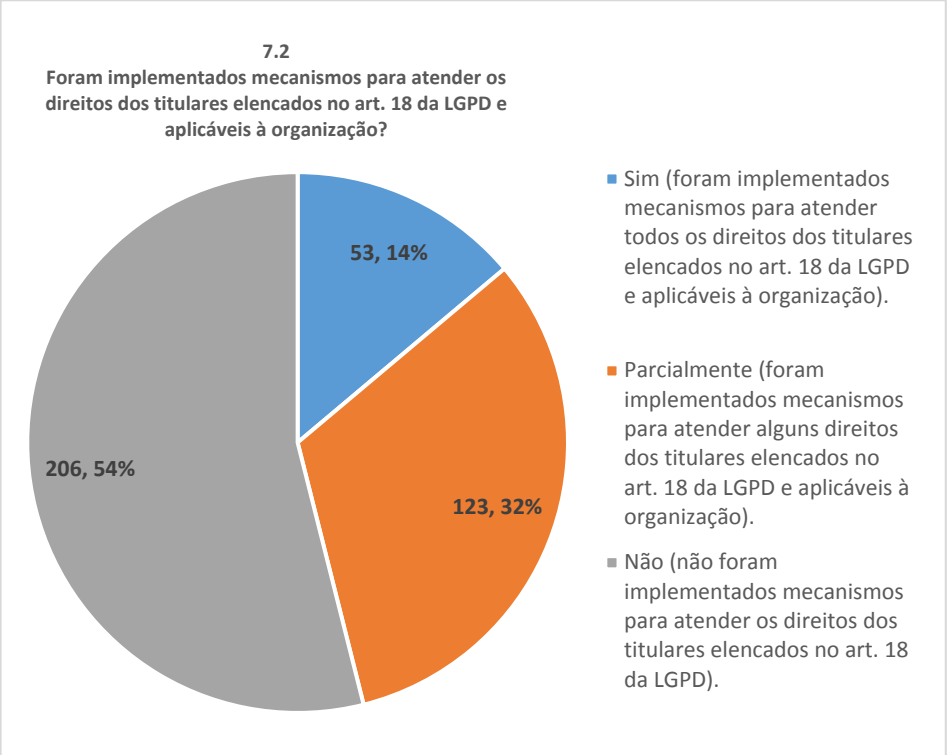
208. *A questão 7.2 buscou verificar se as organizações implementaram mecanismos para atender os direitos dos titulares elencados no art. 18 da LGPD.*

209. *O item 7.3 da ABNT NBR ISO/IEC 27701:2019 recomenda que a organização assegure que os titulares de dados pessoais sejam providos com as devidas informações sobre o tratamento de seus dados. Assim, convém que a organização determine e documente suas obrigações regulatórias, legais e de negócios para com os titulares de dados pessoais e implemente meios para atender a essas obrigações.*

210. *Desse modo, quando aplicável, a organização deve implementar mecanismos para atender aos nove direitos dos titulares estabelecidos no art. 18 da LGPD: confirmação da existência de tratamento; acesso aos dados; correção de dados incompletos, inexatos ou desatualizados; anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nessa lei; portabilidade dos dados; eliminação dos dados; informações sobre uso compartilhado dos dados; informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e revogação do consentimento.*

211. *Entretanto, as respostas (Figura 36) mostraram que somente 14% das organizações implementaram mecanismos para atender todos os direitos dos titulares elencados no art. 18 da LGPD e aplicáveis à sua realidade.*

***Figura 36** - Mecanismos para atender aos direitos dos titulares*



212. *Vale ressaltar que, conforme descrito no inciso V do art. 18 da LGPD, o direito de requisição relacionado à portabilidade demanda regulamentação da ANPD. Outrossim, é importante que as organizações se estruturem para o atendimento das requisições, pois os titulares possuem o direito de obterem informações relacionadas aos seus dados pessoais e a sonegação dessas informações pode resultar em judicialização.*

213. *Ante o exposto, a equipe de auditoria propõe **recomendar** à SGD/ME, ao CNJ e ao CNMP que, considerando o controle realizado sobre a atuação administrativa das organizações sob suas jurisdições, expeçam orientação quanto à implementação de mecanismos para atendimento dos direitos dos titulares elencados no art. 18 da LGPD, considerando as diretrizes estabelecidas no item 7.3 da ABNT NBR ISO/IEC 27701:2019.*

2.1.7. <u>Compartilhamento de dados pessoais</u>

214. *A organização deve documentar detalhes relacionados ao compartilhamento de dados pessoais com terceiros. Ademais, o compartilhamento demanda a adoção de controles adequados para mitigar riscos que possam comprometer a consistência e a proteção dos dados pessoais.*

215. *Diante disso, a LGPD relata que as precauções a serem adotadas entre as partes envolvidas no compartilhamento sejam formalizadas em contrato ou instrumento similar e que cuidados especiais devem ser adotados no caso de transferência internacional desses dados.*

216. *Nesta seção são abordadas questões relacionadas à identificação dos dados pessoais que são compartilhados, à conformidade dos compartilhamentos com a LGPD, ao registro de eventos correlatos aos compartilhamentos e à transferência internacional de dados pessoais.*

2.1.7.1 <u>Dados pessoais compartilhados</u>

217. *A questão 8.1 do questionário buscou verificar se as organizações identificaram os dados pessoais que são compartilhados com terceiros.*

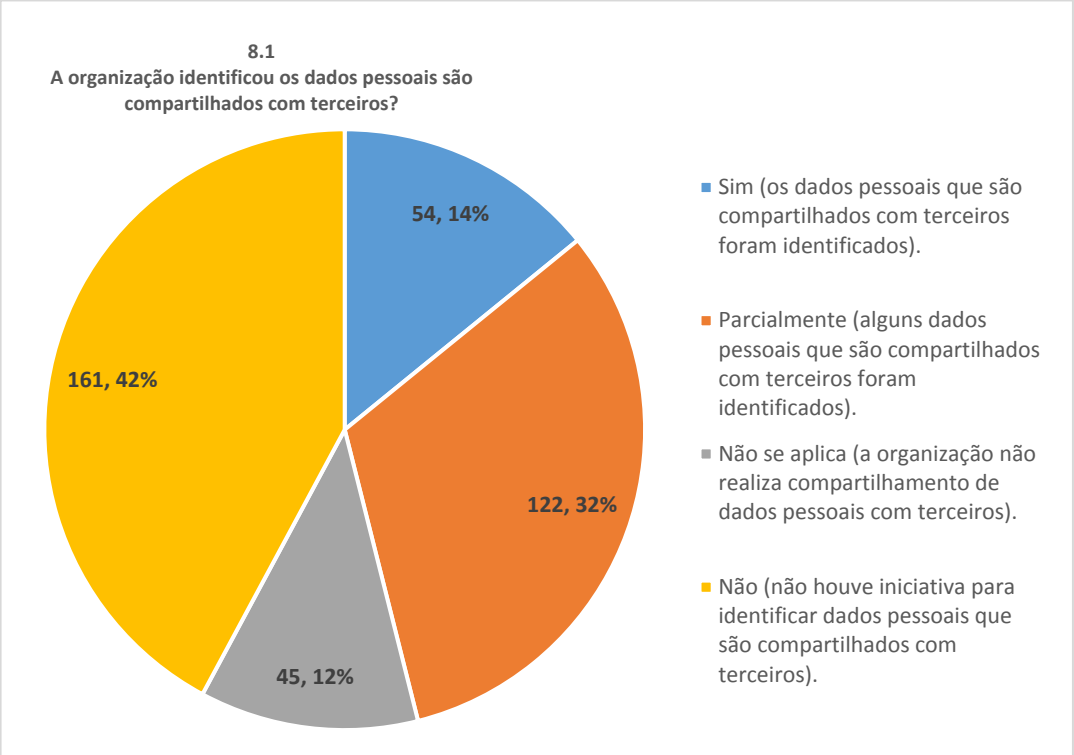
218. *O art. 5º da LGPD traz a seguinte definição (grifou-se):*

> *XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais* ***por órgãos e entidades públicos*** *no cumprimento de suas competências legais,* ***ou entre esses e entes privados****, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;*

219. *No mesmo sentido, o item 7.5.3 da ABNT NBR ISO/IEC 27701:2019 recomenda que a organização registre os casos de transferência e de divulgação de dados pessoais para terceiros ou por terceiros e assegure a cooperação entre as partes para apoiar futuras solicitações relativas às obrigações com os titulares.*

220. *Entretanto, as respostas à questão 8.1 (Figura 37) mostraram que somente 14% das organizações identificaram todos os dados pessoais compartilhados com terceiros.*

Figura 37 *- Identificação de dados pessoais compartilhados com terceiros*



221. *Sem a identificação dos dados pessoais que são compartilhados com terceiros, não é possível assegurar a conformidade com a LGPD, pois tais dados podem ser hospedados por entidades que não tomam os devidos cuidados.*

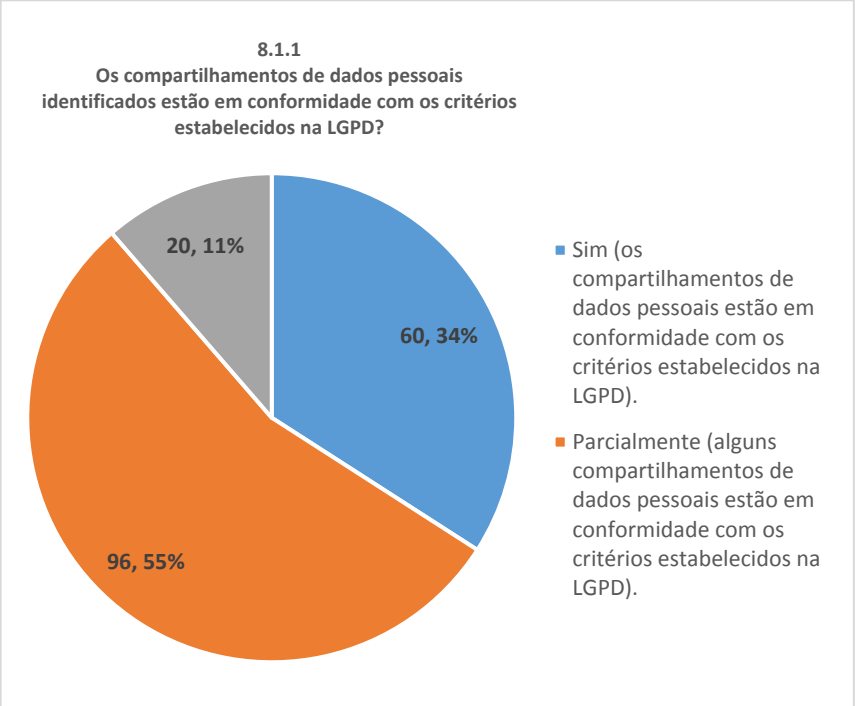
222. *Sob a mesma perspectiva, caso a organização afirmasse que identificou, na totalidade ou em parte, os dados pessoais que são compartilhados com terceiros, eram exibidas as subquestões 8.1.1, 8.1.2 e 8.1.3. A primeira para avaliar se os compartilhamentos identificados estão em conformidade com os critérios estabelecidos na LGPD. A segunda para verificar se as organizações registram eventos relacionados à transferência dos dados pessoais que são compartilhados. E a terceira para averiguar se os compartilhamentos identificados envolvem transferência internacional de dados pessoais.*

223. *Em relação à questão 8.1.1, cumpre frisar que, de acordo com o art. 26 da LGPD, o uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades de execução de políticas públicas e atribuição legal pelas organizações públicas e respeitar os princípios elencados no art. 6º da Lei.*

224. *O § 1º c/c § 2º, também do art. 26 da LGPD, especificam situações de exceção em que a transferência de dados pessoais a entidades privadas é permitida. Sendo que, de acordo com o art. 27, a regra para o compartilhamento de dados de pessoa jurídica de direito público com pessoa de direito privado é comunicar à ANPD e obter consentimento do titular, observadas as exceções previstas nos incisos I, II e III.*

225. *Todavia, as respostas à questão 8.1.1 (Figura 38) mostram que apenas 34% das organizações afirmaram que todos os compartilhamentos estão em conformidade com os critérios estabelecidos na LGPD.*

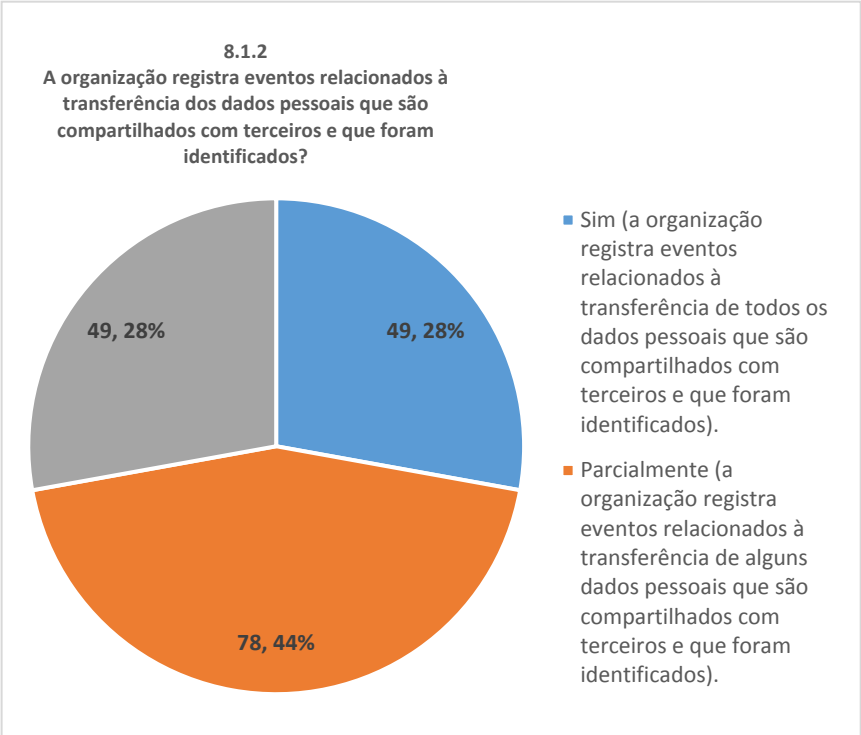
Figura 38 *- Conformidade com a LGPD dos compartilhamentos de dados pessoais*



226. *Quanto à questão 8.1.2, cumpre ressaltar que, em consonância com o disposto no item 7.5.4 da ABNT NBR ISO/IEC 27701:2019, é conveniente que a organização registre quais dados pessoais foram compartilhados, com quem e quando.*

227. *Porém, constatou-se que apenas 28% das organizações registram eventos relacionados à transferência de todos os dados pessoais que são compartilhados (Figura 39).*

Figura 39 *- Registro de eventos de transferência de dados pessoais compartilhados com terceiros*

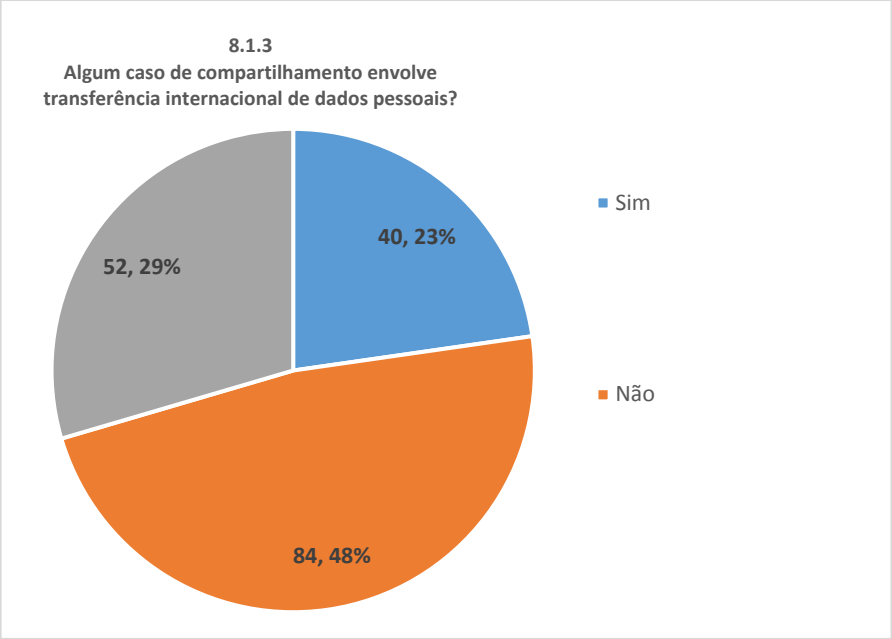


228. *Já em relação à questão 8.1.3, destaca-se que o art. 33 da LGPD relaciona nove casos nos quais é permitida a transferência internacional de dados pessoais. Diante disso, a organização deve avaliar se as transferências internacionais que realiza estão enquadradas em uma dessas hipóteses.*

229. *No mesmo sentido, o item 7.5.2 da ABNT NBR ISO/IEC 27701:2019 remete ser conveniente que a organização especifique e documente os países e as organizações internacionais para os quais os dados pessoais podem ser transferidos e que essas informações estejam disponíveis para os titulares.*

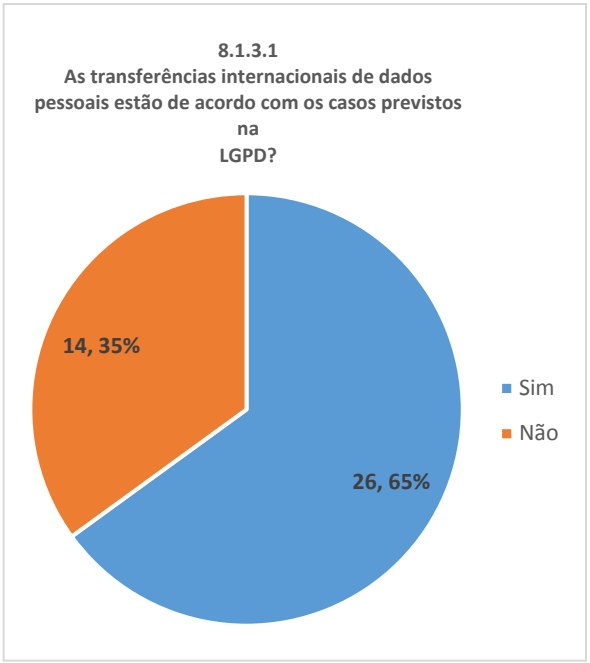
230. *Entretanto, constatou-se que 29% das organizações que responderam à questão afirmaram que ainda não verificaram se há caso de transferência internacional de dados pessoais (Figura 40).*

Figura 40 - *Casos de transferência internacional de dados pessoais*



231. *Por fim, as organizações que afirmaram realizar transferência internacional de dados pessoais tiveram que responder à subquestão 8.1.3.1, que avaliou se tais transferências estavam em conformidade com a LGPD. Das organizações que identificaram algum caso de compartilhamento de dados pessoais que envolve transferência internacional, 65% responderam que as transferências estão de acordo com os casos previstos na LGPD (Figura 41).*

Figura 41 *- Conformidade das transferências internacionais de dados pessoais*



232. *O diagnóstico demonstra a necessidade de as organizações adotarem controles para mitigar riscos relacionados ao compartilhamento de dados pessoais, principalmente pelo fato de não serem eximidas de responsabilidade em casos de violações decorrentes de incidentes no ambiente dos terceiros com os quais compartilha os referidos dados.*

233. *Ao mesmo tempo que a adoção de controles para mitigar riscos associados ao compartilhamento de dados pessoais é importante para evitar incidentes relacionados à violação de dados pessoais, também é relevante que as organizações públicas compartilhem dados pessoais para atender finalidades específicas de execução de políticas públicas (LGPD, art. 26).*

234. *Diante do exposto, a equipe de auditoria propõe **recomendar** à SGD/ME, ao CNJ e ao CNMP que, considerando o controle realizado sobre a atuação administrativa das organizações sob suas jurisdições, expeçam orientação quanto à implementação de procedimentos e controles para o compartilhamento de dados pessoais com terceiros (organizações públicas, privadas e transferência internacional), considerando o disposto nos arts. 5º, inciso XVI, 26, 27 e 33 da LGPD e as diretrizes estabelecidas no item 7.5 da ABNT NBR ISO/IEC 27701:2019.*

2.1.8. Violação de dados pessoais

235. *A organização deve gerenciar incidentes de segurança da informação que envolvem a violação de dados pessoais.*

236. *Nesta seção são abordadas questões relacionadas à identificação, ao registro e ao tratamento de incidentes de violação de dados pessoais. Também é avaliado se a organização dispõe de mecanismo para notificar a ANPD e os titulares nos casos de incidentes que possam acarretar risco ou dano relevante aos titulares.*

2.1.8.1 Plano de resposta a incidentes

237. *A questão 9.1 do questionário buscou verificar se as organizações possuem Plano de Resposta a Incidentes (ou documento similar) que abrange o tratamento de incidentes que envolvem violação de dados pessoais.*

238. *A LGPD, no art. 50, § 2º, inciso I, alínea 'g', recomenda que os controladores implementem um programa de governança em privacidade que, dentre outros aspectos, contemple planos de resposta a incidentes. Outrossim, a ABNT NBR ISO/IEC 27701:2019, no item 6.13.1.1, recomenda que, como parte de um processo de gestão de incidentes de segurança da informação abrangente, a organização estabeleça responsabilidades e procedimentos para assegurar respostas rápidas, efetivas e ordenadas a incidentes que envolvem violação de dados pessoais.*

239. *Entretanto, as respostas à questão 9.1 mostraram que 84% das organizações não possuem plano de reposta a incidentes que abrange o tratamento de incidentes de violação de dados pessoais (Figura 42).*

***Figura 42** - Plano de resposta a incidentes de violação de dados pessoais*

240. *O resultado caracteriza uma situação de risco na qual um incidente de violação de dados pessoais pode ser tratado como outro tipo de incidente de segurança da informação que não demanda ações peculiares como preconiza a LGPD.*

2.1.8.2 Sistema de gestão de incidentes

241. *A questão 9.2 buscou verificar se as organizações possuem sistema para registro de incidentes de segurança da informação que envolvem violação de dados pessoais e a questão 9.3 se possuem sistema para registro das ações adotadas para solucionar esses incidentes. As questões foram abordadas no questionário separadamente porque as organizações podem utilizar um mesmo sistema ou sistemas diferentes para cada uma dessas duas finalidades. No entanto, optou-se por explorar os resultados no mesmo tópico deste relatório.*

242. *O item 6.13.1.1 da ABNT NBR ISO/IEC 27701/2019 ressalta que um processo de gestão de incidentes de segurança da informação abrangente deve estabelecer reponsabilidades e procedimentos para identificação, registro e tratamento de violações de dados pessoais. Ademais, o item 6.13.1.5 da mesma norma descreve que um incidente que envolva dados pessoais pode desencadear uma análise crítica para verificar se uma resposta adequada foi tomada quando necessária. Contudo, um evento de segurança da informação nem sempre desencadeia tal análise, pois pode não apresentar probabilidade significativa de acesso não autorizado a dado pessoal ou a qualquer instalação ou equipamento que armazene esse tipo de dado.*

243. *Assim, o tratamento de incidentes pode envolver, primeiramente, a adoção de solução de contorno para, posteriormente, haver análise crítica e erradicação da causa. Desse modo, convém que a organização possua sistema de informação que auxilie a gestão de incidentes de segurança da informação que envolvem violação de dados pessoais.*

244. *Entretanto, as respostas a essas questões mostraram que 72% das organizações não possuem sistema para registro de incidentes que envolvem violação de dados pessoais (Figura 43) e que 75% não possuem sistema para registro das ações adotadas para solucionar tais incidentes (Figura 44).*

***Figura 43** - Sistema para registro de incidentes de violação de dados pessoais*

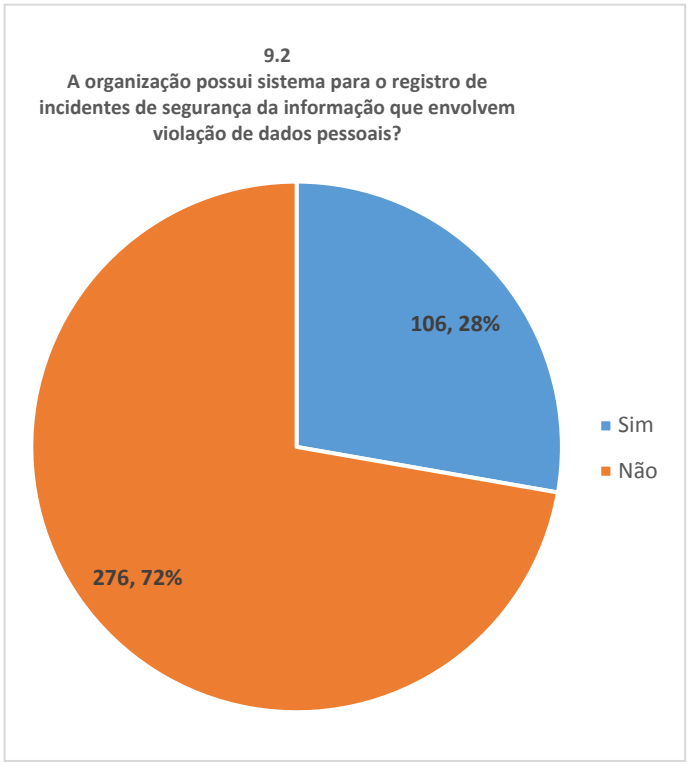
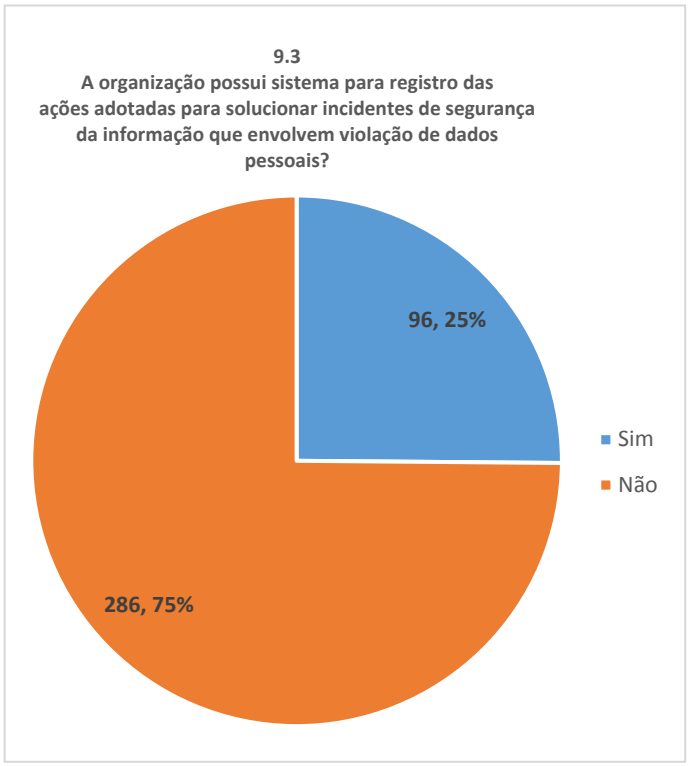


Figura 44 *- Sistema para registro de ações adotadas para solucionar incidentes de violação de dados pessoais*



245. *A diferença nos números das duas questões, provavelmente, ocorreu porque alguns sistemas fazem o registro do incidente, mas não das ações corretivas adotadas.*

246. *Outrossim, sem um sistema de informação que auxilie na gestão de incidentes de segurança da informação que envolvem violação de dados pessoais, a organização tende a não conseguir executar o processo de tratamento e resposta a incidentes com eficiência, tampouco manter e utilizar um histórico de incidentes como aprendizado para reduzir o risco de ocorrências futuras.*

2.1.8.3 Monitoramento de eventos

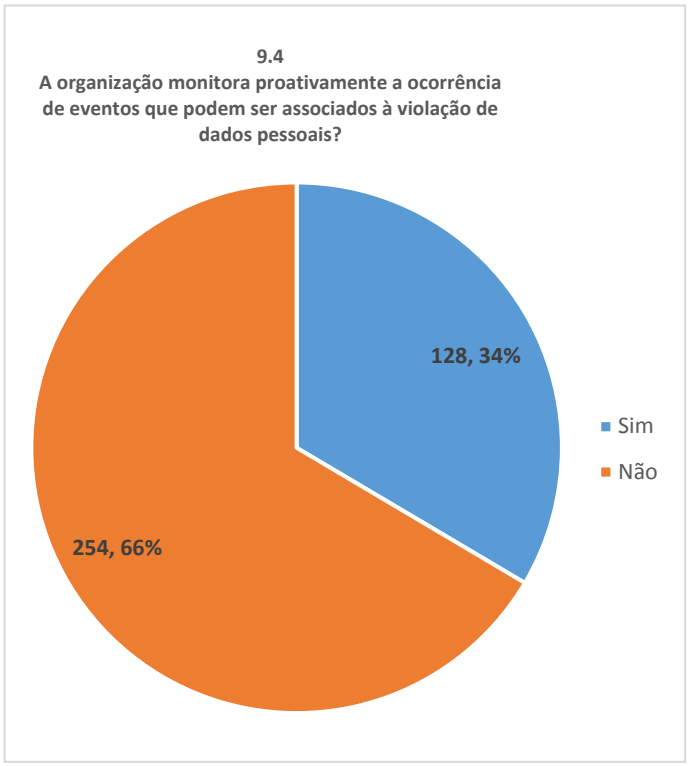
247. *A questão 9.4 buscou verificar se as organizações monitoram proativamente a ocorrência de eventos que podem ser associados à violação de dados pessoais.*

248. *Os itens 6.13.1.4 e 6.13.15 da ABNT NBR ISO/IEC 27701:2019 recomendam que eventos de segurança da informação sejam avaliados para verificar se são incidentes que envolvem violações de dados pessoais, a fim de que sejam adotadas respostas adequadas.*

249. *Assim, convém que a organização implemente mecanismos de monitoramento proativo para que sejam adotadas as medidas adequadas para tratar, de forma tempestiva, ocorrências que possam resultar nessas violações.*

250. *Todavia, as respostas à questão 9.4 mostraram que a maioria das organizações, 66%, não monitora proativamente a ocorrência de eventos associados à violação de dados pessoais (Figura 45).*

Figura 45 *- Monitoramento proativo de eventos associados à violação de dados pessoais*



251. *Essa situação representa alto risco, pois podem ocorrer casos nos quais há violação de dados pessoais e a organização sequer tem conhecimento do ocorrido. Ademais, os impactos decorrentes de casos de violação tendem a ser menores caso a organização adote medidas para combater as ameaças tempestivamente.*

252. *Ante o exposto, a equipe de auditoria propõe* ***recomendar*** *à SGD/ME, ao CNJ e ao CNMP que, considerando o controle realizado sobre a atuação administrativa das organizações sob suas jurisdições, expeçam orientação quanto à elaboração de Plano de Resposta a Incidentes e à implementação de controles para o tratamento de ocorrências relacionadas à violação de dados pessoais, considerando o disposto no art. 50, § 2º, inciso I, alínea 'g', da LGPD e as diretrizes estabelecidas no item 6.13 da ABNT NBR ISO/IEC 27701:2019.*

2.1.8.4 Comunicação de incidente de segurança que possa acarretar risco ou dano ao titular

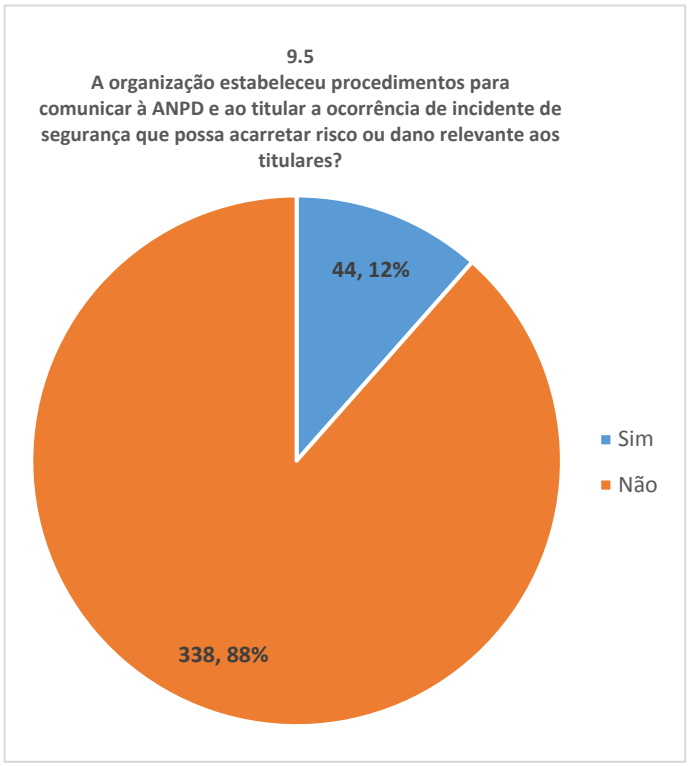
253. *A questão 9.5 buscou verificar se as organizações estabeleceram procedimentos para comunicar à ANPD e ao titular dos dados pessoais a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante ao próprio titular.*

254. *De acordo com art. 48 da LGPD, tal comunicação deve ser feita em prazo razoável e mencionar, no mínimo: a descrição da natureza dos dados pessoais afetados; as informações sobre os titulares envolvidos; a indicação das medidas técnicas e de segurança adotadas para a proteção dos dados; os riscos relacionados ao incidente; e as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. Além disso, caso a organização não encaminhe a comunicação tempestivamente, deverão ser expostos os motivos que levaram à demora. Cumpre complementar que, de acordo com a LGPD, art. 47, os agentes de tratamento ou qualquer pessoa que intervenha em uma das fases do tratamento está obrigada a garantir a segurança dos dados pessoais.*

255. *No mesmo sentido, o item 6.13.1.5 da ABNT NBR ISO/IEC 27701:2019 preconiza que é recomendável que essa comunicação seja contemplada nos procedimentos de resposta a incidentes de segurança da informação.*

256. *Todavia, as respostas à questão 9.5 mostraram que a maioria das organizações, 88%, não estabeleceu procedimentos de comunicação à ANPD e ao titular (Figura 46).*

Figura 46 *- Procedimentos de comunicação à ANPD e ao titular*



257. *A situação encontrada mostra a necessidade de as organizações públicas adotarem medidas para assegurar que os titulares de dados pessoais e a ANPD tenham ciência da ocorrência de situações que podem colocar em risco a privacidade dos titulares.*

258. *Considerando que a ANPD possui orientações específicas a respeito da comunicação de incidentes de segurança envolvendo dados pessoais, a equipe de auditoria entende não ser necessário propor medidas adicionais sobre o assunto, devendo as organizações públicas seguir as diretrizes oficiais da autoridade.*

2.1.9. Medidas de proteção

259. *A organização deve adotar medidas de segurança, técnicas e administrativas, para proteger os dados pessoais. Para isso, convém que sejam implementados controles capazes de mitigar riscos que possam resultar em violação da privacidade.*

260. *Nesta seção serão abordadas questões relacionadas à implementação de controles para restringir e rastrear o acesso a dados pessoais e à avaliação de impacto sobre a proteção de dados pessoais.*

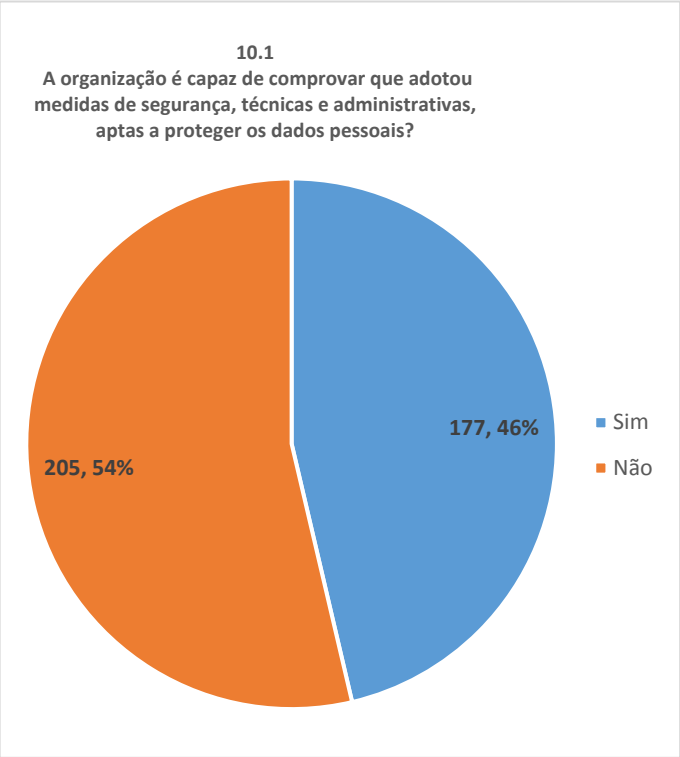
2.1.9.1 Medidas de segurança

261. *A questão 10.1 buscou verificar se as organizações são capazes de comprovar que adotam medidas de segurança, técnicas e administrativas, para proteção dos dados pessoais.*

262. *Segundo o art. 46 da LGPD, os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado. Cumpre ressaltar que a legislação preconiza, no § 1º do art. 46, que a ANPD poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput do mesmo artigo. Ademais, essas medidas são necessárias para que os agentes de tratamento cumpram a obrigação legal de garantir a segurança da informação dos dados pessoais (art. 47 da LGPD).*

263. *No entanto, constatou-se que a maioria das organizações, 54%, não é capaz de comprovar que adotou medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais (Figura 47).*

Figura 47 *- Comprovação de medidas de proteção dos dados pessoais*



264. *O resultado apresentado é preocupante devido ao alto risco de ocorrência de incidentes de violação de dados pessoais em função da ausência de medidas de proteção dos dados pessoais. Além disso, cumpre destacar que, no juízo de gravidade de incidente de segurança que possa causar risco ou dano relevante aos titulares, a ANPD também avaliará a comprovação de que foram adotadas medidas técnicas adequadas (art. 48, § 3º, da LGPD).*

265. *Contudo, enquanto aguardam a edição dos padrões que serão estabelecidos pela ANPD, os controladores podem tomar como referência as boas práticas e normas técnicas de gestão de segurança da informação e de privacidade, como é o caso da ABNT NBR ISO/IEC 27701:2019, que é uma extensão de duas outras normas de gestão da segurança da informação – ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27002:2013 – para gestão da privacidade da informação.*

266. *A título de exemplo, o item 6.1 da ABNT NBR ISO/IEC 27002:2013 recomenda a adoção de uma estrutura de gerenciamento para iniciar e controlar a implementação e a operação da segurança da informação dentro da organização. Outrossim, no item 6.1.1, a mesma norma recomenda que todas as responsabilidades e papeis pela segurança da informação sejam definidos e atribuídos, incluindo as responsabilidades pela proteção de cada ativo e pelo cumprimento de processos de segurança da informação específicos. No mesmo item, também é recomendado que sejam definidas as responsabilidades pelas atividades de gerenciamento de riscos de segurança da informação.*

267. *Ante o exposto, e considerando que a SGD/ME já adotou ações para orientar os órgãos sob sua alçada acerca do assunto, a equipe de auditoria propõe* ***recomendar*** *ao CNJ e ao CNMP que, considerando o controle realizado sobre a atuação administrativa das organizações sob suas jurisdições, expeçam orientação quanto à adoção de medidas de segurança para proteção de dados pessoais, considerando o disposto nos arts. 46 e 47 da LGPD e as boas práticas de gestão de segurança da informação abordadas pela ABNT NBR ISO/IEC 27701:2019.*

2.1.9.2 Controle de acesso em sistemas

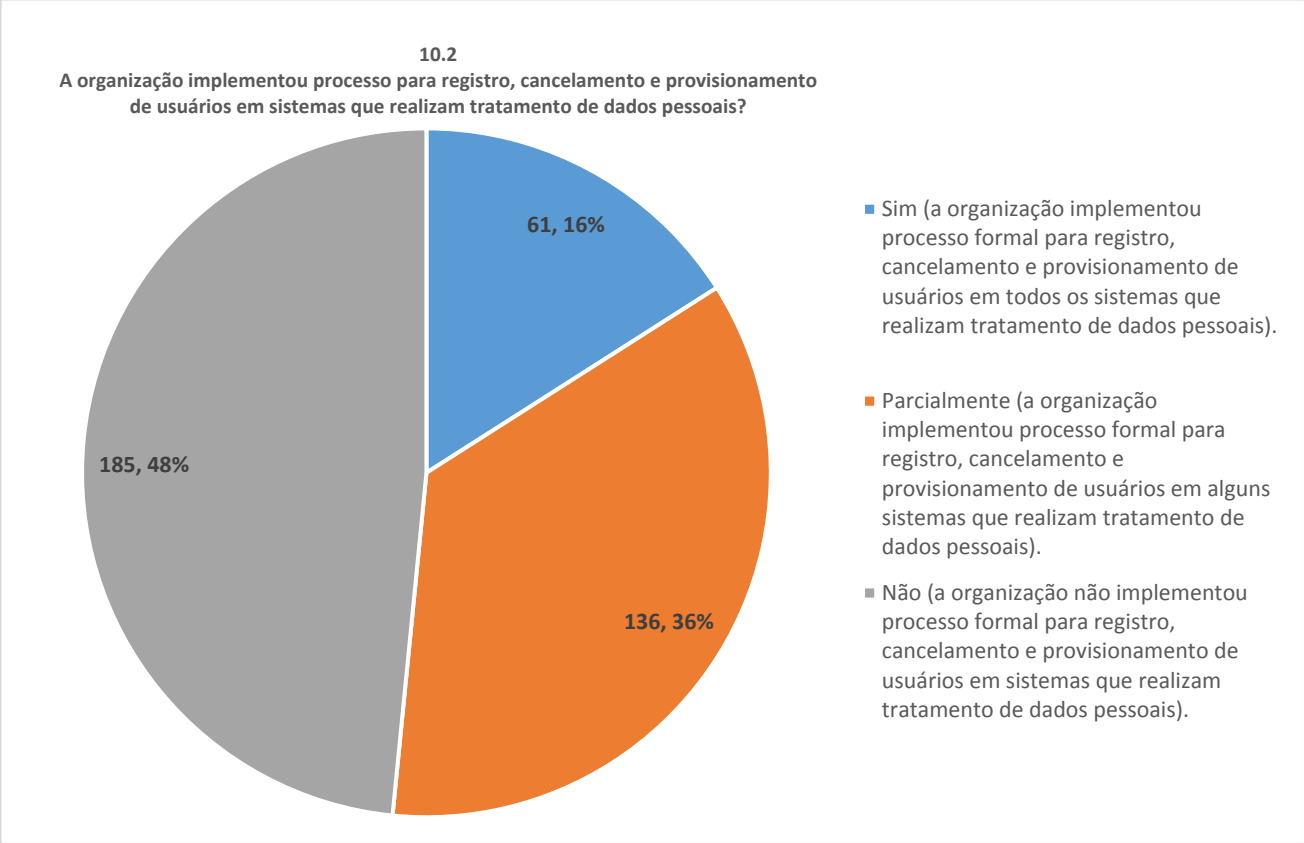
268. *A questão 10.2 buscou verificar se as organizações implementaram processo para registro, cancelamento e provisionamento de usuários em sistemas que realizam tratamento de dados pessoais.*

269. *Dentre as possíveis medidas de segurança que devem ser adotadas para a proteção dos dados pessoais (LGPD, art. 46), inclui-se a gestão do controle de acesso dos usuários. De acordo com os itens 6.6.2.1 e 6.6.2.2 da ABNT NBR ISO/IEC 27701:2019, convém que a organização defina*

processo formal para registro e cancelamento de usuários dos sistemas que realizam tratamento de dados pessoais, bem como para conceder ou revogar os direitos de acesso dos usuários a esses sistemas. A norma também recomenda que a organização mantenha um registro preciso e atualizado dos usuários que tenham sido autorizados a acessar os sistemas de informação e os dados pessoais neles contidos.

270. *No entanto, as respostas à questão 10.2 revelam que apenas 16% das organizações implementaram tal processo em todos os sistemas que realizam tratamento de dados pessoais (Figura 48).*

***Figura 48** - Processo para registro, cancelamento e provisionamento de usuários em sistemas que realizam tratamento de dados pessoais*



271. *A situação encontrada representa alto risco de acesso indevido a dados pessoais, o que pode violar a privacidade dos cidadãos.*

272. *Ante o exposto, a equipe de auditoria propõe **recomendar** à SGD/ME, ao CNJ e ao CNMP que, considerando o controle realizado sobre a atuação administrativa das organizações sob suas jurisdições, expeçam orientação quanto à implementação de processo de controle de acesso de usuários em sistemas que realizam tratamento de dados pessoais, considerando o disposto nos arts. 46 e 47 da LGPD e as diretrizes estabelecidas nos itens 6.6.2.1 e 6.6.2.2 da ABNT NBR ISO/IEC 27701:2019.*

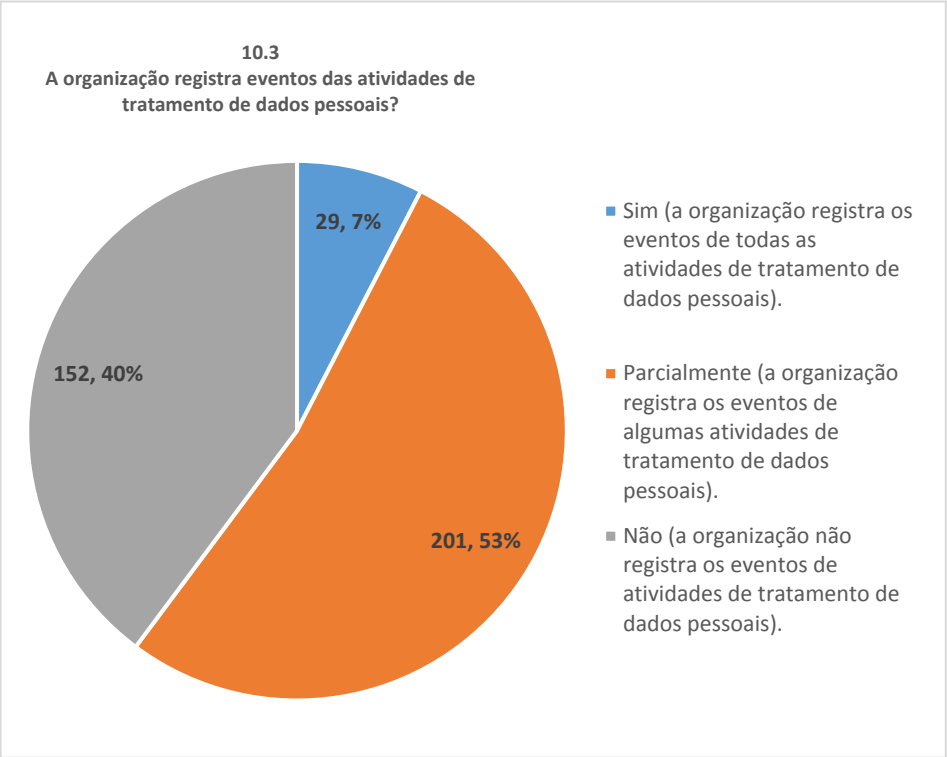
2.1.9.3 <u>Registro de eventos (logs)</u>

273. *A questão 10.3 buscou verificar se as organizações registram eventos das atividades de tratamento de dados pessoais.*

274. *Conforme o item 6.9.4.1 da ABNT NBR ISO/IEC 27701:2019, convém que a organização registre os eventos (logs) das atividades de tratamento de dados pessoais, de forma que seja possível identificar por quem, quando e quais dados pessoais foram acessados. Nos casos em que ocorrem mudanças nos dados, também deve ser registrada a ação realizada (e.g.: inclusão, alteração ou exclusão).*

275. *No entanto, as respostas à questão 10.3 revelam que apenas 7% das organizações registram eventos de todas as atividades de tratamento de dados pessoais (Figura 49).*

Figura 49 *- Registro de eventos das atividades de tratamento de dados pessoais*



276. *O diagnóstico é alarmante, uma vez que a ausência de registros de eventos inviabiliza a rastreabilidade de ocorrências relacionadas à violação de dados pessoais.*

277. *Ante o exposto, a equipe de auditoria propõe* ***recomendar*** *à SGD/ME, ao CNJ e ao CNMP que, considerando o controle realizado sobre a atuação administrativa das organizações sob suas jurisdições, expeçam orientação quanto ao registro de eventos das atividades de tratamento de dados pessoais, considerando as diretrizes estabelecidas no item 6.9.4.1 da ABNT NBR ISO/IEC 27701:2019.*

2.1.9.4 Utilização de criptografia

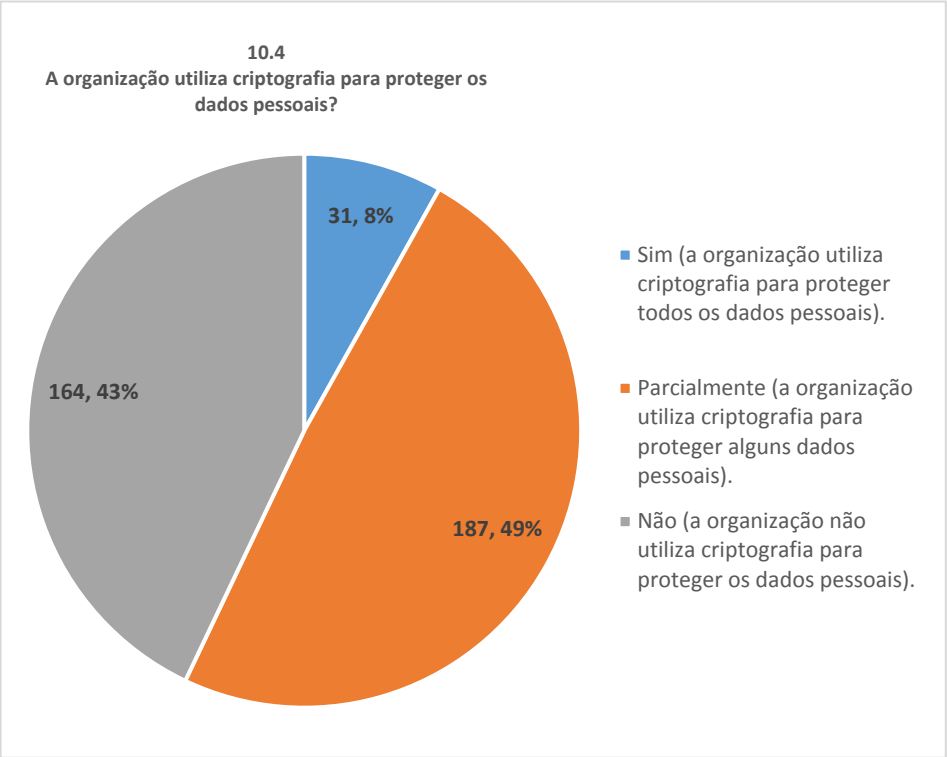
278. *A questão 10.4 buscou verificar se as organizações utilizam criptografia para proteger os dados pessoais.*

279. *Em consonância com o disposto no art. 48, § 3º, da LGPD, a criptografia é uma medida técnica utilizada para tornar ininteligíveis os dados pessoais afetados em caso de incidente de segurança, o que impede que terceiros, não autorizados, consigam acessá-los.*

280. *A sensibilidade dos dados pessoais deve ser considerada na implementação de um programa de governança em privacidade (LGPD, art. 50, § 2º, inciso I, alínea 'c'). Por exemplo, o uso de criptografia pode proteger tipos específicos de dados pessoais, como dados sobre saúde, endereço, número de passaporte e número de licença de motorista (norma técnica ABNT NBR ISO/IEC 27701:2019, item 6.7).*

281. *No entanto, as respostas à questão 10.4 mostram que 43% das organizações não utilizam criptografia para proteger os dados pessoais (Figura 50).*

Figura 50 *- Utilização de criptografia para proteger dados pessoais*



282. *Apesar de a utilização de criptografia não ser obrigatória, a utilização da medida é útil para proteger dados em trânsito e nos locais de armazenamento, mitigando riscos associados à violação de dados pessoais. A adoção de criptografia é recomendada, principalmente, para a proteção de dados pessoais sensíveis ou de crianças e adolescentes.*

283. *Ante o exposto, a equipe de auditoria propõe* ***recomendar*** *à SGD/ME, ao CNJ e ao CNMP que, considerando o controle realizado sobre a atuação administrativa das organizações sob suas jurisdições, expeçam orientação quanto à utilização de criptografia para proteção de dados pessoais, considerando o disposto nos arts. 48, § 3º; e 50, § 2º, inciso I, alínea 'c', da LGPD e as diretrizes estabelecidas no item 6.7 da ABNT NBR ISO/IEC 27701:2019.*

2.1.9.5 Privacy by Design e Privacy by Default

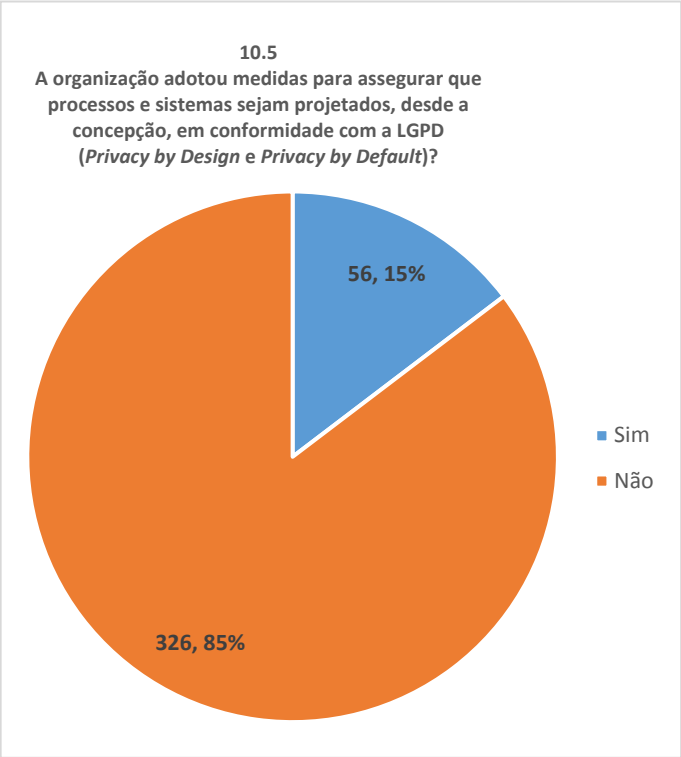
284. *A questão 10.5 buscou verificar se as organizações adotam medidas para assegurar que processos e sistemas sejam projetados, desde a concepção, em conformidade com a LGPD.*

285. *De acordo com o art. 46, § 2º, da LGPD, as medidas de segurança aptas a proteger os dados pessoais devem ser observadas pelos agentes de tratamento desde a fase de concepção do produto ou do serviço até a sua execução.*

286. *No mesmo sentido, a ABNT NBR ISO/IEC 27701:2019, em seu item 7.4, apresenta os conceitos de Privacy by Design e de Privacy by Default como diretrizes para assegurar que os processos e sistemas sejam projetados de forma que a coleta e o tratamento dos dados pessoais estejam limitados ao que é estritamente necessário para o alcance do propósito definido.*

287. *No entanto, as respostas à questão 10.5 demonstram que a maioria das organizações, 85%, não adotou medidas para assegurar que processos e sistemas sejam projetados, desde a concepção, em conformidade com a LGPD (Figura 51).*

Figura 51 *- Privacy by Design e Privacy by Default*



288. *A situação era esperada, pois a cultura de proteção de dados pessoais na APF começou a ser estimulada após a vigência da LGPD. Entretanto, é conveniente que os conceitos de Privacy by Design e de Privacy by Default passem a ser seguidos pelas organizações, pois incorporar tardiamente medidas de proteção dos dados pessoais tende a provocar aumento de custos de implantação e de manutenção, além de riscos de ineficácia das soluções adotadas.*

289. *Ante o exposto, e considerando que a SGD/ME já adotou ações para orientar os órgãos sob sua alçada acerca do assunto, a equipe de auditoria propõe* ***recomendar*** *ao CNJ e ao CNMP que, considerando o controle realizado sobre a atuação administrativa das organizações sob suas jurisdições, expeçam orientação quanto à adoção de medidas de proteção de dados pessoais desde a fase de concepção até a fase de execução de processos e sistemas (Privacy by Design), incluindo a coleta de dados limitada ao que é estritamente necessário ao alcance do propósito definido (Privacy by Default), considerando o disposto no art. 46, § 2º, da LGPD e as diretrizes estabelecidas no item 7.4 da ABNT NBR ISO/IEC 27701:2019.*

2.2. <u>Indicador de adequação à LGPD</u>

290. *De modo a consolidar os dados obtidos e possibilitar a comparação das organizações auditadas, no que tange ao nível de adequação à LGPD, um subconjunto de 42 questões foi escolhido para compor um indicador elaborado com o intuito de resumir as respostas fornecidas por cada organização.*

291. *O cálculo do indicador considerou as possíveis respostas de cada questão selecionada, atribuindo uma nota numérica a cada uma delas. Assim, as respostas dos tipos 'Sim', 'Parcialmente' e 'Não' correspondem, respectivamente, às notas 1, 0,5 e 0; sendo que o valor do indicador é obtido pela soma das notas obtidas em cada uma das questões dividida por 42. Assim, para cada organização, o valor do indicador pode variar de 0 (nota 0 em todas as questões) a 1 (nota 1 em todas as questões). O cálculo citado pode ser representado pela equação a seguir, onde indicador corresponde à soma das notas atribuídas às respostas de cada uma das questões selecionadas (notaResposta(i)), dividida por 42 (número total de questões selecionadas).*

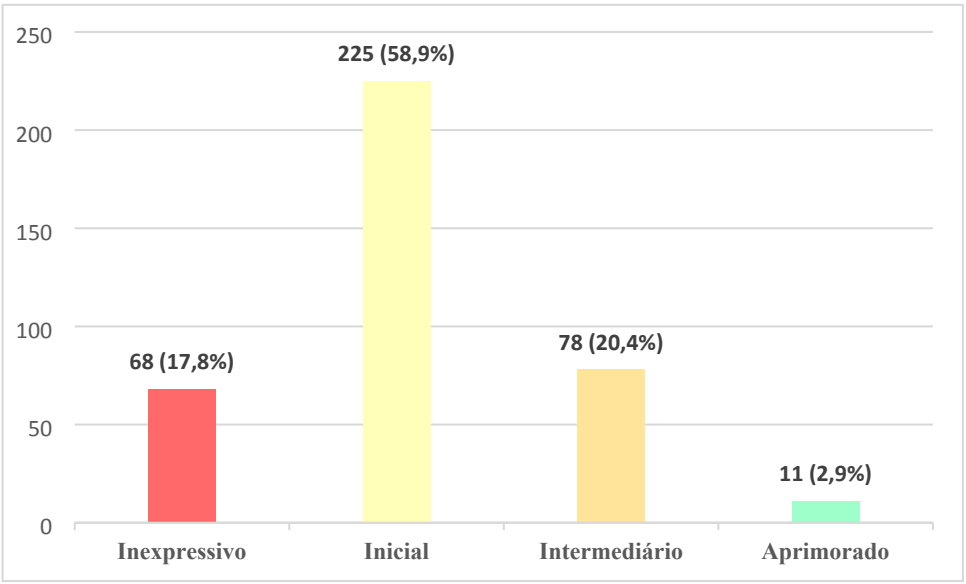
$$indicador = \frac{\sum_{i=1}^{42} notaResposta(i)}{42}$$

292. *O Quadro 1 do Anexo III apresenta as 42 questões selecionadas com as respectivas opções de resposta e as notas atribuídas a cada uma delas.*

293. *A partir do cálculo do indicador, foram definidos quatro níveis de adequação à LGPD: 'Inexpressivo' (indicador menor ou igual a 0,15), 'Inicial (indicador maior do que 0,15 e menor ou igual a 0,5), 'Intermediário' (indicador maior do que 0,5 e menor ou igual a 0,8) e 'Aprimorado' (indicador maior do que 0,8). Assim, conforme o valor do indicador obtido, as organizações foram enquadradas em um desses níveis.*

294. *A Figura 52 apresenta a consolidação da distribuição das 382 organizações em cada nível, o que permite deduzir que a maioria, 58,9%, está ainda no nível 'Inicial.*

Figura 52 *- Distribuição das organizações por níveis de adequação à LGPD*

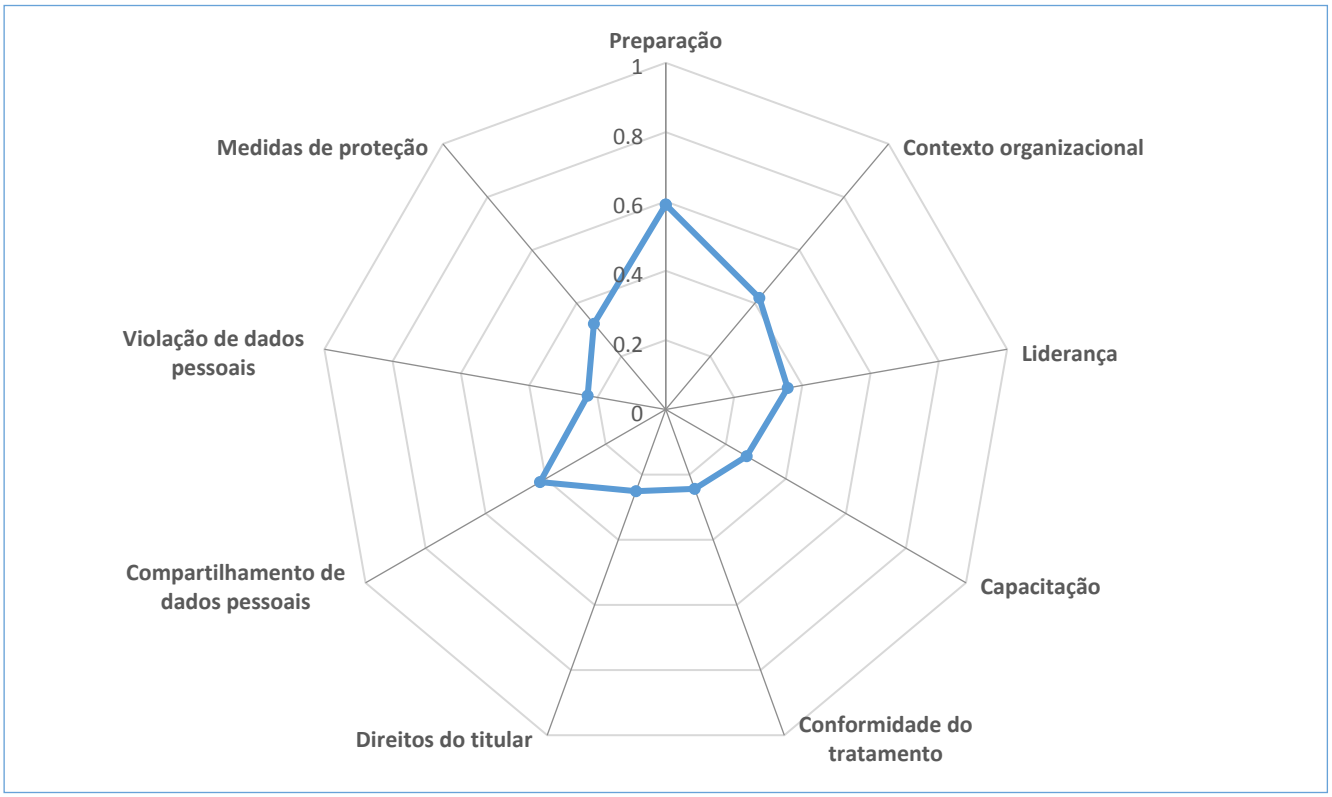


295. *O indicador também pode ser apresentado levando em consideração a nota referente a cada uma das dimensões do questionário: 'Preparação', 'Contexto Organizacional', 'Liderança', 'Capacitação', 'Conformidade do Tratamento', 'Direitos do Titular', 'Compartilhamento de Dados Pessoais', 'Violação de Dados Pessoais' e 'Medidas de Proteção'.*

296. *O valor do indicador de cada dimensão é obtido pela soma das notas obtidas em cada uma das questões da dimensão que foram selecionadas para compor o indicador, dividida pela quantidade de questões selecionadas da dimensão. Assim, para cada organização, o valor do indicador de cada dimensão também pode variar de 0 (nota 0 em todas as questões) a 1 (nota 1 em todas as questões).*

297. *A Figura 53 apresenta um gráfico com o valor médio dos indicadores das 382 organizações em cada dimensão.*

Figura 53 *- Valores médios de indicadores para cada seção do questionário*



298. *Por meio do gráfico, é possível verificar que o maior valor foi obtido na dimensão 'Preparação' (0,59) e que os menores foram atribuídos às dimensões 'Capacitação' (0,27), 'Direitos do Titular' (0,25), 'Conformidade do Tratamento' (0,24) e 'Violação de Dados Pessoais' (0,23).*

299. *A partir deste diagnóstico, constata-se que a maior parte das organizações ainda está iniciando o processo de adequação à LGPD. Contudo, vale ressalvar que o gráfico individual de cada organização pode ser influenciado pelo porte e pelos objetivos do negócio e que, assim, nem todas as organizações devem estar no mesmo patamar em todas as dimensões.*

300. *Diante do exposto, a equipe de auditoria propõe* ***recomendar*** *à SGD/ME, ao CNJ e ao CNMP que, considerando o controle realizado sobre a atuação administrativa das organizações sob suas jurisdições, editem normativos e guias, consultando a ANPD, para auxiliar o processo de adequação à LGPD, incluindo as orientações cujas necessidades foram apontadas nas seções 2.1.1-2.1.9.*

3. Estruturação da Autoridade Nacional de Proteção de Dados

301. *Neste capítulo, serão apresentados uma visão geral e os achados da questão de auditoria referente à ANPD. A primeira parte explora o contexto de criação do órgão, a legislação aplicável, as competências, a estrutura e o planejamento estratégico. Na sequência, constam os quatro achados de auditoria verificados pela equipe de fiscalização após a aplicação dos procedimentos previstos na etapa de planejamento.*

3.1. Visão Geral

3.1.1. Contexto de criação

302. *A partir da experiência observada na União Europeia, onde há legislação específica e autoridades de proteção de dados com maior tradição e atuação no mundo, como a inglesa (Information Commissioner's Office - ICO) e a francesa (Commission nationale de l'informatique et des libertés - CNIL), países da América Latina iniciaram um processo de convergência com o modelo europeu, incluindo o Brasil, que aprovou a LGPD e criou a ANPD.*

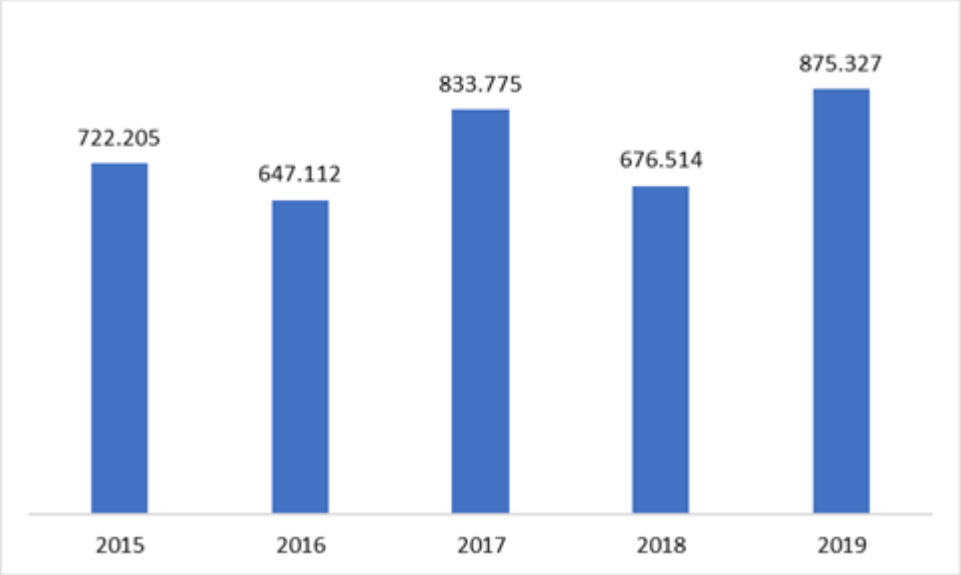
303. *Nos últimos anos, a preocupação com a privacidade dos cidadãos e com a proteção de dados pessoais ganhou destaque no debate público, fazendo com que o tema ocupasse espaço central*

na agenda política de diversos países. Escândalos como o da consultoria de marketing político Cambridge Analytica/Facebook, revelado em 2018, que teria envolvido o compartilhamento ilegal de dados pessoais de milhões de indivíduos, com possíveis reflexos no sistema democrático dos Estados Unidos e do Reino Unido, reforçam a necessidade da existência e da atuação diligente de uma autoridade de proteção de dados independente e autônoma para resguardar os direitos dos titulares e os fundamentos do livre desenvolvimento da personalidade e da autodeterminação informacional.

304. *Conforme pesquisa divulgada pelo escritório de advocacia internacional DLA Piper, desde o início da vigência do Regulamento Geral de Proteção de Dados da União Europeia, mais de 281 mil violações de dados foram notificadas para as autoridades, com o total de multas aplicadas passando de 272 milhões de euros, ou 1,8 bilhão de reais no câmbio atual (1 EUR = R$ 6,18).*

305. *No caso do Brasil, o número total de incidentes de segurança reportados nos últimos anos, considerando todas as modalidades, ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança (CERT.br) é o que consta no gráfico a seguir. Apesar do elevado número, é importante observar que, nesse caso, nem todo incidente de segurança está relacionado necessariamente com uma violação de dados pessoais.*

***Figura 54** - Estatísticas do CERT.br – Incidentes*



***Fonte**: estatísticas dos incidentes reportados ao CERT.br*

306. *No setor privado, pesquisa da empresa Enjoy Safer Technology, feita com 14 países da América Latina em 2020, aponta que 60% das empresas brasileiras pesquisadas sofreram ao menos um incidente de segurança, o que pode expor os dados pessoais tratados a algum tipo de violação. Os vazamentos de dados recentes noticiados pela imprensa, que, no caso mais grave, pode ter afetado até 223 milhões de pessoas, apontam para a necessidade de adoção de medidas de segurança por parte de empresas de todos os portes e setores.*

307. *Portanto, é nesse quadro que está inserida a ANPD, que deve enfrentar desafios importantes e urgentes nesse início de funcionamento da sua estrutura, tendo a missão de construir um ambiente regulatório que tanto aproveite todas as vantagens da digitalização da economia e da sociedade, favorecendo a inovação, quanto proteja efetivamente os titulares de dados pessoais das ameaças crescentes advindas da utilização massiva de seus dados.*

3.1.2. <u>Atribuições e estrutura</u>

308. *A ANPD é o órgão da APF, integrante da Presidência da República, responsável por zelar pela proteção de dados pessoais, por induzir a implementação e por fiscalizar o cumprimento da Lei Geral de Proteção de Dados.*

309. *Apesar de sua criação ter sido prevista no texto original que resultou na Lei 13.709/2018, o dispositivo foi vetado por conter vício de iniciativa no processo legislativo. A sua efetiva criação se deu posteriormente, com a edição da MP 869/2018, convertida na Lei 13.853/2019.*

310. *As competências da ANPD são múltiplas e estão listadas ao longo de todo o texto da LGPD. Entre elas, destacam-se:*

***Figura 55** - Atribuições da ANPD*

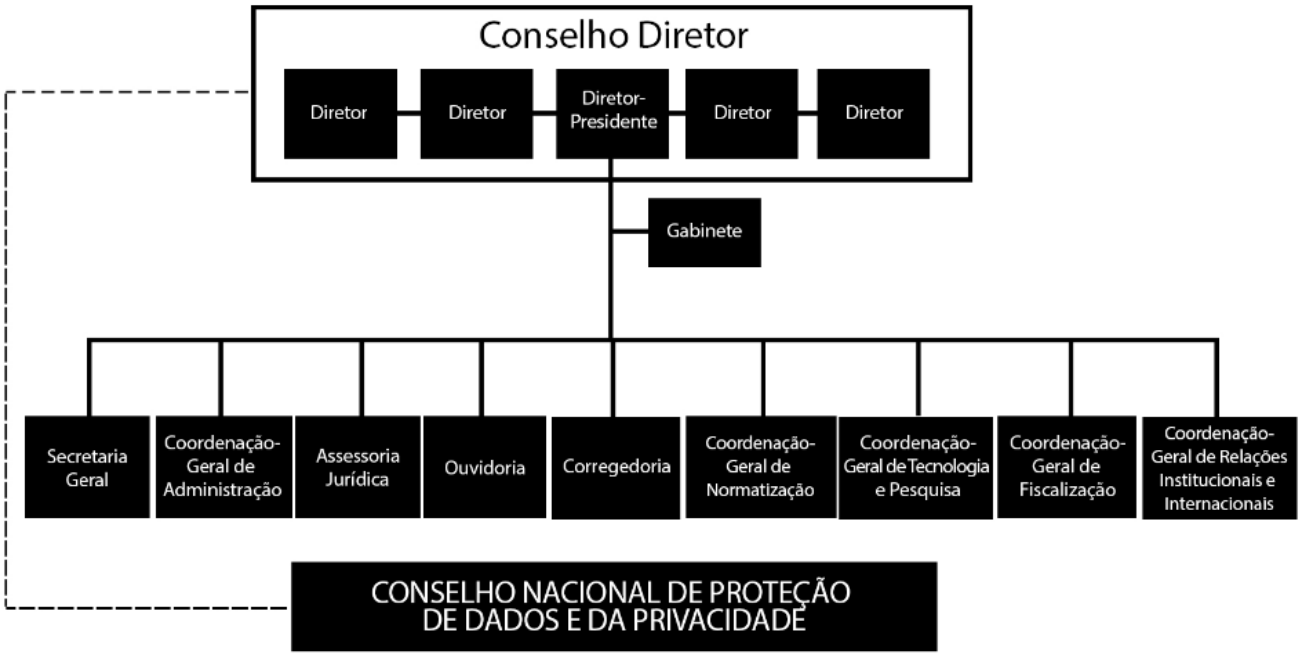
zelar pela proteção dos dados pessoais	elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade	fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação
promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais	promover ações de cooperação com autoridades de proteção de dados pessoais de outros países	editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade
realizar auditorias, ou determinar sua realização, sobre o tratamento de dados pessoais	editar normas e procedimentos simplificados para ME e EPP	deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação da LGPD

***Fonte**: elaboração própria a partir da Lei 13.709/2018.*

311. *A estrutura regimental do órgão foi definida pelo Decreto 10.474, de 26 de agosto de 2020, que entrou em vigor após a nomeação do Diretor-Presidente da instituição, fato que ocorreu em 6 de novembro de 2020. Por sua vez, o Regimento Interno foi publicado pela Portaria-ANPD 1, de 8 de março de 2021.*

312. *O organograma da instituição é detalhado na figura abaixo:*

***Figura 56** - Organograma da ANPD*



***Fonte**: Boletim Informativo 5/2021.*

313. *As decisões da ANPD, a serem tomadas de forma colegiada pelo Conselho-Diretor, serão subsidiadas pela atuação de três órgãos singulares voltados à atividade-fim: (i) Coordenação-Geral de Normatização; (ii) Coordenação-Geral de Fiscalização; e (iii) Coordenação-Geral de Tecnologia e Pesquisa. Além desses, outro órgão, de assistência direta ao Conselho-Diretor, terá atribuições*

importantes no que se refere às competências finalísticas da ANPD, qual seja, a Coordenação-Geral de Relações Institucionais e Internacionais.

314. *Também merece destaque o papel do Conselho Nacional de Proteção de Dados e da Privacidade (CNPD), órgão consultivo que será composto por 23 membros, contendo representantes do governo, instituições da sociedade civil, academia e setor produtivo.*

315. *Suas atribuições envolvem: (i) propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD; (ii) elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; (iii) sugerir ações a serem realizadas pela ANPD; (iv) elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; e (v) disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população.*

316. *Para compor a sua força de trabalho, a ANPD está autorizada a realizar requisição de pessoal, civil ou militar, com caráter obrigatório, ou seja, uma vez feita, os atos são considerados irrecusáveis. Na data de elaboração deste relatório, o órgão contava com 29 servidores, com mais treze em processo de requisição em andamento.*

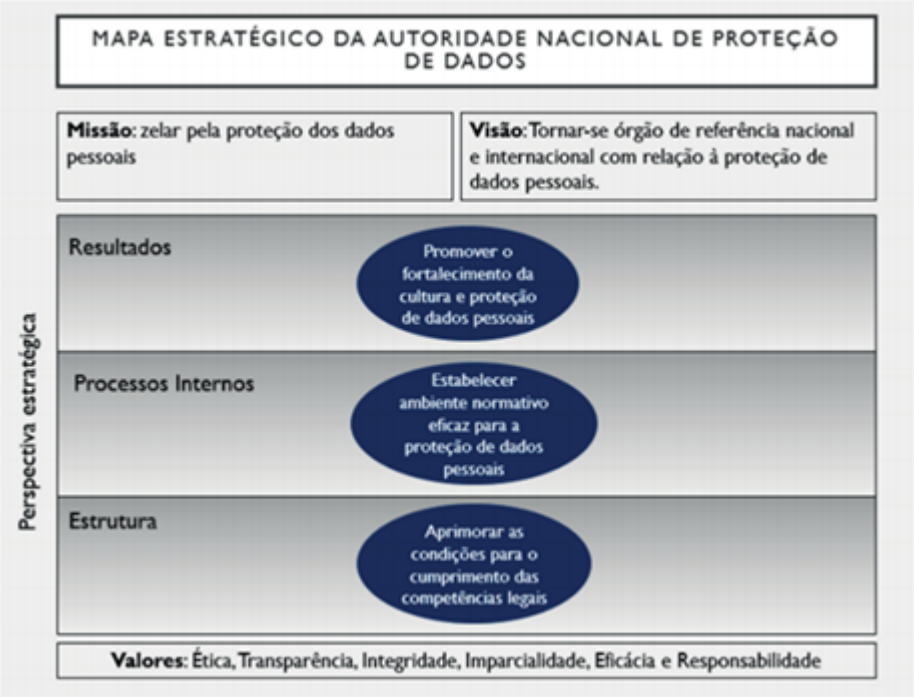
317. *A estrutura física da autoridade ainda é precária, reflexo, entre outras questões, do seu momento inicial de funcionamento, ocupando sede provisória e tendo os serviços de logística e suprimento de materiais realizados pela Presidência da República.*

3.1.3. Planejamento Estratégico

318. *O Planejamento Estratégico da ANPD para o período 2021-2023 foi publicado em 1/2/2021 e apresenta os avanços que o órgão pretende realizar, organizando-os em torno de três objetivos estratégicos: (i) promover o fortalecimento da cultura de proteção de dados pessoais; (ii) estabelecer o ambiente normativo eficaz para a proteção de dados pessoais; e (iii) aprimorar as condições para o cumprimento das competências legais.*

319. *As informações estão dispostas no Mapa Estratégico da ANPD, que agrupa os objetivos em dimensões, além de apresentar a sua missão e visão:*

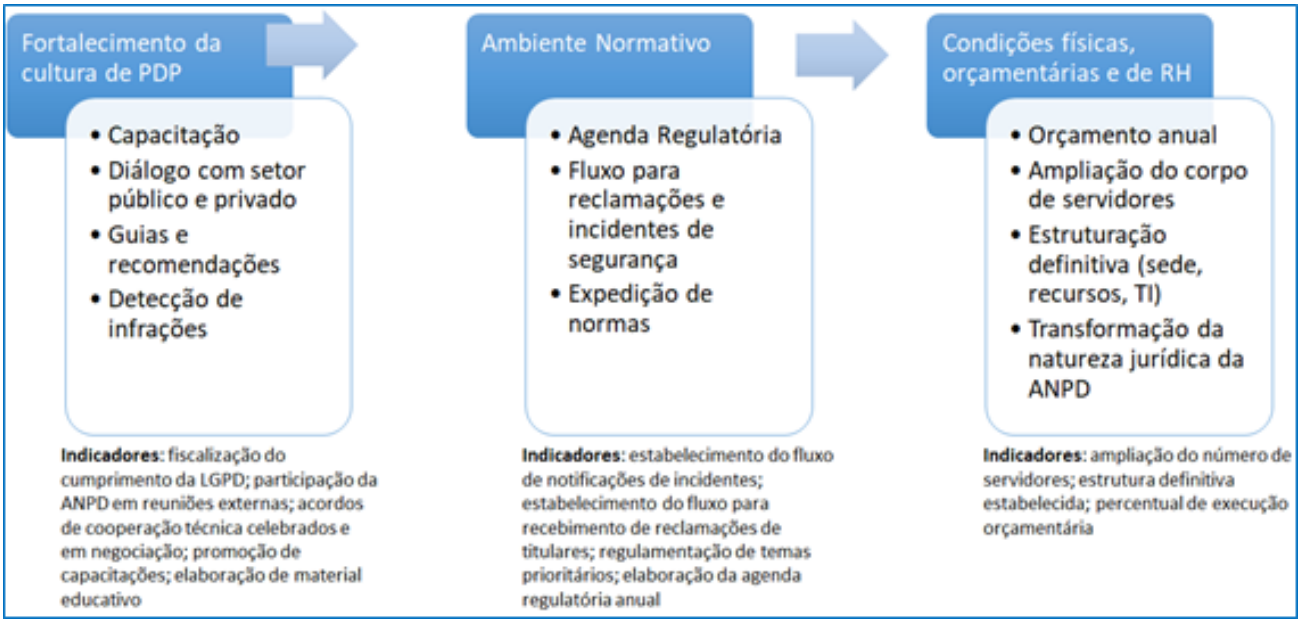
***Figura 57 -** Mapa Estratégico da ANPD*



***Fonte**: Planejamento Estratégico 2021-2023 da ANPD.*

320. *Na sequência, o documento elenca ações estratégicas e indicadores para implementar e acompanhar o desenvolvimento dos objetivos definidos. A figura a seguir consolida as informações:*

***Figura 58** - Ações e indicadores estratégicos da ANPD*



***Fonte**: Apresentação institucional da ANPD, realizada em 9/4/2021 (com modificações).*

321. *As ações estratégicas representam grandes atividades, orientadas pelos objetivos, devendo ser desdobradas em ações táticas e operacionais para a sua execução. Até a data de fechamento deste relatório, ainda não havia sido editado planos táticos ou operacionais com as referidas ações.*

3.2. Achados de auditoria

3.2.1. Conselho Nacional de Proteção de Dados e da Privacidade encontra-se inoperante

3.2.1.1 Situação encontrada

322. *O Conselho Nacional de Proteção de Dados e da Privacidade (CNPD) é órgão integrante da estrutura da ANPD, conforme art. 55-C da LGPD. Apesar de suas importantes atribuições, não havia membros designados até a data de conclusão do relatório preliminar (peça 1013) que foi enviado para comentários dos gestores em 18/6/2021.*

323. *Em relação às dez indicações realizadas por órgãos da administração pública, Câmara dos Deputados, Senado Federal, Conselho Nacional de Justiça, Conselho Nacional do Ministério Público e Comitê Gestor da Internet já haviam escolhidos seus titulares e suplentes. Restavam as indicações dos órgãos do Poder Executivo (Casa Civil, Gabinete de Segurança Institucional, Ministério da Justiça e Segurança Pública, Ministério da Economia e Ministério da Ciência, Tecnologia e Inovações).*

324. *Para as indicações dos representantes da sociedade civil, de instituições científicas, de sindicatos e do setor privado, a ANPD lançou cinco editais de chamamento para o preenchimento de 13 das 23 vagas do conselho, tendo recebido 122 inscrições. Em maio de 2021, o órgão divulgou as listas tríplices contendo indicações de titulares e suplentes a partir do resultado do chamamento público para envio ao Ministro-Chefe da Casa Civil e, posteriormente, ao Presidente da República, responsável pela nomeação.*

325. *Embora não haja prazo legal para entrada em funcionamento do colegiado, a sua atuação é fundamental para trazer mais eficiência para a ANPD, que, com poucos recursos, enfrenta desafios importantes para colocar em prática todas as atividades atribuídas pela legislação. Assim, a ausência do órgão consultivo prejudica de forma decisiva o alcance dos objetivos preconizados na LGPD. É importante ressaltar que o CNPD tem composição multissetorial, característica adotada pelo país para a política nacional de governança da internet, o que deve qualificar o processo decisório da autoridade ao trazer a visão de atores provenientes de diferentes esferas de atuação, mitigando o risco de ações ineficientes e enviesadas.*

326. *Em reunião realizada com a equipe de auditoria, os diretores da ANPD registraram a expectativa de que a primeira reunião do CNPD ocorreria ainda no primeiro semestre deste ano, sendo pauta prioritária as diretrizes para elaboração da Política Nacional de Proteção de Dados e da Privacidade. Ademais, os membros do Conselho-Diretor afirmaram que o CNPD deve ter uma atuação destacada em termos de disseminação do conhecimento, mudança de cultura, elaboração de estudos, benchmarkings e apresentação de melhores práticas, além de constituir espaço para discussões prévias a respeito de temas que serão objeto de regulamentação.*

327. *Entretanto, somente em 10/8/2021, foram publicados os decretos que designaram os membros para compor o CNPD (peça 1048).*

3.2.1.2 Objetos nos quais foi constatado

a) Publicações referentes à indicação e à nomeação dos membros do CNPD.

3.2.1.3 Critério de auditoria

a) Lei 13.709/2018, art. 58-A.

b) Decreto 10.474/2020, arts. 15, 16 e 17.

3.2.1.4 Evidências

a) Registros da reunião realizada com membros do Conselho-Diretor da ANPD (peça 1002).

b) Decretos de 9/8/2021 (peça 1048).

3.2.1.5 Causas

a) Demora no processo de montagem e envio das listas tríplices por parte da ANPD.

b) Demora na indicação dos membros por parte do Poder Executivo.

3.2.1.6 Efeitos

a) Ineficiência, ineficácia e inefetividade da atuação da ANPD.

b) Ausência de diretrizes estratégicas para a elaboração da Política Nacional de Proteção de Dados e da Privacidade.

3.2.1.7 Conclusão

328. *Para o bom funcionamento da ANPD e para o cumprimento dos objetivos preconizados na LGPD, é preciso que sejam envidados esforços no sentido de promover a efetiva entrada em funcionamento do Conselho Nacional de Proteção de Dados e da Privacidade.*

329. *Nesse sentido, ainda restavam pendentes: a indicação dos membros pelo Poder Executivo federal, a designação formal dos titulares e suplentes pelo Presidente da República e o provimento de recursos necessários para a realização das reuniões do colegiado.*

330. *Somente em 10/8/2021, foram publicados os decretos que designaram os membros para compor o CNPD (peça 1048).*

3.2.1.8 Proposta de encaminhamento

331. *Considerando a publicação dos Decretos de 9 de agosto de 2021 que designaram os membros do CNPD, a equipe de auditoria propõe* ***deixar de determinar*** *à Casa Civil da Presidência da República, ao Gabinete de Segurança Institucional da Presidência da República, aos Ministérios da Justiça e Segurança Pública, Economia, e Ciência, Tecnologia e Inovações que indiquem seus representantes para o Conselho Nacional de Proteção de Dados e da Privacidade, consoante atribuições dispostas no art. 15, incisos I, II, III, IV e V do Decreto 10.474, de 26 de agosto de 2020.*

3.2.2. Falta de transparência e de participação de interessados no processo de construção da Agenda Regulatória para o biênio 2021-2022

3.2.2.1 Situação encontrada

332. *Em 27 de janeiro de 2021, a ANPD publicou a Agenda Regulatória para o biênio 2021-2022, por meio da Portaria-ANPD 11/2021. Foram previstos dez temas para regulamentação por parte do órgão, escalonados em três fases para permitir a divisão dos temas ao longo do tempo.*

333. *Mecanismo típico das agências reguladoras, a Agenda Regulatória está prevista no art. 21 da Lei 13.848/2019, consistindo em instrumento de planejamento da atividade normativa que conterá o conjunto dos temas prioritários a serem regulamentados pela agência durante sua vigência. Deve estar alinhada aos objetivos do plano estratégico e ser aprovada pelo Conselho-Diretor ou diretoria colegiada.*

334. *Apesar de elencar os temas objeto de regulamentação futura e de ter sido aprovada por seu Conselho-Diretor, a Agenda Regulatória da ANPD não contou com processo de construção transparente e colaborativo, sendo a escolha e a priorização dos temas objeto de exclusiva deliberação dos seus diretores, conforme relatado em reunião com a equipe de auditoria. Mesmo reconhecendo o esforço dos membros do colegiado em elencar critérios mais objetivos para a escolha final dos temas, como a possibilidade de impactos econômicos, ainda existem riscos importantes na formação da atual agenda, decorrentes de possíveis assimetrias entre o que o Conselho-Diretor entende como prioritário e as expectativas dos agentes de tratamento.*

335. *Embora se trate de instrumento de gestão interna, a agenda regulatória provoca efeitos externos relevantes, motivo pelo qual é importante que sua construção seja feita em um processo marcado pela participação de vários atores, favorecendo a transparência e a publicidade, pois a eventual exclusão de temas críticos pode impactar negativamente o ambiente regulado, com sérios prejuízos causados aos titulares dos dados e às organizações públicas e privadas que realizam atividades de tratamento. A participação do CNPD poderia atenuar a situação, mas, como relatado em achado anterior, o conselho ainda não foi formado.*

336. *Nesses casos, em assuntos de maior importância, a adoção de mecanismos de participação de interessados nos processos de tomada de decisão da ANPD é uma obrigação expressa da lei, conforme determina o art. 55, inciso XIV da LGPD. Segundo o dispositivo, compete ao órgão ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento.*

337. *Ademais, a participação social no processo decisório é reforçada pelo Decreto 9.203/2017, que trata sobre a política de governança da administração pública federal direta, autárquica e fundacional. Pela norma, cabe à alta administração implementar e manter mecanismos, instâncias e práticas de governança em consonância com os princípios e diretrizes elencados. Entre os princípios, destacam-se a melhoria regulatória, a transparência e a prestação de contas e responsabilidade. Por sua vez, são diretrizes de governança pública:*

> *(i) manter processo decisório orientado pelas evidências, pela conformidade legal, pela qualidade regulatória, pela desburocratização e pelo apoio à participação da sociedade;*
>
> *(ii) editar e revisar atos normativos, pautando-se pelas boas práticas regulatórias e pela legitimidade, estabilidade e coerência do ordenamento jurídico e realizando consultas públicas sempre que conveniente; e*
>
> *(iii) promover a comunicação aberta, voluntária e transparente das atividades e dos resultados da organização, de maneira a fortalecer o acesso público à informação.*

338. *Portanto, a ausência de participação de interessados no processo de construção da Agenda Regulatória da ANPD é medida contrária à LGPD e aos princípios e diretrizes de governança pública, destoando do processo colaborativo adotado pelas agências reguladoras.*

339. *A Agência Nacional de Telecomunicações realizou consulta pública aberta a qualquer interessado visando colher sugestões para elaboração da sua Agenda Regulatória referente ao biênio 2021-2022, obtendo 123 contribuições da sociedade. A Agência Nacional de Vigilância Sanitária realizou seminário aberto e duas consultas públicas, uma para a sociedade e outra para os entes de vigilância sanitária, para discutir sua Agenda Regulatória do triênio 2021-2023. A Agência Nacional de Transportes Terrestres conduziu reunião participativa e tomada de subsídios para construir sua Agenda Regulatória 2021-2022. A Agência Nacional de Mineração, entidade criada em 2017, realizou reuniões participativas com agentes públicos e privados com o objetivo de obter sugestões para sua Agenda Regulatória 2020-2021.*

340. *Como visto, em todos os processos citados houve importante participação da sociedade, que serviu para modificar o cenário de intervenção regulatória das entidades responsáveis, equilibrando as necessidades e expectativas de todos os envolvidos.*

341. *A LGPD elenca mais de sessenta temas para atuação da ANPD, seja por meio de normatizações, recomendações, guias, estabelecimento de padrões, divulgação de boas práticas e uma série de outras atividades, muitas delas com nível alto de urgência e criticidade, sendo que a demora nas ações do órgão pode inviabilizar a própria lei. Por ser sua primeira Agenda Regulatória, garantir a participação de outros atores envolvidos com a temática seria medida que ajudaria a diminuir o custo de oportunidade, visto que, em fase inicial e ainda com poucos recursos, qualquer perda de eficiência da ANPD terá impactos significativos para todo o sistema de proteção de dados.*

342. *Após o envio do relatório preliminar para comentário dos gestores, a ANPD editou a Portaria 16, de 8 de julho de 2021, visando sanar os problemas apontados. Referida norma trata do processo de regulamentação no âmbito da autoridade, incorporando os pontos tratados neste achado, motivo pelo qual deve ser levada em consideração na proposta de encaminhamento.*

3.2.2.2 Objetos nos quais foi constatado

a) *Agenda Regulatória 2021-2022 da ANPD.*

3.2.2.3 Critério de auditoria

a) *Lei 13.709/2018, art. 55, inc. XIV.*
b) *Decreto 9.203/2017, arts. 3º, 4º, 5º e 6º.*

3.2.2.4 Evidências

a) *Agenda Regulatória 2021-2022 da ANPD (peça 1008).*
b) *Registros da reunião realizada com membros do Conselho-Diretor da ANPD (peça 1002).*

3.2.2.5 Causas

a) *Falta de estabelecimento de mecanismos de participação no processo de construção da Agenda Regulatória.*

3.2.2.6 Efeitos

a) *Desalinhamento de necessidades e expectativas entre autoridade regulatória e setores regulados.*
b) *Perda potencial de eficiência na atuação da ANPD.*

3.2.2.7 Conclusão

343. *Tendo em vista a busca pela melhoria do ambiente regulatório relativo à temática da proteção de dados, é importante que a ANPD adote mecanismos de maior participação dos agentes de tratamento e da sociedade em geral no processo de construção de sua Agenda Regulatória, visando atender ao disposto na LGPD e alinhando-se aos princípios e diretrizes de governança pública.*

3.2.2.8 Proposta de encaminhamento

344. *Considerando as ações adotadas pela ANPD após o envio do relatório preliminar para comentários, a equipe de auditoria propõe* ***deixar de recomendar*** *à Autoridade Nacional de Proteção de Dados que, na construção e revisão de suas agendas regulatórias, inclua fase voltada à participação dos agentes de tratamento e da sociedade civil, atendendo ao disposto no art. 55, inc. XIV, da Lei 13.709/2018 e aos princípios e diretrizes de governança pública previstos no Decreto 9.203/2017.*

3.2.3. Temas relevantes elencados pela LGPD sem previsão de regulamentação

3.2.3.1 Situação encontrada

345. *A LGPD delega diversas atribuições regulatórias para a ANPD, englobando matérias centrais para a correta aplicação da lei. Assim, a falta de atuação da autoridade na regulamentação dos temas pode inviabilizar o alcance dos objetivos pretendidos pela legislação e impactar o processo de adequação das organizações.*

346. *A seguir são listados alguns dispositivos da LGPD que demandam atuação regulatória da ANPD:*

***Quadro 2** - Lista exemplificativa de atribuições da ANPD*

Art. 4º, § 3º
Dispensa de aplicação da lei para os casos de tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações legais:
*A **autoridade nacional emitirá** opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e **deverá solicitar** aos responsáveis relatórios de impacto à proteção de dados pessoais*
Art. 11, § 3º
*A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de **regulamentação por parte da autoridade nacional**, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências*
Art. 12, § 3º
*A **autoridade nacional poderá dispor** sobre padrões e técnicas utilizados em processos de anonimização e **realizar verificações** acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais*
Art. 13, § 3º
Realização de estudos em saúde pública:
*O acesso aos dados de que trata este artigo será objeto de **regulamentação por parte da autoridade nacional** e das autoridades da área de saúde e sanitárias, no âmbito de suas competências*
Art. 18, V
*O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a **regulamentação da autoridade nacional**, observados os segredos comercial e industrial*
Art. 19, § 3º
*Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de **regulamentação da autoridade nacional**, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento*
Art. 23, § 1º
Tratamento de dados pessoais pelas pessoas jurídicas de direito público:
*A **autoridade nacional poderá dispor** sobre as formas de publicidade das operações de tratamento*
Art. 30
*A **autoridade nacional poderá estabelecer** normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais*
Art. 32
*A **autoridade nacional poderá solicitar** a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e **sugerir a adoção de padrões e de boas práticas** para os tratamentos de dados pessoais pelo Poder Público*
Art. 38
*A **autoridade nacional poderá determinar** ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, **nos termos de regulamento**, observados os segredos comercial e industrial*
Art. 40

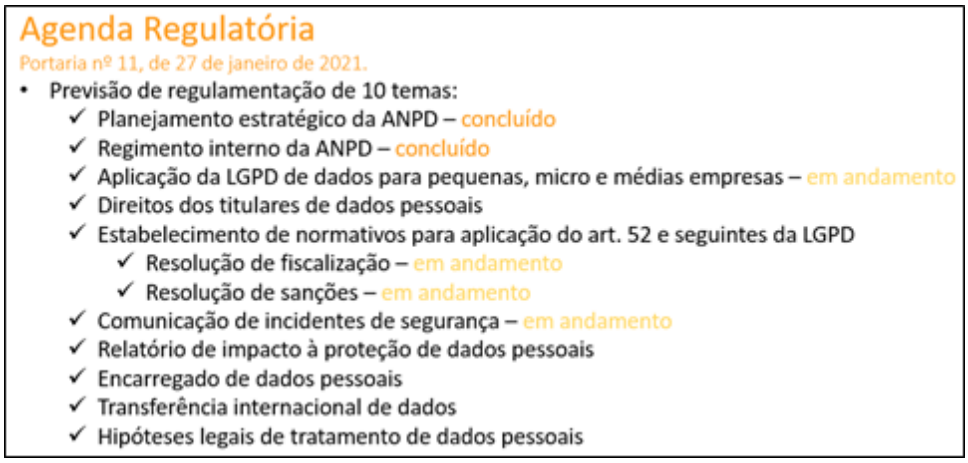
*A **autoridade nacional poderá dispor** sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência*
Art. 41, § 3º
*A **autoridade nacional poderá estabelecer** normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.*
Art. 46, § 1º
Adoção de medidas de segurança pelos agentes de tratamento para proteção de dados pessoais: *A **autoridade nacional poderá dispor** sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei*
Art. 50, § 3º
*As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser **reconhecidas e divulgadas pela autoridade nacional***
Art. 51
*A **autoridade nacional estimulará** a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais*
Art. 55, XVIII
Compete à ANPD: ***Editar normas, orientações e procedimentos simplificados e diferenciados**, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei*
Art. 63
*A **autoridade nacional estabelecerá** normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, consideradas a complexidade das operações de tratamento e a natureza dos dados*

***Fonte**: elaboração própria a partir da Lei 13.709/2018.*

347. *Como visto, são temas variados e complexos, que demandarão tempo e esforço significativo por parte da ANPD para conclusão do processo de regulamentação, considerando ainda as obrigações procedimentais impostas pela LGPD, como a necessidade de submissão de regulamentos e normas à consulta e audiência públicas, bem como à análise de impacto regulatório, antes da sua entrada em vigor.*

348. *Com a publicação da Agenda Regulatória para o biênio 2021-2022, a ANPD definiu quais matérias pretende iniciar a regulamentação no período, considerando a sua capacidade operacional atual. Os temas escolhidos são exibidos a seguir:*

Figura 59 *- Temas da Agenda Regulatória 2021-2022 da ANPD*



Fonte*: Apresentação institucional da ANPD, realizada em 9/4/2021.*

349. *Portanto, ao cotejar os temas da agenda com aqueles elencados na LGPD, é possível concluir que diversas matérias relevantes, a exemplo do uso compartilhado de dados pessoais sensíveis, técnicas de anonimização de dados e adoção de padrões mínimos de segurança pelos agentes de tratamento de dados, não só não serão regulamentadas no próximo biênio, como não possuem qualquer indicativo de quando serão, fato que ocasiona insegurança jurídica para a atuação tanto de órgãos públicos quanto de organizações privadas, os quais são forçados a adotarem medidas próprias que podem não ser compatíveis com a regulação futura e não garantir a efetiva proteção dos direitos dos titulares de dados, sujeitando-os às sanções previstas na lei.*

350. *Reflexos da falta de normatização já podem ser observados também na atuação da própria ANPD, especialmente em casos de maior relevância, a exemplo da discussão em torno da nova política de privacidade do aplicativo de mensagens WhatsApp, em que se discute a possibilidade do compartilhamento e uso de dados pessoais dos usuários da plataforma para empresas parceiras do WhatsApp Business.*

351. *Na Nota Técnica 02/2021/CGTP, a ANPD aponta diversos problemas importantes relativos: à elaboração de relatório de impacto à proteção de dados; às bases legais utilizadas para os tratamentos; ao exercício dos direitos dos titulares; e ao tratamento de dados de crianças e adolescentes. No entanto, em todos os pontos, a ANPD se restringe a recomendar providências que permitam uma maior aderência aos dispositivos da LGPD, registrando que ainda não há regulamentação para os temas, o que, na prática, limita a atuação do órgão e impede a imposição de medidas de cumprimento obrigatório para o WhatsApp, visando maior proteção aos direitos dos titulares dos dados.*

352. *Diante da fase atual de estruturação da ANPD, com poucos recursos materiais e humanos disponíveis, seria natural a redução da capacidade de entrega de resultados, inclusive a edição de atos regulatórios. No entanto, a adoção de um planejamento mais robusto em relação à atuação regulatória do órgão, que envolvesse, mas não se limitasse à elaboração de agendas regulatórias, permitiria oferecer maior previsibilidade aos agentes de tratamento e à sociedade acerca de como a autoridade pretende exercer suas atividades regulatórias, dando transparência e publicidade às etapas envolvidas, seguindo os exemplos adotados por outras agências reguladoras.*

353. *A Agência Nacional de Telecomunicações e a Agência Nacional de Vigilância Sanitária, por exemplo, estabeleceram as diretrizes e etapas de seus processos de regulamentação, por meio da edição de normativos específicos (Portaria-Anatel 927/2015 e Portaria-Anvisa 162/2021). Em ambos são mencionadas ações voltadas ao levantamento ou identificação de necessidades para regulamentação, insumos importantes para a construção das agendas regulatórias.*

354. *Ademais, de acordo com o Decreto 9.203/2017, manter processo decisório orientado pela qualidade regulatória e editar atos normativos a partir de boas práticas regulatórias são diretrizes que*

devem ser observadas na implementação dos mecanismos de governança pública, visando atender aos princípios da capacidade de resposta, da melhoria regulatória e da transparência.

355. *Logo, a adoção de um processo voltado ao planejamento regulatório da ANPD, com a inclusão de ações relacionadas à gestão do seu estoque regulatório, onde poderiam ser previstos procedimentos para identificação dos temas e dimensionamento dos recursos necessários, poderia trazer ganhos diretos para a atuação da autoridade no curto prazo e para o planejamento de longo prazo, especialmente para a formulação das próximas agendas regulatórias, o que deve levar a um aumento na segurança jurídica e consequente melhora no ambiente para os agentes de tratamento, em linha com os princípios e diretrizes de governança pública.*

356. *Após o envio do relatório preliminar para comentário dos gestores, a ANPD editou a Portaria 16, de 8 de julho de 2021, visando sanar os problemas apontados. Referida norma trata do processo de regulamentação no âmbito da autoridade, incorporando os pontos tratados neste achado, motivo pelo qual deve ser levada em consideração na proposta de encaminhamento.*

3.2.3.2 Objetos nos quais foi constatado

a) *Agenda Regulatória 2021-2022 da ANPD.*

3.2.3.3 Critério de auditoria

a) *Lei 13.709/2018, art. 4º, § 3º; art. 11, § 3º; art. 12, § 3º; art. 13, § 3º; art. 18, inc. V; art. 19, § 3º; art. 23, § 1º; art. 30; art. 32; art. 38; art. 40; art. 41, § 3º; art. 46, § 1º; art. 50, § 3º; art. 51; art. 55, inc. XVIII; art. 63.*

3.2.3.4 Evidências

a) *Agenda Regulatória 2021-2022 da ANPD (peça 1008).*
b) *Registros da reunião realizada com membros do Conselho-Diretor da ANPD (peça 1002).*

3.2.3.5 Causas

a) *Limitação de recursos humanos.*
b) *Ausência de processo estruturado de planejamento regulatório, incluindo etapa para a gestão do estoque regulatório.*

3.2.3.6 Efeitos

a) *Inefetividade da Lei Geral de Proteção de Dados.*
b) *Insegurança jurídica para atuação dos agentes de tratamento.*
c) *Adoção de medidas insuficientes para proteção dos dados dos titulares.*
d) *Perda de confiança na capacidade de resposta da ANPD frente aos desafios.*
e) *Enfraquecimento institucional da ANPD.*

3.2.3.7 Conclusão

357. *Para que a LGPD alcance todos os objetivos para os quais foi criada, é imperativa uma atuação ampla, eficaz e coordenada por parte da ANPD. Diante da quantidade de temas delegados para regulamentação por parte da autoridade, a criação de procedimentos direcionados à gestão do estoque regulatório poderia ser a base para atuações futuras do órgão, inserindo-o dentro de um processo maior de planejamento da regulação, o qual permitiria organizar os fluxos de trabalho necessários para uma atuação mais eficiente, seguindo os princípios e diretrizes de governança pública previstos no Decreto 9.203/2017.*

358. *Mesmo com o andamento das ações dispostas na Agenda Regulatória 2021-2022, ainda restam diversas normas e padrões técnicos importantes a serem editados pela ANPD, o que tende a resultar na implementação de medidas não padronizadas entre os agentes de tratamento e, possivelmente, insuficientes para a proteção dos direitos dos titulares de dados.*

3.2.3.8 Proposta de encaminhamento

359. *Considerando as ações adotadas pela ANPD após o envio do relatório preliminar para comentários, a equipe de auditoria propõe* ***deixar de recomendar*** *à Autoridade Nacional de Proteção*

de Dados que institua processo organizacional para estruturação do seu planejamento regulatório, em linha com os princípios e diretrizes de governança pública previstos no Decreto 9.203/2017, com previsão de fases, etapas e demais fluxos de trabalho, incluindo atividades voltadas à gestão do estoque regulatório, as quais devem considerar os temas pendentes de regulamentação elencados na Lei 13.709/2018.

3.2.4. Natureza jurídica da ANPD não confere a independência necessária para uma autoridade de proteção de dados

3.2.4.1 Situação encontrada

360. *O texto original da Lei 13.709/2018 aprovado no Congresso Nacional (Projeto de Lei 53/2018) previa que a ANPD integrava a administração pública indireta, vinculando-se ao Ministério da Justiça, sem subordinação hierárquica, sendo submetida a regime autárquico especial e regida pela Lei 9.986/2000, aplicável às agências reguladoras. Ademais, assegurava à ANPD independência administrativa e autonomia financeira.*

361. *Todo o Capítulo IX do projeto de lei, que tratava da ANPD, foi vetado por vício de inconstitucionalidade em relação ao processo legislativo, considerando que a iniciativa para dispor de leis que versem sobre a criação de órgão da administração pública é privativa do Presidente da República.*

362. *Posteriormente, após nova rodada de discussões, foi editada a MP 869/2018, que criou a ANPD no formato atual, como órgão da administração direta subordinado à Presidência da República, mesmo com papel que se equivale em vários pontos ao de outras entidades regulatórias que atuam sob a natureza de autarquia em regime especial.*

363. *Além de gerar uma situação jurídica incomum, o desenho da instituição prejudica sua independência e se afasta dos modelos adotados em outros países, podendo trazer prejuízos para o sistema de proteção de dados nacional e ainda provocar conflitos de interesse, considerando a subordinação direta à Presidência e a possibilidade de vir a fiscalizar atos da própria administração pública. Do mesmo modo, dificulta as pretensões do país de ingressar em blocos econômicos e organismos internacionais de relevância.*

364. *Ao lado dos aspectos citados, outra situação chamou a atenção da equipe de auditoria. De acordo com estudo da associação Data Privacy Brasil, que analisou dados de países economicamente mais avançados a partir de lista do Fundo Monetário Internacional, a composição da autoridade de proteção de dados brasileira, que conta com três dos cinco diretores de mesma origem institucional, difere da maioria dos países estudados.*

365. *Quanto a esse ponto, é importante destacar que a composição do Conselho-Diretor deve ser realizada buscando um ponto de equilíbrio entre a origem e o perfil dos seus membros, sem qualquer tipo de predominância, tendo em vista que essa característica favorece a tomada de decisões que contemplem de forma mais proporcional as diferentes visões e perspectivas acerca da utilização de dados pessoais, tanto no setor público como no privado, visando a construção de um ambiente regulatório plural e aderente aos objetivos delineados na LGPD.*

366. *Em reunião com a equipe de auditoria, os diretores da ANPD ressaltaram a necessidade de se alterar a natureza jurídica do órgão, visando ter condições de cumprir efetivamente sua missão. Mencionaram fortes restrições de pessoal e a ausência de autonomia financeira, o que impediria a elaboração de orçamentos próprios que contemplassem as demandas indispensáveis para sua estruturação. Não há sistemas informatizados próprios para auxiliar no fluxo dos processos de trabalho e até mesmo os computadores utilizados pelos diretores são pessoais e não institucionais, o que provoca diversos riscos de segurança da informação e expõe o órgão a violações de dados pessoais, causando, além dos impactos materiais, danos irreparáveis à reputação do órgão.*

367. *Mesmo tendo autonomia técnica e decisória prevista na legislação, a subordinação à Presidência da República e a consequente submissão ao poder hierárquico, com ausência de autonomia administrativa e financeira, não conferem à ANPD o grau de independência desejado para uma autoridade de proteção de dados, estando em desacordo com normas e boas práticas internacionais.*

368. *Conforme o artigo 52 do Regulamento Geral de Proteção de Dados da União Europeia, toda autoridade de proteção de dados deve ter assegurada:*

> *(i) total independência no exercício de suas competências, devendo seus membros estarem livres de qualquer influência externa, seja direta ou indireta, sendo vedado procurar ou receber instruções de quem quer que seja;*
>
> *(ii) o provimento de recursos humanos, técnicos e financeiros, além de infraestrutura necessária para o efetivo exercício de suas atribuições;*
>
> *(iii) a escolha de seu quadro de pessoal, que deve ser próprio da autoridade; e*
>
> *(iv) orçamentos anuais separados, com sujeição a controles financeiros que não afetem sua independência.*

369. *A versão mais recente da Convenção 108 do Conselho da Europa para a Proteção das Pessoas com relação ao Tratamento Automatizado de Dados Pessoais prevê, no capítulo 4, que as autoridades de proteção de dados devem agir com completa independência e imparcialidade no desenvolvimento das suas atividades, abstendo-se de procurar ou receber instruções. Ademais, deve ser assegurado o provimento de recursos necessários para o efetivo desempenho das funções.*

370. *A Lei de Privacidade do Consumidor da Califórnia (California Consumer Privacy Act - CCPA), que criou a Agência de Proteção da Privacidade do estado norte-americano, previu que a entidade teria total independência administrativa e seria comandada por um conselho composto por cinco membros, sendo dois escolhidos pelo governador, dois pelo Legislativo estadual e um pela Procuradoria-Geral do Estado. Além disso, continha dispositivo que reservava orçamento específico para o funcionamento da agência.*

371. *Em estudo publicado em 2020 pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE) a respeito da transformação digital no Brasil, a entidade avaliou, entre outros pontos, a constituição da ANPD. Entre as recomendações endereçadas ao país, constam:*

> *(i) reavaliar e revisar as condições estabelecidas nos termos da ANPD no Artigo 55-A da Lei 13.709/2018, a fim de garantir que a Autoridade opere com total independência desde o início de seu estabelecimento;*
>
> *(ii) garantir que as regras para a indicação do Conselho Diretor da ANPD e do CNPD sejam transparentes, imparciais e baseadas em conhecimento técnico; e*
>
> *(iii) garantir ou adequar um orçamento previsível para a ANPD, por meio de um processo transparente.*

372. *Além dos prejuízos causados na atuação direta da ANPD quanto à regulação do sistema de proteção de dados nacional, a falta de independência do órgão pode prejudicar também o desenvolvimento da economia digital baseada em dados, com reflexos imediatos nos negócios das empresas brasileiras no exterior. Isso porque é comum que leis de proteção de dados tenham alcance extraterritorial e fixem critérios adequados para permitir a realização de transferência internacional de dados entre os países envolvidos. Assim, por exemplo, a realização de negócios com empresas situadas no continente europeu pode ser facilitada a depender de uma decisão de adequação de um país aos dispositivos da GDPR, tarefa realizada pela Comissão Europeia. Um dos requisitos objeto de análise nesse caso é justamente a existência e o efetivo funcionamento de uma autoridade independente que assegure o atendimento às diretrizes de proteção de dados.*

373. *Atualmente, na América do Sul, somente Uruguai e Argentina têm decisão favorável da entidade. A mudança do desenho institucional da ANPD poderia alterar esse cenário. Outra possibilidade seria a ratificação pelo Brasil da Convenção 108 do Conselho da Europa, que ainda não ocorreu, com posterior incorporação ao ordenamento jurídico brasileiro, fato que poderia abrir caminho para uma decisão de adequação positiva da Comissão Europeia.*

374. *Com a possibilidade aberta pela LGPD para que seja realizada avaliação quanto à transformação da ANPD em órgão da administração indireta, a instituição conduziu iniciativa nesse sentido e concluiu estudos a respeito da alteração de sua natureza jurídica.*

375. *De maneira a evidenciar a necessidade de fortalecimento da estrutura organizacional, o órgão traçou um panorama comparativo entre autoridades de proteção de dados ao redor do mundo, levando em consideração a quantidade de funcionários, o tamanho da população e o Produto Interno Bruto (em dólares americanos) de cada país. O resultado pode ser visto na tabela abaixo:*

Quadro 3 - *Comparação entre autoridades de proteção de dados*

País	Funcionários	População	PIB
Brasil	31	212.994.000	$ 1.840.000.000.000,00
México	272	126.200.000	$ 1.221.000.000.000,00
Alemanha	253	83.020.000	$ 3.948.000.000.000,00
França	199	66.990.000	$ 2.778.000.000.000,00
Reino Unido	768	66.650.000	$ 2.855.000.000.000,00
Itália	162	60.360.000	$ 2.084.000.000.000,00
Espanha	152	46.940.000	$ 1.419.000.000.000,00
Polônia	154	37.970.000	$ 585.700.000.000,00
Marrocos	24	35.130.000	$ 117.900.000.000,00
Austrália	120	24.990.000	$ 1.434.000.000.000,00
Romênia	50	19.410.000	$ 239.600.000.000,00
Países Baixos	191	17.280.000	$ 913.700.000.000,00
Bélgica	62	11.460.000	$ 542.800.000.000,00
Rep. Checa	115	10.690.000	$ 245.200.000.000,00
Portugal	27	10.280.000	$ 240.700.000.000,00
Suécia	89	10.230.000	$ 556.100.000.000,00
Áustria	36	8.859.000	$ 455.300.000.000,00
Hong Kong	74	7.451.000	$ 362.700.000.000,00
Bulgária	69	7.000.000	$ 65.130.000.000,00
Sérvia	71	6.982.000	$ 50.600.000.000,00
Finlândia	46	5.518.000	$ 276.700.000.000,00
Eslováquia	46	5.458.000	$ 105.900.000.000,00
Noruega	52	5.368.000	$ 434.200.000.000,00
Irlanda	140	4.904.000	$ 382.500.000.000,00
Geórgia	116	3.731.000	$ 17.600.000.000,00
Albânia	37	2.846.000	$ 15.100.000.000,00
Eslovênia	43	2.081.000	$ 54.010.000.000,00
Macedônia	50	2.077.000	$ 12.670.000.000,00
Letônia	26	1.920.000	$ 34.410.000.000,00
Ilhas Maurício	20	1.265.000	$ 14.220.000.000,00
Luxemburgo	33	613.894	$ 70.890.000.000,00
Argentina	48	45.808.747	$ 449.700.000.000,00
Uruguai	76	3.500.000	$ 56.000.000.000,00
Correlação		**61%**	**70%**

Fonte*: Minuta da Nota Técnica 3/SG/ANPD – Projeto Fortalecimento Institucional da ANPD.*

Obs*.: Valor do PIB em dólar americano no ano de 2019.*

376. *Comparando os órgãos internacionais a partir da proporção do número de funcionários por milhão de habitantes, a razão do Brasil é a menor dentre todos os países pesquisados. Ademais, dos dez países de maior PIB, o Brasil é aquele que possui a menor autoridade de proteção de dados em quantidade de funcionários. Portanto, os dados revelam que o tamanho da ANPD apresenta discrepância significativa quando comparado com outros países.*

377. *Assim, a proposta do órgão objetiva a sua transformação em autarquia em regime especial, visando maior autonomia administrativa e financeira, nos moldes previstos originalmente no Projeto de Lei 53/2018, acompanhada de uma reestruturação organizacional e da criação de cargos para expandir as unidades finalísticas e fortalecer as unidades administrativas.*

378. *Dessa forma, a ANPD espera exercer de forma plena suas competências regulatórias e fiscalizatórias, além de ser capaz de atuar na construção de tecnologia e de conhecimento em proteção de dados pessoais, na capacitação de entes públicos e privados, e na disseminação de informação para a sociedade.*

3.2.4.2 <u>Objetos nos quais foi constatado</u>

a) MP 869/2018 e Lei 13.853/2019.

3.2.4.3 Critério de auditoria

a) Regulamento Geral de Proteção de Dados da União Europeia, capítulo 6 (Independent supervisory authorities).

b) Convenção 108 do Conselho da Europa, capítulo 4 (Supervisory authorities).

3.2.4.4 Evidências

a) Registros da reunião realizada com membros do Conselho-Diretor da ANPD (peça 1002).

b) Estudo da Associação Data Privacy Brasil a respeito do perfil dos membros de autoridades de proteção de dados (peça 1003).

c) Estudo da OCDE: A caminho da era digital no Brasil, capítulo 4 (peça 1004).

d) Minuta da Nota Técnica 3/SG/ANPD – Projeto Fortalecimento Institucional da ANPD (peça 1005).

3.2.4.5 Causas

a) Subordinação à Presidência da República.

b) Ausência de autonomia administrativa e financeira.

3.2.4.6 Efeitos

a) Falta de autonomia efetiva para tomar decisões em casos de maior sensibilidade.

b) Dificuldades para composição da força de trabalho.

c) Dificuldades para elaborar orçamentos compatíveis com suas atribuições.

d) Insegurança jurídica provocada pela demora na regulamentação de temas importantes da LGPD.

e) Baixo índice de fiscalizações realizadas.

f) Dificuldade para obtenção de decisão favorável de adequação por parte da Comissão Europeia.

3.2.4.7 Conclusão

379. *Para que a ANPD consiga cumprir com sua missão institucional, é necessário rever a natureza jurídica do órgão, atividade já autorizada pela LGPD, visando dotá-lo de real autonomia para desempenhar suas atribuições, sem restrições que possam inviabilizar o exercício dos papéis regulatório e fiscalizatório que competem à autoridade.*

380. *Nesse sentido, a proposta da ANPD visa equilibrar o tamanho de sua estrutura com a quantidade de competências atribuídas pela LGPD, ao mesmo tempo em que busca maior aderência aos modelos praticados por autoridades de proteção de dados mais consolidadas de outros países, o que deve trazer maior capacidade de resposta do órgão frente às demandas para estruturação de um sistema eficiente que permita equilibrar a proteção dos dados pessoais e o desenvolvimento de uma economia digital baseada em dados.*

3.2.4.8 Proposta de encaminhamento

381. *Diante do exposto, a equipe de auditoria propõe* ***recomendar*** *à Casa Civil da Presidência da República e ao Ministério da Economia que adotem as medidas necessárias para encaminhar proposta visando alterar a natureza jurídica e promover a reestruturação organizacional da Autoridade Nacional de Proteção de Dados, conferindo o grau de independência e os meios necessários para o pleno exercício de suas atribuições, de acordo com o exposto na Nota Técnica 3/SG/ANPD e à semelhança do preconizado em normas internacionais, como o Regulamento Geral de Proteção de Dados da União Europeia e a Convenção 108 do Conselho da Europa.*

4. Boas práticas identificadas

382. *Neste capítulo, são registradas boas práticas e esforços desenvolvidos pelas organizações auditadas e que foram identificados no decorrer da fiscalização.*

4.1. Resolução CNJ 363/2021

383. *No âmbito do Poder Judiciário, destaca-se a Resolução CNJ 363/2021 (peça 999), que estabeleceu medidas para o processo de adequação à LGPD que devem ser adotadas pelos tribunais de primeira e segunda instâncias e pelas cortes superiores, à exceção do Supremo Tribunal Federal. Dentre as medidas, destacam-se: criar Comitê Gestor de Proteção de Dados Pessoais (art. 1º, inciso I), formar grupo de trabalho técnico de caráter multidisciplinar em cada tribunal (art. 1º, inciso III) e organizar programa de conscientização (art. 1º, inciso IX). A resolução também recomenda que o processo de implementação da LGPD contemple, ao menos, as seguintes ações: realização de mapeamento de todas as atividades de tratamento de dados pessoais (art. 2º, inciso I), realização de avaliação das vulnerabilidades (gap assessment) em relação à proteção de dados pessoais (art. 2º, inciso II) e elaboração de plano de ação (roadmap) com a previsão de todas as atividades constantes na resolução (art. 2º, inciso III).*

4.2. Comitê Estratégico de Privacidade e Proteção de Dados Pessoais no âmbito do Ministério da Economia

384. *A Portaria ME 4.424/2021 criou o Comitê Estratégico de Privacidade e Proteção de Dados Pessoais do Ministério da Economia, na forma de instância interna de apoio à governança quanto ao tema de privacidade e proteção de dados pessoais (art. 1º). Dentre as competências do comitê, destacam-se: promover a proteção de dados pessoais e a adequação do Ministério da Economia à LGPD (art. 2º, inciso I), elaborar programa de governança em privacidade e assegurar a implementação de suas ações (art. 2º, inciso III), coordenar iniciativas relacionadas às boas práticas em proteção de dados pessoais (art. 2º, inciso IV) e promover a cultura e os conhecimentos relativos à proteção de dados pessoais (art. 2º, inciso VII).*

4.3. Comissão de Proteção de Dados do Cofecon

385. *A Comissão de Proteção de Dados do Conselho Federal de Economia (Cofecon), criada pela Portaria 31/2020 (peça 1000), tem o papel de orientar o processo de implementação da LGPD do Sistema Cofecon/Corecon com as seguintes competências: avaliar os mecanismos de tratamento e proteção de dados existentes e propor políticas, estratégias e metas; formular princípios e diretrizes para a gestão de dados pessoais e propor sua regulamentação; supervisionar a execução dos planos, projetos e ações; prestar orientações sobre o tratamento e a proteção de dados pessoais; promover o intercâmbio de informações sobre a proteção de dados pessoais com outros órgãos; e elaborar plano de trabalho que contemple: ações de transparência; mapeamento e registro de tratamento de dados; disponibilização de canal de exercício de direitos do titular; revisão de contratos, convênios e instrumentos congêneres.*

4.4. Ações de treinamento e conscientização realizadas pela SGD/ME

4.4.1. Seminário internacional de proteção de dados

386. *O seminário, que foi promovido Secretaria de Governo Digital (SGD) do Ministério da Economia (ME), reuniu especialistas do Brasil e do mundo para debater segurança e privacidade do cidadão no processo de digitalização dos serviços públicos.*

387. *No evento, a SGD/ME apresentou o conceito 'once-only, but privacy first' (apenas uma vez, mas a privacidade vem primeiro), em que a interoperabilidade de sistemas e o compartilhamento de informações entre os órgãos públicos são considerados impulsionadores da transformação digital de serviços, tendo a privacidade e segurança como requisitos essenciais.*

388. *Já o coordenador desta fiscalização, que participou como palestrante do evento, ressaltou a importância da segurança da informação para a efetividade da proteção de dados pessoais, bem como da articulação interna e da participação da alta administração para que se obtenha êxito nos projetos de adequação à LGPD.*

4.4.2. Guias Operacionais para adequação à LGPD da SGD/ME

389. *A SGD/ME preparou um conjunto de ações para fomentar a cultura de proteção de dados e apoiar a evolução da maturidade necessária para adequação à LGPD nos órgãos do Governo Federal.*

390. *Dentre esse conjunto de ações, a SGD/ME disponibilizou um questionário que tem como intuito fornecer um diagnóstico do atual estágio de adequação à LGPD do órgão respondente, auxiliando no direcionamento de esforços e na priorização de ações.*

391. *Disponibilizou também um guia de boas práticas e uma série de guias operacionais para auxiliar na adequação à LGPD dos órgãos do SISP: Programa de Governança em Privacidade, Inventário de Dados Pessoais, Termo de Uso, Avaliação de Riscos, Requisitos e Obrigações quanto à Segurança da Informação e Privacidade, Relatório de Impacto de proteção de dados – RIPD, Segurança em Aplicações Web e Framework de Segurança.*

4.4.3. Escola Virtual.Gov

392. *A Escola Virtual.Gov é o portal do Governo para oferta de capacitação a distância, por meio de cursos online e gratuitos de várias áreas de conhecimento para o desenvolvimento da Administração Pública e da Sociedade.*

393. *Dentre os cursos oferecidos, destacam-se: Introdução à Lei Brasileira de Proteção de Dados Pessoais e Proteção de Dados Pessoais no Setor Público.*

4.5. Gestão de incidentes de segurança de dados pessoais do Banco do Nordeste

394. *Dentre os documentos enviados pelo Banco do Nordeste do Brasil (BNB) junto com suas respostas ao questionário da auditoria, destaca-se o manual de procedimento de gestão de incidentes de segurança de dados pessoais (peça 1001), que é composto das seguintes fases: detecção, categorização, definição de criticidade, análise, contenção e remediação, recuperação, registro, comunicação e base de lições aprendidas.*

395. *O procedimento se inicia com a detecção ou comunicação, por qualquer colaborador do BNB, de um evento que deve ser investigado de maneira aprofundada.*

396. *As subcategorias dos incidentes de segurança de dados pessoais incluem: acesso não autorizado; alteração indevida de dados; alteração sem autorização; destruição de dados; divulgação não autorizada de informações; perda ou roubo de dados; tratamento de dados ilícito; tratamento de dados inadequado; e vazamento de dados.*

397. *Cada subcategoria de incidente está associada a um nível de criticidade e um tempo máximo de atendimento.*

398. *O objetivo da análise é investigar o incidente de segurança de dados pessoais sob diversos aspectos, tais como: avaliar as consequências concretas e prováveis do incidente; verificar se os dados pessoais relacionados ao incidente são armazenados ou transferidos para outros países e sujeitos a outras regulamentações locais; verificar se os dados pessoais relacionados ao incidente pertencem a outro controlador ou se existe relação de controlador conjunto; confirmar se os dados afetados foram tornados públicos e avaliar os possíveis impactos de uma eventual divulgação do incidente na mídia; verificar quais ativos tecnológicos e impactos envolvidos no incidente de segurança de dados pessoais; e comunicar o Encarregado pelo Tratamento de Dados Pessoais sobre a gravidade do incidente.*

399. *O objetivo da contenção e remediação é direcionar as ações necessárias para conter e remediar o incidente de segurança de dados pessoais, e o da recuperação é restabelecer a normalidade.*

400. *As informações coletadas e analisadas devem ser registradas contendo a maior quantidade de detalhes possíveis sobre o incidente de segurança de dados pessoais.*

401. *O Encarregado pelo Tratamento de Dados Pessoais deve avaliar os impactos do incidente, pois sempre que houver risco ou dano relevante aos direitos e liberdades individuais do titular de dados pessoais, o incidente deverá ser comunicado à ANPD e aos titulares afetados.*

402. *Por fim, o objetivo da base de lições aprendidas é a melhoria contínua do processo com base em medidas mitigatórias adotadas em incidentes anteriores.*

4.6. Guia orientativo da ANPD

403. *Já durante a fase final de elaboração deste relatório, em 28/5/2021, a ANPD publicou o 'Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado', com objetivo de estabelecer diretrizes aos agentes de tratamento e explicar quem pode exercer as funções de controlador, operador e encarregado, inclusive com exemplos de casos que ilustram os assuntos abordados, sanando algumas das principais dúvidas que têm sido apresentadas à ANPD.*

5. Comentários dos gestores

404. *A versão preliminar deste relatório foi enviada para receber comentários das seguintes organizações destinatárias de propostas de deliberações: Conselho Nacional de Justiça (peça 1019), Secretaria de Governo Digital e Secretaria Executiva do Ministério da Economia (peças 1020 e 1021), Casa Civil da Presidência da República (peça 1022), Autoridade Nacional de Proteção de Dados (peça 1023) e Conselho Nacional do Ministério Público (peça 1024).*

405. *Os comentários são a oportunidade para que os gestores apresentem suas perspectivas sobre as questões levantadas neste relatório e informações sobre as consequências práticas da implementação das deliberações aventadas, bem como sugestões de eventuais medidas alternativas.*

406. *Cabe ressaltar que após o vencimento dos prazos para envio dos comentários dos gestores, os quais são facultativos, o Conselho Nacional de Justiça e a Secretaria Executiva do Ministério da Economia não apresentaram seus comentários. A seguir, serão analisados os comentários recebidos das demais organizações.*

5.1. Secretaria de Governo Digital do Ministério da Economia

407. *Em sua manifestação (peças 1044 e 1045), os gestores da SGD/ME teceram comentários para cada subitem da recomendação contida no parágrafo 425.1 do relatório preliminar (peça 1013, p. 90-92), detalhando quais já teriam sido atendidos, total ou parcialmente, não atendidos e propondo encaminhamento de alguns para outras organizações, a exemplo de ANPD e GSI/PR. Ademais, sugerem a inclusão de nova recomendação para a ANPD.*

408. *Quanto à sugestão de encaminhamento de cinco recomendações para a ANPD (subitens 425.1.6, 425.1.10, 425.1.11, 425.1.25 e 425.1.26; peça 1045, p. 2-4) e uma para o GSI/PR (subitem 425.1.24; peça 1045, p. 4), a equipe de auditoria deixa de acatar por entender que as competências dessas organizações são complementares e não excludentes com aquelas da SGD/ME, devendo esta Secretaria promover o diálogo institucional e buscar o apoio da ANPD e do GSI/PR para a orientação das organizações sob sua alçada acerca dos temas objeto das deliberações. Nesse sentido, deve harmonizar suas orientações com normativos e publicações vigentes de outros órgãos e entidades competentes no exercício de suas atribuições.*

409. *Em relação à recomendação do subitem 425.1.22 (peça 1045, p. 3-4), atendida pela ANPD, a equipe de auditoria acata a sugestão, motivo pelo qual essa proposta de deliberação foi excluída (parágrafo 258).*

410. *Sobre a sugestão de inclusão de nova recomendação à ANPD (peça 1045, p. 5, parágrafo 11.5.4), a equipe de auditoria deixa de acatar por entender pela sua não viabilidade, pois a elaboração e revisão da Agenda Regulatória da autoridade seguem as diretrizes dispostas na Portaria-ANPD 16, de 8 de julho de 2021.*

411. *Das dezesseis recomendações consideradas atendidas pela SGD/ME (subitens 425.1.1, 425.1.3, 425.1.4, 425.1.7, 425.1.8, 425.1.9, 425.1.12, 425.1.13, 425.1.14, 425.1.15, 425.1.16, 425.1.17, 425.1.19, 425.1.20, 425.1.22, 425.1.23 e 425.1.27; peça 1045, p. 1-4), a equipe de auditoria concluiu que treze foram efetivamente cumpridas, enquanto as outras três devem ser consideradas apenas parcialmente atendidas, conforme análise disposta na tabela a seguir:*

Texto da recomendação	*Comentários da SGD/ME*	*Análise da equipe de auditoria*
425.1.12. à elaboração de Plano de Capacitação que considere a	*Recomendação atendida por meio do documento 'Guia sobre o Programa*	*O tema é tratado de forma esparsa e insuficiente na publicação em questão. Faltou orientação sobre a necessidade de*

Texto da recomendação	*Comentários da SGD/ME*	*Análise da equipe de auditoria*
realização de treinamento e conscientização dos colaboradores em proteção de dados pessoais, considerando as diretrizes estabelecidas nos itens 5.5.2 e 5.5.3 da ABNT NBR ISO/IEC 27701:2019;	*de Governança em Privacidade', além da divulgação de conteúdos em seu sítio na internet.*	*elaborar um Plano de Capacitação propriamente dito, com definição de temas e público-alvo, por exemplo.* *Conclusão: recomendação* ***parcialmente*** *atendida.*
425.1.19. à implementação de mecanismos para atendimento dos direitos dos titulares elencados no art. 18 da Lei 13.709/2018, considerando as diretrizes estabelecidas no item 7.3 da ABNT NBR ISO/IEC 27701:2019;	*Recomendação atendida por meio de diretrizes dispostas no documento 'Guia de Boas Práticas LGPD'.*	*O texto do documento referenciado trata apenas da estrutura organizacional necessária e diretrizes gerais para recebimento dos pedidos decorrentes do exercício dos direitos dos titulares de dados, sem mencionar outros mecanismos, técnicos e administrativos, para seu atendimento. Por exemplo, a realização de gestão do consentimento ou implementação de funcionalidades específicas nos sistemas de informação para que a organização possa atender a pedido de titular para acesso, correção ou exclusão dos dados tratados.* *Conclusão: recomendação* ***parcialmente*** *atendida.*
425.1.20. à implementação de procedimentos e controles para o compartilhamento de dados pessoais com terceiros (organizações públicas, privadas e transferência internacional), considerando o disposto nos arts. 5º, inciso XVI; 26, 27; e 33 da Lei 13.709/2018 e as diretrizes estabelecidas no item 7.5 da ABNT NBR ISO/IEC 27701:2019;	*Recomendação atendida por meio dos documentos 'Guia de Elaboração de Inventário de Dados Pessoais' e 'Guia de Boas Práticas LGPD'.*	*Apesar de existirem procedimentos e controles previstos para o compartilhamento de dados pessoais com organizações públicas e para a transferência internacional de dados, faltam orientações específicas para o compartilhamento com organizações privadas. Esse tipo de operação de tratamento possui algumas restrições elencadas na LGPD e que precisam ser consideradas pelos órgãos públicos, a exemplo daquelas constantes nos arts. 26 e 27.* *Conclusão: recomendação* ***parcialmente*** *atendida.*

Fonte*: elaboração própria.*

412. *A partir do exposto, a equipe de auditoria entende necessário realizar ajustes nas propostas de encaminhamento originais, de maneira a contemplar as ações já adotadas pela SGD/ME – excluindo as treze propostas que foram consideradas efetivamente cumpridas e mantendo as três que foram consideradas apenas parcialmente atendidas.*

5.2. Casa Civil da Presidência da República

413. *Os gestores da Casa Civil se manifestaram (peças 1037 e 1038) no sentido de que a recomendação para a alteração da natureza jurídica da ANPD merece ressalvas. Segundo o órgão, a transformação da ANPD em autarquia implicaria em um aumento significativo de despesas e que o atual cenário de restrições orçamentárias e financeiras imposto pela Emenda Constitucional 95/2016 ('Teto de Gastos'), pela Lei Complementar (LC) 173/2020 e pela Lei de Diretrizes Orçamentárias (LDO) seria incompatível com a proposta. Ademais, afirma também que a natureza jurídica da autoridade não impede, por si só, que ela exerça todas as competências que lhe foram outorgadas pela LGPD.*

414. *Com relação a esse ponto, a equipe de auditoria entende que o achado demonstra sob várias perspectivas as fragilidades do desenho institucional adotado atualmente para a ANPD e os prejuízos que a situação provoca para todo o sistema de proteção de dados.*

415. *Quanto aos aspectos orçamentários e financeiros, estes devem ser levados em consideração no estudo de conveniência e oportunidade para adoção da recomendação, que representa deliberação de cumprimento não obrigatório pelo gestor, apesar de ser considerada fundamental para o sucesso da ANPD. A equipe de fiscalização é da opinião de que todos os aspectos citados pelos gestores da Casa Civil são importantes, porém superáveis com o devido planejamento e dimensionamento das medidas necessárias para implementação da deliberação, que podem inclusive ser escalonadas no tempo. Por exemplo, as restrições impostas pela LC 173/2020 expiram em 31/12/2021, enquanto as dotações orçamentárias podem estar previstas no próximo ciclo orçamentário, com o envio dos projetos de LDO e Lei Orçamentária Anual para o Congresso contemplando o pleito, em todo ou em parte, a depender da avaliação feita pelo Poder Executivo.*

416. *Por esses motivos, entende-se que a recomendação deve ser mantida nos seus exatos termos.*

5.3. Autoridade Nacional de Proteção de Dados (ANPD)

417. *Em sua manifestação (peças 1042 e 1043), os gestores da ANPD apontaram medidas em curso que visam atender a três das recomendações endereçadas ao órgão: i) orientações quanto ao papel do encarregado; ii) maior participação social na elaboração da agenda regulatória; e iii) organização de processo para estruturar a atuação regulatória.*

418. *Para o primeiro ponto, entendem que a publicação do 'Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado' atende a recomendação. Entretanto, a equipe de auditoria mantém a proposta nos exatos termos originais (parágrafo 149), pois, apesar da boa prática adotada pelo órgão, a recomendação é específica para o normativo que ainda será editado e o guia mencionado não tem caráter vinculante.*

419. *Quanto aos demais pontos, a ANPD publicou a Portaria 16, de 8 de julho de 2021, a qual trata do processo de regulamentação no âmbito da autoridade, abordando todos os itens destacados nos achados correspondentes deste relatório. Desse modo, a equipe de auditoria entende adequado alterar as propostas originais, conforme relatado nos tópicos dos achados (seções 3.2.2 e 3.2.3).*

5.4. Conselho Nacional do Ministério Público (CNMP)

420. *Em sua manifestação (peça 1031), o Encarregado pela Proteção de Dados do CNMP salientou que aquele Conselho exerce função dúplice no tocante às medidas necessárias à adaptação à LGPD:*

> *(...) De um lado, por tratar-se de órgão público que realiza o tratamento de dados pessoais, para o exercício de suas missões constitucionais previstas no art. 130-A da Constituição, fez-se necessária a adoção de providências internas de conformidade.*
>
> *(...)*
>
> *De outra banda, o CNMP possui a missão de exercer função de órgão setorial de controle, nos termos do art. 55-J, §3º, da LGPD e do art. 130-A da Constituição, o que impõe supervisão quanto à observância dos princípios e regras da LGPD – e das demais leis que versam, direta ou indiretamente sobre proteção de dados, no ordenamento jurídico pátrio – pelos ramos e unidades do Ministério Público brasileiro.*

421. *Com relação à primeira função, o gestor informou que 'foi constituído, por meio da Portaria CNMP-PRESI nº 35, de 05 de março de 2020, Grupo de Trabalho, objetivando a implementação da LGPD na estrutura orgânica interna do CNMP'. A referida portaria foi acostada à peça 1034 destes autos.*

422. *Quanto à segunda função, o gestor salientou também que 'foi constituído, por meio da Portaria CNMP-PRESI nº 55, de 14 de abril de 2020, Grupo de Trabalho para a regulamentação setorial da proteção de dados no âmbito do MP brasileiro'. A referida portaria foi acostada à peça 1035 destes autos.*

423. *Informou também que:*

> *O GT confeccionou Anteprojeto de Resolução, que aborda todos os aspectos apontados pelo Relatório Preliminar do TCU como pendências, além de definir estrutura orgânica mínima, tanto pelo CNMP, para o exercício das sobreditas atividades de controle, quanto pelos ramos e unidades do Ministério Público.*

424. *O referido anteprojeto foi acostado à peça 1033 destes autos. Entretanto, considerando que a aludida resolução está pendente de apreciação pelo Plenário do CNMP e ainda pode sofrer alterações, não foi analisado se aborda todos os aspectos apontados por este relatório.*

425. *Neste ponto, destaca-se que, exatamente devido a essa segunda função, a de órgão setorial de controle, o CNMP também é destinatário da proposta de recomendação para que edite normativos e guias para auxiliar o processo de adequação à LGPD das organizações sob sua jurisdição (parágrafo 454.1).*

426. *Assim, embora ações já tenham sido iniciadas, as informações apresentadas pelo CNMP não demandaram alterações no relatório e nas propostas de encaminhamento.*

6. Trabalhos futuros

427. *Os resultados obtidos por esta fiscalização mostraram que é necessário acompanhar as futuras ações de adequação à LGPD que serão realizadas pelas organizações da APF. Nesse sentido, convém que sejam planejadas ações de controle externo com foco em privacidade e proteção de dados pessoais no setor público federal, de forma a propiciar a continuidade do presente trabalho e a indução de avanços na implementação da LGPD pelas organizações auditadas, como parte de uma estratégia de atuação do TCU em proteção de dados e privacidade ou, até mesmo, em governança de dados.*

428. *Dentre essas ações, propõe-se analisar a conveniência e oportunidade, como continuidade desta fiscalização, da execução de auditorias de conformidade em amostra das organizações que responderam ao questionário. A seleção da amostra deve considerar critérios de relevância e risco, incluindo o nível de adequação à LGPD computado com base nas respostas autodeclaradas pelas organizações.*

429. *Outra possível ação é acompanhar continuamente a evolução das organizações públicas federais em relação ao nível de adequação à LGPD. O acompanhamento seria realizado por meio da disponibilização permanente de um questionário online, similar ao utilizado nesta fiscalização, o qual poderia ser respondido voluntariamente a qualquer momento para obtenção de diagnóstico a respeito da evolução da organização respondente quanto à adequação à LGPD.*

430. *Também se propõe a construção de um painel de informações a ser alimentado, inicialmente, com os dados referentes às respostas ao questionário coletadas por meio desta fiscalização e, posteriormente, com as respostas do questionário online, de modo a mostrar de forma atualizada a evolução da adequação à LGPD das organizações públicas federais.*

431. *Outra linha de ação necessária é acompanhar o andamento da agenda regulatória da ANPD, bem como suas ações e procedimentos instaurados para assegurar os direitos dos titulares e a proteção de dados pessoais. No mesmo sentido, é conveniente que sejam acompanhadas a atuação do CNPD e a elaboração e a execução da Política Nacional de Proteção de Dados e Privacidade.*

432. *Antes disso, as organizações auditadas esperam receber relatórios individuais de feedback a respeito de seus níveis atuais de adequação à LGPD, que deverão ser elaborados e enviados após autorização do acórdão a ser proferido em decorrência desta fiscalização.*

7. Conclusão

433. *Esta auditoria elaborou diagnóstico acerca dos controles implementados pelas organizações públicas federais para adequação à LGPD, o qual foi obtido por meio das 382 respostas recebidas para o questionário online e apresentado em função das nove dimensões avaliadas: preparação, contexto organizacional, liderança, capacitação, conformidade do tratamento, direitos do titular, compartilhamento de dados pessoais, violação de dados pessoais e medidas de proteção.*

434. *Inicialmente, verificou-se que apenas 45% das organizações respondentes concluíram a preparação (identificação e planejamento) das medidas necessárias para a adequação à LGPD (Seção 2.1.1).*

435. *Quanto ao contexto organizacional (Seção 2.1.2), chama atenção que 77% das organizações ainda não identificaram todas as categorias de titulares de dados pessoais com os quais mantém relacionamento; 51% não conduziram iniciativa para identificar os operadores; 70% não avaliaram a existência de tratamento de dados que envolve controlador conjunto; apenas 17% identificaram todos os processos de negócio que realizam tratamento de dados pessoais; e 14% identificaram todos os dados pessoais que tratam. Ademais, dentre as organizações que identificaram os processos organizacionais que realizam tratamento de dados pessoais e os respectivos dados pessoais, de maneira integral ou parcial, apenas 33% analisaram os riscos dos tratamentos de dados pessoais.*

436. *Na dimensão de liderança (Seção 2.1.3), o resultado é alarmante, pois cerca de uma em cada quatro organizações não possui política de segurança da informação e 65% não possuem política de classificação da informação, sendo que apenas 57% dessas políticas abrangem diretrizes para classificação de dados pessoais e somente 18% abrangem diretrizes para identificar dados pessoais sensíveis e de crianças e de adolescentes; apenas 18% possuem política de proteção de dados pessoais; e 31% ainda não nomearam encarregado pelo tratamento de dados pessoais.*

437. *Quanto às iniciativas de conscientização e capacitação dos colaboradores (Seção 2.1.4), o resultado também é preocupante, pois apenas a minoria das organizações, 29%, possui plano de capacitação que abrange a proteção de dados pessoais, sendo que somente 54% desses planos consideram que pessoas que exercem funções com responsabilidades essenciais relacionadas à proteção de dados pessoais devem receber treinamento diferenciado. Ademais, apenas 10% das organizações treinaram todos os colaboradores diretamente envolvidos em atividades que realizam tratamento de dados pessoais.*

438. *Com relação à dimensão de conformidade do tratamento com os ditames da LGPD (Seção 2.1.5), verificou-se que somente 46% das organizações identificaram e documentaram as finalidades das atividades de tratamento de dados pessoais (11% identificaram todas as finalidades e 35% identificaram apenas algumas finalidades), sendo que, dentre essas organizações, 51% não avaliaram se coletam apenas os dados estritamente necessários e 61% não avaliaram se os dados pessoais são retidos (armazenados) durante o tempo estritamente necessário.*

439. *Dentre os direitos do titular (Seção 2.1.6), constatou-se que 75% das organizações ainda não elaboraram política de privacidade e que somente 14% implementaram mecanismos para atender todos os direitos dos titulares elencados no art. 18 da LGPD.*

440. *Mais um ponto alarmante é que somente 14% das organizações identificaram todos os dados pessoais compartilhados com terceiros e que 42% delas sequer realizaram iniciativa para identificar possíveis compartilhamentos (Seção 2.1.7).*

441. *O resultado no que tange à gestão de incidentes que envolvem violação de dados pessoais também é alarmante (Seção 2.1.8), pois constatou-se que 84% das organizações não possuem plano de resposta a incidentes que abrange o tratamento de incidentes de violação de dados pessoais; 72% não possuem sistema para registro de incidentes que envolvem violação de dados pessoais e 75% não possuem sistema para registro das ações adotadas para solucionar tais incidentes; 66% não monitoram proativamente a ocorrência de eventos associados à violação de dados pessoais; e 88% não estabeleceram procedimentos de comunicação à ANPD e ao titular.*

442. *Na última dimensão, medidas de proteção aos dados pessoais (Seção 2.1.9), a situação encontrada também é preocupante, pois 54% das organizações declararam que não são capazes de comprovar que adotaram medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais; apenas 16% implementaram controle de acesso em todos os sistemas que realizam o tratamento de dados pessoais; 7% registram eventos de todas as atividades de tratamento de dados pessoais; 43% não utilizam criptografia para proteger os dados pessoais; e 85% não adotaram medidas para assegurar que processos e sistemas sejam projetados, desde a concepção, em conformidade com a LGPD (de acordo com os conceitos de Privacy by Design e de Privacy by Default).*

443. *Além das respostas ao questionário, também foi realizada análise por meio de um indicador calculado com base em um subconjunto de 42 questões selecionadas, com objetivo de comparar as organizações auditadas no que tange ao nível de adequação à LGPD (Seção 2.2). A partir dos valores do indicador, as organizações foram classificadas em quatro níveis – inexpressivo, inicial, intermediário e aprimorado – e os resultados mostraram que: 17,8% estão no nível inexpressivo; 58,9% estão no nível inicial; 20,4% estão no nível intermediário e 2,9% estão no nível aprimorado (Figura 52).*

444. *Os valores do indicador também foram calculados para cada uma das seções do questionário e os melhores resultados foram obtidos na dimensão preparação e os piores nas dimensões capacitação, direitos do titular, conformidade do tratamento e violação de dados pessoais (Figura 53).*

445. *Assim, a conclusão do diagnóstico acerca dos controles implementados pelas organizações públicas federais para adequação à LGPD apresentou situação de alto risco à privacidade dos cidadãos que têm dados pessoais coletados e tratados pela APF.*

446. *Em relação à estruturação da ANPD, avaliou-se a composição do órgão e as ações iniciais adotadas para cumprir com as competências atribuídas pela LGPD. Foram realizadas, para tanto, coletas de informações a partir de normativos e documentos oficiais, além de reuniões com os membros do Conselho-Diretor, com posterior análise e comparação com os critérios de auditoria.*

447. *O primeiro achado diz respeito ao Conselho Nacional de Proteção de Dados e da Privacidade, órgão consultivo da ANPD que se encontra inoperante. Pelas importantes atribuições que possui, como sugerir ações para a autoridade e disseminar o conhecimento em proteção de dados para a sociedade, a ausência do conselho traz prejuízos para o desempenho da ANPD como um todo.*

448. *Os dois achados seguintes dizem respeito à Agenda Regulatória da ANPD, publicada no início do ano e que contém os temas que serão objeto de regulamentação por parte do órgão no biênio 2021-2022. Apesar dos efeitos externos relevantes que provoca, verificou-se que o processo de formação do instrumento e priorização dos temas não contou com a participação dos agentes de tratamento e da sociedade em geral, fato que permitiria alcançar um maior equilíbrio entre o que a autoridade entende como prioritário e as necessidades dos demais atores envolvidos.*

449. *Ademais, diversos temas importantes elencados pela LGPD não só não serão regulamentados no biênio como não há expectativa de quando os serão, ocasionando insegurança jurídica para a atuação tanto de organizações públicas quanto privadas.*

450. *No quarto achado, verificou-se que a natureza jurídica da ANPD, nos moldes previstos pela LGPD, não confere o grau de independência desejado para uma autoridade de proteção de dados, estando em desacordo com normas, boas práticas e experiências internacionais. A situação limita de forma decisiva a atuação da ANPD e pode impactar a decisão de adequação do Brasil pela Comissão Europeia para fins de realização de transferência internacional de dados, com reflexos negativos para as empresas brasileiras. Tal decisão ainda pode ser seguida por outros blocos econômicos, potencializando os efeitos negativos de uma eventual inadequação.*

451. *Conforme previsto nos arts. 14 e 15 da Resolução-TCU 315/2020, os achados e as propostas preliminares foram apresentados à ANPD, à Casa Civil da Presidência da República, ao Ministério da Economia, ao CNJ, à SGD/ME e ao CNMP e seus comentários foram considerados na elaboração da versão final deste artefato. Cumpre ressaltar que o relatório não foi enviado para comentários das 91*

organizações que foram objeto da deliberação referente à elaboração de Política de Segurança da Informação, decisão amparada pelo disposto no art. 14, § 2º, inc. I, da Resolução-TCU 315/2020.

452. *Por fim, a LGPD considera, em seu art. 5º, inciso I, que dado pessoal é a 'informação relacionada a pessoa natural identificada ou identificável'. Por sua vez, o regulamento europeu (General Data Protection Regulation – GDPR) esclarece que (tradução livre): dados pessoais são quaisquer informações relacionadas a uma pessoa natural identificada ou identificável; a identificação pode ser direta ou indireta, incluindo todos os dados que são ou podem ser atribuídos a uma pessoa de qualquer forma; e, uma vez que a definição inclui qualquer informação, é forçoso presumir que o termo 'dados pessoais' deve ser interpretado da forma mais ampla possível.*

453. *Essa definição revela-se coerente com a disciplina jurídica da proteção de dados, pois uma interpretação extensiva do conceito privilegia sua condição de direito fundamental, ampliando o seu âmbito de proteção. Assim, considera-se que o questionário da auditoria coletou os seguintes dados pessoais dos respondentes: nome, e-mail, telefone e cargo ou função. Além disso, algumas organizações informaram dados adicionais de forma espontânea, como matrícula de servidor público (por exemplo, peças 593, 594, 702 e 705) e número de CPF (peças 695 e 722). Desse modo, a equipe de auditoria propõe que esses dados pessoais coletados por meio do questionário e as peças do processo que contém dados pessoais que foram informados por algumas organizações auditadas sejam classificados como sigilosos nos termos do art. 31, § 1º, inciso I, da Lei 12.527/2011 (Lei de Acesso à Informação – LAI).*

8. Propostas de encaminhamento

454. *Diante do exposto, submetem-se os autos à consideração do Relator, Ministro Augusto Nardes, com as seguintes propostas:*

454.1. recomendar à Secretaria de Governo Digital do Ministério da Economia, com fundamento no art. 11 da Resolução - TCU 315/2020, que, considerando o controle realizado sobre a atuação administrativa das organizações sob sua jurisdição, edite normativos e guias, consultando a Autoridade Nacional de Proteção de Dados e o Gabinete de Segurança Institucional da Presidência da República, para auxiliar o processo de adequação das organizações à LGPD, incluindo orientações quanto:

454.1.1. à identificação de normativos correlatos ao tratamento de dados pessoais aplicáveis à organização, considerando as diretrizes estabelecidas no item 5.2.1 da ABNT NBR ISO/IEC 27701:2019;

454.1.2. à adequação dos contratos firmados com os operadores de forma a estabelecer, claramente, os papéis e responsabilidades relacionados à proteção de dados pessoais, considerando as diretrizes estabelecidas no item 7.2.6 da ABNT NBR ISO/IEC 27701:2019;

454.1.3. à avaliação da ocorrência de tratamento de dados pessoais com o envolvimento de controlador conjunto e à definição de papeis e responsabilidades de cada um dos controladores, considerando as diretrizes estabelecidas no item 7.2.7 da ABNT NBR ISO/IEC 27701:2019;

454.1.4. à elaboração de Política de Classificação da Informação que considere a classificação de dados pessoais, considerando o disposto nos arts. 5º, inciso II, 11 e 14 da Lei 13.709/2018 e no art. 31, § 1º, da Lei 12.527/2011, bem como as diretrizes estabelecidas no item 6.5.2 da ABNT NBR ISO/IEC 27701:2019;

454.1.5. à elaboração de Política de Proteção de Dados Pessoais, considerando as diretrizes estabelecidas no item 6.2.1.1 da ABNT NBR ISO/IEC 27701:2019;

454.1.6. à elaboração de Plano de Capacitação que considere a realização de treinamento e conscientização dos colaboradores em proteção de dados pessoais, considerando as diretrizes estabelecidas nos itens 5.5.2 e 5.5.3 da ABNT NBR ISO/IEC 27701:2019;

454.1.7. à elaboração de Política de Privacidade, considerando o disposto nos arts. 6º, incisos IV e VI, 9º e 23, inciso I, da Lei 13.709/2018 e as diretrizes estabelecidas nos itens 7.3.2 e 7.3.3 da ABNT NBR ISO/IEC 27701:2019;

454.1.8. à implementação de mecanismos para atendimento dos direitos dos titulares elencados no art. 18 da Lei 13.709/2018, considerando as diretrizes estabelecidas no item 7.3 da ABNT NBR ISO/IEC 27701:2019;

454.1.9. à implementação de procedimentos e controles para o compartilhamento de dados pessoais com terceiros (organizações públicas, privadas e transferência internacional), considerando o disposto nos arts. 5º, inciso XVI; 26, 27; e 33 da Lei 13.709/2018 e as diretrizes estabelecidas no item 7.5 da ABNT NBR ISO/IEC 27701:2019;

454.1.10. à elaboração de Plano de Resposta a Incidentes e à implementação de controles para o tratamento de ocorrências relacionadas à violação de dados pessoais, considerando o disposto no art. 50, § 2º, inciso I, alínea 'g', da Lei 13.709/2018 e as diretrizes estabelecidas no item 6.13 da ABNT NBR ISO/IEC 27701:2019;

454.1.11. à implementação de processo de controle de acesso de usuários em sistemas que realizam tratamento de dados pessoais, considerando o disposto nos arts. 46 e 47 da Lei 13.709/2018 e as diretrizes estabelecidas nos itens 6.6.2.1 e 6.6.2.2 da ABNT NBR ISO/IEC 27701:2019;

454.1.12. à implementação de registro de eventos das atividades de tratamento de dados pessoais, considerando as diretrizes estabelecidas no item 6.9.4.1 da ABNT NBR ISO/IEC 27701:2019; e

454.1.13. à utilização de criptografia para proteção de dados pessoais, considerando o disposto nos arts. 48, § 3º; e 50, § 2º, inciso I, alínea 'c', da Lei 13.709/2018 e as diretrizes estabelecidas no item 6.7 da ABNT NBR ISO/IEC 27701:2019;

454.2. recomendar ao Conselho Nacional de Justiça e ao Conselho Nacional do Ministério Público, com fundamento no art. 11 da Resolução - TCU 315/2020, que, considerando o controle realizado sobre a atuação administrativa das organizações sob suas jurisdições, editem normativos e guias, consultando a Autoridade Nacional de Proteção de Dados, para auxiliar o processo de adequação das organizações à LGPD, incluindo orientações quanto:

454.2.1. ao planejamento das medidas necessárias para adequação à LGPD, considerando as diretrizes estabelecidas no item 5.4.2 da ABNT NBR ISO/IEC 27701:2019;

454.2.2. à identificação de normativos correlatos ao tratamento de dados pessoais aplicáveis à organização, considerando as diretrizes estabelecidas no item 5.2.1 da ABNT NBR ISO/IEC 27701:2019;

454.2.3. à identificação das categorias de titulares de dados pessoais com os quais se relacionam, considerando as diretrizes estabelecidas no item 7.2.8 da ABNT NBR ISO/IEC 27701:2019;

454.2.4. à identificação dos operadores que realizam tratamento de dados pessoais em seus nomes, considerando as diretrizes estabelecidas no item 5.2.2 da ABNT NBR ISO/IEC 27701:2019;

454.2.5. à adequação dos contratos firmados com os operadores de forma a estabelecer, claramente, os papéis e responsabilidades relacionados à proteção de dados pessoais, considerando as diretrizes estabelecidas no item 7.2.6 da ABNT NBR ISO/IEC 27701:2019;

454.2.6. à avaliação da ocorrência de tratamento de dados pessoais com o envolvimento de controlador conjunto e à definição de papeis e responsabilidades de cada um dos controladores, considerando as diretrizes estabelecidas no item 7.2.7 da ABNT NBR ISO/IEC 27701:2019;

454.2.7. à identificação dos processos de negócio que realizam tratamento de dados pessoais, bem como dos respectivos responsáveis, considerando o disposto nos arts. 3º, 5º, inciso X, e 37 da Lei 13.709/2018 e as diretrizes estabelecidas no item 7.2.8 da ABNT NBR ISO/IEC 27701:2019;

454.2.8. à identificação dos dados pessoais que são tratados por elas, bem como dos locais de armazenamento desses dados, considerando o disposto nos arts. 5º, inciso I, e 37 da Lei 13.709/2018 e as diretrizes estabelecidas no item 7.2.8 da ABNT NBR ISO/IEC 27701:2019;

454.2.9. à avaliação de riscos relacionados aos processos de tratamento de dados pessoais, considerando o disposto no art. 50, §2º, alínea 'd', da Lei 13.709/2018 e as diretrizes estabelecidas no item 5.4.1.2 da ABNT NBR ISO/IEC 27701:2019;

454.2.10. à elaboração de Política de Classificação da Informação que considere a classificação de dados pessoais, considerando o disposto nos arts. 5º, inciso II, 11 e 14 da Lei 13.709/2018 e no art. 31, § 1º, da Lei 12.527/2011, bem como as diretrizes estabelecidas no item 6.5.2 da ABNT NBR ISO/IEC 27701:2019;

454.2.11. à elaboração de Política de Proteção de Dados Pessoais, considerando as diretrizes estabelecidas no item 6.2.1.1 da ABNT NBR ISO/IEC 27701:2019;

454.2.12. à elaboração de Plano de Capacitação que considere a realização de treinamento e conscientização dos colaboradores em proteção de dados pessoais, considerando as diretrizes estabelecidas nos itens 5.5.2 e 5.5.3 da ABNT NBR ISO/IEC 27701:2019;

454.2.13. à identificação e à documentação das finalidades das atividades de tratamento de dados pessoais, considerando o disposto no art. 6º, inciso I, da Lei 13.709/2018 e as diretrizes estabelecidas no item 7.2.1 da ABNT NBR ISO/IEC 27701:2019;

454.2.14. à necessidade de avaliar se coletam apenas os dados estritamente necessários para as finalidades de tratamento de dados pessoais e se os dados são retidos durante o tempo estritamente necessário às mesmas necessidades, considerando o disposto no art. 6º, incisos II e III, da Lei 13.709/2018 e as diretrizes estabelecidas nos itens 7.4.1 e 7.4.7 da ABNT NBR ISO/IEC 27701:2019;

454.2.15. à identificação e à documentação das bases legais que fundamentam as atividades de tratamento de dados pessoais, considerando o disposto nos arts. 7º e 23 da Lei 13.709/2018 e as diretrizes estabelecidas no item 7.2.2 da ABNT NBR ISO/IEC 27701:2019;

454.2.16. à manutenção de registro das operações de tratamento de dados pessoais, considerando o disposto no art. 37 da Lei 13.709/2018 e as diretrizes estabelecidas no item 7.2.8 da ABNT NBR ISO/IEC 27701:2019;

454.2.17. à elaboração do Relatório de Impacto à Proteção de Dados Pessoais e de implementar controles para mitigar os riscos identificados, considerando o disposto no art. 5º, inciso XVII, da Lei 13.709/2018 e as diretrizes estabelecidas no item 7.2.5 da ABNT NBR ISO/IEC 27701:2019;

454.2.18. à elaboração de Política de Privacidade, considerando o disposto nos arts. 6º, incisos IV e VI, 9º e 23, inciso I, da Lei 13.709/2018 e as diretrizes estabelecidas nos itens 7.3.2 e 7.3.3 da ABNT NBR ISO/IEC 27701:2019;

454.2.19. à implementação de mecanismos para atendimento dos direitos dos titulares elencados no art. 18 da Lei 13.709/2018, considerando as diretrizes estabelecidas no item 7.3 da ABNT NBR ISO/IEC 27701:2019;

454.2.20. à implementação de procedimentos e controles para o compartilhamento de dados pessoais com terceiros (organizações públicas, privadas e transferência internacional), considerando o disposto nos arts. 5º, inciso XVI; 26, 27; e 33 da Lei 13.709/2018 e as diretrizes estabelecidas no item 7.5 da ABNT NBR ISO/IEC 27701:2019;

454.2.21. à elaboração de Plano de Resposta a Incidentes e à implementação de controles para o tratamento de ocorrências relacionadas à violação de dados pessoais, considerando o disposto no art. 50, § 2º, inciso I, alínea 'g', da Lei 13.709/2018 e as diretrizes estabelecidas no item 6.13 da ABNT NBR ISO/IEC 27701:2019;

454.2.22. à adoção de medidas de segurança para proteção de dados pessoais, considerando o disposto nos arts. 46 e 47 da Lei 13.709/2018 e as boas práticas de gestão de segurança da informação abordadas pela ABNT NBR ISO/IEC 27701:2019;

454.2.23. à implementação de processo de controle de acesso de usuários em sistemas que realizam tratamento de dados pessoais, considerando o disposto nos arts. 46 e 47 da Lei 13.709/2018 e as diretrizes estabelecidas nos itens 6.6.2.1 e 6.6.2.2 da ABNT NBR ISO/IEC 27701:2019;

454.2.24. à implementação de registro de eventos das atividades de tratamento de dados pessoais, considerando as diretrizes estabelecidas no item 6.9.4.1 da ABNT NBR ISO/IEC 27701:2019;

454.2.25. à utilização de criptografia para proteção de dados pessoais, considerando o disposto nos arts. 48, § 3º; e 50, § 2º, inciso I, alínea 'c', da Lei 13.709/2018 e as diretrizes estabelecidas no item 6.7 da ABNT NBR ISO/IEC 27701:2019; e

454.2.26. à adoção de medidas de proteção de dados pessoais desde a fase de concepção até a fase de execução de processos e sistemas (Privacy by Design), incluindo a coleta de dados limitada ao que é estritamente necessário ao alcance do propósito definido (Privacy by Default), considerando o disposto no art. 46, § 2º, da Lei 13.709/2018 e as diretrizes estabelecidas no item 7.4 da ABNT NBR ISO/IEC 27701:2019;

454.3. recomendar à Casa Civil da Presidência da República e ao Ministério da Economia, com fundamento no art. 11 da Resolução - TCU 315/2020, que adotem as medidas necessárias para alterar a natureza jurídica e promover a reestruturação organizacional da Autoridade Nacional de Proteção de Dados, conferindo o grau de independência e os meios necessários para o pleno exercício de suas atribuições, de acordo com o exposto na Nota Técnica 3/SG/ANPD e à semelhança do preconizado em normas internacionais, como o Regulamento Geral de Proteção de Dados da União Europeia e a Convenção 108 do Conselho da Europa;

454.4. recomendar à Autoridade Nacional de Proteção de Dados, com fundamento no art. 11 da Resolução - TCU 315/2020, que oriente as organizações públicas quanto às responsabilidades, aos perfis e requisitos profissionais desejáveis, bem como sobre os locais apropriados de lotação do encarregado no normativo relacionado ao tema que está previsto na agenda regulatória da instituição, em consonância com o disposto no art. 41, § 3º, da Lei 13.709/2018;

454.5. deixar de recomendar à Autoridade Nacional de Proteção de Dados, com fundamento no inciso I do parágrafo único do art. 16 da Resolução - TCU 315/2020 e tendo em conta a publicação da Portaria-ANPD 16, de 8 de julho de 2021, que:

454.5.1. na construção e revisão de suas agendas regulatórias, inclua fase voltada à participação dos agentes de tratamento e da sociedade civil, atendendo ao disposto no art. 55, inc. XIV, da Lei 13.709/2018 e aos princípios e diretrizes de governança pública previstos no Decreto 9.203/2017; e

454.5.2. institua processo organizacional para estruturação do seu planejamento regulatório, em linha com os princípios e diretrizes de governança pública previstos no Decreto 9.203/2017, com previsão de fases, etapas e demais fluxos de trabalho, incluindo atividades voltadas à gestão do estoque regulatório, as quais devem considerar os temas pendentes de regulamentação elencados na Lei 13.709/2018;

454.6. dar ciência às organizações relacionadas na peça 1012, com fundamento no art. 9º, inciso I da Resolução - TCU 315/2020, que a ausência de estabelecimento formal de uma Política de Segurança da Informação afronta o disposto no art. 15, inc. II do Decreto 9.637/2018 c/c art. 9º da Instrução Normativa GSI/PR 1/2020, no art. 19, inciso II, da Resolução 396/2021 do Conselho Nacional de Justiça, e no art. 22, inciso III, da Resolução 156/2016 do Conselho Nacional do Ministério Público;

454.7. deixar de determinar à Casa Civil da Presidência da República, ao Gabinete de Segurança Institucional da Presidência da República, aos Ministérios da Justiça e Segurança Pública, Economia, e Ciência, Tecnologia e Inovações, com fundamento no inciso I do parágrafo único do art. 16 da Resolução - TCU 315/2020 e tendo em conta a publicação dos Decretos de 9 de agosto de 2021, que indiquem seus representantes para o Conselho Nacional de Proteção de Dados e da Privacidade, consoante atribuições dispostas no art. 15, incisos I, II, III, IV e V do Decreto 10.474, de 26 de agosto de 2020;

454.8. nos termos do art. 8º da Resolução - TCU 315/2020, fazer constar, na ata da sessão em que estes autos forem apreciados, comunicação do relator ao colegiado no sentido de monitorar as recomendações contidas nos itens 454.1-454.4;

454.9. encaminhar cópias eletrônicas do acórdão decorrente desta fiscalização, bem como do relatório e do voto que fundamentarem este último, à ANPD, à SGD/ME, ao CNJ, ao CNMP, à Casa Civil da Presidência da República, ao Gabinete de Segurança Institucional da Presidência da República, bem como às demais organizações públicas auditadas;

454.10. autorizar a Secretaria de Fiscalização de Tecnologia da Informação a dar ampla divulgação às informações e aos produtos derivados da execução desta auditoria, excetuando as informações pessoais dos gestores respondentes, a fim de contribuir para a melhoria das organizações públicas em relação à adequação à LGPD;

454.11. classificar como públicos os dados das respostas individuais das organizações ao questionário da auditoria, conforme o art. 3º, inciso I, da LAI, excetuando as informações pessoais dos gestores respondentes, que devem ser classificadas como sigilosas, em consonância com o art. 31, § 1º, inciso I, da LAI;

454.12. autorizar a Secretaria de Fiscalização de Tecnologia da Informação a compartilhar os dados das respostas individuais das organizações ao questionário da auditoria, excetuando as informações pessoais dos gestores respondentes, com a ANPD, a SGD/ME, o CNJ e o CNMP, observando as respectivas jurisdições, a fim de contribuir com a orientação das organizações em relação à adequação à LGPD;

454.13. classificar como público o presente processo, nos termos da Resolução-TCU 294/2018, arts. 4º e 8º, com exceção das peças 593, 594, 602, 603, 687, 688, 689, 695, 696, 698, 699, 701, 702, 703, 704, 705, 706, 707, 708, 709, 710, 711, 719, 720, 722, 723, 724, 726, 727, 728, 730, 734, 735, 737, 743, 745, 749, 750, 751, 754, 757, 758, 759, 760, 761, 764, 769, 771, 772, 774, 775, 776, 777, 784, 785, 786, 788, 789, 793, 794, 796, 797, 798, 799, 800, 801, 803, 806, 807, 808, 809, 813, 814, 815, 816, 817, 818, 819, 821, 822, 823, 826, 827, 830, 832, 838, 840, 845, 846, 848, 850, 851, 890, 891, 892, 893, 900, 919, 924, 926, 927, 929, 930, 931, 935, 936, 938, 939, 941, 945, 946, 947, 948, 949, 973, 985, 987, 988, 992, 996 e 1041 – que devem ser classificadas como sigilosas por conterem informações pessoais de gestores respondentes, em consonância com o art. 31, § 1º, inciso I, da LAI;

454.14. por falta de enquadramento legal, levantar o sigilo das seguintes peças referentes a ofícios de comunicação da auditoria: 7-46, 48-57, 59-113, 206-237, 239-283, 286-400, 551, 552, 568, 569, 570, 576-582, 611-683 e 716;

454.15. por falta de enquadramento legal, levantar o sigilo das seguintes peças referentes a respostas de comunicações por parte das organizações auditadas: 731, 756, 773, 899, 912, 913, 922, 925, 937, 946, 1013, 1040 e 1045.

454.16. arquivar o presente processo, com fulcro no art. 169, inciso V, do Regimento Interno do TCU."

2. Por sua vez, o Ministério Público junto ao TCU, à peça 1.057, manifesta-se de acordo com a instrução da unidade técnica e acrescenta sugestão de que "*as peças 1052 a 1055 sejam desentranhadas do presente feito, com base nos arts. 2º, X, e 17 da Resolução TCU 259/2014, e encaminhadas à Secretaria de Fiscalização de Infraestrutura de Energia Elétrica, unidade técnica destinatária da comunicação que informa ao TCU a incorporação da Amazonas Geração e Transmissão de Energia S/A pelas Centrais Elétricas do Norte do Brasil S/A (Eletronorte), consoante CE PR 0108/2021, de 17/8/2021*".

É o relatório.

VOTO

Trata-se de auditoria com o objetivo de avaliar as ações governamentais e os riscos à proteção de dados pessoais por meio da elaboração de diagnóstico acerca dos controles implementados pelas organizações públicas federais para adequação à Lei Geral de Proteção de Dados.

2. A análise abrangeu 382 organizações a respeito de aspectos relacionados à condução de iniciativas para providenciar a adequação à LGPD e às medidas implementadas para o cumprimento das exigências estabelecidas na Lei. Além disso, a avaliação da ANPD explorou itens relacionados à estrutura organizacional da entidade, à condução de suas atribuições e à regulamentação de aspectos citados na legislação.

3. O método utilizado para avaliar as mencionadas organizações foi o de autoavaliação de controles internos (do inglês *Control Self-Assessment – CSA*), por meio do qual foi disponibilizado questionário eletrônico para que os gestores preenchessem as respostas que melhor refletiam a situação das respectivas organizações com relação aos controles relacionados à LGPD.

4, A fiscalização foi estruturada a partir de três questões de auditoria:

Q1) As organizações se estruturaram para a condução de iniciativas de adequação à LGPD?

Q2) As organizações implementaram medidas e controles de proteção de dados pessoais para adequação à LGPD?

Q3) A ANPD e o CNPD (Conselho Nacional de Proteção de Dados) estão estruturados e em operação conforme estabelecido na LGPD?

5. As duas primeiras questões foram desdobradas em perguntas específicas contempladas em um questionário respondido, de forma *online*, pelas 382 organizações públicas federais analisadas, enquanto a última gerou outro grupo de perguntas que foram respondidas por meio de reuniões realizadas com membros da ANPD.

II – CONTEXTO

6. Preliminarmente à análise das conclusões da auditoria realizada pela Secretaria de Fiscalização de Tecnologia da Informação – Sefti, cabe uma breve avaliação do contexto da LGPD.

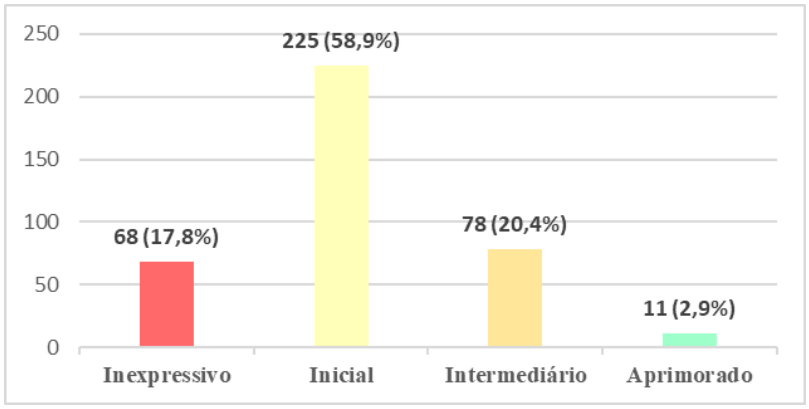
7. A Lei 13.709/2018, inspirada no Regulamento Geral de Proteção de Dados (do inglês *General Data Protection Regulation* – GDPR) da União Europeia (EU), define diretrizes sobre o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica, com o intuito de proteger os direitos fundamentais de liberdade e de privacidade, assim como o livre desenvolvimento da personalidade da pessoa natural.

8. A LGPD foi sancionada em 14 de agosto de 2018 e, inicialmente, entraria em vigência dezoito meses após sua publicação, porém a Medida Provisória (MP) 869/2018 prorrogou esse prazo por mais seis meses. Contudo, devido à pandemia da Covid-19, foi publicada nova MP (959/2020) que prorrogaria novamente o prazo citado e que levaria a entrada em vigor da legislação para maio de 2021. No entanto, após discussão no Senado, o prazo total de 24 meses foi mantido e a Lei passou a vigorar em setembro de 2020, após sanção presidencial.

9. Esses diversos aspectos afetos a um cenário de incertezas quanto ao início de vigência da legislação e à criação da Autoridade Nacional de Proteção de Dados (ANPD) – órgão responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional – contribuíram para que as organizações públicas não estivessem devidamente estruturadas no início da vigência da Lei.

10. Nesse contexto, a fiscalização constatou que a maioria das organizações públicas federais, 76,7%, está no grau inexpressivo ou inicial do processo de adequação à LGPD, conforme a figura a seguir:

Grau de adequação das organizações auditadas à LGPD

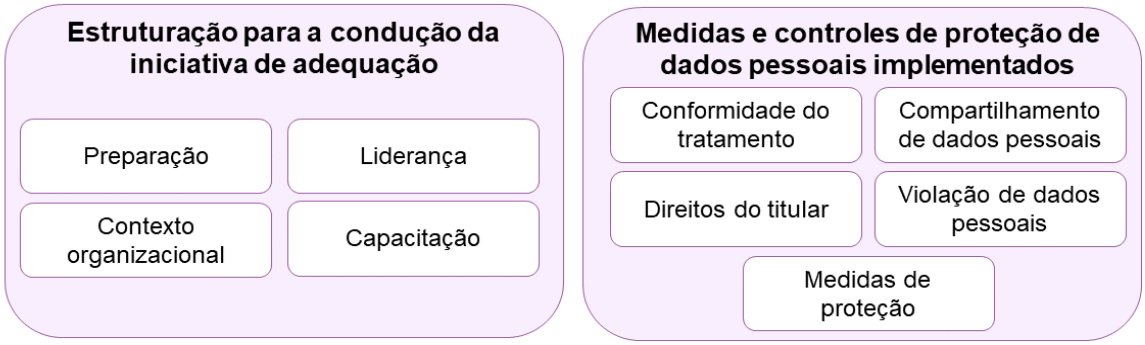


11. A relevância do tema é notória, conforme detalha o relatório precedente. Mesmo após a aprovação da LGPD, o Brasil tem sido vítima de graves ataques que resultaram no vazamento de dados pessoais. Pode-se destacar a divulgação pela imprensa do vazamento de dados de mais de 200 milhões de brasileiros ocasionado por falha de segurança em sistema do Ministério da Saúde e o denominado "megavazamento" que expôs dados de 223 milhões de brasileiros, além de informações de veículos e de CNPJs.

III – DIMENSÕES DA ANÁLISE

12. O questionário de autoavaliação de controles foi disponibilizado em formato eletrônico para que as organizações preenchessem as respostas que melhor refletiam sua situação com relação aos controles relacionados à LGPD. Além de permitir que as organizações verificassem quais controles associados à essa lei geral foram implementados, as questões também puderam ser utilizadas como referência para a condução de futuras iniciativas de adequação.

13. No aludido questionário foram inseridas 60 questões organizadas em nove dimensões: preparação, contexto organizacional, liderança, capacitação, conformidade do tratamento, direitos do titular, compartilhamento de dados pessoais, violação de dados pessoais e medidas de proteção. Essas questões foram agrupadas a partir de duas perspectivas: *(i)* estruturação para a condução da iniciativa de adequação e *(ii)* medidas e controles de proteção de dados pessoais implementados, conforme ilustra a figura a seguir:



14. Quanto à primeira dimensão – Preparação - o levantamento demonstra que apenas 45% das organizações concluíram iniciativa de identificação e planejamento das medidas necessárias à adequação. Acrescente-se que 49% delas ainda não elaboraram plano de ação para atendimento integral à LGPD.

15. No tocante à segunda dimensão - Contexto organizacional – as respostas demonstram que a maioria das organizações, 76%, conduziu iniciativa para identificar esses normativos. Por outro lado, 77% ainda não identificaram todas as categorias de titulares de dados pessoais com os quais mantém relacionamento.

16. Ainda nessa dimensão foi avaliado se as organizações conduziram iniciativa para verificar se há operadores que realizam tratamento de dados pessoais em seus nomes e identificar esses

operadores, se for o caso. Ao consolidar as respostas fornecidas pelas organizações, constatou-se que mais da metade, 51%, não conduziu ações para identificar os operadores. Vale destacar que essa identificação é um ponto chave para a efetividade da proteção dos dados pessoais, uma vez que são responsáveis por realizarem tratamento de dados em nome das organizações.

17. A propósito, para avaliar a efetividade do processo de identificação de operadores, caso a organização informasse que a iniciativa foi concluída e que levou à identificação de todos esses atores, era exibida a subquestão para avaliar se os contratos firmados com os operadores identificados foram adequados de forma a estabelecer, claramente, os seus papéis e responsabilidades com relação à proteção de dados pessoais. As respostas a essa questão demonstram que apenas 15% das organizações adequaram todos os contratos firmados com os operadores identificados.

18. O resultado da pergunta afeta a "Processos que realizam tratamento de dados pessoais" também se mostrou preocupante, uma vez que apenas 17% das organizações identificaram todos os processos de negócio que realizam tratamento de dados pessoais. Segundo a Sefti, "*essa é uma das tarefas elementares em um projeto de adequação, pois é a partir dessa identificação que é possível avaliar os riscos inerentes a cada processo e identificar informações relevantes como: o propósito do tratamento, a base legal que justifica esse tratamento e as categorias de titulares de dados envolvidas*". Nessa mesma linha, a minoria das organizações, 14%, identificou todos os dados pessoais que tratam.

19. Em relação à terceira dimensão – Liderança – as questões relacionaram-se à nomeação do encarregado e à existência de políticas que buscam assegurar a segurança das informações e a proteção dos dados pessoais.

20. As respostas ao questionário demonstram que 24% das organizações não possuem Política de Segurança da Informação ou instrumento similar. Na mesma linha, apenas 35% das organizações possuem Política de Classificação da Informação e 18% das organizações mantem Política de Proteção de Dados Pessoais ou documento similar.

21. Quanto à nomeação de encarregado pelo tratamento de dados pessoais, pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares de dados pessoais e a ANPD (art. 5º, inciso VIII, da LGPD), as respostas demonstram que a maioria das organizações, 69%, cumpriu a orientação legal.

22. Em relação à "Capacitação", as respostas demonstram que a minoria das organizações, 29%, possui Plano de Capacitação que abrange a proteção de dados pessoais, o que representa um risco organizacional, uma vez que a LGPD é uma legislação técnica e de difícil compreensão, que exige estudo para que as organizações adquiram maturidade no tema. Além disso, a pesquisa demonstrou que quase metade das organizações que elaboraram o plano, 46%, não considerou a necessidade de que pessoas que exercem funções com responsabilidades essenciais relacionadas à proteção de dados pessoais deveriam receber treinamento diferenciado.

23. No que tange à conformidade do tratamento, a organização deve estar apta a demonstrar que o gerenciamento de dados pessoais que realiza está de acordo com a legislação. Os dados da pesquisa ilustram que somente 11% das organizações identificaram e documentaram todas as finalidades das atividades de tratamento de dados pessoais.

24. Quanto às bases legais, definidas no art. 7º, que relaciona dez hipóteses nas quais tratamento de dados pessoais poderá ser realizado, 46% afirmaram que nenhuma base legal que fundamenta as atividades de tratamento de dados pessoais foi identificada e documentada.

25. A questão afeta às operações de tratamento de dados pessoais demonstrou que 82% das organizações não possuem um registro instituído para consolidar informações relacionadas às características das atividades de tratamento de dados pessoais. Nesse particular, vale esclarecer a existência do Guia de Elaboração de Inventário de Dados Pessoais da Secretaria de Governo Digital (SGD) do Ministério da Economia (ME), que abrange diretrizes para a elaboração de inventário de dados pessoais.

26. Ainda nessa dimensão, somente 2% das organizações elaboram Relatório de impacto à proteção de dados pessoais (RIPD) que abrange todos os processos de tratamento de dados pessoais que podem gerar riscos aos titulares.

27. Por sua vez, no quesito "direitos do titular", no sentido de que a organização deve assegurar que os titulares tenham acesso às informações relacionadas ao tratamento de seus dados pessoais, foram abordadas questões relacionadas à elaboração da política de privacidade e ao atendimento dos direitos dos titulares.

28. O art. 6º da LGPD relaciona, além da boa-fé, dez princípios que as atividades de tratamento de dados pessoais devem observar, dos quais destacam-se o livre acesso, que representa a garantia aos titulares de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais (inciso IV); e a transparência, que representa a garantia aos titulares de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento (inciso VI).

29. Nesse particular, foi constatado que 75% das organizações ainda não elaboraram documentação relativa à política de privacidade, o que demonstra que não é dada a devida transparência ao titular de como os seus dados pessoais são tratados. Para os casos em que a organização informasse que possuía Política de Privacidade ou documento similar, era exibida a subquestão para verificar se o artefato estava publicado na internet. As respostas demostraram que maioria das organizações não comunica, de maneira clara e concisa, informações relativas ao tratamento de dados pessoais.

30. Quanto aos mecanismos para atender os direitos dos titulares, uma vez que a organização deve implementá-los para atender aos nove direitos estabelecidos no art. 18 da LGPD, as respostas mostraram que somente 14% das organizações cumpriram a orientação para atender todos esses direitos elencados no art. 18 da LGPD.

31. No tocante à dimensão "Compartilhamento de dados pessoais", que demanda a adoção de controles adequados para mitigar riscos que possam comprometer a consistência e a proteção dos dados pessoais, foi constatado que apenas 14% das organizações identificaram todos os dados pessoais compartilhados com terceiros. Sem a identificação desses dados, não é possível assegurar a conformidade com a LGPD, uma vez que tais dados podem ser hospedados por entidades que não adotam os devidos cuidados.

32. Ainda quanto a essa dimensão, caso a organização afirmasse que identificou, na totalidade ou em parte, os dados pessoais que são compartilhados com terceiros, eram exibidas algumas subquestões: a primeira para avaliar se os compartilhamentos identificados estão em conformidade com os critérios estabelecidos na LGPD; a segunda para verificar se as organizações registram eventos relacionados à transferência dos dados pessoais que são compartilhados; e a terceira para averiguar se os compartilhamentos identificados envolvem transferência internacional de dados pessoais.

33. As respostas a essas questões demonstram que apenas 34% das organizações afirmaram que todos os compartilhamentos estão em conformidade com os critérios estabelecidos na LGPD. E que 28% das organizações registram eventos relacionados à transferência de todos os dados pessoais que são compartilhados

34. O contexto apresentado ilustra a necessidade de as organizações adotarem controles para mitigar riscos relacionados ao compartilhamento de dados pessoais, principalmente, segundo a unidade técnica, "*pelo fato de não serem eximidas de responsabilidade em casos de violações decorrentes de incidentes no ambiente dos terceiros com os quais compartilha os referidos dados*".

35. Quanto à dimensão "Violação de dados pessoais", o trabalho abordou questões relacionadas à identificação, ao registro e ao tratamento de incidentes de violação de dados pessoais.

36. Com efeito, a LGPD, no art. 50, § 2º, inciso I, alínea "g", recomenda que os controladores implementem um programa de governança em privacidade que, dentre outros aspectos, contemple planos de resposta a incidentes. Contudo, a pesquisa identificou que 84% das organizações não possuem plano de reposta a incidentes que abrange o tratamento de incidentes de violação de dados pessoais.

37. Além disso, as respostas mostraram que 72% das organizações não possuem sistema para registro de incidentes que envolvem violação de dados pessoais e que 75% não possuem sistema para registro das ações adotadas para solucionar tais incidentes. A propósito, conforme registro da unidade técnica, "*sem um sistema de informação que auxilie na gestão de incidentes de segurança da informação que envolvem violação de dados pessoais, a organização tende a não conseguir executar o processo de tratamento e resposta a incidentes com eficiência, tampouco manter e utilizar um histórico de incidentes como aprendizado para reduzir o risco de ocorrências futuras*".

38. No tocante à última dimensão - Medidas de proteção – avaliou-se os controles que a organização deve adotar para proteger os dados pessoais.

39. De acordo com o art. 46 da LGPD, os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado. No entanto, constatou-se que a maioria das organizações, 54%, não é capaz de comprovar que adotou medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais.

40. O resultado apresentado é sensível devido ao alto risco de ocorrência de incidentes de violação de dados pessoais em função da ausência de medidas de proteção dos dados pessoais. Além disso, cumpre destacar que, no juízo de gravidade de incidente de segurança que possa causar risco ou dano relevante aos titulares, a ANPD deverá avaliar a comprovação de que foram adotadas medidas técnicas adequadas, nos termos de art. 48, § 3º, da LGPD.

41. A questão relativa à "Controle de acesso em sistemas" identificou que apenas 16% das organizações implementaram tal processo em todos os sistemas que realizam tratamento de dados pessoais, o que representa alto risco de acesso indevido a dados pessoais e, consequentemente, pode violar a privacidade dos cidadãos.

42. Para a questão que buscou verificar se as organizações registram eventos das atividades de tratamento de dados pessoais, as respostas revelam que somente 7% das organizações registram eventos de todas as atividades de tratamento de dados pessoais, fato preocupante uma vez que a ausência de registros de eventos inviabiliza a rastreabilidade de ocorrências relacionadas à violação de dados pessoais.

43. Nessa linha, ainda, a pesquisa detectou que 43% das organizações não utilizam criptografia para proteger os dados pessoais. De acordo com a Sefti, "a*pesar de a utilização de criptografia não ser obrigatória, a utilização da medida é útil para proteger dados em trânsito e nos locais de armazenamento, mitigando riscos associados à violação de dados pessoais*".

IV - INDICADOR DE ADEQUAÇÃO À LGPD

45. Com o objetivo de consolidar os dados obtidos na pesquisa e viabilizar a comparação das organizações auditadas em relação ao nível de adequação à LGPD, a Sefti selecionou 42 questões para a composição de indicador elaborado com o intuito de resumir as respostas fornecidas por cada organização, conforme detalhado no relatório precedente.

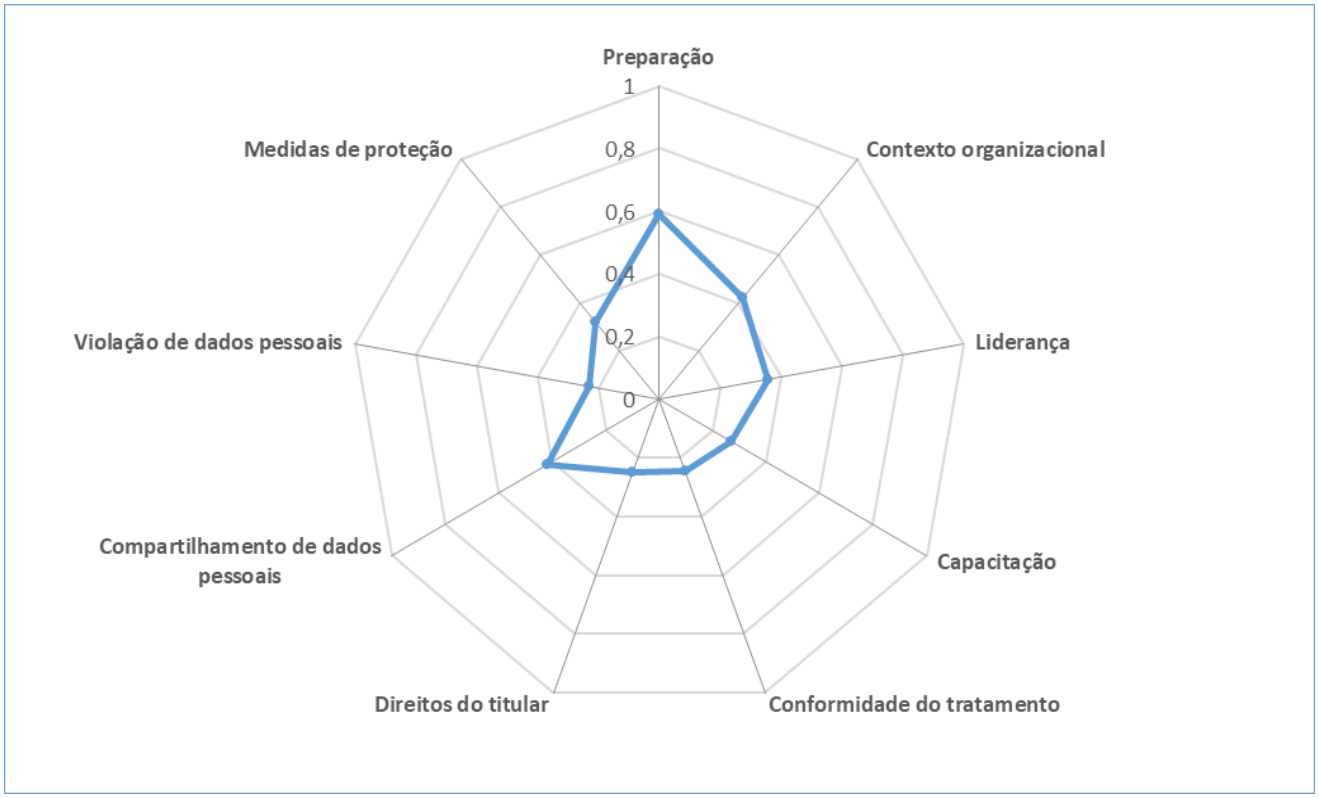
46. A partir do cálculo desse indicador, foram definidos quatro níveis de adequação à LGPD: "Inexpressivo" (indicador menor ou igual a 0,15), "Inicial (indicador maior do que 0,15 e menor ou igual a 0,5), "Intermediário" (indicador maior do que 0,5 e menor ou igual a 0,8) e "Aprimorado" (indicador maior do que 0,8). Assim, conforme o valor do indicador obtido, as organizações foram enquadradas em um desses níveis.

47. De acordo com a figura apresentada no parágrafo 10 deste voto, a consolidação da distribuição das 382 organizações em cada nível indica que 76,7% delas está no grau inexpressivo ou inicial do processo de adequação à LGPD.

48. O indicador também pode ser apresentado levando em consideração a nota referente a cada uma das dimensões do questionário: "Preparação", "Contexto Organizacional", "Liderança",

"Capacitação", "Conformidade do Tratamento", "Direitos do Titular", "Compartilhamento de Dados Pessoais", "Violação de Dados Pessoais" e "Medidas de Proteção".

49. O valor do indicador de cada dimensão foi obtido pela soma das notas atribuídas a cada uma das questões das referidas dimensões dividida pela quantidade de questões selecionadas da dimensão. Assim, para cada organização, o valor do indicador de cada dimensão também pode variar de 0 (nota 0 em todas as questões) a 1 (nota 1 em todas as questões). O resultado obtido está ilustrado na figura a seguir:

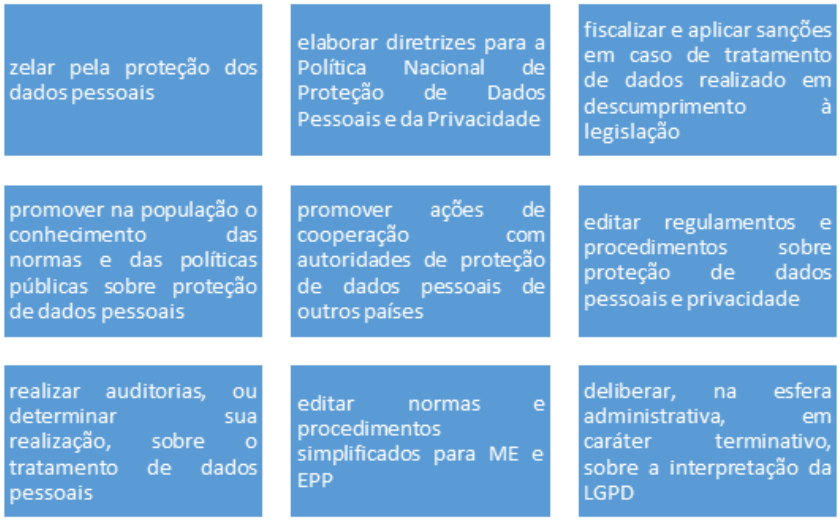


50. A partir da visão fornecida por este diagnóstico, percebe-se que a maior parte das organizações ainda está iniciando o processo de adequação à LGPD, razão pela qual entendo oportuno recomendar à SGD/ME, ao CNJ e ao CNMP que editem normativos e guias para a atuação administrativa das organizações sob suas jurisdições.

51. Considerando a relevância da matéria, entendo por bem que as orientações presentes no acórdão a ser proferido sejam monitoradas pela Secretaria de Fiscalização de Tecnologia da Informação (Sefti). Além disso, oportuno que seja determinado que a unidade técnica responsável por este trabalho considere na Estratégia de Fiscalização do TCU em segurança da informação e proteção de dados 2022-2025 a execução de auditorias que avaliem incidentes críticos envolvendo vazamento de dados ocorridos na Administração Pública Federal.

V - ESTRUTURAÇÃO DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

52. A ANPD é órgão integrante da Presidência da República, responsável por zelar pela proteção de dados pessoais, por induzir a implementação e por fiscalizar o cumprimento da Lei Geral de Proteção de Dados. Tem múltiplas competências conforme ilustra a figura a seguir elaborado pela equipe de fiscalização a partir da Lei 13.709/2018:



53. A ANPD está autorizada a realizar requisição de pessoal, civil ou militar, com caráter obrigatório, ou seja, uma vez feita, os atos são considerados irrecusáveis. Na data de elaboração do relatório de auditoria, o órgão contava com 29 servidores e com mais treze em processo de requisição em andamento.

54. Percebe-se, diante da dimensão de suas atribuições, que a estrutura física da Autoridade é precária em função do seu momento inicial de funcionamento, ocupando sede provisória e tendo os serviços de logística e suprimento de materiais realizados pela Presidência da República.

55. Nesse contexto, também cabe destacar o papel do Conselho Nacional de Proteção de Dados e da Privacidade (CNPD), órgão consultivo composto por 23 membros, contendo representantes do governo, instituições da sociedade civil, academia e setor produtivo, cujas atribuições são:

(*i*) propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD;

(*ii*) elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade;

(*iii*) sugerir ações a serem realizadas pela ANPD;

(*iv*) elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; e

(*v*) disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população.

56. O Conselho Nacional de Proteção de Dados e da Privacidade (CNPD) é órgão integrante da estrutura da ANPD, conforme art. 55-C da LGPD. Apenas em 10/8/2021 foram publicados os decretos que designaram os membros para compor esse Conselho.

57. Em relação a Estruturação da Autoridade Nacional de Proteção de Dados, a equipe identificou em seu relatório três questões a serem tratadas:

(*i*) Falta de transparência e de participação de interessados no processo de construção da Agenda Regulatória para o biênio 2021-2022;

(*ii*) Temas relevantes elencados pela LGPD sem previsão de regulamentação; e

(*iii*) Natureza jurídica da ANPD que não confere a independência necessária para uma autoridade de proteção de dados

58. A ANPD publicou, em janeiro de 2021, a Agenda Regulatória para o biênio 2021-2022, por meio da Portaria-ANPD 11/2021, com previsão de dez temas para regulamentação por parte do órgão, escalonados em três fases. Essa agenda representa mecanismo típico das agências reguladoras, previsto no art. 21 da Lei 13.848/2019.

59. A Sefti aponta que "*apesar de elencar os temas objeto de regulamentação futura e de ter sido aprovada por seu Conselho-Diretor, a Agenda Regulatória da ANPD não contou com processo de construção transparente e colaborativo, sendo a escolha e a priorização dos temas objeto de exclusiva deliberação dos seus diretores, conforme relatado em reunião com a equipe de auditoria*". A adoção de mecanismos de participação de interessados nos processos de tomada de decisão da ANPD é uma obrigação expressa da lei, conforme determina o art. 55, inciso XIV da LGPD.

60. A participação social no processo decisório é reforçada pelo Decreto 9.203/2017, que estabelece que cabe à alta administração implementar e manter mecanismos, instâncias e práticas de governança em consonância com os princípios e diretrizes elencados, a exemplo da melhoria regulatória, transparência e prestação de contas. Cabe esclarecer que, após o envio do relatório preliminar para comentário dos gestores, a ANPD editou a Portaria 16, de 8 de julho de 2021, visando sanar os problemas apontados, razão pela qual se faz desnecessária recomendação nesse sentido.

61. Outro ponto identificado foi a limitação de recursos humanos e a ausência de processo estruturado de planejamento regulatório, incluindo etapa para a gestão do estoque, para as competências atribuídas à ANPD, o que pode gerar: Inefetividade da Lei Geral de Proteção de Dados; Insegurança jurídica para atuação dos agentes de tratamento; Adoção de medidas insuficientes para proteção dos dados dos titulares; Perda de confiança na capacidade de resposta da ANPD frente aos desafios; e Enfraquecimento institucional da ANPD.

62. Não obstante os desafios para a solução dessas questões, considerando as ações adotadas pela ANPD após o envio do relatório preliminar para comentários, a equipe de auditoria propôs deixar de recomendar à Autoridade Nacional de Proteção de Dados que institua processo organizacional para estruturação do seu planejamento regulatório, em linha com os princípios e diretrizes de governança pública previstos no Decreto 9.203/2017.

63. Por fim, foi apontado que a Natureza jurídica da ANPD não confere a independência necessária para uma autoridade de proteção de dados. Entendo ser esta uma das principais questões a serem tratadas nos presentes autos.

64. De acordo com o relatório precedente, "*em reunião com a equipe de auditoria, os diretores da ANPD ressaltaram a necessidade de se alterar a natureza jurídica do órgão, visando ter condições de cumprir efetivamente sua missão. Mencionaram fortes restrições de pessoal e a ausência de autonomia financeira, o que impediria a elaboração de orçamentos próprios que contemplassem as demandas indispensáveis para sua estruturação. Não há sistemas informatizados próprios para auxiliar no fluxo dos processos de trabalho e até mesmo os computadores utilizados pelos diretores são pessoais e não institucionais, o que provoca diversos riscos de segurança da informação e expõe o órgão a violações de dados pessoais, causando, além dos impactos materiais, danos irreparáveis à reputação do órgão*".

65. Ainda segundo a equipe, "*mesmo tendo autonomia técnica e decisória prevista na legislação, a subordinação à Presidência da República e a consequente submissão ao poder hierárquico, com ausência de autonomia administrativa e financeira, não conferem à ANPD o grau de independência desejado para uma autoridade de proteção de dados, estando em desacordo com normas e boas práticas internacionais*".

66. Essa questão é de absoluta relevância nacional. A matéria tratada pela ANPD, em época na qual as informações das pessoas físicas e jurídicas são armazenadas em diversos sistemas informatizados, é de extrema sensibilidade. O mau uso dessas informações poderá causar grandes problemas na esfera política, social e econômica.

67. Nessa linha, por exemplo, de acordo com o artigo 52 do Regulamento Geral de Proteção de Dados da União Europeia, toda autoridade de proteção de dados deve ter assegurada:

> (*i*) total independência no exercício de suas competências, devendo seus membros estarem livres de qualquer influência externa, seja direta ou indireta, sendo vedado procurar ou receber instruções de quem quer que seja;

(*ii*) o provimento de recursos humanos, técnicos e financeiros, além de infraestrutura necessária para o efetivo exercício de suas atribuições;

(*iii*) a escolha de seu quadro de pessoal, que deve ser próprio da autoridade; e

(*iv*) orçamentos anuais separados, com sujeição a controles financeiros que não afetem sua independência.

68. Além do mencionado regulamento, existem diversas diretivas internacionais no mesmo sentido que foram destacadas pela unidade técnica, a exemplo da Convenção 108 do Conselho da Europa para a Proteção das Pessoas com relação ao Tratamento Automatizado de Dados Pessoais e a Lei de Privacidade do Consumidor da Califórnia (*California Consumer Privacy Act - CCPA*).

69. De maneira a ilustrar a necessidade de fortalecimento da estrutura organizacional, o órgão traçou um panorama comparativo entre autoridades de proteção de dados ao redor do mundo, levando em consideração a quantidade de funcionários, o tamanho da população e o Produto Interno Bruto (em dólares americanos) de cada país, conforme tabela a seguir:

País	Funcionários	População	PIB
Brasil	31	212.994.000	$ 1.840.000.000.000,00
México	272	126.200.000	$ 1.221.000.000.000,00
Alemanha	253	83.020.000	$ 3.948.000.000.000,00
França	199	66.990.000	$ 2.778.000.000.000,00
Reino Unido	768	66.650.000	$ 2.855.000.000.000,00
Itália	162	60.360.000	$ 2.084.000.000.000,00
Espanha	152	46.940.000	$ 1.419.000.000.000,00
Polônia	154	37.970.000	$ 585.700.000.000,00
Marrocos	24	35.130.000	$ 117.900.000.000,00
Austrália	120	24.990.000	$ 1.434.000.000.000,00
Romênia	50	19.410.000	$ 239.600.000.000,00
Países Baixos	191	17.280.000	$ 913.700.000.000,00
Bélgica	62	11.460.000	$ 542.800.000.000,00
Rep. Checa	115	10.690.000	$ 245.200.000.000,00
Portugal	27	10.280.000	$ 240.700.000.000,00
Suécia	89	10.230.000	$ 556.100.000.000,00
Áustria	36	8.859.000	$ 455.300.000.000,00
Hong Kong	74	7.451.000	$ 362.700.000.000,00
Bulgária	69	7.000.000	$ 65.130.000.000,00
Sérvia	71	6.982.000	$ 50.600.000.000,00
Finlândia	46	5.518.000	$ 276.700.000.000,00
Eslováquia	46	5.458.000	$ 105.900.000.000,00
Noruega	52	5.368.000	$ 434.200.000.000,00
Irlanda	140	4.904.000	$ 382.500.000.000,00
Geórgia	116	3.731.000	$ 17.600.000.000,00
Albânia	37	2.846.000	$ 15.100.000.000,00
Eslovênia	43	2.081.000	$ 54.010.000.000,00
Macedônia	50	2.077.000	$ 12.670.000.000,00
Letônia	26	1.920.000	$ 34.410.000.000,00
Ilhas Maurícic	20	1.265.000	$ 14.220.000.000,00
Luxemburgo	33	613.894	$ 70.890.000.000,00
Argentina	48	45.808.747	$ 449.700.000.000,00
Uruguai	76	3.500.000	$ 56.000.000.000,00
Correlação		**61%**	**70%**

Fonte: Minuta da Nota Técnica 3/SG/ANPD – Projeto Fortalecimento Institucional da ANPD.

Obs.: Valor do PIB em dólar americano no ano de 2019.

70. Com base na tabela, a estrutura do Brasil é a menor dentre todos os países pesquisados. Ademais, dos dez países de maior PIB, o Brasil é aquele que possui a menor autoridade de proteção de dados em quantidade de funcionários. Portanto, os dados revelam que o tamanho da ANPD apresenta discrepância significativa quando comparado com outros países.

71. Desse modo, entendo apropriada recomendação à Casa Civil da Presidência da República para que avalie no trato do tema a transformação da ANPD em agência reguladora ou autarquia em regime especial, visando dar a ela maior autonomia administrativa e financeira, nos moldes previstos

originalmente no Projeto de Lei 53/2018, acompanhada de uma reestruturação organizacional e da criação de cargos para expandir as unidades finalísticas e fortalecer as unidades administrativas.

71.1. A propósito, registro que na data de 13/6/2022 foi editada a Medida Provisória nº 1.124 que alterou a Lei nº 13.709/2018 e transformou a Autoridade Nacional de Proteção de Dados em autarquia de natureza especial, assim como alterou a Estrutura Regimental da ANPD.

71.2. Considerando tratar-se de Medida Provisória, ainda sujeita à validação do Congresso Nacional, entendo oportuno manter a retromencionada recomendação.

V – ENCAMINHAMENTO

72. Os resultados obtidos por esta fiscalização demostraram a relevância do acompanhamento das ações de adequação à LGPD que serão realizadas pelas organizações da APF, razão pela qual convém que sejam planejadas atuações de controle externo na matéria, de modo a viabilizar a continuidade do presente trabalho e a indução de avanços na implementação da LGPD pelas organizações auditadas, como parte de uma estratégia de atuação do TCU em proteção de dados e privacidade ou, até mesmo, em governança de dados.

73. No âmbito dessas ações, a unidade técnica sugere futuras fiscalizações relevantes deste Tribunal, a exemplo de:

(*i*) execução de auditorias de conformidade em amostra das organizações que responderam ao questionário, considerando critérios de relevância e risco, incluindo o nível de adequação à LGPD computado com base nas respostas autodeclaradas pelas organizações;

(*ii*) acompanhamento contínuo da evolução das organizações públicas federais em relação ao nível de adequação à LGPD, realizado por meio da disponibilização permanente de um questionário *online,* similar ao utilizado nesta fiscalização, o qual poderia ser respondido voluntariamente a qualquer momento para obtenção de diagnóstico a respeito da evolução da organização respondente quanto à adequação à LGPD; e

(*iii*) construção de um painel de informações a ser alimentado, inicialmente, com os dados referentes às respostas ao questionário coletadas por meio desta fiscalização e, posteriormente, com as respostas do questionário *online*, de modo a demonstrar de forma atualizada a evolução da adequação à LGPD das organizações públicas federais.

74. Por fim, registro que recebi e incorporei valiosa contribuição apresentada pelo Ministro Aroldo Cedraz para o aprimoramento do acórdão que ora se apresenta à consideração do Plenário.

74.1. Sua Excelência sugere o desdobramento do item que se refere à implementação de procedimentos e controles para o compartilhamento de dados pessoais com terceiros (organizações públicas, privadas e transferência internacional), "*de modo a proporcionar maior clareza sobre o tratamento diferenciado que deve ser dispensado ao uso de dados pessoais de forma compartilhada no âmbito dos órgãos integrantes do 'corpo único' da Administração Direta Federal, em relação ao compartilhamento de tais informações com os demais órgãos públicos e organizações privadas, inclusive de âmbito internacional*".

74.2. Acrescenta, ainda, especial preocupação em relação ao "*fato de que o compartilhamento e a integração de dados no âmbito da Administração Pública dependem da atuação de centenas de gestores individuais, todos sujeitos ao mesmo comportamento de aversão ao risco, com consequências danosas para a eficiência da gestão do Estado e para a prestação de serviços ao cidadão*", em especial quanto "*às responsabilidades dos agentes de tratamento de dados pessoais, objeto do Capítulo VI da Lei Geral de Proteção de Dados – o controlador e o operador – e à forma como tais encargos estão sendo exercidos no âmbito do Poder Executivo Federal*".

74.3. Em sua declaração, Sua Excelência destaca que o tema foi objeto de atenção da Autoridade Nacional de Proteção de Dados (ANPD), por meio do Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Contudo, ressalva que "*essa não seja a melhor interpretação do que dispõe o art. 4º do Decreto-Lei 200/1967, que atribui personalidade jurídica*

indivisível à Administração Direta, ainda que esta seja constituída por órgãos e serviços integrados na estrutura administrativa da Presidência da República e de seus Ministérios".

74.4. Com efeito, o Decreto 7.579/2011, que dispõe sobre o Sistema de Administração dos Recursos de Tecnologia da Informação – SISP, atribuiu à Secretaria de Governo Digital do Ministério da Economia o papel de Órgão Central do SISP, cujas competências abrangem "*definir, elaborar, divulgar e implementar as políticas, as diretrizes e as normas gerais relativas à gestão dos recursos do SISP" (art. 4º, inciso II), cabendo aos Órgãos Setoriais dos Ministérios e da Presidência da República a responsabilidade por 'cumprir e fazer cumprir as políticas, diretrizes e normas gerais emanadas do Órgão Central'"* (art. 6º, inciso III).

74.5. Nesse contexto, não seria razoável sugerir que no caso do uso compartilhado de dados pessoais pelo poder público, hipótese prevista explicitamente pela LGPD, fosse "*adotado comportamento diverso, com a responsabilidade normativa distribuída por inúmeros órgãos integrantes de um mesmo sistema. Dada a possibilidade de que cada Ministério ou Secretaria adote regras próprias, distintas e potencialmente incompatíveis entre si, restaria impossibilitado o alcance dos objetivos de máximo rendimento e redução de custos operacionais, previsto no § 3º do art. 30 do Decreto-Lei 200/1967*".

74.6. Desse modo, como estrutura administrativa única e integrada, a Administração Direta admite a existência de um único controlador, a quem competem, nos termos do art. 5º, inciso VI da LGPD, as decisões referentes ao tratamento de dados pessoais, cabendo tal responsabilidade ao Órgão Central do SISP, em consonância com o Decreto 7579/2011.

74.7. Diante desse cenário complexo, acolho sugestão de recomendação adicional direcionada à ANPD para que:

> 9.4.2. aperfeiçoe os normativos e guias expedidos pela instituição, em especial o Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, considerando que os órgãos e serviços da Administração Direta constituem estrutura administrativa única e integrada na qual a gestão de recursos de tecnologia da informação encontra-se organizada em sistema próprio, em cujo âmbito o tratamento de dados pessoais comporta a atuação de um único controlador e múltiplos operadores, que devem agir de forma coordenada para imprimir o máximo rendimento e reduzir os custos operacionais da Administração, em consonância com o disposto no art. 30 do Decreto-Lei 200/1967; art. 26 da Lei 13.709/2018; e art. 1º do Decreto 7.579/2011.

75. Feitas essas considerações, registro minha concordância com o parecer da Sefti, com as sugestões acrescidas pelo Ministro Aroldo Cedraz e pelo MPTCU, cujos argumentos e propostas de encaminhamento incorporo às minhas razões de decidir, e VOTO para que este Tribunal adote a minuta de Acórdão que trago à apreciação deste Colegiado.

TCU, Sala das Sessões Ministro Luciano Brandão Alves de Souza, em tagDataSessao.

Ministro JOÃO AUGUSTO RIBEIRO NARDES
Relator

DECLARAÇÃO DE VOTO

Trata-se de auditoria com o objetivo de avaliar as ações governamentais e os riscos à proteção de dados pessoais por meio de diagnóstico acerca dos controles implementados pelas organizações públicas federais para adequação à Lei 13.709/2008, conhecida comoLei Geral de Proteção de Dados ou LGPD.

2. Agradeço desde já ao Ministro Augusto Nardes pela gentileza de ter retirado o presente processo de pauta para que eu tivesse a oportunidade de me debruçar sobre o assunto de forma amiúde e, assim, pudesse oferecer minhas contribuições para as já robustas análises e conclusões trazidas por Sua Excelência no relatório e no voto que havia trazido ao conhecimento do colegiado.

3. Nesse sentido, registro meus elogios à Secretaria de Fiscalização de TI, bem como ao eminente Relator e sua equipe, pelo competente trabalho que resultou em propostas que contaram com a acolhida dos gestores, reforçando o papel do TCUcomo indutor do aprimoramento da gestão de TI na Administração Pública Federal, com foco, neste momento, na proteção de dados pessoais dos cidadãos custodiados pelo Estado.

4. Esclareço, desde já, que não tenho ressalvas às conclusões presentes nos autos, muito bem fundamentadas no relatório e voto precedentes, e acredito que a implementação das recomendações propostas é essencial para tornar mais seguro o ambiente público digital.

5. Ocorre que a atenção que costumo dispensar aos processos que envolvem o aperfeiçoamento do ecossistema digital sob a responsabilidade do Governo Federal me levaram a ponderar sobre as dificuldades que tenho observado quanto à aparente dicotomia entre a necessidade de integração de sistemas e plataformas que amparam a prestação de serviços públicose os necessários cuidados com a segurança da informação, em especial, com a proteção dos dados de que tratam os presentes autos.

6. Como sabemos, até quando a privacidade e a segurança da informação não estão em foco, o Estado avança em ritmo próprio, como vimos no Acórdão 1.103/2019-TCU-Plenário, de relatoria do Ministro Vital do Rego, que identificou os reflexos da lentidão das iniciativas de desburocratização com o uso da transformação digital.

7. Problemas similares foram assinalados quando da análise da Plataforma de Cidadania Digital, iniciativa do Ministério da Economia que visa oferecer aos órgãos e entidades da APF mecanismo unificado paradisponibilização de serviços públicos digitais, a qual foi objeto do Acórdão 3.145/2020-TCU-Plenário, de minha lavra.

8. Não é surpresa, portanto,a necessidade de que este Tribunal indique correções periódicas de rumos na jornada de evolução da burocracia pública rumo a um Brasil 100% Digital. Nesse contexto, a Sefti mantém-se atenta aos riscos de eventuais tropeçose propôs diversas recomendações aos órgãos pertinentes, desta feita sob o ângulo da privacidade de dados.

9. Como consequência, o eminente relator propõe que oConselho Nacional de Justiça e o Conselho Nacional do Ministério Públicosejam orientados, nos limites de sua atuação administrativa, a editarguias e normativos para auxiliar o processo de adequação das organizações sob suas respectivas jurisdições à LGPD,em relação a 26 (vinte e seis) temas diferentes.

10. De modo similar, a Secretaria de Governo Digital do Ministério da Economia é alvo de recomendações em relação a 13 (treze) aspectos, a exemplo daelaboração de Política de Privacidade; da elaboração de Política de Proteção de Dados Pessoais; e, em especial, daimplementação de

procedimentos e controles para o compartilhamento de dados pessoais com terceiros – organizações públicas e privadas, nacionais e internacionais.

11. Entendo que este último ponto demanda um maior aprofundamento das reflexões já constantes dos autos, uma vez que a correta identificação do cidadão-usuário e de seus atributos pessoais é passo essencial na cadeia de valor em uma miríade de serviços públicos digitais, os quais com frequência dependem da interação entre diferentes órgãos e entidades para serem prestados de forma eficiente.

12. Em outras palavras, a implementação plena de um governo 100% digital exige que tal compartilhamento de dados pessoais no âmbito do Estado, para melhoria da gestão das políticas públicas e do atendimento ao cidadão, seja não apenas esperado, como também cobrado pela sociedade e pelos órgãos de controle.

13. Nessa linha, o Decreto 10.332/2020, queinstituiu a Estratégia de Governo Digital,previuem seu art. 3ºa obrigatoriedade de inclusão de **ações de interoperabilidade** de sistemas nos planos de transformação digital dos órgãos e entidades. Já aLei 14.129/2021, queestabelece princípios, regras e instrumentos para o governo digital, tornou obrigatória em seu art. 39 a instituição de **mecanismo de interoperabilidade** com o propósito de aprimorar a gestão de políticas públicas e aumentar a confiabilidade dos cadastros.

14. Ora, interoperabilidade só existe quando há possibilidade de compartilhamento de dados e,eventualmente, de APIs e aplicações. Como regra, serviços são prestados de maneira mais simples e ágilquando a informação pessoal fornecida por um indivíduo a certo órgão pode ser usada por outro órgão do mesmo corpo. Refiro-me, no caso, à própria União.

15. O TCU tem se manifestado sobre o assunto, a exemplo dorecente Acórdão2.279/2021-TCU-Plenário, de minha relatoria, que tratou de acompanhamento nas plataformas de compartilhamentos de dados.

16. Naquela ocasião, foi verificado que, no momento de compartilhar os dados sob sua responsabilidade, gestores apresentam os conhecidos sintomas de aversão ao risco, que se manifestam sob a forma de dificuldades na interpretação de normas sobre a concessão de acesso a outros órgãos. Assim, **optam pela solução mais simples e segura de negar qualquer pedido**.

17. Nessa visão limitada, aquilo que não é compartilhado certamente não ofende qualquer estatuto de proteção de dados. É essencial lembrar, por outro lado, que essa postura fere de morte o princípio da eficiência, tão importante para a Administração Pública quanto a legalidade de suas ações.

18. Os percalços dessa dinâmica foram assim exemplificados na ocasião pela Sefti, **verbis**:

> *300.1 os órgãos consumidores demoram para realizar o pedido de autorização de acesso aos dados porque precisam especificar a finalidade desse acesso e estimar o volume de dados a serem acessados, que, nesse caso, nem sempre é uma informação fácil de se obter ou produzir;*
> *300.2 também é necessário coletar assinaturas de autoridades superiores no órgão, que precisam se responsabilizar sobre a proteção dos dados pessoais, o que atrasa significativamente o processo, por poder envolver o pronunciamento da autoridade máxima do órgão ou de várias autoridades, e haver divergências de interpretação entre essas autoridades – no caso da Receita, por exemplo, para acessar dados como CPF e CNPJ, exige-se a assinatura do dirigente máximo do órgão ou unidades inferiores;*
> *300.3 em alguns casos o órgão gestor dos dados só autoriza o acesso ao órgão consumidor se este também autorizar o acesso às suas informações, o que, na prática, mais impede do que estimula o compartilhamento de dados;*

300.4 muitas vezes existe falta de preparação tecnológica para compartilhar os dados ou dúvida jurídica sobre a possibilidade de disponibilização de uma informação, o que acaba afetando o compartilhamento de outras informações que são, em tese, de fácil disponibilização.

19. No Voto que amparou o referido acórdão, consignei que a insegurança dos gestores sobre o compartilhamento de dados teria sido aumentada após o advento da LGPD, acrescentando:

> *O quadro parece ter-se agravado especialmente depois do início da vigência da Lei Geral de Proteção de Dados Pessoais (LGPD) e da consequente possiblidade de responsabilização individual, o que acaba atrasando ou mesmo impedindo todo o processo.*
> *(...)*
>
> *Em suma, mesmo com o apoio da SGD para intermediar a concessão de acesso, um dos principais obstáculos continua sendo como promover e, sobretudo, conciliar o enquadramento dos dados sob os diversos enfoques previstos na legislação vigente, em especial quanto aos níveis de compartilhamento (Decreto 10.046/2019), à Lei de Acesso à Informação (Lei 12.527/2011) e à proteção de dados pessoais (Lei 13.709/2018).*
>
> *Há, portanto, um nó a ser desatado. Por um lado, conforme já exposto, o arcabouço normativo obriga o Estado a integrar seus dados a fim de prestar melhores serviços e oferecer políticas públicas eficientes e íntegras ao cidadão. Por outro, condiciona-se a permissão de acesso às definições de cada gestor de dados, pessoalmente responsabilizado pela tradução das múltiplas – e não raro contraditórias – exigências legais em requisitos que são impostos aos órgãos que necessitam das informações sob sua guarda.*
>
> *Quem mais sofre com isso, como sempre, é o cidadão. Enquanto grande parte dos órgãos continua a oferecer serviços que não se comunicam com os demais, mantendo cadastros redundantes e exigindo a apresentação de informações e certidões já disponíveis ao poder público, os* ***usuários se veem obrigados a fazer verdadeira peregrinação pelas "igrejinhas do Estado", não raro com as paradas de praxe nos indefectíveis cartórios a fim de colher mais um carimbo em algum papel que servirá para comprovar, pela enésima vez, dados pessoais daquele indivíduo.***
>
> *Não podemos nos conformar com tal situação. É preciso estabelecer, de uma vez por todas, o conceito de que o* ***relacionamento do cidadão no nível federal se dá com a União, e não com o ministério X, a autarquia Y ou a secretaria Z.*** *Assim, se o indivíduo já forneceu seus dados pessoais a qualquer desses órgãos para obter determinado serviço, não cabe ao receptor dessa informação impor restrições para que outros entes a acessem, uma vez que o detentor e guardião dos dados é o Estado. (grifos no original)*

20. Como afirmei no parágrafo acima, na visão do cidadão, seurelacionamento se dá com a União, e não com cada órgão em separado. É complicada a jornada de quem busca o estado com alguma necessidade particular e, não raro,acaba perdido em um emaranhado de guichês, físicos ou digitais, que são interdependentes, mas não se comunicam. Para o pobre indivíduo, nada disso faz sentido. E ele tem razão, talvez mais do que imagina.

21. Ocorre que, se considerarmos que a União,como regra, executa suas atribuições de forma **desconcentrada**, com o auxílio deorganizações da Administração Direta, torna-se ainda mais justificável a indignaçãodo cidadão.Ora, ministérios, secretarias e outros órgãos federais são fruto da distribuição **interna** de competências e atribuições, com vinculação hierárquica, no âmbito do Poder Executivo Federal.

22. Não é demais lembrar que tal condição foi estabelecida de forma explícita há 55 anos pelo Decreto-Lei 200/1967, cujo art. 4º diferencia claramente a "Administração Direta, que se constitui dos **serviços integrados na estrutura administrativa** da Presidência da República e dos Ministérios", das entidades da Administração Indireta, estas sim dotadas, cada uma, de personalidade jurídica própria.

23. Não por acaso, nos referimos a ministérios e secretarias como “órgãos”, termo que nos remete a ideia de partes integrantes de um só corpo. Tal analogia é tão precisa quanto antiga. Conforme nos ensina a Bíblia, o apóstolo Paulo, ao tratar de divisões indevidas nos primórdios da igreja cristã, assim orientou por carta os Coríntios:

> O corpo não é composto de um só membro, mas de muitos.Se o pé disser: "Porque não sou mão, não pertenço ao corpo", nem por isso deixa de fazer parte do corpo.E se o ouvido disser: "Porque não sou olho, não pertenço ao corpo", nem por isso deixa de fazer parte do corpo.Se todo o corpo fosse olho, onde estaria a audição? Se todo o corpo fosse ouvido, onde estaria o olfato?

24. Curiosamente, o relato bíblico se assemelha muito mais do que gostaríamos às situações observadas por este Tribunal, em relação ao comportamento do Estado brasileiro.Como demonstrado no relatório que embasou o Acórdão 2.279/2021, é comum que órgãos da Administração Diretase neguem a compartilharinformações essenciais ao funcionamento de outros órgãos do mesmo ente federativo. Há casos em que isso ocorre até entre secretarias e estruturas de um mesmo ministério!

25. Aos que se preocupam com o fato de que o administrador público só pode fazer aquilo que a Lei autoriza de forma explícita, não é demais ressaltar a existência de um conjunto amplo e amadurecido denormas que determinam o compartilhamento de dados e a interoperabilidade de sistemas, a exemplo das Leis 13.444/2017, 13.460/2017 e 13.726/2018, e dos Decretos 8.936/2016, 10.046/2019 e 10.332/2020. Isso sem falar na próprialGPD, em seus artigos 7º, inciso III; 11, inciso II, “b” e “g”; 23; 25 e 26.

26. O que, então, leva os órgãos a agirem em dissonância com as normas?A resposta, parece-me, está nos incentivos percebidos pelos responsáveis por tais ações.

27. Apesar da existência de arcabouço normativo direcionado àtransformação digital do Estado, sua implementação depende da atuação firme no combate à inércia da cultura burocrática vigente, apegada aos carimbos e aos dados custodiados sob sete chaves. Na linha de frente dessa batalha, os gestores públicos, com conhecida aversão ao risco, se veem intimidados pelas potenciais consequências negativas que poderiam advir dacessãode dados a terceiros, especialmente após o advento da LGPD.

28. Afinal, está claramente disposto no art. 42 da referida lei que o“controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo”.

29. Ou seja, recorrendo aos fundamentos da governança pública, temos umclássico conflito de agência em que os operadores de dados públicos estão envolvidos. Mesmo diante de diretrizes claras em prol do compartilhamento de dados, esses agentes, ao se verem diante dos riscos de responsabilização individual, tendem a optar pelo caminho que minimiza o risco, ou seja: negar ou elevar demasiadamente o esforço necessário para acesso a dados sob sua responsabilidade.

30. Na tentativa de contornar esse obstáculo, o Acórdão 2.279/2021 recomendou ao Comitê Central de Governança de Dados, instituído pelo Decreto 10.046/2019, que definisse “procedimento padrão para autorização de acesso a dados, que possa ser adotado ou customizado pelos órgãos interessados e que contemple, pelo menos, procedimentos internos céleres (fast track) aplicáveis a conjuntos de dados categorizados em nível específico pelos gestores de dados, com poucas instâncias decisórias e simplificação de exigências”.

31. Porém, ao compulsar o voto do Ministro Augusto Nardes e as pertinentes recomendações ora propostas, tive a nítida sensação de que, ao enfatizar a necessidade de reforço das medidas previstas na LGPD, no tocante ao tratamento de dados pessoais e seu compartilhamento com entidades

externas, o Acórdão ora proposto por Sua Excelência poderia, como efeito colateral indesejável, vir a sepultar de vez nossas esperanças quanto à melhoria da integração de serviços e políticas públicas no âmbito do Poder Executivo Federal.

32. Refiro-me, em particular, à proposta derecomendação à Secretaria de Governo Digital do Ministério da Economia,presente no item 9.1.9,que trata da necessáriaelaboração de normativo sobreo assunto, nos seguintes termos:

> 9.1.9. à implementação de procedimentos e controles para o compartilhamento de dados pessoais com terceiros (organizações públicas, privadas e transferência internacional), considerando o disposto nos arts. 5º, inciso XVI; 26, 27; e 33 da Lei 13.709/2018 e as diretrizes estabelecidas no item 7.5 da ABNT NBR ISO/IEC 27701:2019;

33. Por todo o exposto, peço vênias ao eminente relator para **sugerirque a deliberação em tela seja subdividida em dois itens**, de modo a proporcionar maior clareza sobre o tratamento diferenciado que deve ser dispensado ao uso de dados pessoais de forma compartilhada no âmbito dos órgãos integrantes do "corpo único" da Administração Direta Federal, em relação ao compartilhamento de tais informações com os demais órgãos públicos e organizações privadas, inclusive de âmbito internacional.

34. Nesse sentido, proponho a Sua Excelência a seguinte redação, com a necessária renumeração dos itens subsequentes do Acórdão, a fim de melhor compatibilizar o processo de transformação digital da Administração Pública Federal com a necessária proteção aos dados pessoais dos cidadãos:

> 9.1.9. à implementação de procedimentos internos mais céleres (fast track) e controles simplificados para o uso compartilhado de dados pessoais no âmbito dos órgãos da Administração Direta, considerando o disposto nos arts. 7º, inciso III; 11, inciso II, "b" e "g"; 23; 25; 26 e 27, inciso II, da Lei 13.709/2018 e as diretrizes estabelecidas no item 7.5 da ABNT NBR ISO/IEC 27701:2019;
>
> 9.1.10. à implementação de procedimentos e controles para o compartilhamento de dados pessoais com terceiros (organizações públicas não integrantes da Administração Direta, entidades privadas e transferência internacional), considerando o disposto nos arts. 5º, inciso XVI; 26, 27; e 33 da Lei 13.709/2018 e as diretrizes estabelecidas no item 7.5 da ABNT NBR ISO/IEC 27701:2019;

***

35. Ademais, causa-me especial preocupação o fato de que o compartilhamento e a integração de dados no âmbito da Administração Pública dependem da atuação de centenas de gestores individuais, todos sujeitos ao mesmo comportamento de aversão ao risco, com consequências danosas para a eficiência da gestão do Estado e para a prestação de serviços ao cidadão.

36. Refiro-me, em particular, às responsabilidades dos agentes de tratamento de dados pessoais, objeto do Capítulo VI da Lei Geral de Proteção de Dados – ocontrolador e o operador – e à forma como tais encargos estão sendo exercidos no âmbito do Poder Executivo Federal.

37. O tema foi objeto de atenção da Autoridade Nacional de Proteção de Dados (ANPD), por meio do Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, nos seguintes termos:

> 2.3. Controlador pessoa jurídica de direito público
>
> 19. Situação peculiar é a das pessoas jurídicas de direito público, cujas competênciasdecisóriassãodistribuídas internamente entre diferentes órgãospúblicos. É o que

> ocorre, por exemplo, com a União (pessoa jurídica de direito público) e os Ministérios (órgãospúblicos despersonalizados que integram a União e realizam tratamento de dados pessoais conforme o previsto na legislação).
>
> 20. Nesses casos, deve-se considerar dois aspectos centrais. De um lado, conforme o art. 5o, VI, da LGPD, **o controlador é a União, pessoa jurídica de direito público** que, em últimaanálise, é a responsável pelas obrigações decorrentes da lei, de instrumentos contratuais ou de atos ilícitos praticados pelos seus órgãos e servidores.
>
> 21. **De outro lado, a LGPD atribuiu aos órgãospúblicosobrigaçõestípicas de controlador**, indicando que, no setor público, essas obrigações devem ser distribuídas entre as principais unidades administrativas despersonalizadas que integram a pessoa jurídica de direito público e realizam tratamento de dados pessoais.
>
> 22. Nesse sentido, a União, como controladora, é a responsável perante a LGPD, mas as atribuições de controlador, por força da desconcentração administrativa, **são exercidas pelos órgãospúblicos que desempenham funções em nome da pessoa jurídica da qual fazem parte**, fenômeno que caracteriza a distribuição interna das competências. É o que se verifica nas hipóteses de uso compartilhado de dados pessoais (art. 26), de atendimento àsexigências da ANPD (art. 29) e de aplicação de sanções administrativas (art. 52, § 3o). (grifos no original)

38. Com todo o respeito devido à ANPD, instância administrativa máxima no que se refere à expedição de orientações sobre a aplicação da LGPD, nos termos do art. 55-K daquela Lei, entendo que essa não seja a melhor interpretação do que dispõe o art. 4º do Decreto-Lei 200/1967, que atribui personalidade jurídica indivisível à Administração Direta, ainda que esta seja constituída por órgãos e serviços integrados na estrutura administrativa da Presidência da República e de seus Ministérios.

39. Ademais, o art. 30 do referido Decreto-Lei prevê explicitamente que atividades comuns a todos os órgãos da Administração e que necessitem de coordenação central devem ser organizados na forma de sistemas, sob orientação normativa do respectivo órgão central, a quem compete zelar pelo fiel cumprimentos das leis e dos regulamentos pertinentes.

> Art. 30. Serão organizadas sob a forma de sistema as atividades de pessoal, orçamento, estatística, administração financeira, contabilidade e auditoria, e serviços gerais, além de outras atividades auxiliares comuns a todos os órgãos da Administração que, a critério do Poder Executivo, necessitem de coordenação central.
>
> § 1º Os serviços incumbidos do exercício das atividades de que trata este artigo consideram-se integrados no sistema respectivo e ficam, consequentemente, sujeitos à orientação normativa, à supervisão técnica e à fiscalização específica do órgão central do sistema, sem prejuízo da subordinação ao órgão em cuja estrutura administrativa estiverem integrados.
>
> § 2º O chefe do órgão central do sistema é responsável pelo fiel cumprimento das leis e regulamentos pertinentes e pelo funcionamento eficiente e coordenado do sistema.
>
> § 3º É dever dos responsáveis pelos diversos órgãos competentes dos sistemas atuar de modo a imprimir o máximo rendimento e a reduzir os custos operacionais da Administração.

40. No âmbito do Poder Executivo federal, tal comando deu origem ao Decreto 7.579/2011, que dispõe sobre o Sistema de Administração dos Recursos de Tecnologia da Informação – SISP.

41. Não por acaso, o referido Decreto atribui à Secretaria de Governo Digital do Ministério da Economia o papel de Órgão Central do SISP, cujas competências abrangem "definir, elaborar, divulgar e implementar as políticas, as diretrizes e as normas gerais relativas à gestão dos recursos do SISP" (art. 4º, inciso II), cabendo aos Órgãos Setoriais dos Ministérios e da Presidência da República a responsabilidade por "cumprir e fazer cumprir as políticas, diretrizes e normas gerais emanadas do Órgão Central" (art. 6º, inciso III).

42. Ademais, é imperioso considerar que a coleta e o tratamento de dados pessoais em um Estado digital são realizados quase exclusivamente por intermédio de recursos tecnológicos, ainda que, em etapas iniciais ou situações excepcionais dos processos de trabalho, tais atividades eventualmente se utilizem do papel ou de outros meios analógicos.

43. Outrossim, cabe destacar que as leis e os decretos que dispõem sobre o compartilhamento de dados e a interoperabilidade de sistemas, citados anteriormente, atribuem ao Órgão Central do SISP a responsabilidade por normatizar o assunto no âmbito do sistema, promover as ações necessárias por parte dos demais órgãos e fiscalizar o cumprimento das normas pertinentes.

44. Não me parece razoável, portanto, sugerir que no caso do uso compartilhado de dados pessoais pelo poder público, hipótese prevista explicitamente pela LGPD, seja adotado comportamento diverso, com a responsabilidade normativa distribuída por inúmeros órgãos integrantes de um mesmo sistema. Dada a possibilidade de que cada Ministério ou Secretaria adote regras próprias, distintas e potencialmente incompatíveis entre si, restaria impossibilitado o alcance dos objetivos de máximo rendimento e redução de custos operacionais, previsto no § 3º do art. 30 do Decreto-Lei 200/1967.

45. Por tais motivos, entendo que, como estrutura administrativa única e integrada, a Administração Direta admite, portanto, a existência de um único controlador, a quem competem, nos termos do art. 5º, inciso VI da LGPD, as decisões referentes ao tratamento de dados pessoais, cabendo tal responsabilidade ao Órgão Central do SISP, em consonância com o Decreto 7579/2011.

46. Por sua vez, os órgãos setoriais do SISP atuariam como múltiplos operadores, distribuídos nos diversos Ministérios e demais órgãos, responsáveis por realizar o tratamento de dados pessoais em nome do controlador e de acordo com as instruções por ele fornecidas, conforme previsto no art. 5º, inciso VII e art. 39 da multicitada Lei.

47. É forçoso ressaltar, entretanto, as limitações impostas à atuação do TCU nesse tema, uma vez que, nos termos do art. 30 da LGPD, compete à Autoridade Nacional de Proteção de Dados o estabelecimento de normas complementares sobre o uso compartilhado de dados pessoais, a exemplo do Guia Orientativo do qual consta o atual entendimento daquele órgão sobre a definição dos agentes de tratamento de dados pessoais.

48. Por outro lado, ressalto igualmente que não pode o Tribunal de Contas da União se omitir diante de assunto de tamanha relevância, diante dos prejuízos causados à eficiência da Administração Pública pela falta de compartilhamento e integração de dados entre órgãos e entidades do Estado, conforme sobejamente demonstrados em múltiplos Acórdãos desta Corte.

49. Diante do exposto, sugiro ao eminente Relator a inclusão de recomendação adicional direcionada à ANPD no item 9.4 do Acórdão proposto por Sua Excelência, transformando a deliberação já proposta por Sua Excelência no subitem 9.4.1 e acrescentando o subitem 9.4.2, nos seguintes termos:

> 9.4. recomendar à Autoridade Nacional de Proteção de Dados, com fundamento no art. 11 da Resolução - TCU 315/2020, que:
>
> 9.4.1. oriente as organizações públicas quanto às responsabilidades, aos perfis e requisitos profissionais desejáveis, bem como sobre os locais apropriados de lotação do encarregado no normativo relacionado ao tema que está previsto na agenda regulatória da instituição, em consonância com o disposto no art. 41, § 3º, da Lei 13.709/2018;
>
> 9.4.2. aperfeiçoe os normativos e guias expedidos pela instituição, em especial o Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, considerando queos órgãos e serviços da Administração Direta constituem estrutura administrativa única e integrada na qual a gestão de recursos de tecnologia da informação encontra-se organizada em sistema próprio, em cujo âmbito o tratamento de dados pessoais comporta a atuação de um único

controlador e múltiplos operadores, que devem agir de forma coordenada paraimprimir o máximo rendimento e reduzir os custos operacionais da Administração, em consonância com o disposto no art. 30 do Decreto-Lei 200/1967;art. 26da Lei 13.709/2018; e art. 1º do Decreto 7.579/2011.

Registro meus agradecimentos ao eminente Ministro Augusto Nardes pela gentileza de aguardar a presente manifestação e acolher as sugestões que ora apresento, ao tempo em que renovo os elogios às equipes de seu gabinete e da unidade técnica pela excelência do trabalho apresentado e registro meu integral apoio ao Acórdão proposto por Sua Excelência.

TCU, Sala das Sessões, em 6 de abrilde 2022.

AROLDO CEDRAZ
Ministro

ACÓRDÃO Nº 1384/2022 – TCU – Plenário

1. Processo nº TC 039.606/2020-1.
1.1. Apenso: 005.267/2021-8.
2. Grupo I – Classe de Assunto: V – Auditoria.
3. Interessados/Responsáveis: não há.
4. Órgãos/Entidades: Advocacia-Geral da União; Agência Brasileira de Desenvolvimento Industrial; Agência Brasileira de Inteligência; Agência Brasileira de Promoção de Exportações e Investimentos; e outros.
5. Relator: Ministro Augusto Nardes.
6. Representante do Ministério Público: Procurador Júlio Marcelo de Oliveira.
7. Unidade Técnica: Secretaria de Fiscalização de Tecnologia da Informação (Sefti).
8. Representação legal: Juliana Andrade Litaiff (44.123/OAB-DF), Luiza Rocha Jacobsen (46.824/OAB-DF) e outros, representando Serviço Nacional de Aprendizagem do Transporte - Conselho Nacional; Juliana Andrade Litaiff (44.123/OAB-DF), Luiza Rocha Jacobsen (46.824/OAB-DF) e outros, representando Serviço Social do Transporte - Conselho Nacional; Leonardo Andrade Simon, Roberto Parucker e outros, representando Centrais Elétricas do Norte do Brasil S.a.; Cássio Augusto Muniz Borges (91152/OAB-RJ), Francisco de Paula Filho (7.530/OAB-DF) e outros, representando Serviço Social da Indústria - Departamento Nacional; Grazielle Fernandes Pettene, Anna Paula Bottrel Souza (143.502/OAB-RJ), Adriana Diniz de Vasconcellos Guerra (191.390-A/OAB-SP), Saulo Benigno Puttini (42.154/OAB-DF), Pedro Jose de Almeida Ribeiro (163.187/OAB-RJ), Maritisa Mara Gambirasi Carcinoni, Carina Gallardo Rey (132.226/OAB-RJ), Tais Guida Fonseca Guedes (156.097/OAB-RJ), Marcia Aita Almeida (13.539/OAB-DF), Melissa Monte Stephan (118.596/OAB-RJ), Denilson Ribeiro de Sena Nunes (96.320/OAB-RJ), Andre de Castro Oliveira Pereira Braga (201.971/OAB-RJ), Ana Paula Barbosa de Sa (140.352/OAB-RJ), Marcelo Sampaio Vianna Rangel (90.412/OAB-RJ), Rodrigo Sales da Rocha Abreu (155.278/OAB-RJ) e Maria Joana Carneiro de Moraes (158.738/OAB-RJ), representando Banco Nacional de Desenvolvimento Econômico e Social; Leonor Chaves Maia de Sousa (20321/OAB-CE), Arnaldo de Morais Moreira Fernandes Vieira e outros, representando Banco do Nordeste do Brasil S.A..

9. Acórdão:

VISTO, relatado e discutido o presente processo de auditoria realizada em 382 organizações públicas federais para avaliar a aderência de suas ações às diretrizes estabelecidas pela Lei Geral de Proteção de Dados - LGPD, autorizada pelo Acórdão 2.909/2020-TCU-Plenário;

ACORDAM os ministros do Tribunal de Contas da União, reunidos em sessão do Plenário, ante as razões expostas pelo Relator, em:

9.1. recomendar à Secretaria de Governo Digital do Ministério da Economia, com fundamento no art. 11 da Resolução - TCU 315/2020, que, considerando o controle realizado sobre a atuação administrativa das organizações sob sua jurisdição, edite normativos e guias, consultando a Autoridade Nacional de Proteção de Dados e o Gabinete de Segurança Institucional da Presidência da República, para auxiliar o processo de adequação das organizações à LGPD, incluindo orientações quanto:

9.1.1. à identificação de normativos correlatos ao tratamento de dados pessoais aplicáveis à organização, considerando as diretrizes estabelecidas no item 5.2.1 da ABNT NBR ISO/IEC 27701:2019;

9.1.2. à adequação dos contratos firmados com os operadores de forma a estabelecer, claramente, os papéis e responsabilidades relacionados à proteção de dados pessoais, considerando as diretrizes estabelecidas no item 7.2.6 da ABNT NBR ISO/IEC 27701:2019;

9.1.3. à avaliação da ocorrência de tratamento de dados pessoais com o envolvimento de controlador conjunto e à definição de papeis e responsabilidades de cada um dos controladores, considerando as diretrizes estabelecidas no item 7.2.7 da ABNT NBR ISO/IEC 27701:2019;

9.1.4. à elaboração de Política de Classificação da Informação que considere a classificação de dados pessoais, considerando o disposto nos arts. 5º, inciso II, 11 e 14 da Lei 13.709/2018 e no art. 31, § 1º, da Lei 12.527/2011, bem como as diretrizes estabelecidas no item 6.5.2 da ABNT NBR ISO/IEC 27701:2019;

9.1.5. à elaboração de Política de Proteção de Dados Pessoais, considerando as diretrizes estabelecidas no item 6.2.1.1 da ABNT NBR ISO/IEC 27701:2019;

9.1.6 à elaboração de Plano de Capacitação que considere a realização de treinamento e conscientização dos colaboradores em proteção de dados pessoais, considerando as diretrizes estabelecidas nos itens 5.5.2 e 5.5.3 da ABNT NBR ISO/IEC 27701:2019;

9.1.7. à elaboração de Política de Privacidade, considerando o disposto nos arts. 6º, incisos IV e VI, 9º e 23, inciso I, da Lei 13.709/2018 e as diretrizes estabelecidas nos itens 7.3.2 e 7.3.3 da ABNT NBR ISO/IEC 27701:2019;

9.1.8. à implementação de mecanismos para atendimento dos direitos dos titulares elencados no art. 18 da Lei 13.709/2018, considerando as diretrizes estabelecidas no item 7.3 da ABNT NBR ISO/IEC 27701:2019;

9.1.9. à implementação de procedimentos internos mais céleres (**fast track**) e controles simplificados para o uso compartilhado de dados pessoais no âmbito dos órgãos da Administração Direta, considerando o disposto nos arts. 7º, inciso III; 11, inciso II, "b" e "g"; 23; 25; 26 e 27, inciso II, da Lei 13.709/2018 e as diretrizes estabelecidas no item 7.5 da ABNT NBR ISO/IEC 27701:2019;

9.1.10. à implementação de procedimentos e controles para o compartilhamento de dados pessoais com terceiros (organizações públicas não integrantes da Administração Direta, entidades privadas e transferência internacional), considerando o disposto nos arts. 5º, inciso XVI; 26, 27; e 33 da Lei 13.709/2018 e as diretrizes estabelecidas no item 7.5 da ABNT NBR ISO/IEC 27701:2019;

9.1.11. à elaboração de Plano de Resposta a Incidentes e à implementação de controles para o tratamento de ocorrências relacionadas à violação de dados pessoais, considerando o disposto no art. 50, § 2º, inciso I, alínea "g", da Lei 13.709/2018 e as diretrizes estabelecidas no item 6.13 da ABNT NBR ISO/IEC 27701:2019;

9.1.12. à implementação de processo de controle de acesso de usuários em sistemas que realizam tratamento de dados pessoais, considerando o disposto nos arts. 46 e 47 da Lei 13.709/2018 e as diretrizes estabelecidas nos itens 6.6.2.1 e 6.6.2.2 da ABNT NBR ISO/IEC 27701:2019;

9.1.13. à implementação de registro de eventos das atividades de tratamento de dados pessoais, considerando as diretrizes estabelecidas no item 6.9.4.1 da ABNT NBR ISO/IEC 27701:2019; e

9.1.14. à utilização de criptografia para proteção de dados pessoais, considerando o disposto nos arts. 48, § 3º; e 50, § 2º, inciso I, alínea "c", da Lei 13.709/2018 e as diretrizes estabelecidas no item 6.7 da ABNT NBR ISO/IEC 27701:2019;

9.2. recomendar ao Conselho Nacional de Justiça e ao Conselho Nacional do Ministério Público, com fundamento no art. 11 da Resolução - TCU 315/2020, que, considerando o controle realizado sobre a atuação administrativa das organizações sob suas jurisdições, editem normativos e guias, consultando a Autoridade Nacional de Proteção de Dados, para auxiliar o processo de adequação das organizações à LGPD, incluindo orientações quanto:

9.2.1. ao planejamento das medidas necessárias para adequação à LGPD, considerando as diretrizes estabelecidas no item 5.4.2 da ABNT NBR ISO/IEC 27701:2019;

9.2.2. à identificação de normativos correlatos ao tratamento de dados pessoais aplicáveis à organização, considerando as diretrizes estabelecidas no item 5.2.1 da ABNT NBR ISO/IEC 27701:2019;

9.2.3. à identificação das categorias de titulares de dados pessoais com os quais se relacionam, considerando as diretrizes estabelecidas no item 7.2.8 da ABNT NBR ISO/IEC 27701:2019;

9.2.4. à identificação dos operadores que realizam tratamento de dados pessoais em seus nomes, considerando as diretrizes estabelecidas no item 5.2.2 da ABNT NBR ISO/IEC 27701:2019;

9.2.5. à adequação dos contratos firmados com os operadores de forma a estabelecer, claramente, os papéis e responsabilidades relacionados à proteção de dados pessoais, considerando as diretrizes estabelecidas no item 7.2.6 da ABNT NBR ISO/IEC 27701:2019;

9.2.6. à avaliação da ocorrência de tratamento de dados pessoais com o envolvimento de controlador conjunto e à definição de papeis e responsabilidades de cada um dos controladores, considerando as diretrizes estabelecidas no item 7.2.7 da ABNT NBR ISO/IEC 27701:2019;

9.2.7. à identificação dos processos de negócio que realizam tratamento de dados pessoais, bem como dos respectivos responsáveis, considerando o disposto nos arts. 3º, 5º, inciso X, e 37 da Lei 13.709/2018 e as diretrizes estabelecidas no item 7.2.8 da ABNT NBR ISO/IEC 27701:2019;

9.2.8. à identificação dos dados pessoais que são tratados por elas, bem como dos locais de armazenamento desses dados, considerando o disposto nos arts. 5º, inciso I, e 37 da Lei 13.709/2018 e as diretrizes estabelecidas no item 7.2.8 da ABNT NBR ISO/IEC 27701:2019;

9.2.9. à avaliação de riscos relacionados aos processos de tratamento de dados pessoais, considerando o disposto no art. 50, §2º, alínea "d", da Lei 13.709/2018 e as diretrizes estabelecidas no item 5.4.1.2 da ABNT NBR ISO/IEC 27701:2019;

9.2.10. à elaboração de Política de Classificação da Informação que considere a classificação de dados pessoais, considerando o disposto nos arts. 5º, inciso II, 11 e 14 da Lei 13.709/2018 e no art. 31, § 1º, da Lei 12.527/2011, bem como as diretrizes estabelecidas no item 6.5.2 da ABNT NBR ISO/IEC 27701:2019;

9.2.11. à elaboração de Política de Proteção de Dados Pessoais, considerando as diretrizes estabelecidas no item 6.2.1.1 da ABNT NBR ISO/IEC 27701:2019;

9.2.12. à elaboração de Plano de Capacitação que considere a realização de treinamento e conscientização dos colaboradores em proteção de dados pessoais, considerando as diretrizes estabelecidas nos itens 5.5.2 e 5.5.3 da ABNT NBR ISO/IEC 27701:2019;

9.2.13. à identificação e à documentação das finalidades das atividades de tratamento de dados pessoais, considerando o disposto no art. 6º, inciso I, da Lei 13.709/2018 e as diretrizes estabelecidas no item 7.2.1 da ABNT NBR ISO/IEC 27701:2019;

9.2.14. à necessidade de avaliar se coletam apenas os dados estritamente necessários para as finalidades de tratamento de dados pessoais e se os dados são retidos durante o tempo estritamente necessário às mesmas necessidades, considerando o disposto no art. 6º, incisos II e III, da Lei 13.709/2018 e as diretrizes estabelecidas nos itens 7.4.1 e 7.4.7 da ABNT NBR ISO/IEC 27701:2019;

9.2.15. à identificação e à documentação das bases legais que fundamentam as atividades de tratamento de dados pessoais, considerando o disposto nos arts. 7º e 23 da Lei 13.709/2018 e as diretrizes estabelecidas no item 7.2.2 da ABNT NBR ISO/IEC 27701:2019;

9.2.16. à manutenção de registro das operações de tratamento de dados pessoais, considerando o disposto no art. 37 da Lei 13.709/2018 e as diretrizes estabelecidas no item 7.2.8 da ABNT NBR ISO/IEC 27701:2019;

9.2.17. à elaboração do Relatório de Impacto à Proteção de Dados Pessoais e de implementar controles para mitigar os riscos identificados, considerando o disposto no art. 5º, inciso XVII, da Lei 13.709/2018 e as diretrizes estabelecidas no item 7.2.5 da ABNT NBR ISO/IEC 27701:2019;

9.2.18. à elaboração de Política de Privacidade, considerando o disposto nos arts. 6º, incisos IV e VI, 9º e 23, inciso I, da Lei 13.709/2018 e as diretrizes estabelecidas nos itens 7.3.2 e 7.3.3 da ABNT NBR ISO/IEC 27701:2019;

9.2.19. à implementação de mecanismos para atendimento dos direitos dos titulares elencados no art. 18 da Lei 13.709/2018, considerando as diretrizes estabelecidas no item 7.3 da ABNT NBR ISO/IEC 27701:2019;

9.2.20. à implementação de procedimentos e controles para o compartilhamento de dados pessoais com terceiros (organizações públicas, privadas e transferência internacional), considerando o disposto nos arts. 5º, inciso XVI; 26, 27; e 33 da Lei 13.709/2018 e as diretrizes estabelecidas no item 7.5 da ABNT NBR ISO/IEC 27701:2019;

9.2.21. à elaboração de Plano de Resposta a Incidentes e à implementação de controles para o tratamento de ocorrências relacionadas à violação de dados pessoais, considerando o disposto no art. 50, § 2º, inciso I, alínea "g", da Lei 13.709/2018 e as diretrizes estabelecidas no item 6.13 da ABNT NBR ISO/IEC 27701:2019;

9.2.22. à adoção de medidas de segurança para proteção de dados pessoais, considerando o disposto nos arts. 46 e 47 da Lei 13.709/2018 e as boas práticas de gestão de segurança da informação abordadas pela ABNT NBR ISO/IEC 27701:2019;

9.2.23. à implementação de processo de controle de acesso de usuários em sistemas que realizam tratamento de dados pessoais, considerando o disposto nos arts. 46 e 47 da Lei 13.709/2018 e as diretrizes estabelecidas nos itens 6.6.2.1 e 6.6.2.2 da ABNT NBR ISO/IEC 27701:2019;

9.2.24. à implementação de registro de eventos das atividades de tratamento de dados pessoais, considerando as diretrizes estabelecidas no item 6.9.4.1 da ABNT NBR ISO/IEC 27701:2019;

9.2.25. à utilização de criptografia para proteção de dados pessoais, considerando o disposto nos arts. 48, § 3º; e 50, § 2º, inciso I, alínea "c", da Lei 13.709/2018 e as diretrizes estabelecidas no item 6.7 da ABNT NBR ISO/IEC 27701:2019; e

9.2.26. à adoção de medidas de proteção de dados pessoais desde a fase de concepção até a fase de execução de processos e sistemas (**Privacy by Design**), incluindo a coleta de dados limitada ao que é estritamente necessário ao alcance do propósito definido (**Privacy by Default**), considerando o disposto no art. 46, § 2º, da Lei 13.709/2018 e as diretrizes estabelecidas no item 7.4 da ABNT NBR ISO/IEC 27701:2019;

9.3. recomendar à Casa Civil da Presidência da República e ao Ministério da Economia, com fundamento no art. 11 da Resolução - TCU 315/2020, que adotem as medidas necessárias para alterar a natureza jurídica e promover a reestruturação organizacional da Autoridade Nacional de Proteção de Dados, conferindo o grau de independência e os meios necessários para o pleno exercício de suas atribuições, de acordo com o exposto na Nota Técnica 3/SG/ANPD e à semelhança do preconizado em normas internacionais, como o Regulamento Geral de Proteção de Dados da União Europeia e a Convenção 108 do Conselho da Europa;

9.4. recomendar à Autoridade Nacional de Proteção de Dados, com fundamento no art. 11 da Resolução - TCU 315/2020, que:

9.4.1. oriente as organizações públicas quanto às responsabilidades, aos perfis e requisitos profissionais desejáveis, bem como sobre os locais apropriados de lotação do encarregado no normativo relacionado ao tema que está previsto na agenda regulatória da instituição, em consonância com o disposto no art. 41, § 3º, da Lei 13.709/2018;

9.4.2. aperfeiçoe os normativos e guias expedidos pela instituição, em especial o Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, considerando que os órgãos e serviços da Administração Direta constituem estrutura administrativa única e integrada na qual a gestão de recursos de tecnologia da informação encontra-se organizada em sistema próprio, em cujo âmbito o tratamento de dados pessoais comporta a atuação de um único controlador e múltiplos operadores, que devem agir de forma coordenada para imprimir o máximo rendimento e reduzir os custos operacionais da Administração, em consonância com o disposto no art. 30 do Decreto-Lei 200/1967; art. 26 da Lei 13.709/2018; e art. 1º do Decreto 7.579/2011;

9.5. dar ciência às organizações relacionadas na peça 1012, com fundamento no art. 9º, inciso I da Resolução - TCU 315/2020, que a ausência de estabelecimento formal de uma Política de Segurança da Informação afronta o disposto no art. 15, inc. II do Decreto 9.637/2018 c/c art. 9º da Instrução Normativa GSI/PR 1/2020, no art. 19, inciso II, da Resolução 396/2021 do Conselho Nacional de Justiça, e no art. 22, inciso III, da Resolução 156/2016 do Conselho Nacional do Ministério Público;

9.6. determinar à Secretaria de Fiscalização de Tecnologia da Informação (Sefti) que:

9.6.1. promova monitoramento das recomendações contidas nos itens 9.1 ao 9.4 deste acórdão;

9.6.2. considere na Estratégia de Fiscalização do TCU em segurança da informação e proteção de dados 2022-2025 a execução de auditorias que avaliem incidentes críticos envolvendo vazamento de dados ocorridos na Administração Pública Federal;

9.7. desentranhar as peças 1052 a 1055 do presente feito, com base nos arts. 2º, X, e 17 da Resolução TCU 259/2014, e encaminhá-las à Secretaria de Fiscalização de Infraestrutura de Energia Elétrica, unidade técnica destinatária da comunicação que informa ao TCU a incorporação da Amazonas Geração e Transmissão de Energia S/A pelas Centrais Elétricas do Norte do Brasil S/A (Eletronorte), consoante CE PR 0108/2021, de 17/8/2021";

9.8. encaminhar cópias eletrônicas deste acórdão, bem como do relatório e do voto que o fundamentam à ANPD, à SGD/ME, ao CNJ, ao CNMP, à Casa Civil da Presidência da República, ao Gabinete de Segurança Institucional da Presidência da República, bem como às demais organizações públicas auditadas;

9.9. autorizar a Secretaria de Fiscalização de Tecnologia da Informação, sob a coordenação do Relator, a dar ampla divulgação às informações e aos produtos derivados da execução desta auditoria, excetuando as informações pessoais dos gestores respondentes, a fim de contribuir para a melhoria das organizações públicas em relação à adequação à LGPD;

9.10. classificar como públicos os dados das respostas individuais das organizações ao questionário da auditoria, conforme o art. 3º, inciso I, da LAI, excetuando as informações pessoais dos gestores respondentes, que devem ser classificadas como sigilosas, em consonância com o art. 31, § 1º, inciso I, da LAI;

9.11. autorizar a Secretaria de Fiscalização de Tecnologia da Informação a compartilhar os dados das respostas individuais das organizações ao questionário da auditoria, excetuando as informações pessoais dos gestores respondentes, com a ANPD, a SGD/ME, o CNJ e o CNMP, observando as respectivas jurisdições, a fim de contribuir com a orientação das organizações em relação à adequação à LGPD;

9.12. classificar como público o presente processo, nos termos da Resolução-TCU 294/2018, arts. 4º e 8º, com exceção das peças 593, 594, 602, 603, 687, 688, 689, 695, 696, 698, 699, 701, 702, 703, 704, 705, 706, 707, 708, 709, 710, 711, 719, 720, 722, 723, 724, 726, 727, 728, 730, 734, 735, 737, 743, 745, 749, 750, 751, 754, 757, 758, 759, 760, 761, 764, 769, 771, 772, 774, 775, 776, 777, 784, 785, 786, 788, 789, 793, 794, 796, 797, 798, 799, 800, 801, 803, 806, 807, 808, 809, 813, 814, 815, 816, 817, 818, 819, 821, 822, 823, 826, 827, 830, 832, 838, 840, 845, 846, 848, 850, 851, 890, 891, 892, 893, 900, 919, 924, 926, 927, 929, 930, 931, 935, 936, 938, 939, 941, 945, 946, 947, 948, 949, 973, 985, 987, 988, 992, 996 e 1041 – que devem ser classificadas como sigilosas por conterem informações pessoais de gestores respondentes, em consonância com o art. 31, § 1º, inciso I, da LAI;

9.13. levantar o sigilo das seguintes peças referentes a ofícios de comunicação da auditoria: 7-46, 48-57, 59-113, 206-237, 239-283, 286-400, 551, 552, 568, 569, 570, 576-582, 611-683 e 716;

9.14. levantar o sigilo das seguintes peças referentes a respostas de comunicações por parte das organizações auditadas: 731, 756, 773, 899, 912, 913, 922, 925, 937, 946, 1013, 1040 e 1045.

10. Ata n° 22/2022 – Plenário.
11. Data da Sessão: 15/6/2022 – Ordinária.
12. Código eletrônico para localização na página do TCU na Internet: AC-1384-22/22-P.
13. Especificação do quórum:
13.1. Ministros presentes: Ana Arraes (Presidente), Walton Alencar Rodrigues, Benjamin Zymler, Augusto Nardes (Relator), Bruno Dantas e Vital do Rêgo.
13.2. Ministros-Substitutos presentes: Marcos Bemquerer Costa e André Luís de Carvalho.

(Assinado Eletronicamente)
ANA ARRAES
Presidente

(Assinado Eletronicamente)
AUGUSTO NARDES
Relator

Fui presente:

(Assinado Eletronicamente)
CRISTINA MACHADO DA COSTA E SILVA
Procuradora-Geral

Guia do Framework de Privacidade e Segurança da Informação

PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI)

Versão 1.1.3

Brasília, março de 2024

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS

Esther Dweck

Ministra

SECRETARIA DE GOVERNO DIGITAL

Rogério Souza Mascarenhas

Secretário de Governo Digital

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Leonardo Rodrigo Ferreira

Diretor de Privacidade e Segurança da Informação

COORDENAÇÃO-GERAL DE PRIVACIDADE

Julierme Rodrigues da Silva

Coordenador-Geral de Privacidade

COORDENAÇÃO-GERAL DE SEGURANÇA DA INFORMAÇÃO

Loriza Andrade Vaz de Melo

Coordenadora-Geral de Segurança da Informação

EQUIPE TÉCNICA DE ELABORAÇÃO

Adriano de Andrade Moura

Afrânio Henrique Teixeira Machado

Bruno Pierre Rodrigues de Sousa

Erion Dias Monteiro

Ivaldo Jeferson De Santana Castro

Francisco Magno Felix Nobre

Julierme Rodrigues da Silva

Leonard Keyzo Yamaoka Batista

Marcus Paulo Barbosa Vasconcelos

Rafael da Silva Ribeiro

Raphael César Estevão

Rogério Vinícius Matos Rocha

Romário César de Almeida

Valdecy Oliveira de Araújo

William Oliveira Lima

Yuri Arcanjo De Carvalho

EQUIPE TÉCNICA DE REVISÃO

Adriano de Andrade Moura

Bruno Pierre Rodrigues de Sousa

Julierme Rodrigues da Silva

Rogério Vinícius Matos Rocha

Histórico de Versões

Data	Versão	Descrição	Autor
04/11/2022	1.0	Primeira versão do Guia do Framework de Privacidade e Segurança da Informação	Equipe Técnica de Elaboração
30/03/2023	1.1	Atualizações realizadas no Guia do Framework de Privacidade e Segurança da Informação, conforme destacado no Anexo VI.	Equipe Técnica de Revisão
14/06/2023	1.1.1	Ajuste da medida 31.2 contemplada no Anexo V, conforme destacado no Anexo VI.	Equipe Técnica de Revisão
06/09/2023	1.1.2	Padronização do termo “Unidade de Controle Interno” e atualização da Figura 5.	Equipe Técnica de Revisão
21/03/2024	1.1.3	Ajuste da fórmula do iMC em alinhamento com a Ferramenta do Framework.	Equipe Técnica de Revisão

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS, ACRÔNIMOS E SIGLAS

ABNT/NBR	Associação Brasileira de Normas Técnicas
ANPD	Autoridade Nacional de Proteção de Dados
APF	Administração Pública Federal
API	*Application Programming Interface* (Interface de Programação de Aplicação)
Audin	Auditoria Interna
CGU	Controladoria-Geral da União
CIS	*Center for Internet Security*
Ciset	Secretarias de Controle Interno
CSA	*Control Self-Assessment*
DNS	*Domain Name System* (Sistema de Nomes de Domínio)
DSIC	Departamento de Segurança da Informação e Comunicações
Dump	Contém um registro da estrutura de tabela e ou dados de um banco de dados, e normalmente está na forma de uma lista de declarações SQL.
E-CIBER	Estratégia Nacional de Segurança Cibernética
ETIR	Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais
EUA	Estados Unidos da América
GCD	Governança no Compartilhamento de Dados
GI	Grupo de Implementação
GRC	Governança, Riscos e *Compliance*
GSI/PR	Gabinete de Segurança Institucional da Presidência da República
IDP	Inventário de Dados Pessoais
IDS	*Intrusion Detection System* (Sistema de Detecção de Intrusão)
IN	Instrução Normativa
iMC	*Indicador de Maturidade por Controle*
IoT	*Internet of Things* (Internet das Coisas)
IP	*Internet Protocol*
iPriv	Indicador de Privacidade
IPS	*Intrusion Prevention System* (Sistema de Prevenção de Intrusão)
iSeg	Indicador de Segurança
ISO/IEC	*International Organization of Standardization/International Electrotechnical Commission*
ITAM	*IT Asset Management* (Gerenciamento de Ativos de TI)
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados Pessoais

MCI	Marco Civil da Internet
NC	Normas Complementares
NIST	*National Institute of Standards and Technology*
NSC	Núcleo de Segurança e Credenciamento
PDCA	Método iterativo de gestão de quatro passos (*Plan, Do, Check e Act*), utilizado para o controle e melhoria contínua de processos e produtos.
PMC	Somatório das pontuações das medidas avaliadas no controle QMC
PNSI	Política Nacional de Segurança da Informação
PPSI	Programa de Privacidade e Segurança da Informação
QMC	Quantidade de Medidas do Controle
QMNAC	Quantidade de Medidas não Aplicáveis do Controle
RIPD	Relatório de Impacto de Proteção de Dados
SaaS	*Software as a Service* (Software como um Serviço)
SCI	Sistema de Controle Interno
SGD/MGI	Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos
SGIP	Sistema de Gerenciamento de Informações de Privacidade
SIEM	*Security Information and Event Management* (Gerenciamento e Correlação de Eventos de Segurança)
SLA	*Service Level Agreement* (Acordo de Nível de Serviço)
SQL injection	*Structured Query Language Injection*
TCU	Tribunal de Contas da União
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
URL	*Uniform Resource Locator*
USB	*Universal Serial Bus*

SUMÁRIO

AVISO PRELIMINAR E AGRADECIMENTOS

O presente Guia, especialmente recomendado e dirigido aos órgãos e às entidades da Administração Pública Federal – APF, visa a difundir as melhores práticas em matéria de privacidade e segurança da informação, em atendimento à Política Nacional de Segurança da Informação (PNSI – Decreto nº 9.637, de 26 de dezembro de 2018), ao "CAPÍTULO VII – DA SEGURANÇA E DAS BOAS PRÁTICAS" da Lei Geral de Proteção de Dados Pessoais - LGPD (Lei nº 13.709, de 14 de agosto de 2018) e outros normativos vigentes sobre o tema de privacidade, proteção de dados pessoais e segurança da informação, o que não impede de ser aproveitado por outras instituições que busquem orientações sobre o tema.

Este documento é de autoria exclusiva da Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos, contendo referências a publicações e a outros documentos técnicos, com destaque para aqueles do *Center for Internet Security* (CIS)[1], do *National Institute of Standards and Technology* (NIST)[2], da *International Standardization Organization/Eletrotechnical Commission* (ISO/IEC)[3] e da Associação Brasileira de Normas Técnicas (ABNT NBR)[4]. Muitas das referências foram traduzidas de forma livre pelos técnicos da SGD com propósitos educativos e não comerciais a fim de difundir tais conhecimentos para as instituições públicas.

Nesse cenário, a Secretaria de Governo Digital enfatiza que:

a) não representa, tampouco se manifesta em nome do CIS, do NIST, da ABNT NBR ou da ISO/IEC e vice-versa;

b) não se manifesta em nome do TCU, da CGU, do GSI e da ANPD;

c) não é coautora das publicações internacionais abordadas;

d) não assume nenhuma responsabilidade administrativa, técnica ou jurídica pelo uso ou pela interpretação inadequados, fragmentados ou parciais do presente **Guia**;

e) caso o leitor deseje se certificar de que atende integralmente os requisitos das publicações do CIS, do NIST ou da ISO/IEC em suas versões originais, na língua inglesa, deverá consultar diretamente as fontes oficiais de informação ofertadas pelas referidas instituições.

Agradecimento especial ao CIS, ao NIST, à ABNT NBR e à ISO/IEC pelas valiosas

[1] Disponível em: https://www.cisecurity.org/
[2] Disponível em: https://www.nist.gov/
[3] Disponível em: https://www.iso.org/standards.html
[4] Disponível em: https://www.abntcatalogo.com.br/

contribuições para a comunidade de privacidade e segurança da informação.

Cumpre também reconhecer a fundamental parceria com o Governo do Reino Unido, no âmbito do Programa de Acesso Digital, que viabilizou o desenvolvimento de uma ferramenta para aplicação do framework proposto por esta publicação.

INTRODUÇÃO

O **Guia do Framework de Privacidade e Segurança da Informação** é uma adição à série de guias operacionais[5] elaborados pela Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos para fomentar a privacidade, a proteção de dados pessoais e a segurança da informação[6].

O objetivo deste **Guia** é propor às instituições públicas diretrizes no sentido de auxiliar a identificação, o acompanhamento e o preenchimento das lacunas de privacidade e segurança da informação presentes na instituição com base nas obrigações da PNSI e LGPD, bem como, nos controles elaborados pelo (a) CIS, NIST, ISO/IEC e ABNT NBR.

O **Framework de Privacidade e Segurança da Informação** constante deste **Guia** está organizado nos seguintes capítulos e anexos:

- O Capítulo 1 destaca sua fundamentação e estruturação dos controles;
- O Capítulo 2 descreve o controle de estruturação básica de gestão em privacidade e segurança da informação;
- O Capítulo 3 descreve os controles de segurança cibernética adotados pelo framework;
- O Capítulo 4 descreve os controles de privacidade adotados pelo framework;
- O Capítulo 5 trata da implementação dos controles de privacidade e segurança cibernética;
- O Capítulo 6 contempla a forma de avaliação de maturidade da instituição;
- O Capítulo 7 menciona a utilização de uma ferramenta para acompanhamento da implementação deste **Framework**.
- O Capítulo 8 apresenta as considerações finais, ressaltando os benefícios esperados com a aplicação do framework pelas instituições;
- O Anexo I apresenta o modelo de avaliação de criticidade de sistemas;
- O Anexo II traz uma lista com os normativos do GSI/PR;
- O Anexo III apresenta o controle de estruturação básica em privacidade e segurança da informação;
- O Anexo IV lista em formato de questões as medidas dos controles CIS; e

[5] Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd
[6] Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

- O Anexo V elenca em formato de questões as medidas dos controles de privacidade.

Ressalta-se que a instituição é livre para adequar todas as proposições deste documento a sua realidade. A abordagem proposta oferece uma sugestão de uso dos controles e medidas de privacidade e segurança da informação, contudo, esse fato não exclui a necessidade de que a instituição compreenda sua própria postura de risco institucional. A intenção é ajudar a organização a concentrar seus esforços com base nos recursos disponíveis, integrando-os a qualquer processo de gestão de risco pré-existente.

Nesse sentido, reforça-se que a adoção do framework não equivale necessariamente ao cumprimento da legislação brasileira vigente sobre privacidade, proteção de dados pessoais e segurança da informação, em especial a PNSI e a Lei nº 13.709, de 14 de agosto de 2018 – LGPD. Contudo, o presente Guia seguramente poderá auxiliar a instituição adotante a atingir os objetivos previstos nas normas correlatas, ao permitir a visualização da maturidade de seus trabalhos de privacidade, de proteção de dados, e de segurança da informação de forma a ampliar a implementação das melhores práticas sobre o tema.

Este **Guia** será revisto e atualizado anualmente ou sempre que se fizer necessária a inclusão de ajustes para acompanhar o amadurecimento dos processos de privacidade e segurança da informação, bem como para alinhamento às novas determinações especificadas pela ANPD e GSI.

1. FUNDAMENTAÇÃO E ESTRUTURAÇÃO DOS CONTROLES

O **Framework de Privacidade e Segurança da Informação** é resultado de extensa pesquisa de abordagens e modelos para implementação de controles e medidas que visam a assegurar a privacidade, a proteção de dados pessoais e a segurança da informação.

Existe uma gama extraordinária de normas, frameworks e guias disponíveis atualmente no mercado sobre os temas de privacidade, proteção de dados pessoais e segurança da informação. Esses modelos e orientações variam desde os mais abrangentes, com controles e medidas aplicáveis em qualquer negócio, até os mais específicos, que consideram detalhes de normas vigentes em um país específico. Ambos os casos necessitam de uma adaptação para a realidade de quem os adota.

A estratégia utilizada para a construção do Framework deste **Guia** não consistiu em adotar uma única referência específica e sim na combinação de algumas das mais abrangentes. A combinação se justifica pela complementação, na medida do possível, dos *gaps* presentes em cada referência adotada de forma a atender a pluralidade de serviços e de tratamento de dados pessoais pelo Poder Público. A APF tem diversos órgãos, com políticas públicas próprias e atribuições institucionais específicas, isto é, o que se aplica a um órgão, pode não se aplicar a outro.

A fundamentação do **Framework** aborda normas legais de conformidade e é inspirada na: abordagem de controles e implementação do CIS (CIS, 2021), estrutura do núcleo do *Privacy Framework* (NIST, 2020) e normas ISO/IEC e ABNT NBR. Tal fundamentação é destacada pelas seções a seguir.

Importante ressaltar que este **Guia** não substitui a avaliação dos documentos originais que embasaram a estruturação deste **Framework**.

1.1 Normas Legais de Conformidade

A necessidade de elaboração e adoção de um Framework de Privacidade e Segurança da Informação vem ao encontro da exigência de conformidade com normas vigentes, tais como a Lei n° 13.709, de 14 de agosto de 2018 - LGPD, as publicações ANPD e as Instruções Normativas (INs) ou Normas Complementares (NCs) estabelecidas pelo GSI/PR que serão destacadas na sequência deste **Guia**.

Embora a LGPD, as publicações ANPD e os Normativos do GSI/PR demandem as principais ações de conformidade em privacidade, proteção de dados pessoais e segurança da informação, isto não isenta a alta administração e o gestor do negócio de

estarem cientes e em conformidade com outras normas relativas à segurança da informação, a proteção de dados e privacidade vigentes, dentre as quais pode-se destacar:

- Privacidade, com especial atenção à proteção de dados pessoais e dados pessoais sensíveis dos titulares:
    - Lei nº 12.527, de 18 de novembro de 2011, Lei de Acesso à Informação (LAI);
    - Lei nº 12.965, de 23 de abril de 2014, Marco Civil da Internet (MCI);
    - Decreto nº 10.046, de 09 de outubro de 2019, Governança no Compartilhamento de Dados (GCD);
    - IN SGD/ME nº 117, de 19 de novembro de 2020[7];
    - IN SGD/ME nº 31, de 23 de março de 2021[8];
    - Documentos e Publicações da ANPD[9].
- Segurança da Informação, com especial atenção quanto à segurança cibernética:
    - Decreto nº 10.222, de 05 de fevereiro de 2020, Estratégia Nacional de Segurança Cibernética (E-CIBER);
    - Decreto nº 10.748, de 16 de julho de 2021, Rede Federal de Gestão de Incidentes Cibernéticos;
    - Portaria GSI/PR nº 93, de 18 de outubro de 2021, Glossário de Segurança da Informação.

1.1.1 *LGPD*

A LGPD dispõe sobre o tratamento de dados pessoais das pessoas naturais, dispostos em meio físico ou digital, definindo as hipóteses em que tais dados podem legitimamente ser utilizados por terceiros e estabelecendo mecanismos para proteger os titulares dos dados contra usos inadequados.

A lei é aplicável ao tratamento de dados realizado por pessoas naturais ou por pessoas jurídicas de direito público ou privado, e tem o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade

[7] Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-sgd/me-n-117-de-19-de-novembro-de-2020-289515596
[8] Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-31-de-23-de-marco-de-2021-310081084
[9] Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes

da pessoa natural.

Seu objetivo é proteger os direitos fundamentais relacionados à esfera informacional do titular de dados pessoais. Assim, a Lei introduziu uma série de novos direitos que asseguram maior transparência quanto ao tratamento dos dados e conferem protagonismo ao titular quanto ao seu uso.

Dentre as diversas ações a serem observadas na LGPD, destacam-se os direitos dos titulares de dados pessoais, previstos no Capítulo III, as hipóteses de tratamento previstas no Capítulo II, o tratamento de dados pessoais pelo Poder Público, previsto no Capítulo IV, as obrigações dos agentes de tratamento, previstas no Capítulo VI, a transferência internacional de dados pessoais, prevista no Capítulo V e a segurança de dados pessoais e as boas práticas a serem observadas no Capítulo VII.

1.1.2 *Publicações da ANPD*

A Autoridade Nacional de Proteção de Dados (ANPD) tem a missão precípua de zelar pela proteção de dados pessoais e por regulamentar e fiscalizar o cumprimento da LGPD no País, a fim de promover a devida proteção aos direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade dos indivíduos. Suas principais competências estão listadas no artigo 55-j da LGPD. No cumprimento dessas competências, a ANPD tem realizado diversas publicações, e há perspectivas da publicação de enunciados, que servirão de substantiva orientação aos órgãos da Administração Pública Federal na conformidade à LGPD. As publicações da ANPD podem ser encontradas no sítio da Autoridade na internet em Publicações da ANPD[10].

1.1.3 *Normativos do GSI*

O GSI/PR planeja, coordena e supervisiona a atividade de segurança da informação no âmbito da APF. O GSI/PR, na condição de órgão governante superior, publica normativos (INs e NCs) de cumprimento obrigatório que norteiam as ações de segurança da informação na APF.

Diversos domínios relacionados à segurança da informação e cibernética já são contemplados por INs e NCs vigentes, dentre as quais podem-se destacar a IN GSI/PR nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da APF, a IN GSI/PR nº 5, de 31 de agosto de 2021, que dispõe sobre os requisitos mínimos de segurança da informação para

[10] Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes

utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da APF e a NC nº 05/IN01/DSIC/GSIPR, e seu anexo que disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da APF.

As demais INs e NCs do GSI, entre outras legislações, portarias e mais detalhes podem ser acessados em: Normativos GSI[11].

1.1.4 *PNSI*

Com o objetivo de estabelecer estrutura e modelo de governança para a integração e a coordenação nacional das atividades de segurança da informação, o GSI/PR coordenou uma série de ações voltadas para a elaboração da Política Nacional de Segurança da Informação (PNSI).

A PNSI tem por finalidade assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação em âmbito nacional. Essa política abrange: segurança cibernética, defesa cibernética, segurança física e a proteção de dados organizacionais.

Para mais detalhes, a Política Nacional de Segurança da Informação instituída pelo Decreto nº 9.637, de 26 de dezembro de 2018 pode ser acessada em: PNSI GSI/PR.

1.2 Estruturação básica de gestão em privacidade e segurança da informação

A estruturação básica de gestão em privacidade e segurança da informação tem bases na política de governança da APF direta, autárquica e fundacional estabelecida no Decreto nº 9.203, de 22 de novembro de 2017, que define governança pública como o conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade, bem como apresenta o conceito de gestão de riscos como o processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos.

O Decreto ainda destaca como diretrizes da governança pública dois comandos relacionados ao contexto do presente documento: "direcionar ações para a busca de

[11] Disponível em: https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/legislacao

resultados para a sociedade, encontrando soluções tempestivas e inovadoras para lidar com a limitação de recursos e com as mudanças de prioridades, bem como implementar controles internos fundamentados na gestão de risco, que privilegiará ações estratégicas de prevenção antes de processos sancionadores".

Tal norma fornece direcionadores para a alta administração das organizações da APF direta, autárquica e fundacional, que deverão estabelecer, manter, monitorar e aprimorar sistemas de gestão de riscos e controles internos com vistas à identificação, à avaliação, ao tratamento, ao monitoramento e à análise crítica de riscos que possam impactar a implementação da estratégia e a consecução dos objetivos da organização no cumprimento da sua missão institucional, observados os princípios indicados no Decreto.

Dessa forma, a Estrutura Básica de Gestão em Privacidade e Segurança da Informação no âmbito dos órgãos e entidades da APF, direta e indireta, contempla os seguintes papéis fundamentais para condução e implementação deste **Framework**:

- o Gestor de Tecnologia da Informação e Comunicação, dentre outras atribuições, nos termos da Portaria nº 778, de 4 de abril de 2019, responsável por planejar, implementar e melhorar continuamente os controles de privacidade e segurança da informação em soluções de tecnologia da informação e comunicações, considerando a cadeia de suprimentos relacionada à solução;
- o Encarregado pelo Tratamento de Dados Pessoais, dentre outras atribuições, nos termos do art. 41, §2º, da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD), responsável por conduzir o diagnóstico de privacidade, bem como orientar, no que couber, os gestores proprietários dos ativos de informação, responsáveis pelo planejamento, implementação e melhoria contínua dos controles de privacidade em ativos de informação que realizem o tratamento de dados pessoais ou dados pessoais sensíveis;
- o Gestor de Segurança da Informação, dentre outras atribuições, nos termos da Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional, da Presidência da República - GSI/PR, responsável por planejar, implementar e melhorar continuamente os controles de segurança da informação em ativos de informação;
- o Responsável pela Unidade de Controle Interno, atuará no apoio, supervisão e monitoramento das atividades desenvolvidas pela primeira linha de defesa

prevista pela Instrução Normativa CGU nº 3, de 9 de junho de 2017;

- o Comitê de Segurança da Informação ou estrutura equivalente, para deliberar sobre os assuntos relativos à Política Nacional de Segurança da Informação;
- a Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR, que constituirá a rede de equipes, integrada pelos órgãos e pelas entidades da APF, coordenada pelo Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo do GSI/PR; e
- a Política de Segurança da Informação - POSIN, implementada a partir da formalização e aprovação por parte da autoridade máxima da instituição, com o objetivo de estabelecer diretrizes, responsabilidades, competências e subsídios para a gestão da segurança da informação.

O responsável pela Unidade de Controle Interno integra a segunda linha de defesa nos termos da IN CGU nº 3, de 9 de junho de 2017. Os demais papéis que constituem a Estrutura Básica de Gestão em Privacidade e Segurança da Informação, juntamente com os proprietários de ativos, gestores do negócio ou de políticas públicas, compõem a primeira linha de defesa, quando se tratar de controles de privacidade e segurança da informação, tendo o Encarregado o papel de apoiar com orientações nas questões que envolvam privacidade e proteção de dados pessoais nos termos do art. 41, da Lei 13.709/2018.

1.3 Abordagem de controles e implementação de cibersegurança

O CIS é uma organização sem fins lucrativos voltada para a comunidade, responsável pelo *CIS Critical Security Controls v8* e *CIS Controls v8 Privacy Companion Guide,* melhores práticas reconhecidas globalmente para proteger sistemas e dados de TI. Lidera uma comunidade global de profissionais de TI para evoluir continuamente esses padrões e fornecer produtos e serviços para proteger proativamente contra ameaças emergentes.

O Guia CIS v.8 adota as funções de Cibersegurança do Framework do NIST como complemento às medidas trazidas no documento. O NIST é uma agência governamental não regulatória da administração de tecnologia do Departamento de Comércio dos Estados Unidos. Na área de segurança Cibernética ela tem como função identificar e desenvolver diretrizes de risco de segurança cibernética para uso voluntário de proprietários e operadores de infraestrutura crítica.

Os controles e medidas de cibersegurança deste **Guia** foram embasados no Guia

CIS Controls v8, o qual compartilha percepções sobre ataques e invasores, identifica as causas básicas e as traduz em classes de ação defensiva. Além disso, o CIS, por meio do seu Guia, mapeia seus controles com estruturas regulatórias e de *compliance*, a fim de garantir o alinhamento e trazer prioridade e foco para eles. Adicionalmente, o CIS identifica, em seu Guia, problemas e barreiras comuns (como avaliação inicial e roteiros de implementação), e os resolve como uma comunidade.

Os Controles CIS são desenvolvidos por uma comunidade de especialistas em TI que aplicam sua experiência em primeira mão como defensores cibernéticos para criar essas melhores práticas de segurança globalmente aceitas. Esses especialistas vêm de uma ampla gama de setores, incluindo varejo, manufatura, saúde, transporte, educação, governo, entre outros.

A aplicação dos controles do CIS consiste em um importante passo de um processo para orientar o programa de melhoria de segurança da instituição, sendo **importante destacar que o documento não se trata de "somente uma lista" de boas práticas que podem ajudar na segurança da instituição, e sim de um documento confiável com recomendações de segurança e suporte de uma comunidade de especialista para tornar os controles implementáveis, utilizáveis, escaláveis e alinhados com todos os requisitos de segurança da indústria ou do governo.**

Vale ressaltar que o TCU considera uma boa prática a implementação dos controles do CIS v8, visto que os utiliza no acompanhamento de controles críticos de segurança cibernética das organizações públicas federais. A implementação desses controles, inicialmente, foi aprovada por meio do Acórdão 1.109/2021-TCU-Plenário (TC 036.620/2020-3, auditoria de *backup/restore* dos órgãos e entidades da APF). Nesse sentido, o TCU mediante o Acórdão 1.768/2022-TCU-Plenário reforçou a adoção dos dezoito controles críticos da versão 8 do CIS a serem gradativamente verificados ao longo de sete ciclos de execução de auditorias nas instituições públicas. Mais detalhes podem ser encontrados em Auditoria de Cibersegurança do TCU.

1.3.1 *CIS Controls - Cibersegurança*

O documento *CIS Critical Security Controls v8*[12] é um conjunto de ações priorizadas que atuam coletivamente na defesa de sistemas e infraestrutura de rede por meio de controles que aplicam as melhores práticas para mitigar os mais comuns tipos

[12] Disponível em: https://www.cisecurity.org/controls

de ataques cibernéticos.

O Guia *CIS Controls v8* é composto de 18 controles que abordam os diversos temas da cibersegurança, tais como: ativos, cópia segura, proteção de dados, contas e acesso, incidentes, vulnerabilidades, monitoramento e auditoria, entre outros.

A estrutura dos controles do CIS apresenta os seguintes elementos:

- Visão geral: Uma breve descrição da intenção do Controle e sua utilidade como ação defensiva;
- Por que este controle é crítico? Uma descrição da importância deste Controle no bloqueio, mitigação ou identificação de ataques, e uma explicação de como os invasores exploram ativamente a ausência deste Controle;
- Medidas de Segurança: uma tabela das ações específicas que as empresas devem realizar para implementar o Controle.

1.3.2 *CIS Guia Complementar de Privacidade*

Quanto à privacidade e proteção de dados pessoais, o CIS por meio do documento CIS *Controls Privacy Guide*[13], tem o objetivo de desenvolver as melhores práticas e orientações para a implementação dos *CIS Critical Security Controls* (*CIS Controls*), levando em consideração os impactos na privacidade e proteção de dados pessoais tratados pela instituição. O Guia apoia os objetivos dos Controles CIS, alinhando os princípios de privacidade e destacando possíveis preocupações referentes à proteção de dados pessoais que possam surgir ao utilizar os Controles CIS.

As orientações apresentadas no CIS *Controls Privacy Guide* contribuem para que a equipe de TI, jurídica ou outras com responsabilidades pela privacidade e proteção de dados pessoais na instituição possam identificar oportunidades e agregar suas considerações previamente na implementação dos controles de cibersegurança em seus sistemas informacionais, abordando a segurança dos dados pessoais por padrão desde a sua concepção. Portanto, recomenda-se a leitura do CIS *Controls Privacy Guide* durante a implementação dos controles e medidas de cibersegurança.

1.3.3 *Grupos de Implementação*

As medidas contidas nos controles do CIS auxiliam a mitigação das

[13] Disponível em: https://www.cisecurity.org/insights/white-papers/cis-controls-v8-privacy-companion-guide

vulnerabilidades dos mais comuns aos mais avançados tipos de ataque. Dessa forma, existem medidas com mais complexidade em serem implementadas do que outras.

O CIS elaborou uma metodologia de implementação das medidas que auxiliam a mitigação das vulnerabilidades numa organização. Essa metodologia consiste em 3 Grupos de Implementação (GI). O primeiro GI representa uma instituição de pequeno a médio porte com limitação no corpo de profissionais em TI e na experiência em cibersegurança. O segundo GI representa uma instituição que emprega indivíduos responsáveis por gerenciar e proteger a infraestrutura de TI. Por fim, o terceiro GI emprega especialistas em segurança especializados nas diferentes facetas da segurança cibernética.

Reforça-se que os três GIs acima tentam criar uma identificação de perfil e ajudar a instituição no amadurecimento das linhas de defesa, de forma gradativa. Esse quadro não impede que medidas de segurança de perfil mais avançado sejam implementados na instituição.

Vale ressaltar que cada GI indica medidas de segurança cibernética que devem ser atendidas e são cumulativas a cada GI avançado.

1.3.4 *NIST Cybersecurity Framework*

O Framework de Cibersegurança do NIST[14] conceitua a Estrutura Básica de Segurança Cibernética. Trata-se de um conjunto de atividades de segurança cibernética que visam a produzir resultados desejados e referências aplicáveis que são comuns em setores de infraestrutura crítica.

A Estrutura Básica consiste em cinco funções simultâneas e contínuas — **Identificar, Proteger, Detectar, Responder** e **Recuperar**. Quando analisadas em conjunto, essas funções fornecem uma visão estratégica de alto nível do ciclo de vida do gerenciamento do risco de segurança cibernética de uma organização.

- **Identificar** - Desenvolver uma compreensão organizacional para gerenciar o risco de segurança cibernética no que tange a sistemas, pessoas, ativos, dados e recursos.

As atividades na função **"Identificar"** são fundamentais para o uso eficiente do Guia de Aperfeiçoamento da Segurança Cibernética para Infraestrutura Crítica[15]. Uma organização é capaz de focar e priorizar seus esforços de forma consistente com sua

[14] Disponível em: https://www.nist.gov/cyberframework/framework
[15] Disponível em: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018pt.pdf

estratégia de gerenciamento de riscos e demandas empresariais, a partir da compreensão do contexto de seu nicho, dos recursos que suportam funções críticas e dos riscos de segurança cibernética envolvidos. Os exemplos de Categorias de resultados dentro desta Função incluem: Gerenciamento de Ativos; Ambiente Empresarial; Governança; Avaliação de Risco; e Estratégia de Gerenciamento de Risco.

- **Proteger** - Desenvolver e implementar proteções necessárias para garantir a prestação de serviços críticos.

A função **"Proteger"** fornece apoio à capacidade de limitar ou conter o impacto de uma possível ocorrência de segurança cibernética. Os exemplos de Categorias de resultados dentro desta Função incluem: Gerenciamento de Identidade e Controle de Acesso; Conscientização e Treinamento; Segurança de Dados; Processos e Procedimentos de Proteção da Informação; Manutenção; e Tecnologia de Proteção.

- **Detectar** - Desenvolver e implementar atividades necessárias para identificar a ocorrência de um evento de segurança cibernética.

A função **"Detectar"** permite a descoberta oportuna de ocorrências de segurança cibernética. Os exemplos de Categorias de resultados dentro desta Função incluem: Anomalias e Ocorrências; Monitoramento Contínuo de Segurança; e Processos de Detecção.

- **Responder** - Desenvolver e implementar atividades apropriadas para agir contra um incidente de segurança cibernética detectado.

A função **"Responder"** suporta a capacidade de conter o impacto de um possível incidente de segurança cibernética. Exemplos de Categorias de resultados dentro desta Função incluem: Planejamento de Resposta; Notificações; Análise; Mitigação; e Aperfeiçoamentos.

- **Recuperar** - Desenvolver e implementar atividades apropriadas para manter planos de resiliência e restaurar quaisquer recursos ou serviços que foram prejudicados devido a um incidente de segurança cibernética.

A função **"Recuperar"** oferece apoio ao restabelecimento pontual para as operações normais de modo a reduzir o impacto de determinado incidente de segurança cibernética. Os exemplos de Categorias de resultados dentro desta Função incluem: Planejamento de Restabelecimento; Aperfeiçoamentos; e Notificações.

1.4 Abordagem de controles e implementação de privacidade

Os controles e medidas de privacidade foram baseados nas principais referências de privacidade disponibilizadas atualmente. Foram utilizadas como base as normas ISO/IEC relativas à privacidade e proteção de dados pessoais e como referência complementar o Framework de Privacidade do NIST publicado em 2020[16]. Todos os controles e medidas presentes nestas duas referências foram correlacionados com a LGPD, considerando também orientações dos Guias publicados pela ANPD.

A ISO/IEC é uma organização internacional não governamental independente, com membros de normalização de vários países. Ela reúne especialistas para compartilhar conhecimento e desenvolver normas internacionais voluntárias, baseadas em consenso e relevantes para o mercado mundial que apoiam a inovação e soluções para os desafios globais. Já a ABNT NBR é um conjunto de normas e diretrizes de caráter técnico que tem como função padronizar processos nacionais e internacionais para a elaboração de produtos e serviços no Brasil.

Dentre os diversos documentos publicados pela ISO/IEC e ABNT NBR este **Guia de Framework de Privacidade e Segurança da Informação** tem como base principal as seguintes publicações: ISO/IEC 29100:2011[17], ISO/IEC 29151:2017[18], ABNT NBR ISO/IEC 27701:2019[19], ISO/IEC 27018:2014[20], ISO/IEC 29134:2017[21] e a ABNT NBR ISO/IEC 29184:2021[22].

Além das publicações ISO/IEC e ABNT NBR mencionadas, o Framework de Privacidade do NIST teve uma contribuição bastante significativa na construção deste **Guia.** O NIST é uma agência governamental não regulatória da administração de tecnologia do Departamento de Comércio dos Estados Unidos que promove a inovação e a competitividade industrial nos EUA (Estados Unidos da América) por meio do avanço da ciência, dos padrões e da tecnologia de medição de forma a aumentar a segurança econômica e melhorar a qualidade de vida. Em relação à privacidade de dados, ela tem como função: o gerenciamento de risco de privacidade por meio da conexão entre a empresa e os responsáveis pela missão, funções e responsabilidades organizacionais,

[16] Disponível em: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020pt.pdf
[17] Disponível em: https://www.iso.org/standard/45123.html
[18] Disponível em: https://www.iso.org/standard/62726.html
[19] Disponível em: https://www.abntcatalogo.com.br
[20] Disponível em: https://www.iso.org/standard/61498.html
[21] Disponível em: https://www.iso.org/standard/62289.html
[22] Disponível em: https://www.abntcatalogo.com.br

e atividades de proteção à privacidade.

1.4.1 *ISO/IEC 29100:2011*

Esta norma internacional fornece uma estrutura de alto nível para a proteção de dados pessoais em sistemas de TI e Tecnologia da Informação e comunicação (TIC). É de natureza geral e coloca os aspectos organizacionais, técnicos e processuais em uma estrutura geral de privacidade.

A estrutura de privacidade trazida por essa norma destina-se a ajudar as organizações a definir seus requisitos de proteção de privacidade relacionados a dados pessoais tratados em um ambiente de TIC:

- especificando uma terminologia de privacidade comum;
- definindo os atores e seus papéis no processamento de dados pessoais;
- descrevendo os requisitos de proteção da privacidade; e
- referenciando princípios de privacidade conhecidos.

A seção 5 dessa norma apresenta os princípios de privacidade organizados em uma estrutura derivada de princípios desenvolvidos por vários países e organizações internacionais. Esses princípios devem ser usados para orientar o projeto, desenvolvimento e implementação de políticas e controles de privacidade. Além disso, eles podem servir como uma linha base no monitoramento e medição de aspectos de desempenho, *benchmarking* e auditoria de programas de gerenciamento de privacidade em uma organização.

Os princípios mencionados acima foram analisados e utilizados na construção dos controles de privacidade deste **Guia**.

1.4.2 *ISO/IEC 29151:2017*

A ISO/IEC 29151:2017 estabelece controles e diretrizes para atender aos requisitos identificados por uma avaliação de risco e impacto relacionado à proteção de dados pessoais.

Em particular, essa norma traz diretrizes baseadas na ISO/IEC 27002:2013[23], levando em consideração os requisitos para o processamento de dados pessoais que podem ser aplicáveis no contexto do(s) ambiente(s) de risco de segurança da informação de uma organização.

[23] Disponível em: https://www.iso.org/standard/54533.html

A ISO/IEC 27002:2013 fornece diretrizes para as organizações sobre a segurança da informação e práticas de gerenciamento. Esta norma foi projetada para ser usada por organizações que pretendem:

- selecionar controles dentro do processo de implementação de um Sistema de Gestão de Segurança da Informação baseado na ISO/IEC 27001[24];
- implementar controles de segurança da informação comumente aceitos;
- desenvolver suas próprias diretrizes de gerenciamento de segurança da informação.

Já a ISO/IEC 27001:2013 apresenta os requisitos para sistemas de gestão da segurança da informação.

A ISO/IEC 29151:2017 apresenta ainda uma extensão de controles voltados especificamente para a proteção de dados pessoais, baseados na ISO/IEC 29100:2011 e é aplicável a todos os tipos e tamanhos de organizações que atuam como controladores de dados pessoais, incluindo instituições públicas e privadas, entidades governamentais e organizações sem fins lucrativos.

A construção deste **Framework** se baseou principalmente na análise do Anexo A da ISO/IEC 29151:2017 que discorre sobre a extensão dos controles voltados para a proteção de dados pessoais.

1.4.3 *ABNT NBR ISO/IEC 27701:2019*

A ABNT NBR ISO/IEC 27701:2019 especifica os requisitos e orientações para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gerenciamento de Informações de Privacidade (SGIP) na forma de uma extensão da ABNT NBR ISO/IEC 27001:2013[25] e ABNT NBR ISO/IEC 27002:2013[26] para gerenciamento de privacidade no contexto da organização.

Esse padrão traz os requisitos relacionados ao SGIP e fornece orientações para que os controladores e operadores de dados pessoais possam aperfeiçoar o programa de governança sobre os dados pessoais sob suas responsabilidades. A ABNT NBR ISO/IEC 27701:2019 é aplicável a todos os tipos e tamanhos de organizações, incluindo instituições públicas e privadas, entidades governamentais e organizações sem fins lucrativos.

[24] Disponível em: https://www.iso.org/standard/54534.html
[25] Disponível em: https://www.abntcatalogo.com.br
[26] Disponível em: https://www.abntcatalogo.com.br

Especificamente, em seus capítulos 7 e 8, a norma ABNT NBR ISO/IEC 27701:2019 traz diretrizes adicionais para controladores e operadores de dados pessoais, abordando os seguintes temas: condições para o tratamento, direitos dos titulares de dados pessoais, *Privacy by Default* e *Privacy by Design e* compartilhamento, transferência e divulgação de dados pessoais. A construção deste **Guia** se baseou principalmente na análise desses capítulos.

1.4.4 *ISO/IEC 27018:2014*

A ISO/IEC 27018:2014 é uma norma internacional sobre privacidade em serviços de computação em nuvem promovido pela indústria. É considerada um adendo à ISO/IEC 27001:2013, o primeiro código de prática internacional para privacidade na nuvem. Ela ajuda os provedores de serviços em nuvem que processam dados pessoais na avaliação de riscos e na implementação de controles para a proteção desses dados.

A ISO/IEC 27018:2014 se apresenta na forma de uma extensão da ISO/IEC 27001:2013 e ISO/IEC 27002:2013 voltada para o contexto de processamento de dados pessoais em nuvem. Ela apresenta ainda uma extensão de controles voltados especificamente para a proteção de dados pessoais em nuvem, baseados na ISO/IEC 29100:2011.

O objetivo dessa norma, quando usada em conjunto com os objetivos e controles de segurança da informação na ISO/IEC 27002:2013, é criar um conjunto comum de categorias e controles de segurança que podem ser implementados por um provedor de serviços de computação em nuvem pública atuando como um operador de dados pessoais.

A construção do **Guia** se baseou principalmente na análise do Anexo A que aborda a extensão dos controles voltados para a proteção dos dados pessoais tratados em nuvem por operadores terceiros.

1.4.5 *ISO/IEC 29134:2017*

A ISO/IEC 29134:2017 é uma norma internacional que fornece diretrizes para um processo de Avaliação de Impacto à Privacidade, estrutura e conteúdo que vai compor o Relatório de Impacto à Proteção de Dados Pessoais (RIPD). Os dois instrumentos são aplicáveis a todos os tipos e tamanhos de organizações e normalmente são conduzidos por uma organização que leva sua responsabilidade a sério ao tratar dados pessoais.

A construção do **Guia** se baseou principalmente na análise de impacto de

privacidade e na confecção do RIPD tratada na norma ISO/IEC 29134:2017 para que as instituições possam atender aos requisitos legais necessários.

1.4.6 *ABNT NBR ISO/IEC 29184:2021*

A ABNT NBR ISO/IEC 29184:2021 apresenta diretrizes que formatam o conteúdo e a estrutura das políticas (avisos) de privacidade *on-line*, bem como o processo de solicitação de consentimento para coletar e tratar dados pessoais dos titulares.

A análise dessa norma auxiliou principalmente na construção de controles voltados para a abertura, transparência e notificação neste **Guia**.

1.4.7 *NIST Privacy Framework*

O NIST Privacy Framework é destinado a ajudar as organizações a identificar e gerenciar o risco de privacidade para criar produtos e serviços inovadores, protegendo a privacidade dos indivíduos. Esse Framework conceitua a Estrutura Básica de Privacidade e aborda um conjunto de funções de privacidade de dados pessoais, resultados desejados e referências aplicáveis que são comuns em setores de infraestrutura crítica.

As funções organizam as atividades fundamentais de privacidade em mais alto nível. Elas ajudam uma organização a expressar a sua gestão do risco de privacidade, ao entender e gerenciar o tratamento de dados, possibilitando decisões concernentes à gestão de risco, e ao determinar como interagir com os indivíduos, além de estabelecer melhorias ao aprender com atividades anteriores.

As funções não foram criadas para serem aplicadas de forma sequencial. Ao contrário, as funções devem ser aplicadas simultânea e continuamente para formar ou aprimorar uma cultura operacional que trate da natureza dinâmica do risco de privacidade.

A Estrutura Básica consiste em cinco funções simultâneas e contínuas — **Identificar-P, Governar-P, Controlar-P, Comunicar-P, Proteger-P**. Quando analisadas em conjunto, essas funções fornecem uma visão estratégica de alto nível do ciclo de vida do gerenciamento do risco de privacidade de uma organização.

- **Identificar-P** - Desenvolve o entendimento organizacional para gerenciar riscos de privacidade dos indivíduos decorrentes do processamento de dados.

As atividades na função **“Identificar-P”** são fundamentais para avaliar as

circunstâncias em que os dados são tratados, entendendo os interesses de privacidade dos indivíduos que são servidos ou afetados direta ou indiretamente por uma instituição, além de realizar avaliações de risco, permite que uma organização entenda o ambiente de negócios em que está funcionando, e identifique e priorize riscos de privacidade.

- **Governar-P** - Desenvolve e implementa a estrutura de governança organizacional para permitir uma compreensão contínua das prioridades de gestão de riscos da organização que são transmitidas pelo risco de privacidade.

A função **"Governar-P"** é fundamental para atividades de nível organizacional, como estabelecer valores e políticas de privacidade, identificar requisitos legais/regulatórios e entender a tolerância ao risco organizacional que permite que uma instituição concentre e priorize esforços que sejam consistentes com a sua estratégia de gestão de riscos e necessidades de negócios.

- **Controlar-P** – Desenvolve e implementa atividades adequadas para permitir que organizações ou indivíduos gerenciem dados com detalhamento suficiente para gerenciar riscos de privacidade.

A função **"Controlar-P"** leva em consideração o gerenciamento do processamento de dados do ponto de vista da organização e do indivíduo.

- **Comunicar-P** – Desenvolve e implementa atividades adequadas para permitir que organizações e indivíduos tenham uma compreensão confiável e permaneçam engajados em um diálogo sobre como os dados são processados, além dos riscos de privacidade a eles associados.

A função **"Comunicar-P"** reconhece que, tanto as organizações quanto os indivíduos gostariam de saber como os dados são processados para gerenciar o risco de privacidade de forma eficaz.

- **Proteger-P** - Desenvolve e implementa medidas para o processamento de dados.

A função **"Proteger-P"** abrange a proteção de dados para evitar eventos de privacidade relacionados à cibersegurança e a sobreposição entre privacidade e gerenciamento de riscos de cibersegurança.

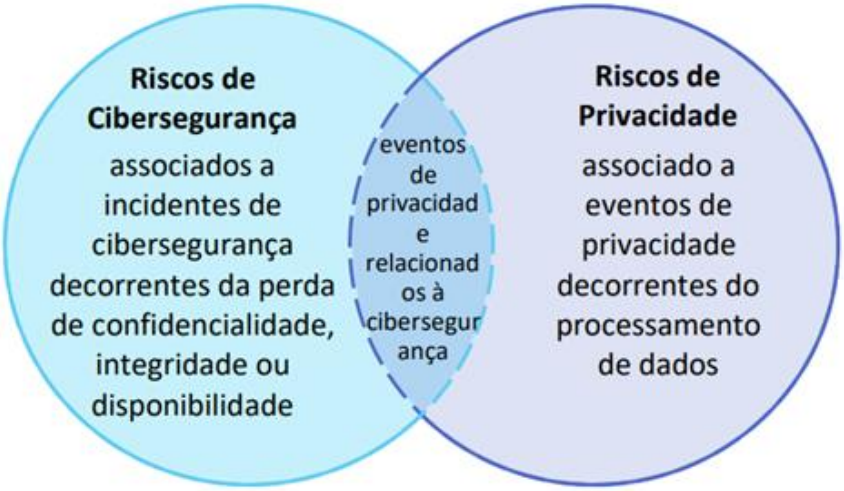
O núcleo do Framework de Privacidade do NIST é composto por Funções, Categorias e Subcategorias. Esses elementos do núcleo trabalham juntos.

As Categorias são as subdivisões de uma função em grupos de resultados de privacidade intimamente ligados às necessidades programáticas e atividades

específicas. Essas Categorias representam grupos de domínios específicos de privacidade e podem ser interpretadas como controles. Já as subcategorias dividem ainda mais uma categoria em resultados específicos de atividades técnicas e/ou de gestão que podem ser interpretadas em ações ou medidas de proteção de dados pessoais e privacidade. Elas fornecem um conjunto de resultados que, embora não sejam completos, ajudam a validar o efeito do que foi encontrado em cada categoria.

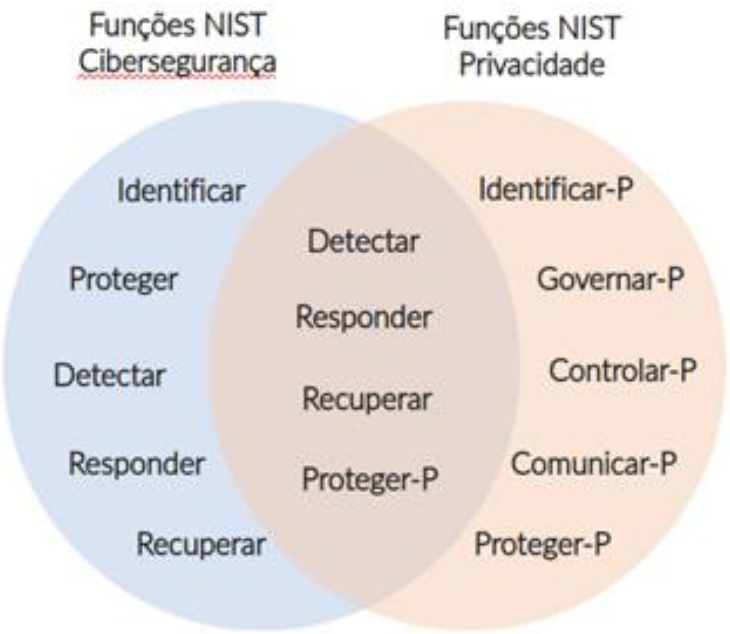
Embora o *Cybersecurity Framework* tenha sido criado para cobrir todos os tipos de incidentes de cibersegurança, ele pode ser usado para alavancar mais apoio à gestão de riscos dos eventos de privacidade, como pode ser visto na Figura 1 abaixo.

Figura 1: RELAÇÃO ENTRE OS RISCOS DE CIBERSEGURANÇA E PRIVACIDADE.



Portanto, existe uma relação entre a área de privacidade e cibersegurança. De acordo com o NIST, a privacidade e a cibersegurança compartilham funções para atender aos eventos de privacidade relacionados à cibersegurança, conforme Figura 2 a seguir.

Figura 2: RELAÇÃO ENTRE AS FUNÇÕES DE CIBERSEGURANÇA E PRIVACIDADE.



1.4.8 *Guias Orientativos da ANPD*

Considerando o papel fundamental da ANPD de orientação e normatização da proteção de dados pessoais, a Autoridade vem elaborando Guias Orientativos com o objetivo de delinear parâmetros que possam auxiliar entidades e órgãos públicos nas atividades de adequação e de implementação da LGPD. As orientações apresentadas no Guia Orientativo de Tratamento de Dados Pessoais pelo Poder Público[27] constituem um primeiro passo no processo de delimitação das interpretações sobre a LGPD aplicáveis ao Poder Público.

Para a construção deste Guia, foram utilizadas as seções “V. Compartilhamento de Dados Pessoais Pelo Poder Público” e “VI. Divulgação de Dados Pessoais”, do Guia Orientativo de Tratamento de Dados Pessoais pelo Poder Público da ANPD. É importante ressaltar que a inclusão destas seções não substitui a leitura desse e de outros Guias da ANPD.

1.5 Estruturação dos controles

Os controles que compõem este **Framework** estão organizados nas seguintes categorias:

[27] Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_tratamento_de_dados_pessoais_pelo_poder_publico___defeso_eleitoral.pdf

- Estruturação básica de gestão em privacidade e segurança da informação:
  - Controle 0;
- Segurança cibernética:
  - Controles de 1 a 18;
- Privacidade:
  - Controles de 19 a 31.

2. CONTROLE DE ESTRUTURAÇÃO BÁSICA DE GESTÃO EM PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

O controle de estruturação básica de gestão em privacidade e segurança da informação visa a atender às ações específicas de conformidade básica estabelecidas na IN SGD/ME nº 94, de 23 de dezembro de 2022, IN CGU nº 3, de 9 de junho de 2017, IN GSI/PR nº 1, de 27 de maio de 2020 e LGPD - Lei nº 13.709, de 14 de agosto de 2018.

A alta administração desempenha papel fundamental na estruturação proposta por este controle, especialmente, no que se refere a garantir que tal estruturação seja estabelecida no órgão ou entidade.

A lista das medidas deste controle consta do Anexo III. Tais medidas focam, em maior parte, nos papeis e estruturas fundamentais para a condução da implementação deste **Framework.**

No próximo capítulo serão abordados os controles de cibersegurança.

3. CONTROLES DE CIBERSEGURANÇA

Neste capítulo, serão apresentados os controles de cibersegurança fundamentados no CIS 8.

Cada seção subsequente apresenta um resumo do controle e o porquê implementá-lo, bem como a aplicabilidade e as implicações (consequências) da implementação do controle para a privacidade.

Mais detalhes sobre a aplicação dos controles de cibersegurança podem ser consultados no Guia *CIS Controls v8* e sobre aspectos de privacidade, especificamente no que se refere aos princípios de privacidade na implementação dos controles CIS, podem ser observados no Guia *CIS Controls Privacy Guide*.

As medidas, em formato de pergunta, a serem aplicadas para cada controle estão detalhadas no Anexo II deste **Guia**. As medidas foram organizadas de acordo com a sequência de funções do *NIST Cybersecurity Framework.* Além disso, foi realizado um mapeamento com os identificadores originais das medidas do *CIS Controls v8.*

3.1 Controle 1: Inventário e Controle de Ativos Institucionais

Gerenciar ativamente (inventariar, rastrear e corrigir) todos os ativos institucionais conectados à rede, com o objetivo de identificar precisamente quais necessitam ser monitorados e/ou protegidos dentro da empresa, mapeando todos os ativos não autorizados para uma possível remoção ou remediação futura.

Por que implementar?

As instituições não podem defender aquilo que não está mapeado ou não se tem conhecimento de sua existência. Por esta razão, ter um inventário de ativos institucionais é essencial para que uma atitude de defesa possa acontecer. Neste intuito o Inventário e Controle de Ativos Institucionais desempenha um papel crítico no monitoramento de segurança, resposta a incidentes, backup e recuperação de sistemas. As organizações devem saber quais dados são essenciais para elas, e a gestão adequada de ativos ajudará a identificar os ativos institucionais que mantêm ou gerenciam esses dados críticos, para que as medidas de segurança apropriadas possam ser aplicadas. Isso também ajudará na identificação de ativos não autorizados e não gerenciados para removê-los ou remediá-los.

Vale ressaltar que entram na lista de ativos:

- dispositivos de usuário final (computador institucional, dispositivos portáteis e móveis);
- dispositivos de rede;
- dispositivos não computacionais;
- dispositivos de *Internet of Things* (IoT);
- Servidores (conectados fisicamente à infraestrutura, virtualmente, remotamente, e aqueles em ambientes de nuvem)

Além disso, as INs GSI/PR nº 1 de 27 de maio de 2020, nº 3 de 28 de maio de 2021, nº 5 de 31 de agosto de 2021 e NCs nº 08 /IN01/DSIC/GSIPR e nº 12 /IN01/DSIC/GSIPR preveem ações a serem observadas e implementadas neste controle.

3.1.1 *Aplicabilidade e Implicações de Privacidade*

Princípios de privacidade devem ser incorporados ao processo de inventário de dispositivos, tanto do ponto de vista tecnológico quanto do processual.

O conhecimento sobre um dispositivo, onde está localizado, quem o está usando e como está usando pode fornecer informações pessoais. Muitas instituições utilizam o nome ou identificador de um indivíduo, que o vincula explicitamente ao dispositivo.

Assim, os inventários de ativos do órgão devem ser tratados com a possibilidade de conter dados pessoais. Em algum momento, é possível que o software de monitoramento e de rastreamento afete a privacidade dos funcionários e a segurança dos dados pessoais.

Fique Atento!

A Secretaria de Governo Digital disponibiliza em seu portal um Modelo de Política de Gestão de Ativos, com enfoque em prover diretrizes para gestão de ativos que constitui referência importante para instituições e profissionais de segurança da informação, que desejam realizar o gerenciamento de ativos da instituição.

Disponível em: Modelo de Política de Gestão de Ativos

3.2 Controle 2: Inventário e Controle de Ativos de Software

Gerenciar ativamente (inventariar, rastrear e corrigir) todo o software na rede para que apenas o software autorizado seja instalado e possa ser executado, e que todo o software não autorizado e não gerenciado seja encontrado e impedido de instalação ou

execução.

Por que implementar?

Um inventário de software completo é um recurso crítico para prevenir ataques. Os atacantes realizam varreduras na infraestrutura do órgão continuamente em busca de versões vulneráveis de software que possam ser exploradas. Contudo, sem um inventário completo dos ativos de software, um órgão não pode determinar se possui software vulnerável ou se há violações de licenciamento em potencial.

É fundamental inventariar, compreender, avaliar e gerenciar todos os softwares conectados à infraestrutura. Além de revisar seu inventário de software para identificar quaisquer ativos executando software que não sejam necessários para suas atividades.

Além disso, as INs GSI/PR nº 1 de 27 de maio de 2020 e nº 3 de 28 de maio de 2021, preveem ações a serem observadas e implementadas neste controle.

3.2.1 *Aplicabilidade e Implicações de Privacidade*

Princípios de privacidade devem ser incorporados ao processo de inventário de software, tanto do ponto de vista tecnológico quanto processual.

Os inventários de software listam softwares autorizados instalados em dispositivos aprovados pela instituição. Esses ativos de software estão diretamente vinculados a indivíduos específicos podendo coletar e manipular seus dados pessoais.

Certos ativos de software podem conter informações sobre funcionários e em algum momento, é possível que o software de monitoramento e rastreamento afete negativamente a privacidade dos funcionários e a segurança dos dados pessoais.

Os tipos de dados comuns coletados para este controle incluem, entre outros, informações sobre o dispositivo, como modelo, proprietário, *Internet Protocol* (IP) e nome do dispositivo.

Essas informações podem ser armazenadas em uma planilha disponível para um administrador de sistema ou hospedadas em um banco de dados local armazenado na rede corporativa.

3.3 Controle 3: Proteção de Dados

Utilizar processos e ferramentas para identificar, classificar, manusear, reter e descartar dados.

Por que implementar?

No momento atual sabemos que os dados podem não estar apenas dentro da estrutura das instituições; podemos ter dados na nuvem, em dispositivos portáteis do usuário final, compartilhados com parceiros ou com serviços *on-line* em qualquer lugar do mundo.

As organizações possuem uma série de dados, que são importantes para o negócio, dentre eles os dados pessoais. O tratamento desses dados deve estar de acordo com as regulamentações de proteção de dados e privacidade pois a não conformidade pode afetar os direitos e garantias dos titulares de dados, além de acarretar prejuízos financeiros e reputacionais.

A proteção de dados está ganhando cada vez mais destaque no cenário global e as organizações estão aprendendo que o respeito ao uso e gestão apropriados de dados são fundamentais, não se restringindo apenas à criptografia. Os dados devem ser gerenciados de maneira adequada em todo o seu ciclo de vida.

A perda de controle da organização sobre os dados protegidos ou sensíveis é um sério e frequente impacto relatado no negócio. A adoção da criptografia dos dados, tanto em trânsito quanto em repouso, pode fornecer mitigação contra o comprometimento dos dados e, ainda mais importante, é um requisito regulatório para a maioria dos dados controlados.

Além disso, as INs GSI/PR nº 1 de 27 de maio de 2020, nº 2 de 5 de fevereiro de 2013, nº 3 de 6 de março de 2013, nº 4 de 26 de março de 2020, nº 5 de 31 de agosto de 2021, nº 6 de 23 de dezembro de 2021 e NCs nº 01/IN02/NSC/GSIPR, e seus anexos (Anexo A e Anexo B), nº 08 /IN01/DSIC/GSIPR, nº 09 /IN01/DSIC/GSIPR e nº 20 /IN01/DSIC/GSIPR, preveem ações a serem observadas e implementadas neste controle.

3.3.1 *Aplicabilidade e Implicações de Privacidade*

A implementação do controle de proteção de dados pode ajudar a proteger uma infinidade de informações em uma rede corporativa, incluindo Informações de

Identificação Pessoais. Sem as medidas listadas aqui, muitas das informações pessoais de clientes estariam em risco de exposição não autorizada.

Estabelecer e manter um Esquema de Classificação de Dados não precisa necessariamente ser realizado de forma automatizada por meio de software, mas os administradores de TI e os responsáveis pela privacidade devem ter um conhecimento geral dos tipos de dados coletados. Os funcionários de TI devem saber como identificar e relatar instâncias de dados pessoais recém-descobertos.

Quaisquer dados armazenados em sistemas em nuvem também devem ser protegidos, e os dados pessoais armazenados devem ser explicitamente entendidos e aprovados. O descarte de dados pessoais armazenados deve ser realizado de maneira segura em consulta com a equipe de segurança da informação da instituição ou com a política existente. Isso deve ser realizado para todos os papéis físicos, mídias digitais e plataformas de IoT e móveis.

3.4 Controle 4: Configuração Segura de Ativos Institucionais e Software

Estabelecer e manter a configuração segura de ativos institucionais (dispositivos de usuário final, incluindo portáteis e móveis; dispositivos de rede; dispositivos não computacionais/*IoT*; e servidores) e software (sistemas operacionais e aplicações).

Por que implementar?

As configurações padrões para ativos e softwares são normalmente voltadas para a facilidade de implantação e uso, em vez da segurança. Controles básicos, serviços e portas abertas, contas ou senhas padrão e pré-instalação de software desnecessário podem ser explorados se deixados em seu estado padrão.

Referente às atualizações de configuração de segurança, elas precisam ser gerenciadas e mantidas ao longo do ciclo de vida dos ativos e software da instituição. Elas precisam ser rastreadas e aprovadas por meio de um processo de fluxo de trabalho de gestão de configuração para manter um registro que pode ser revisado para *compliance*, aproveitado para resposta a incidentes e para apoiar auditorias.

Além disso, as INs GSI/PR nº 4 de 26 de março de 2020, nº 5 de 31 de agosto de 2021 e NCs nº 08 /IN01/DSIC/GSIPR e nº 12 /IN01/DSIC/GSIPR, preveem ações a serem observadas e implementadas neste controle.

3.4.1 *Aplicabilidade e Implicações de Privacidade*

As configurações seguras para ativos institucionais e software podem ajudar a viabilizar a privacidade dos funcionários, evitando violações de dados e invasões de contas. Algumas configurações podem ser vistas como vulnerabilidades absolutas, enquanto outras configurações podem enfraquecer um sistema ou software e torná-lo mais suscetível a um ataque bem-sucedido. Com isso, a maioria das medidas dentro deste controle pode ter um impacto na privacidade quando implementada em uma instituição.

Determinadas configurações de hardware e software podem afetar negativamente a privacidade dos funcionários. Portanto, é necessária uma revisão de privacidade nas definições de configuração para garantir que determinados produtos não armazenem ou transmitam, intencionalmente ou não, dados pessoais de funcionários.

A configuração de determinados ativos e softwares pode fazer com que dados, incluindo dados pessoais, sejam coletados, e estes podem conter informações confidenciais. Os administradores devem entender as configurações e habilitar funções para que essas informações não fiquem desprotegidas.

3.5 Controle 5: Gestão de Contas

Usar processos e ferramentas para atribuir e gerenciar autorização de credenciais para contas de usuário, contas de administrador, contas de serviço para ativos e softwares institucionais.

Por que implementar?

É mais fácil para um agente de ameaça (externo ou interno) obter acesso não autorizado a ativos ou dados da organização usando credenciais de usuário válidas do que “hackeando” o ambiente. Existem várias formas de obter acesso a contas de usuário; como por exemplo:

- senhas fracas;
- contas ainda válidas depois que um colaborador deixa de trabalhar na organização;
- contas de teste;
- contas compartilhadas;
- contas de serviço incorporadas em aplicações para scripts;

- um usuário com a mesma senha que ele usa para uma conta *on-line* que foi comprometida (em um *dump* de senha pública);
- engenharia social em um usuário para fornecer sua senha;
- malware para capturar senhas ou tokens na memória ou na rede.

Contas administrativas ou com privilégio alto são alvos preferenciais porque permitem que atacantes adicionem novas contas ou façam alterações em ativos que podem torná-los mais vulneráveis a ataques. As contas de serviço também são críticas, pois geralmente são compartilhadas entre as equipes, internas e externas à organização e as vezes desconhecidas, apenas para serem reveladas em auditorias de gestão de contas padrão.

Além disso, as INs GSI/PR nº 2 de 5 de fevereiro de 2013 e NCs nº 01/IN02/NSC/GSIPR e seus anexos (Anexo A e Anexo B), preveem ações a serem observadas e implementadas neste controle.

3.5.1 *Aplicabilidade e Implicações de privacidade*

O gerenciamento de contas é aplicável a todos os aplicativos, dispositivos e serviços. Todos os usuários precisarão de uma conta para acessar aplicativos, dispositivos e provedores de serviços internos ou externos.

Em razão disso, medidas devem ser gerenciadas durante o controle de acesso para evitar que, dados pessoais possam vazar por meio da criação, uso e divulgação de credenciais. O armazenamento seguro de informações de contas e outros dados relativos à autenticação também devem ser verificados durante a gestão de contas. Os sistemas que armazenam informações de contas precisam permanecer atualizados em relação aos patches de segurança, garantindo a aplicação dos métodos seguros de armazenamento, de acordo com as práticas de segurança utilizadas para proteger as informações antes de usar qualquer serviço.

3.6 Controle 6: Gestão do Controle de Acesso

Usar processos e ferramentas para criar, atribuir, gerenciar e revogar credenciais de acesso e privilégios para contas de usuário, administrador e serviço para ativos e software institucionais.

Por que implementar?

Deve ser assegurado que os usuários tenham acesso apenas aos dados ou ativos

institucionais apropriados para suas funções e garantir que haja autenticação forte para dados ou funções corporativas críticas ou sensíveis. As contas devem ter apenas a autorização mínima necessária para a função. O desenvolvimento de direitos de acesso consistentes para cada função e a atribuição de funções aos usuários é uma prática recomendada.

Além disso, as INs GSI/PR nº 1 de 27 de maio de 2020, nº 2 de 5 de fevereiro de 2013, nº 5 de 31 de agosto de 2021 e NCs nº 01/IN02/NSC/GSIPR, e seus anexos (Anexo A e Anexo B) e nº 12 /IN01/DSIC/GSIPR, preveem ações a serem observadas e implementadas neste controle.

3.6.1 *Aplicabilidade e Implicações de Privacidade*

O Controle de Gerenciamento de Acesso destina-se a gerenciar grande parte do processo de autenticação e autorização, desde como um usuário acessa um dispositivo até a revogação de credenciais e privilégios de acesso.

As informações de identificação pessoal são frequentemente armazenadas em sistemas de autenticação e autorização. Esses sistemas precisam ser configurados de maneira que preserve a privacidade. Geralmente, o gerenciamento de acesso automatizado é preferido, pois ajuda a evitar exposições acidentais de informações privadas e confidenciais por pessoas. A revogação de direitos deve ser preferencialmente realizada também de forma automatizada.

A falha em controlar o acesso, mesmo de administradores, pode ser um requisito de conformidade ou pode levar a acesso e divulgação não autorizados.

Registros (*Logs*) relativos à sistemas de autenticação e autorização em geral podem registrar ações privadas e consequentemente podem ser usados para comprometer a privacidade. Devido a esse e outros fatores, é uma prática recomendada auditar e verificar regularmente quem tem acesso aos dados de autenticação e autorização e manter esses dados apenas pelo tempo necessário.

Os sistemas de informação que ajudam os administradores a gerenciar direitos e privilégios dentro da organização podem coletar dados pessoais ao cadastrar usuários. Administradores e provedores de serviços terceirizados (operadores, conforme art. 5º, inciso VII da LGPD) geralmente terão acesso a esses dados. Isso também vale para os sistemas de autenticação usados para usuários remotos.

Fique Atento!

A Secretaria de Governo Digital disponibiliza em seu portal um Modelo de Política de Gestão de Controle de Acessos com enfoque em prover diretrizes para controle de acesso que constitui referência importante para instituições e profissionais de segurança da informação, que desejam realizar o gerenciamento dos acessos da instituição.

Disponível em: Modelo de Política de Controle de Acesso

3.7 Controle 7: Gestão Contínua de Vulnerabilidades

Desenvolver um plano para avaliar e rastrear vulnerabilidades continuamente em todos os ativos dentro da infraestrutura da organização, a fim de remediar e minimizar a janela de oportunidade para atacantes. Monitorar as fontes públicas e privadas para novas informações sobre ameaças e vulnerabilidades.

Por que implementar?

Compreender e gerenciar vulnerabilidades em uma rede corporativa é uma atividade contínua, que requer tempo, foco e recursos. Por isso, os profissionais de segurança devem ter informações oportunas de ameaças disponíveis, tais como:

- Atualizações de software;
- Patches;
- Avisos de segurança;
- Boletins de ameaças.

Além de revisar regularmente seu ambiente para identificar essas vulnerabilidades antes que os atacantes o façam e as explorem para obter acesso ao ambiente.

Além disso, a IN GSI/PR nº 4, de 26 de março de 2020 prevê ações a serem observadas e implementadas neste controle.

3.7.1 *Aplicabilidade e Implicações de Privacidade*

Este controle é voltado ao monitoramento de possíveis vulnerabilidades em softwares ou hardwares usados pela instituição. Abrange processos para tomada de decisões com ações proativas e correções naquilo que possa comprometer a privacidade, incluindo ações defensivas.

A combinação do inventário de ativos com as ferramentas e o ecossistema de software usado para varredura de vulnerabilidades podem compartilhar dados pessoais com outras instituições.

Portanto a recomendação do uso de softwares de gerenciamento de vulnerabilidades deve ser usada de modo a coletar somente o necessário uma vez que essas ferramentas podem coletar informações pessoais sem o consentimento do titular.

Fique Atento!

A Secretaria de Governo Digital disponibiliza em seu portal um Guia de Gerenciamento de Vulnerabilidades com enfoque no gerenciamento de vulnerabilidades que constitui uma referência importante para instituições e profissionais de segurança da informação, que desejam realizar a construção de processos para o gerenciamento das vulnerabilidades.

Disponível em: Guia de Gerenciamento de Vulnerabilidades

3.8 Controle 8: Gestão de Registros de Auditoria

Coletar, alertar, analisar e reter logs de eventos com o objetivo de ajudar a detectar, compreender ou se recuperar de um ataque.

Por que implementar?

A coleta e análise de log são procedimentos críticos para que uma organização possa detectar atividades maliciosas rapidamente. Em certas ocasiões, os registros de auditoria são a única evidência de um ataque bem-sucedido.

A gestão de registros de auditoria deve ser mantida em constante monitoramento e uso, porque os atacantes sabem que muitas organizações mantêm logs de auditoria para fins de conformidade, entretanto raramente os analisam. Baseado nesse conhecimento, eles conseguem ocultar sua localização, um software malicioso ou atividades nas máquinas das vítimas. Caso os processos de análise de log sejam

insatisfatórios ou inexistentes, os atacantes às vezes, podem controlar as máquinas das vítimas por meses ou anos sem que sejam percebidos pela organização-alvo.

Além disso, as INs GSI/PR nº 1 de 27 de maio de 2020, nº 4 de 26 de março de 2020, nº 5 de 31 de agosto de 2021 e NCs nº 08 /IN01/DSIC/GSIPR e nº 21 /IN01/DSIC/GSIPR, preveem ações a serem observadas e implementadas neste controle.

Fique Atento!

A Secretaria de Governo Digital disponibiliza em seu portal um Modelo de Política de Gestão de Registros (Logs) de Auditoria com o objetivo de prover diretrizes para a gestão de registros de auditoria, uma referência importante para instituições e profissionais de segurança da informação, que desejam realizar a gestão dos registros (logs).

Disponível em: Modelo de Política de Gestão de Registros (Logs) de Auditoria

3.8.1 *Aplicabilidade e Implementações de Privacidade*

Os logs são muito úteis, tanto para desenvolvedores quanto para equipe de TI, na melhoria e na solução de problemas, porém podem armazenar informações pessoais, trazendo implicações para privacidade.

Eles podem conter todo tipo de informação pessoal (nomes, e-mails etc). Para evitar isso, deve ser definido um processo de gerenciamento de log de auditoria que leve em consideração a privacidade e, além disso, deve ser acordado previamente como estes logs serão tratados por terceiros (operadores, conforme art. 5º, inciso VII da LGPD).

Medidas de segurança devem ser aplicadas como por exemplo criptografia e controle de acesso a fim de evitar violações. A proteção no armazenamento também deve ser considerada com ações defensivas incluindo ambientes terceirizados devidamente e explicitamente acordados.

3.9 Controle 9: Proteções de E-mail e Navegador Web

Melhorar as proteções e detecções de vetores de ameaças de e-mail e web, pois são oportunidades para atacantes manipularem o comportamento humano por meio do engajamento direto.

Por que implementar?

Navegadores Web e clientes de e-mail são pontos de entrada muito comuns para atacantes em virtude de sua interação direta com usuários dentro das instituições.

Conteúdos podem ser criados para atrair ou enganar os usuários para que revelem suas credenciais, forneçam dados sensíveis ou forneçam um canal aberto onde os atacantes obtenham acesso, aumentando assim o risco para a corporação.

Além disso, a IN GSI nº 1, de 27 de maio de 2020 prevê ações a serem observadas e implementadas neste controle.

3.9.1 *Aplicabilidade e Implicações de Privacidade*

As medidas deste controle podem ajudar a proteger os dados pessoais, e devem ser cuidadosamente consideradas para que:

- Extensões de navegador não cometam ações maliciosas ou até mesmo a coleta de informações pessoais desnecessárias.
- Filtros de *Uniform Resource Locator* - URL ajudam a impedir acessos a recursos de rede e outros tipos acessos indevidos, além de rastrear os recursos acessados ou de tentativas realizadas pelos usuários.
- Os servidores de e-mail não retenham informações por muito tempo, pois podem agravar o risco de violação de dados.
- Os Servidores de DNS - *Domain Name System* (Sistema de Nomes de Domínio) que manipulam dados de natureza sensível, sejam dados em trânsito ou dados armazenados, devem ser adequadamente protegidos.

3.10 Controle 10: Defesas Contra Malware

Impedir ou controlar a instalação, disseminação e execução de aplicações, códigos ou scripts maliciosos em ativos da organização.

Por que implementar?

Os softwares maliciosos estão em constante evolução e adaptação. Os ataques ocorrem por meio de vulnerabilidades em dispositivos de usuário final e geralmente depende do comportamento inseguro do usuário, como clicar em links, abrir anexos, instalar software ou perfis, ou inserir unidade flash USB (*Universal Serial Bus*).

As defesas contra malware devem ser capazes de operar neste ambiente dinâmico por meio de automação, atualização rápida e oportuna e integração com outros processos, como gestão de vulnerabilidade e resposta a incidentes. Eles devem ser implantados em todos os possíveis pontos de entrada e ativos institucionais para detectar, impedir a propagação ou controlar a execução de software ou código malicioso.

Além disso, a IN GSI/PR nº 5, de 31 de agosto de 2021 e a NC nº 08 /IN01/DSIC/GSIPR, preveem ações a serem observadas e implementadas neste controle.

3.10.1 *Aplicabilidade e Implicações de Privacidade*

A implementação das medidas de segurança contra malware contidas neste controle podem evitar que um malware instalado em um sistema possa coletar informação de identificação pessoal.

Os logs e alertas do software *antimalware* defensivo devem ser armazenados em um local seguro e o acesso deve ser restrito para evitar roubo ou vazamento de dados pessoais que tenham sido coletados.

3.11 Controle 11: Recuperação de Dados

Criar e manter práticas de recuperação de dados que sejam capazes de restaurar os ativos da organização para um estado pré-incidente ou o estado mais confiável possível.

Por que implementar?

Os órgãos precisam de muitos tipos de dados para tomar decisões de negócios e, quando esses dados não estão disponíveis ou não são confiáveis, eles podem impactar o órgão.

Quando os atacantes comprometem os ativos, fazem alterações nas configurações, adicionam contas e, frequentemente, adicionam softwares ou scripts, essas alterações nem sempre são fáceis de identificar, podendo incluir, adicionar ou alterar entradas de registro, abrir portas, desligar serviços de segurança, excluir logs ou outras ações maliciosas que tornam o sistema inseguro. Nem toda ação precisa ser maliciosa; erros humanos também podem causar os mesmos danos. Portanto, é importante ter a capacidade de ter backups ou espelhos recentes para recuperar ativos

e dados institucionais de volta a um estado confiável conhecido.

Vale ressaltar também o aumento exponencial de *ransomware*, caso em que o atacante realiza a criptografia dos dados de um órgão em uma forma de “sequestro” e em seguida exige um resgaste para restauração ou para não divulgação e venda dos dados. Nesta situação, um backup recente não comprometido seria útil para recuperar o sistema a um estado confiável, porém o risco de venda ou divulgação dos dados criptografados continuaria.

Além disso, as IN GSI/PR nº 3 de 28 de maio de 2021, nº 3 de 6 de março de 2013 e a NC nº 09 /IN01/DSIC/GSIPR, preveem ações a serem observadas e implementadas neste controle.

3.11.1 *Aplicabilidade e Implicações de Privacidade*

A aplicação deste controle destina-se a auxiliar a instituição na preparação para a recuperação de um incidente cibernético. Existem preocupações de privacidade com muitas medidas de segurança dentro deste controle.

A equipe de TI precisará criar backups das informações corporativas como parte desse controle. Informações de identificação pessoal contidas em registros precisarão ter backup.

Testar se os backups podem realmente ser restaurados é uma parte importante do processo de recuperação de dados.

A restauração de backups durante o teste deve ser feita com cuidado. Se os dados confidenciais forem restaurados, esse sistema deve ser devidamente protegido e excluído com segurança após a conclusão do exercício.

Fique Atento!

A Secretaria de Governo Digital disponibiliza em seu portal um Modelo de Política de Backup com enfoque em prover diretrizes para as políticas de backup e restauração de dados digitais que constitui referência importante para instituições e profissionais de segurança da informação, que desejam realizar a construção das políticas de backup e restauração de dados digitais da instituição.

Disponível em: Modelo de Política de Backup

3.12 Controle 12: Gestão da Infraestrutura de Rede

Estabeleça, implemente e gerencie ativamente (rastreie, reporte, corrija) os dispositivos de rede, a fim de evitar que atacantes explorem serviços de rede e pontos de acesso vulneráveis.

Por que implementar?

A infraestrutura de rede segura é uma defesa essencial contra os ataques. Isso inclui uma arquitetura de segurança apropriada, abordando vulnerabilidades que são, muitas vezes, introduzidas com configurações padrão, monitoramento de alterações e reavaliação das configurações atuais.

Neste caso, a segurança da rede deve estar em constante mudança, o que exige uma reavaliação regular dos diagramas de arquitetura, configurações, controles de acesso e fluxos de tráfego permitidos, de forma a evitar que os atacantes tirem proveito das configurações de dispositivos de rede que se tornam menos seguras com o tempo.

Além disso, a IN GSI/PR nº 4, de 26 de março de 2020 prevê ações a serem observadas e implementadas neste controle.

3.12.1 *Aplicabilidade e Implicações de Privacidade*

A aplicação deste controle visa a garantir que a infraestrutura de rede seja mantida e configurada adequadamente durante todo o seu ciclo de vida.

O design e a segmentação de rede inadequados podem levar a menores graus de privacidade para usuários da rede corporativa. A falha em documentar as decisões destinadas a melhorar a privacidade pode prejudicar os desenvolvimentos futuros em um programa de privacidade em expansão.

Logs relacionados a sistemas de autenticação e autorização em geral podem registrar dados privados. A coleta dessas entradas de log pode ser benéfica para os esforços de investigação durante a resposta a incidentes; no entanto, eles também podem ser usados para comprometer a privacidade. Devido a esse e outros fatores, é uma prática recomendada auditar e verificar regularmente quem tem acesso aos dados pessoais registrados em logs relacionados a sistemas de autenticação e autorização.

3.13 Controle 13: Monitoramento e Defesa da Rede

Implementar processos e ferramentas para que a organização estabeleça o monitoramento e a defesa de rede contra ameaças de segurança em toda a sua

infraestrutura de rede e base de usuários.

Por que implementar?

Não podemos confiar que as defesas da rede sejam perfeitas. Os adversários continuam a evoluir e amadurecer à medida que compartilham ou vendem informações.

As ferramentas de segurança somente são eficazes se oferecerem suporte a um processo de monitoramento contínuo que permita à equipe ser alertada e responder rapidamente a incidentes de segurança.

Ter uma consciência situacional abrangente aumenta a velocidade de detecção e resposta, que é fundamental para minimizar um possível impacto negativo para o órgão, por exemplo, ao responder rapidamente quando um *malware* é descoberto, credenciais são roubadas ou quando dados sensíveis são comprometidos.

Além disso, as IN GSI/PR nº 4 de 26 de março de 2020, nº 5 de 31 de agosto de 2021 e NCs nº 08 /IN01/DSIC/GSIPR e nº 12 /IN01/DSIC/GSIPR, preveem ações a serem observadas e implementadas neste controle.

3.13.1 *Aplicabilidade e Implicações de Privacidade*

A visibilidade da rede permite entender os tipos e a frequência dos ataques enfrentados pela instituição. Para tal, as medidas de segurança e o monitoramento de rede desse controle se concentram na instalação, configuração e monitoramento de software que auxiliam nessas atividades. Essas soluções poderão ter acessos privilegiados às informações na rede que podem ter implicações de privacidade de dados pessoais.

As empresas devem garantir que as ferramentas SIEM – *Security Information and Event Management (Gerenciamento e Correlação de Eventos de Segurança)* - não estejam alertando regularmente sobre informações que contenham dados pessoais e, portanto, sejam enviados aos analistas de segurança para revisão manual. Tal configuração será diferente das soluções SIEM que alertam a TI sobre a existência de informações pessoais e senhas em texto simples.

As informações de tráfego de rede coletadas pelo IDS - *Intrusion Detection System* (Sistema de Detecção de Intrusão), IPS - *Intrusion Prevention System* (Sistema de Prevenção de Intrusão) e *softwares* de filtragem de aplicativos, juntamente com alertas gerados a partir de uma variedade de fontes, devem ser armazenadas e protegidas

adequadamente para evitar um vazamento de dados que possam conter dados pessoais.

3.14 Controle 14: Conscientização e Treinamento de Competências sobre Segurança

Implantar e manter um programa de conscientização de segurança que possa influenciar e conscientizar o comportamento dos colaboradores, tornando-os devidamente qualificados e assim atingir o objetivo de reduzir riscos de segurança cibernética da organização.

Por que implementar?

As ações das pessoas podem causar incidentes, intencionalmente ou não. É mais fácil para um atacante induzir um usuário a clicar em um link ou abrir um anexo de e-mail para instalar malware e entrar na rede de uma organização, do que fazer um *exploit* de rede diretamente. Nenhum programa de segurança pode lidar com o risco cibernético de maneira eficaz sem um meio de lidar com essa vulnerabilidade humana fundamental. Cada usuário do órgão em qualquer nível tem riscos diferentes.

Os treinamentos e conscientizações devem ser atualizados regularmente. Isso aumentará a cultura de segurança.

Além disso, a IN GSI/PR nº 6, de 23 de dezembro de 2021 e NCs nº 08 /IN01/DSIC/GSIPR, nº 17 /IN01/DSIC/GSIPR e nº 18 /IN01/DSIC/GSIPR, preveem ações a serem observadas e implementadas neste controle.

3.14.1 *Aplicabilidade e Implicações de Privacidade*

A aplicação deste controle destina-se a garantir que os colaboradores recebam treinamento de segurança direcionado para suas funções e responsabilidades específicas, mas devido ao escopo deste **Guia de Framework de Privacidade e Segurança da Informação** este controle deve levar em consideração o treinamento através da lente de conscientização de privacidade.

Administradores de TI com acessos privilegiados podem tomar decisões ruins se não forem treinados sobre o uso apropriado de seus acessos e as consequências de violações de dados sigilosos e de dados pessoais.

Os usuários e provedores de serviços devem entender os requisitos de privacidade e proteção de dados pessoais exigidos pela organização e como proteger esses dados. Cabe ao controlador comunicar os requisitos de privacidade e garantir que eles sejam

atendidos.

3.15 Controle 15: Gestão de Provedor de Serviços

Com o objetivo de garantir a proteção das informações, sistemas e processos críticos da organização, estabeleça um processo para avaliar os provedores de serviços que operem e mantenham estes ativos da organização.

Por que implementar?

Normalmente as organizações contam com fornecedores e parceiros para ajudar a gerenciar seus dados ou contam com infraestrutura de terceiros para aplicações ou funções essenciais.

Violações de terceiros costumam impactar significativamente uma organização, como por exemplo os ataques de *ransomware* que podem ser realizados indiretamente, quando há um bloqueio de um de seus provedores de serviço, causando a interrupção nos negócios, ou diretamente, criptografando os dados da organização.

A maioria das regulamentações de segurança, privacidade e proteção de dados exigem que sua proteção seja estendida a prestadores de serviços terceirizados. A confiança de terceiros é uma função central de Governança, Riscos e *Compliance* (GRC), pois os riscos que não são gerenciados dentro da organização são transferidos para entidades fora da organização.

Além disso, as IN GSI/PR nº 3 de 6 de março de 2013, nº 4 de 26 de março de 2020, nº 5 de 31 de agosto de 2021 e NC nº 09 /IN01/DSIC/GSIPR, preveem ações a serem observadas e implementadas neste controle.

3.15.1 *Aplicabilidade e Implicações de Privacidade*

Algumas instituições utilizam os provedores de serviços em nuvem para e-mail ou armazenamento. Este controle abrange as ações que devem ser tomadas para garantir que os provedores de serviços terceirizados estejam protegendo adequadamente os dados de seus clientes e seus próprios sistemas. As medidas recomendadas para este controle incluem entender quais provedores de serviços estão em uso, quais tipos de dados eles armazenam e monitorar seu desempenho. Considere escolher fornecedores que tenham certificações de privacidade ou alguma outra auditoria independente de suas próprias práticas de privacidade.

Os provedores de serviços (operadores, conforme art. 5º, inciso VII da LGPD)

podem utilizar, vender ou compartilhar dados pessoais obtidos por meio de seus clientes.

Os dados pessoais podem ser fornecidos diretamente como parte de uma função comercial ou criados por meio do uso de um produto ou serviço, como firewalls ou outros dispositivos de rede.

Provedores de serviços ao coletar e utilizar os dados pessoais, devem declará-los claramente nos acordos de nível de serviço – SLAs *(Service Level Agreement)*. Controles de segurança relacionados aos dados pessoais também devem ser explicitamente escritos e acordados antes do uso.

3.16 Controle 16: Segurança de Aplicações

Gerenciar o ciclo de vida de segurança de todos os softwares desenvolvidos e adquiridos internamente, a fim de prevenir, detectar e corrigir falhas de segurança.

Por que implementar?

As organizações usam aplicações para gerenciar seus dados mais sensíveis e controlar o acesso aos recursos do sistema. Na ausência de credenciais, um atacante pode usar a própria aplicação para comprometer os dados, em vez de uma sequência elaborada de invasão de rede e sistema que tenta desviar dos controles e sensores de segurança da rede.

As aplicações de hoje são desenvolvidas, operadas e mantidas em um ambiente altamente complexo, diverso e dinâmico, sendo executadas em várias plataformas: web, móvel, nuvem etc., com arquiteturas de aplicações que são mais complexas do que as estruturas legadas de cliente/servidor ou servidor de banco de dados web.

As vulnerabilidades de aplicação podem estar presentes por vários motivos: design inseguro, infraestrutura insegura, erros de codificação, autenticação fraca e falha no teste para condições incomuns ou inesperadas. Os atacantes podem explorar vulnerabilidades específicas, incluindo buffer overflows, exposição à *Structured Query Language* (SQL) *injection*, *cross-site scripting*, falsificação de solicitações entre sites e *click-jacking* de código para obter acesso a dados sensíveis ou assumir o controle de ativos vulneráveis dentro da infraestrutura como um ponto de partida para novos ataques. Aplicações e sites também podem ser usados para coletar credenciais, dados ou tentar instalar malware nos dispositivos de usuários que os acessam.

Atualmente é mais comum adquirir plataformas de *Saas - Software as a Service*

(Software como um Serviço), nas quais o *software* é desenvolvido e gerenciado inteiramente por terceiros. Isso traz desafios para as organizações que precisam saber quais riscos estão aceitando na utilização do serviço.

Além disso, as IN GSI/PR nº 3 de 6 de março de 2013, nº 5 de 31 de agosto de 2021 e NC nº 09 /IN01/DSIC/GSIPR, preveem ações a serem observadas e implementadas neste controle.

3.16.1 *Aplicabilidade e Implicações de Privacidade*

A aplicação do controle se concentra principalmente nos esforços que desenvolvedores de software podem realizar para evitar vulnerabilidades exploráveis em seu código, que podem levar à exposição não autorizada de dados pessoais. A maioria das medidas contidas neste controle não está diretamente relacionada à proteção de dados pessoais. Bibliotecas de software de terceiros e APIs - *Application Programming Interface* (Interfaces de Programação de Aplicativos) podem coletar informações por meio de seu uso. Os dados que esses componentes de terceiros podem coletar devem ser claramente declarados nos *SLAs*. Os controles de segurança relacionados aos dados pessoais também devem ser explicitamente escritos e acordados com fornecedores de componentes de terceiros antes do uso.

Todos os desenvolvedores devem ser treinados sobre os requisitos de privacidade relativos ao tratamento de dados pessoais e como incluir privacidade no design, uma vez que bibliotecas de software de terceiros, componentes, APIs e *logs* dos sistemas podem coletar e armazenar dados pessoais. Os dados que estes componentes de terceiros podem coletar devem ser claramente indicados nos *SLAs*.

Fique Atento!

A Secretaria de Governo Digital disponibiliza em seu portal três Guias voltados ao desenvolvimento seguro que apresentam instruções claras sobre tema.

Disponíveis em:

Guia de Requisitos Mínimos de Privacidade e Segurança da Informação para Aplicações Web

Guia de Requisitos Mínimos de Privacidade e Segurança da Informação para APIs

Guia de Requisitos Mínimos de Privacidade e Segurança da Informação para

Aplicativos Móveis

3.17 Controle 17: Gestão de Resposta a Incidentes

Proteger as informações e a reputação da organização, desenvolvendo e implementando uma infraestrutura de resposta a incidentes (por exemplo: planos, definição de papéis, treinamento, comunicações, gerenciamento de supervisão) para descobrir um ataque de forma ágil, e depois, conter efetivamente o impacto, eliminar a presença do atacante, e restaurar a integridade da rede e dos sistemas da organização.

Por que implementar?

Um programa abrangente de segurança cibernética inclui proteções, detecções, resposta e recursos de recuperação. O objetivo principal da resposta a incidentes é identificar ameaças na organização, responder a elas antes que possam se espalhar e remediá-las antes que possam causar danos. É necessário entender todo o escopo de um incidente, como aconteceu e o que pode ser feito para evitar que aconteça novamente, com o objetivo de solucionar o incidente de forma eficiente.

Quando ocorre um incidente, se uma organização não tem um plano documentado - mesmo com boas pessoas - é quase impossível saber os procedimentos de investigação corretos, relatórios, coleta de dados, responsabilidade de gestão, protocolos legais e estratégia de comunicação que permitirão a organização entender, gerenciar e recuperar com sucesso.

Junto com a detecção, contenção e erradicação, a comunicação com as partes interessadas é fundamental. Se quisermos reduzir a probabilidade de impacto material devido a um evento cibernético, a liderança da organização deve saber qual o impacto potencial que pode haver, para que possam ajudar a priorizar as decisões de remediação ou restauração que melhor apoiem a organização. Essas decisões de negócios podem ser baseadas em conformidade regulatória, regras de divulgação, acordos de nível de serviço com parceiros ou clientes, receita ou impactos de missão.

Além disso, as INs GSI/PR nº 1 de 27 de maio de 2020, nº 2 de 24 de julho de 2020, nº 3 de 28 de maio de 2021, nº 4 de 26 de março de 2020 e NCs nº 05 /IN01/DSIC/GSIPR, e seu anexo e nº 08 /IN01/DSIC/GSIPR, preveem ações a serem observadas e implementadas neste controle.

3.17.1 *Aplicabilidade e Implicações de Privacidade*

A aplicação do controle auxilia as instituições no planejamento e na resposta a um incidente cibernético. Existem dois aspectos de privacidade do controle. O primeiro é como responder a um incidente de privacidade. O segundo é como manter a privacidade de todos os indivíduos ao responder a um incidente cibernético.

As equipes de resposta a incidentes ao longo de suas funções, podem ter acesso a dados pessoais, então eles podem manipular de forma inadequada essas informações.

Os membros da equipe de resposta a incidentes coletarão informações de vários sistemas em toda a rede corporativa enquanto realizam suas funções para entender a maneira e o escopo de uma intrusão.

Todos os dados coletados durante as atividades de resposta a incidentes precisam ser protegidos, pois geralmente são dados pessoais, mas também podem ser necessários para procedimentos legais futuros.

Fique Atento!

A Secretaria de Governo Digital disponibiliza em seu portal um Guia de Resposta a Incidentes de Segurança, com enfoque em incidentes que envolvam dados pessoais, que constitui referência importante para instituições e profissionais de segurança da informação, que desejam realizar o tratamento de incidentes cibernéticos.

Disponível em: Guia de Resposta a Incidentes de Segurança

3.18 Controle 18: Testes de Invasão

Testar a eficácia e a resiliência dos ativos institucionais por meio da identificação e exploração de fraquezas nos controles de segurança e da simulação das ações e objetivos de um atacante.

Por que implementar?

Uma postura defensiva bem-sucedida requer um programa abrangente de políticas e governança eficazes, fortes defesas técnicas, combinadas com a ação apropriada das pessoas. Em um ambiente complexo onde a tecnologia está em constante evolução e novas técnicas dos atacantes aparecem regularmente, as organizações devem testar periodicamente seus controles para identificar lacunas e

avaliar sua resiliência. Este teste pode ser da perspectiva de rede externa, rede interna, aplicação, sistema ou dispositivo. Pode incluir engenharia social de usuários ou desvios de controle de acesso físico.

Testes de invasão independentes podem fornecer percepções valiosas e objetivas sobre a existência de vulnerabilidades em ativos institucionais e humanos, e a eficácia das defesas e controles de mitigação para proteger contra impactos adversos para a organização. Eles fazem parte de um programa abrangente e contínuo de gestão e aprimoramento de segurança. Eles também podem revelar fraquezas do processo, como gestão de configuração ou treinamento do usuário final incompletos ou inconsistentes.

3.18.1 *Aplicabilidade e Implicações de Privacidade*

A aplicação do controle tem como objetivo simular efetivamente as ações de um invasor externo e/ou interno em um ambiente corporativo. Isso pode incluir a exploração de uma fraqueza ou vulnerabilidade em um sistema ou rede. Muitas das medidas dentro do controle contêm impactos de privacidade de dados pessoais que podem ser mitigados por meio de políticas e acordos claramente escritos antes que qualquer teste seja realizado.

Como parte do processo de teste, informações pessoais podem ser obtidas pelos testadores de invasão.

Quaisquer dados coletados por testadores de invasão ao longo de seu envolvimento devem ser bem protegidos. Ambas as organizações devem concordar com as técnicas de descarte de dados.

Os dados obtidos por testadores de invasão não devem ser compartilhados. Caso ocorra o compartilhamento, os testadores de invasão devem notificar rapidamente a organização.

4. CONTROLES DE PRIVACIDADE

Neste capítulo serão apresentados os controles de privacidade, ressaltando a importância de sua implementação.

As medidas, em formato de pergunta, a serem aplicadas para cada controle estão detalhadas no Anexo V deste **Guia**.

4.1 Controle 19: Inventário e Mapeamento

As operações de tratamento de dados pessoais por sistemas, produtos, processos ou serviços devem ser identificadas e inventariadas.

Por que implementar?

De acordo com o art. 37 da LGPD o controlador e o operador devem manter registradas as operações de tratamento de dados pessoais que realizam, especialmente quando baseadas no legítimo interesse.

O Registro de Operações de tratamento de dados pessoais representa uma operação importante de governança de dados pessoais e de subsídio para avaliação de impacto à proteção de dados pessoais com vistas a verificar a conformidade da instituição no que se refere ao preconizado pela LGPD.

Um modo de manter os registros de tratamento de dados pessoais é manter um inventário ou uma lista das atividades de tratamento que a organização realiza.

A atividade contempla os processos de negócio que realizam tratamento de dados pessoais, bem como o Inventário de Dados Pessoais (IDP) que aborda, por exemplo:

- agentes de tratamento (Controlador e Operador);
- encarregado;
- finalidade e hipótese do tratamento;
- compartilhamento dados pessoais;
- transferência internacional;
- propósitos para o tratamento;
- uma descrição das categorias dos dados pessoais e dos titulares de dados pessoais tratados pela instituição (por exemplo, crianças);
- o tempo de retenção dos dados pessoais;
- uma descrição geral das medidas de segurança técnica e organizacional.

Fique Atento!

A Secretaria de Governo Digital disponibiliza em seu portal um Guia de Inventário de Dados Pessoais, que incentiva a adoção de registros das operações de tratamento de dados pessoais e suas respectivas avaliações, sob a ótica dos princípios da LGPD e contém importantes instruções para que as instituições e seus colaboradores possam elaborar um inventário de dados pessoais.

Disponível em: Guia de Elaboração de Inventário de Dados Pessoais

4.2 Controle 20: Finalidade e Hipóteses Legais

A organização deve identificar, especificar e documentar as finalidades, hipóteses de tratamento e bases legais que fundamentam as atividades de tratamento de dados pessoais e dados pessoais sensíveis.

Por que implementar?

A partir da promulgação da LGPD não é mais possível tratar dados pessoais com finalidades genéricas. Determinar a finalidade específica do tratamento de dados, junto com a hipótese de tratamento e as bases legais que fundamentam o tratamento, significa realizá-lo para propósitos legítimos, específicos, explícitos e informados ao titular, ou seja, os órgãos devem justificar para qual finalidade usarão cada um dos dados pessoais coletados.

O princípio da finalidade previsto no art. 6°, inciso I da LGPD estabelece que o tratamento de dados pessoais pelo Poder Público deve estar sempre associado a uma finalidade pública, que seja **legítima, específica, explícita e informada.** Da mesma forma, o princípio da adequação presente no art. 6°, inciso II da LGPD estabelece que o tratamento esteja compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

Especificar as finalidades para as quais os dados pessoais são tratados permite garantir que o processamento dos dados pessoais esteja em conformidade com a LGPD e esteja fundamentado em uma base legal permitida.

Para que o tratamento de dados pessoais possa acontecer, é necessário estar amparado em uma das hipóteses legais previstas no art. 7° e 11 da LGPD. Tais hipóteses são as diretrizes gerais que autorizam a atividade de tratamento de dados

por qualquer controlador.

Além disso, para que o órgão possa tratar os dados pessoais, a LGPD, em seu art. 7°, inciso III e art. 11, inciso II, alínea b, determina que ao executar uma política pública, esta deve estar prevista em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres.

Importante ressaltar que a especificação da finalidade e a identificação da hipótese de tratamento e a base legal que respalda a política pública deve acontecer antes que o tratamento de dados pessoais seja realizado.

Por fim, o princípio da finalidade estabelece uma limitação ao tratamento posterior dos dados pessoais. Assim, eventual uso secundário dos dados pessoais somente pode ser realizado para uma finalidade que seja compatível com a finalidade original do tratamento desses dados.

4.3 Controle 21: Governança

A governança em privacidade estabelece uma metodologia abrangente que influenciará permanentemente os processos de tomada de decisão com base em riscos de impacto à privacidade e melhorias contínuas na maturidade.

Por que implementar?

A LGPD estabelece no Art. 50 que os controladores e operadores, no âmbito de suas competências, poderão formular regras de boas práticas e de governança que definam as condições de organização, bem como, o regime de funcionamento, procedimentos e outras ações referentes à governança em privacidade e proteção de dados pessoais.

As organizações devem implementar medidas apropriadas para estabelecer uma governança eficiente relacionada ao processamento de dados pessoais.

Para aumentar a confiança de todas as partes interessadas é necessário que os gestores do gerenciamento de segurança, proteção de dados pessoais e risco ampliem tanto a frequência quanto a amplitude da comunicação, para assim assegurar que o uso dos dados pessoais seja granular, com finalidades específicas e com riscos mapeados e sob controle.

Uma das ações importantes a ser observada no âmbito da governança é a implementação de um programa de governança em privacidade que demonstre o

comprometimento das partes envolvidas em adotar processos e políticas internas que assegurem o cumprimento, de normas e boas práticas relativas à proteção de dados pessoais.

Fique Atento!

A Secretaria de Governo Digital disponibiliza em seu portal um Guia de Boas Práticas da LGPD e um Guia de Elaboração de um Programa de Governança em Privacidade que apresenta os principais pontos da LGPD, fornecendo os subsídios para a criação de um programa institucional de gerenciamento de privacidade.

Disponível em:

Guia de Boas Práticas da LGPD

Guia de Elaboração de um Programa de Governança em Privacidade

4.4 Controle 22: Políticas, Processos e Procedimentos

Definir, desenvolver, divulgar, implementar e atualizar políticas, processos e procedimentos operacionais, internos e externos que regem as ações relativas à proteção de dados pessoais e privacidade, e controles para programas, sistemas de informação ou tecnologias que envolvam o tratamento de dados pessoais.

Por que implementar?

O art. 50 da LGPD prevê que os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

O órgão deve desenvolver e implementar políticas, processos e procedimentos para gerenciar e monitorar os requisitos regulatórios, legais, de risco, ambientais e operacionais da organização que sejam compreendidos para informar a administração sobre o gerenciamento dos riscos que impactam na privacidade e proteção de dados

pessoais.

4.5 Controle 23: Conscientização e Treinamento

As pessoas envolvidas no tratamento de dados são instruídas e conscientizadas sobre privacidade, sendo treinadas para desempenhar suas funções e responsabilidades relacionadas à privacidade de acordo com as políticas, processos, procedimentos, acordos e valores de privacidade da organização.

Por que implementar?

Tendo como base o disposto previsto no art. 50 da LGPD, os controladores e operadores, no âmbito de suas competências, devem aplicar medidas educativas periódicas apropriadas para as pessoas que têm acesso aos dados pessoais. O programa de treinamento deve:

a) implementar e manter uma estratégia abrangente de treinamento e conscientização destinada a garantir que o pessoal entenda suas responsabilidades e procedimentos de proteção de dados pessoais;
b) criar mecanismos para manter o pessoal com responsabilidades de proteção de dados pessoais atualizado sobre os desenvolvimentos no ambiente regulatório, contratual e tecnológico que possam afetar a conformidade de privacidade pela organização;
c) administrar treinamento básico e direcionado de proteção dados pessoais com base em funções, regularmente (por exemplo, anual) ou conforme necessário (por exemplo, após um incidente);
d) garantir que o pessoal certifique (manualmente ou eletronicamente) a aceitação das responsabilidades pelos requisitos de proteção de dados pessoais periodicamente.
e) incluir a conscientização sobre notificação de incidentes para assegurar que membros relevantes estejam cientes das possíveis consequências para a organização (por exemplo, consequências legais, perda de negócios e dano reputacional ou da marca).

4.6 Controle 24: Minimização de Dados

O órgão, dentro dos limites de suas competências legais, deve implementar ações para não coletar e tratar de forma inadequada ou excessiva os dados pessoais dos

titulares de dados pessoais e tratar a mínima quantidade de dados necessários para atingir a finalidade legal desejada.

Por que implementar?

Conforme estabelecido no art. 18 da LGPD, o titular dos dados pessoais tem direito a obter do controlador, em relação aos dados pessoais por ele tratados, a qualquer momento e mediante requisição, a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a Lei.

O Controlador, portanto, deve limitar a quantidade de dados pessoais tratados ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados, em aderência ao princípio da necessidade preconizado pelo art. 6º, inciso III da LGPD.

As organizações não devem coletar dados pessoais indiscriminadamente. Tanto a quantidade quanto o tipo de dados pessoais coletados devem ser limitados ao necessário para cumprir a(s) finalidade(s) legítima(s) especificada(s) pelo controlador.

Em qualquer tratamento de dados pessoais que seja realizado pela organização, deve-se considerar cuidadosamente quais dados pessoais serão necessários para atender à finalidade específica antes de prosseguir com o tratamento.

4.7 Controle 25: Gestão do Tratamento

A gestão do tratamento visa a limitar o uso, a retenção e a divulgação de dados pessoais ao que for estritamente necessário para cumprir propósitos específicos, explícitos e legítimos.

Por que implementar?

O princípio da necessidade, previsto no art. 6º da LGPD, estabelece que o tratamento deve ser limitado ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

As organizações devem implementar medidas apropriadas para limitar o tratamento de dados pessoais para fins legítimos e pretendidos e reter os dados pessoais apenas pelo tempo necessário para cumprir os propósitos declarados ou para

cumprir as leis aplicáveis.

Vale ressaltar que os dados pessoais devem ser gerenciados em conformidade com a estratégia de risco da organização para proteger a privacidade dos indivíduos, aumentar a gerenciabilidade e permitir a implementação de princípios de privacidade.

4.8 Controle 26: Acesso e Qualidade

O acesso e qualidade visam a garantir que os direitos do titular, quanto ao tratamento de dados pessoais, sejam atendidos e assegurar que sejam feitos de forma exata, clara, relevante e atualizado de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento. Assegurar também o livre acesso aos titulares para consulta facilitada e gratuita sobre a integralidade de seus dados pessoais.

Por que implementar?

Conforme os princípios do livre acesso e qualidade dos dados estabelecido no art. 6º da LGPD e os direitos do titular de dados pessoais, previsto no art. 18, o controlador deve garantir aos titulares o acesso facilitado e gratuito a seus dados pessoais, bem como sobre a integralidade de seus dados pessoais com direito a correção de dados incompletos, inexatos ou desatualizados. E ainda, garantir, aos titulares, a exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

A viabilização do livre acesso do titular dos dados pessoais e a adoção de práticas que visem a assegurar a qualidade do dado pessoal proporcionam que os dados coletados estejam exatos e relevantes para o cumprimento da lei.

A organização deve também implementar processos para garantir que o tratamento de dados pessoais seja preciso, completo, atualizado, adequado e relevante para a finalidade de uso e implementar medidas para garantir a precisão dos dados pessoais coletados.

4.9 Controle 27: Compartilhamento, Transferência e Divulgação

Assim como ocorre com outras operações de tratamento, o compartilhamento, a transferência e a divulgação de dados pessoais devem ser realizados em conformidade com a LGPD, observando os princípios, as bases legais, garantia dos direitos dos titulares e outras regras específicas aplicáveis.

Por que implementar?

De acordo com o art. 26 da LGPD o uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei. Já a comunicação ou uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado, o art. 27, deverá ser informado à autoridade nacional e dependerá de consentimento do titular.

A transferência internacional de dados pessoais está prevista na LGPD e deve ser realizada conforme os art. 33 a 36.

Ressalta-se que a organização no tocante a este controle deve, principalmente, identificar e documentar as finalidades específicas para o compartilhamento de dados pessoais.

A organização deve implementar medidas apropriadas para garantir que quaisquer compartilhamentos, transferências e divulgações de dados pessoais atendam requisitos de conformidade relevantes.

Fique Atento!

A ANPD disponibiliza em seu portal um Guia de Tratamento de Dados Pessoais pelo Poder Público que apresenta instruções claras sobre compartilhamento de dados pessoais pelo Poder Púbico.

Disponível em: Guia de Tratamento de Dados Pessoais pelo Poder Público da ANPD

4.10 Controle 28: Supervisão em Terceiros

A supervisão em terceiros visa a garantir, através de meios contratuais ou outros, como políticas internas obrigatórias, que o terceiro destinatário implemente ações previstas pelo controlador no intuito de atender aos requisitos de conformidade com as leis e regulamentos de proteção de dados em vigor e requisitos de privacidade.

Por que implementar?

O art. 39 da LGPD estabelece 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.

As organizações devem implementar medidas apropriadas para garantir que contratados e processadores de dados pessoais cumpram as cláusulas contratuais previstas no momento do estabelecimento de acordo entre as partes interessadas.

Um contrato pode estabelecer as responsabilidades de cada parte diferentemente, porém, para ser consistente com este documento, convém que todos os controles sejam considerados e incluídos na informação documentada.

Fique Atento!

A Secretaria de Governo Digital disponibiliza em seu portal um Guia de Requisitos e Obrigações quanto à Segurança da Informação e à Privacidade que orienta a adequação do processo de contratação para contemplar os requisitos mais importantes de segurança e privacidade dos dados.

Disponível em: Guia de Requisitos e Obrigações quanto a Privacidade e à Segurança da Informação

4.11 Controle 29: Abertura, Transparência e Notificação

O órgão, ao efetuar o tratamento de dados pessoais no exercício de suas competências legais ou execução de políticas públicas, deverá dar publicidade sobre a finalidade e a forma como o dado será tratado.

Por que implementar?

A Abertura, Transparência e Notificação buscam atender o princípio de transparência da LGPD, art. 6º, inciso VI. O referido princípio, de acordo com a lei, é a “garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial”.

O controlador, ao tratar dados pessoais, deve atender a este princípio, assegurando a disponibilização de informações claras, precisas e facilmente

acessíveis aos titulares sobre o tratamento de seus dados.

As informações exigidas pela LGPD devem ser disponibilizadas de forma adequada, ostensiva, em linguagem simples e acessível, de modo a assegurar o efetivo conhecimento do titular a respeito das atividades de tratamento realizadas pelo controlador, bem como sobre os seus direitos e a forma de exercê-lo.

Constitui uma boa prática manter as informações de forma clara e atualizada no que diz respeito à previsão legal, finalidade, procedimentos e às práticas utilizadas para a execução dessas atividades e divulgá-las em meios de fácil acesso, preferencialmente na página eletrônica dos órgãos e das entidades responsáveis.

Fique Atento!

A Secretaria de Governo Digital disponibiliza em seu portal um Guia de Elaboração de Termo de Uso e Política de Privacidade que apresenta instruções claras sobre como criar um termo de uso e política de privacidade.

Disponível em: Guia de Elaboração de Termo de Uso e Política de Privacidade

4.12 Controle 30: Avaliação de Impacto, Monitoramento e Auditoria

Este controle visa a avaliar a necessidade de implementar, onde apropriado, uma avaliação de impacto à proteção de dados pessoais, quando novos tratamentos ou mudanças no tratamento existente de dados pessoais forem planejados e documentar medidas adotadas para a mitigação dos riscos identificados. Além disso, o controle visa a revisão contínua da postura de proteção de dados pessoais e privacidade da organização por meio de monitoramento e auditoria interna ou de forma independente para verificar a eficácia das medidas protetivas, políticas, processos e procedimentos implementados objetivando a conformidade com leis e regulamentos relativos à proteção de dados pessoais e privacidade.

Por que implementar?

A LGPD define o RIPD como uma documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Conforme previsto nos art. 4º, 10, 32 e 38, a ANPD poderá solicitar aos controladores, responsáveis pelo tratamento de dados pessoais, relatórios de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento, nos termos de regulamento, observados os segredos comercial e industrial.

As medidas para remediar uma violação de privacidade devem ser proporcionais aos riscos associados à violação, mas devem ser implementadas o mais rápido possível (a menos que proibido de outra forma, por exemplo, interferência em uma investigação legal).

O art. 50 da LGPD estabelece que sejam realizadas atualizações do programa de governança em privacidade com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas das medidas técnicas e administrativas adotadas.

Fique Atento!

A Secretaria de Governo Digital disponibiliza em seu portal um Guia de Avaliação de Riscos que orienta a identificação e a mensuração de riscos de segurança e privacidade, mitigando-os com a utilização dos controles mais indicados, e um Guia de Elaboração de Relatório de Impacto à Proteção de Dados Pessoais que orienta a elaboração de documento de comunicação e transparência que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos, bem como propõe medidas, salvaguardas e mecanismos de mitigação.

Documentação disponível em:

Guia de Elaboração de Avaliação de Riscos

Guia de Elaboração de Relatório de Impacto à Proteção de Dados Pessoais

4.13 Controle 31: Segurança Aplicada à Privacidade

Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Por que implementar?

Os dados pessoais sob os cuidados e custódia do Poder Público devem ser protegidos conforme orientações previstas na LGPD em seus artigos 46, 47, 49 e 50.

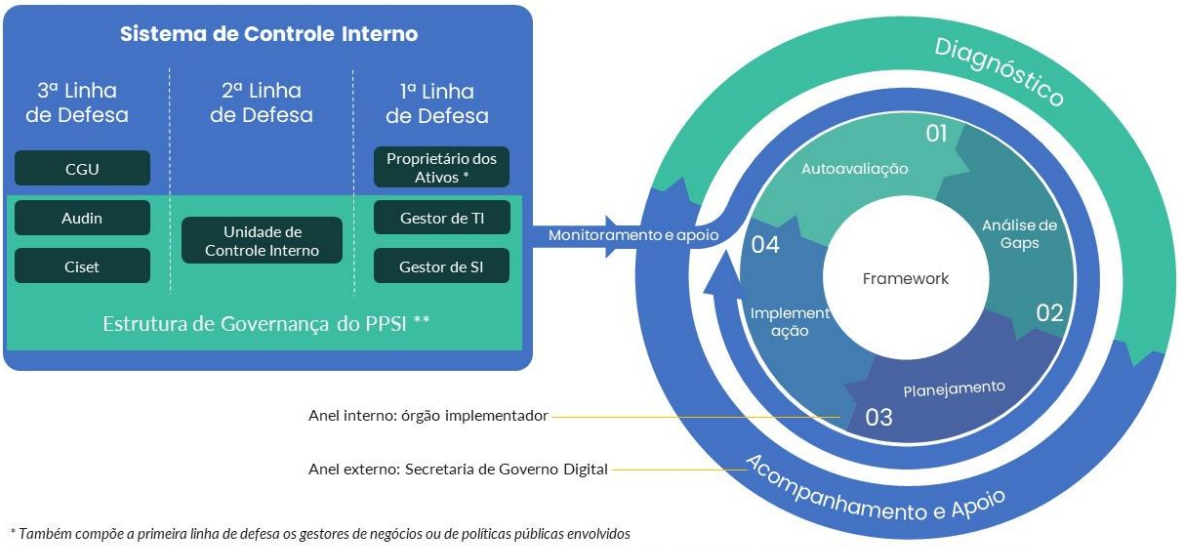
Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais devem de forma estruturada atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na LGPD e às demais normas regulamentares.

Os dados pessoais sob custódia da organização devem ser protegidos por controles apropriados, de acordo com os resultados de uma avaliação de risco de ameaça e/ou impacto na privacidade.

5. IMPLEMENTAÇÃO

Neste capítulo é descrita a metodologia de implementação deste **Framework de Privacidade e Segurança da Informação**. A metodologia adotada é composta pela atuação de um Sistema de Controle Interno (SCI) e pela execução de dois ciclos de execução de atividades, um interno e outro externo. O SCI tem a função de monitorar e apoiar a execução do ciclo interno. O ciclo externo tem a função de acompanhar e apoiar o órgão implementador do **Framework** em suas ações por meio de diagnósticos de maturidade. O ciclo interno é inspirado no ciclo PDCA[28] globalmente difundido nas instituições em diversas frentes e é executado pelo órgão implementador do **Framework**. A Figura 3 resume a metodologia de implementação a ser empregada na aplicação deste **Framework** mostrando como estão relacionados ao SCI com os principais atores e as atividades a serem executadas.

Figura 3: METODOLOGIA DE IMPLEMENTAÇÃO DO FRAMEWORK.



5.1 Sistema de Controle Interno

O SCI envolvido com a implementação deste **Framework** é dividido em três linhas de defesa, conforme o previsto pela IN nº 3, de 9 de junho de 2017 publicada pela Controladoria-Geral da União (CGU). A primeira linha de defesa é responsável por identificar, avaliar, controlar e mitigar os riscos, guiando o desenvolvimento e a implementação de políticas e procedimentos internos destinados a garantir que as

[28] Disponível em: https://www.iso-9001-checklist.co.uk/learn-about-ISO-9001.htm

atividades sejam realizadas de acordo com as metas e objetivos da organização. As instâncias de segunda linha de defesa estão situadas ao nível da gestão e objetivam assegurar que as atividades realizadas pela primeira linha sejam desenvolvidas e executadas de forma apropriada. A terceira linha de defesa é representada pela atividade de auditoria interna governamental, que presta serviços de avaliação e de consultoria com base nos pressupostos de autonomia técnica e de objetividade.

Na primeira linha de defesa atuam os Gestores de TI, os Gestores de Segurança da Informação, os Proprietários de Ativos e os Gestores do negócio ou de políticas públicas envolvidos. A segunda linha de defesa tem a atuação da Unidade de Controle Interno do órgão implementador do **Framework**. Na terceira linha de defesa, atuam a CGU, Auditoria Interna (Audin) e a Ciset[29], detalhes sobre atuação dessa linha de defesa podem ser observados na IN CGU nº 3, de 2017.

5.1.1 *Estrutura de Governança do Programa de Privacidade e Segurança da Informação (PPSI)*

A primeira e a segunda linha de defesa, citadas na introdução deste capítulo, representam a estrutura principal responsável pela governança do PPSI. A terceira linha de defesa compõe a mencionada estrutura de governança nos casos em que a Unidade de Controle Interno acumular os papéis da segunda e terceira linha de defesa.

O PPSI é constituído por um conjunto de ações de adequação nas áreas de privacidade e segurança da informação, desenvolvidas dentro do escopo das disciplinas de governança, pessoas, metodologia, tecnologia e gestão de maturidade, implementadas de forma concomitante e incremental. Tais ações são lideradas pela Diretoria de Privacidade e Segurança da Informação da Secretaria de Governo Digital, voltadas para aumento do grau de maturidade e de resiliência dos órgãos e das entidades integrantes do Sistema de Administração dos Recursos de TI (SISP) do Poder Executivo Federal.

A proposição deste **Framework** e sua implementação são ações resultantes do PPSI. Para saber mais sobre o PPSI visite a página sobre Segurança e Proteção de Dados mantida pela SGD/MGI.

A seguir, é destacado o realizado por cada papel da primeira e segunda linha de defesa na implementação do **Framework**.

[29] Secretarias de Controle Interno (Ciset) da Presidência da República, da Advocacia-Geral da União, do Ministério das Relações Exteriores e do Ministério da Defesa, e respectivas unidades setoriais.

- Papéis na primeira linha de defesa.

O Gestor de TI atua para planejar, implementar, melhorar e otimizar continuamente os processos e procedimentos que envolvem a área de TI.

Por sua vez, a atuação do Gestor de SI se concentra na criação e administração das métricas e indicadores da área de segurança da informação, gerencia as oportunidades de aplicação de tecnologia e interage com outras áreas de maneira a assegurar a segurança das informações da empresa.

Por fim, os Proprietários de Ativos e Gestores do negócio ou de políticas públicas são responsáveis pelos controles primários, inclusive envolvendo adoção de medidas de privacidade e proteção de dados pessoais, no que se refere à implementação das políticas públicas durante a execução de atividades e tarefas, no âmbito de seus macroprocessos finalísticos e de apoio.

- Papel na segunda linha de defesa.

A Unidade de Controle Interno ou estruturas equivalentes contribui no sentido de assegurar que os controles de privacidade e segurança da informação sejam executados de forma apropriada, por meio do desempenho das funções de apoio, supervisão e monitoramento das atividades desenvolvidas pela primeira linha de defesa.

- Papel do Encarregado na Estrutura de Governança do PPSI.

O Encarregado desempenha o papel de fomentar e orientar o planejamento, a implementação e melhoria contínua dos controles de privacidade em serviços ou produtos que realizem o tratamento de dados pessoais ou dados pessoais sensíveis. Apoiando, no que couber, a primeira e segunda linhas de defesa.

5.2 Ciclo Externo

A implementação deste **Framework** é auxiliada pela SGD por meio das ações de diagnóstico, acompanhamento e apoio presentes no anel externo da Figura 3. O diagnóstico terá como base os controles e medidas do próprio **Framework**, e o acompanhamento e apoio se baseará nos resultados desse diagnóstico tal como o nível de maturidade do órgão implementador em privacidade e segurança da informação. Esse nível de maturidade varia conforme a execução das ações de implementação deste **Framework** representado pelo ciclo interno da Figura 3.

5.2.1 *Diagnóstico*

O diagnóstico permite que a SGD tenha uma visão do nível de maturidade dos órgãos em relação à privacidade e segurança, bem como uma visão dos controles e medidas identificados pela análise de *gaps,* etapa do ciclo interno*.* Tal análise possibilita a identificação das medidas de privacidade e segurança da informação a serem adotadas como melhorias e priorizadas em plano de ação.

5.2.2 *Acompanhamento e Apoio*

A SGD atuará no acompanhamento da implementação das melhorias priorizadas no plano de ação, etapa de implementação do ciclo interno, e fornecerá apoio com reuniões técnicas, indicação e produção de material orientativo para auxiliar na implementação dos controles e das medidas de privacidade e segurança da informação.

5.3 Ciclo Interno

O ciclo interno é composto por etapas a serem executadas pelo órgão implementador deste **Framework**, com o apoio da SGD por meio das ações que compõem o ciclo externo. O ciclo inspira-se no modelo PDCA, que é um mecanismo interativo e contínuo estruturado em quatro fases para a gestão: Planejar, Fazer, Checar e Agir.

Como nenhum processo é perfeito e sempre é possível aprimorá-lo, a abordagem do PDCA oferece condições para gerir seu funcionamento com foco na qualidade. Como ele consiste em um método cíclico de aperfeiçoamento, as instituições e profissionais que empregam um ciclo semelhante ao PDCA estão sempre em evolução usando o aprendizado de ações anteriores. Eles agregam os conhecimentos recém adquiridos no intuito de planejar novamente, eliminar falhas, desperdícios e aumentar sua competitividade.

Dessa forma, as etapas do ciclo interno de execução do **Framework** são: Autoavaliação, Análise de Gaps, Planejamento e Implementação. Tais etapas são apresentadas a seguir.

5.3.1 *Autoavaliação*

A autoavaliação terá como finalidade o autoconhecimento do órgão acerca dos controles e medidas adotados em segurança cibernética e privacidade. Para tal, será disponibilizado um questionário por meio de uma ferramenta fornecida pela SGD que

apresentará um Dashboard para auxiliar no direcionamento das ações. As questões constantes da ferramenta são as elencadas pelas medidas dos controles constantes dos Anexos III, IV e V deste documento.

A abordagem adotada para fazer essa autoavaliação será o *Control Self-Assessment* (CSA[30]) destacada pelas seções 6.2 e 6.3 deste documento.

5.3.2 *Análise de Gaps*

Esta etapa consiste, a partir das respostas fornecidas na etapa anterior, em identificar quais as falhas, lacunas ou melhorias relacionadas com privacidade e segurança da informação foram identificadas na autoavaliação. Uma vez identificados os *gaps* segue-se para a próxima etapa do ciclo interno de execução do **Framework**.

5.3.3 *Planejamento*

A etapa de planejamento tem como finalidade estabelecer um plano de ação com as medidas de privacidade e segurança da informação a serem implementadas ou melhoradas.

A priorização das medidas de privacidade e segurança da informação que constarão do plano de ação deve considerar a realidade institucional e considerar parâmetros que auxiliem na identificação de quais medidas priorizar.

Inicialmente, indica-se a priorização das medidas relacionadas com o controle de estruturação básica de gestão em privacidade e segurança da informação identificado neste **Framework** como Controle 0 - Estrutura Básica de Gestão em Privacidade e Segurança da Informação.

No âmbito da segurança cibernética, a metodologia baseada nos GIs do CIS fornece um excelente parâmetro nas escolhas ou determinação das medidas a serem implementadas ou priorizadas.

O GI1 do CIS tem foco na higiene cibernética por meio de medidas que devem ser implementadas por qualquer negócio ou instituição, pois abordam as práticas gerais que a maioria das instituições devem tomar para proteger seus sistemas dos ataques mais comuns ou impedir ataques gerais não direcionados (Figura 4).

Nesse cenário, este **Framework** propõe que as instituições públicas, independentemente da complexidade do ambiente tecnológico, devem adotar as 56 medidas do GI1 do CIS.

[30] https://portal.tcu.gov.br/fiscalizacao-de-tecnologia-da-informacao/atuacao/autoavaliacao-de-controles/

A adoção dos GIs 2 e 3 do CIS levará em consideração se a instituição mantém em seu ambiente tecnológico algum sistema relevante crítico, a partir de análise com base no Modelo de Avaliação de Criticidade de Sistemas apresentado pelo Anexo I.

Dessa forma, se a instituição identifica algum sistema com nível de criticidade deve-se adotar os controles dos GIs 2 e/ou 3 do CIS.

Figura 4: GRUPOS DE IMPLEMENTAÇÃO DO CIS COM DESTAQUE PARA HIGIENE CIBERNÉTICA (ADAPTADO DO CIS CONTROL v8)

Em relação à priorização das medidas de privacidade, adotou-se também a implementação por grupos. Assim como em segurança cibernética, serão 3 Grupos (GI1, GI2 e GI3).

A abordagem adotada por este **Framework** para a escolha das medidas que constarão no GI1 de privacidade se baseia nas obrigações dispostas na LGPD.

A priorização das medidas de privacidade para o GI1 neste **Framework** se baseou também, de forma complementar, na adoção das funções "Identificar-P" e "Governar-P" sugeridas pelo *NIST Privacy Framework* como método simplificado para criar ou aprimorar um programa de privacidade.

Seguindo a mesma ideia da segurança cibernética, este **Framework** propõe que as instituições públicas, independentemente da complexidade do ambiente tecnológico, devem adotar as medidas constantes no GI1 de privacidade, conforme explicado pelos parágrafos acima.

Os GI2 e GI3 de privacidade se basearam nas boas práticas estabelecidas nas

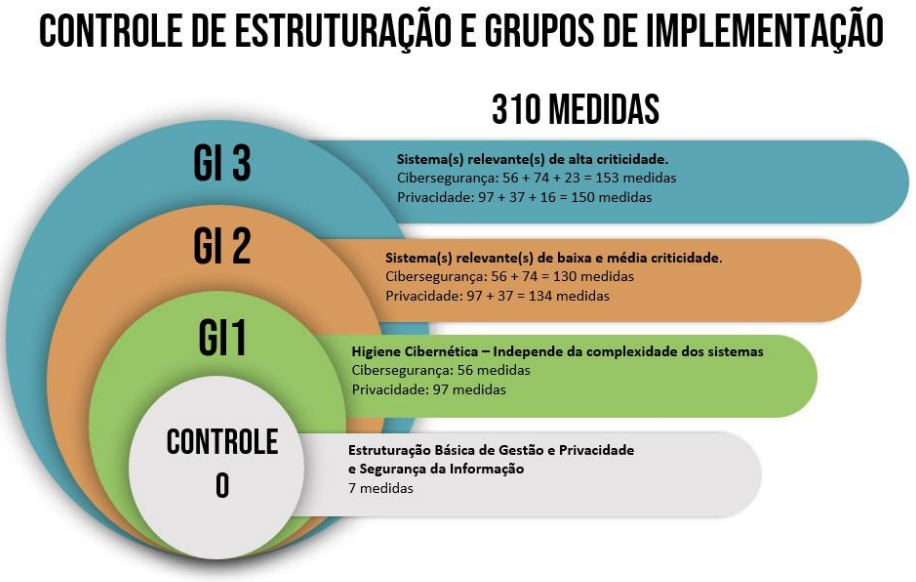
normas, frameworks e guias que fundamentaram este **Framework**, conforme capítulo 1. Assim como estabelecido na priorização das medidas de segurança cibernética, as medidas dos GI2 e GI3 de privacidade levará em consideração o nível de criticidade dos sistemas em seu ambiente tecnológico.

A tabela abaixo sintetiza os GIs que devem ser adotados na aplicação deste **Framework**.

Tabela 1: GRUPOS DE IMPLEMENTAÇÃO UTILIZADOS NESTE FRAMEWORK

Grupo de Implementação	Framework - Aplicação das medidas
GI1	Aplicável para todas as instituições e seus ambientes tecnológicos independente da complexidade do(s) sistema(s)
GI1 + GI2	Aplicável para ambientes tecnológicos que sustentam sistema(s) relevante(s) de baixa e média criticidade
GI1 + GI2 + GI3	Aplicável para ambientes tecnológicos que sustentam sistema(s) relevante(s) de alta criticidade

Figura 5: DISTRIBUIÇÃO DAS MEDIDAS NOS GRUPOS DE IMPLEMENTAÇÃO



A Figura 5 apresenta em maiores detalhes a relação entre os GIs, incluindo a quantidade agregada de medidas a serem implementadas e os requisitos para implementação em cada GI, destacando também o total de medidas do Controle 0 – Estruturação básica de gestão em privacidade e segurança da informação. Cumpre destacar que as medidas do Controle 0 devem ser implementadas pela instituição independente da complexidade dos sistemas.

Cumpre evidenciar que as medidas do Framework destacadas pela Tabela 1

e Figura 5 devem ser considerados para a aplicação em toda a cadeia de suprimentos envolvida com o sistema e ambiente tecnológico que o sustenta.

Esta etapa de Planejamento pode auxiliar no sentido de fornecer parâmetros aos gestores públicos no planejamento orçamentário prevendo contratações de bens, tais como firewall e roteadores, serviços (por exemplo, software de gestão de incidentes), licenças de antivírus, e recursos humanos especializados tais como analistas de segurança, consultores em privacidade, desenvolvedores, entre outros. Essas contratações servem para alavancar suas operações em privacidade e segurança cibernética e entregar resultados com mais efetividade, eficácia, eficiência, transparência e lisura dos entes públicos.

5.3.4 *Implementação*

Após a autoavaliação do ambiente do órgão, a análise de *gaps* e o planejamento das atividades a serem executadas para melhorar a privacidade e a segurança da informação, deve-se implementar os processos (controles e medidas) determinados na etapa anterior de acordo com as normas de proteção de dados pessoais, privacidade e segurança cibernética vigentes, para que o órgão mitigue ou aceite possíveis impactos a serem causados no negócio, devido as vulnerabilidades e ameaças de segurança cibernética.

Quando aplicável, devem ser atendidos de forma prioritária os controles e medidas recomendadas em Notas Técnicas, ou instrumentos equivalentes, a serem publicadas pela Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos.

Além disso é necessário que o órgão eduque e treine todos os envolvidos no processo para garantir que estejam comprometidos com as atividades de conformidade e que tudo ocorra conforme o planejamento realizado na etapa anterior.

É recomendado também que órgão estabeleça e execute procedimentos de monitoramento das implementações dos controles e medidas planejados para documentar as dificuldades e os progressos durante a execução, isso permite um aprendizado necessário ao time envolvido durante todo o processo.

A realização de testes exaustivos dos controles e medidas implementados aumentam a confiabilidade no sistema em relação à segurança cibernética, à proteção de dados pessoais e à privacidade.

Finalizada esta etapa, inicia-se novamente o clico interno com nova autoavaliação

dentro do ciclo de melhoria contínua.

A SGD disponibiliza ferramenta que automatiza o ciclo interno, destacado por este capítulo, a ser realizado pelos órgãos e entidades. O capítulo 7 deste Guia apresenta informações sobre a referida ferramenta.

6. MATURIDADE

A maturidade tem foco na avaliação e gestão do grau de proteção dos sistemas no ambiente de privacidade e cibernético. Os mecanismos para medir este grau são constituídos pelos índices de maturidade em privacidade e segurança da informação do órgão, que o subsidiarão na implementação e monitoramento dos controles e medidas de privacidade e segurança cibernética.

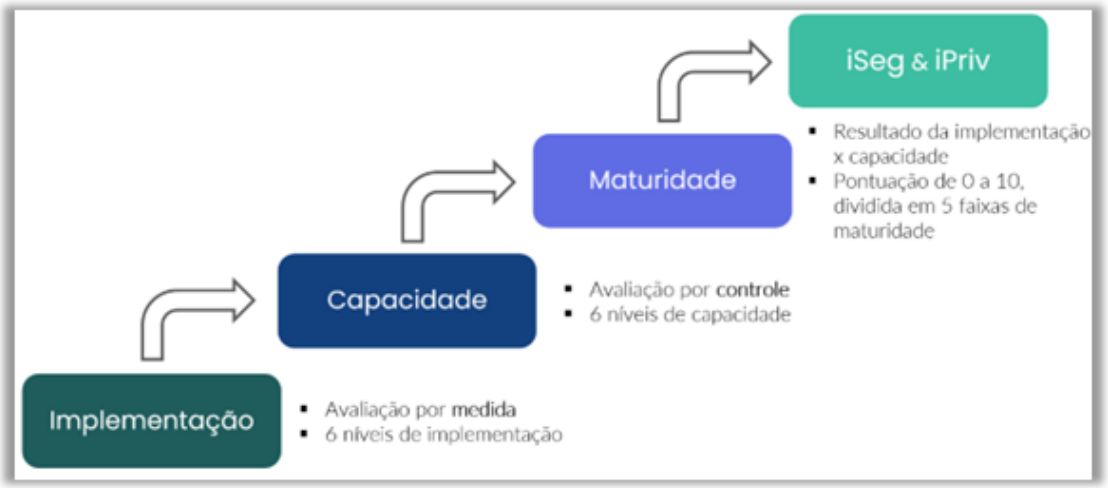
6.1 Capacidade e Maturidade

Para expressar o desempenho quanto ao atendimento dos controles previstos neste **Framework**, propõe-se realizar avaliações de capacidade e de maturidade para obtenção dos indicadores de maturidade em privacidade (iPriv) e em segurança da informação (iSeg) da sua organização.

Para isso, deverá ser adotada uma abordagem em profundidade, com avaliação do nível de implementação de cada medida, passando pela avaliação do nível de capacidade e maturidade por controle, o que resultará nos indicadores iSeg e iPriv.

A imagem a seguir demonstra todos os níveis necessários para compor a avaliação:

Figura 6: ETAPAS NECESSÁRIAS PARA REALIZAR A AVALIAÇÃO



A avaliação de maturidade consiste nas seguintes etapas:

1. Implementação: Avaliação e seleção do nível de implementação por medida.
2. Capacidade: Avaliação e seleção do nível de capacidade por controle.
3. Maturidade: Obtenção do nível de maturidade por controle.

4. iSeg & iPriv: Obtenção do índice de maturidade em segurança (iSeg) e do índice de maturidade em privacidade (iPriv) com base nas respostas fornecidas em relação à adoção das medidas de cada controle.

6.2 Quem deve executar a avaliação?

A presente avaliação poderá ser aplicada pela própria organização, considerando o método CSA, ou no que couber pela Unidade de Controle Interno da instituição.

Para avaliação da segurança da informação pela própria organização, por meio do método CSA, o responsável será o Gestor de Segurança da Informação, que deve contar com o apoio do Gestor de TI e, caso necessário, consultar o Encarregado pelo Tratamento de Dados Pessoais, bem como, os proprietários de ativos e gestores de negócios ou de políticas públicas envolvidos.

Para privacidade, o Encarregado pelo Tratamento de Dados Pessoais é quem atua na condução da avaliação, que deve contar com o apoio do Gestor de Segurança da Informação e do Gestor de TI. Também poderá ser necessário consultar os proprietários de ativos, gestores de negócios ou de políticas públicas envolvidos que tratam dados pessoais ou dados pessoais sensíveis.

Ressalta-se que, apesar das temáticas privacidade e segurança da informação possuírem forte relação, conforme exposto no framework, os indicadores iPriv e iSeg devem ser avaliados e calculados separadamente, gerando dois indicadores isolados. Dessa forma, as quatro etapas para avaliação devem ser aplicadas isoladamente tanto para os controles e medidas de privacidade quanto para os de segurança da informação.

6.3 Etapas da avaliação

6.3.1 *Implementação: Avaliação e seleção do nível de implementação por medida*

O avaliador deverá analisar cada uma das medidas listadas neste framework, individualmente, aplicando um nível de implementação para cada uma delas.

O nível de implementação expressa uma análise sobre a amplitude de implementação da respectiva medida, considerando a abrangência de ativos de informação que possuem aplicabilidade.

O avaliador deverá selecionar um dos níveis de implementação listados na tabela a seguir para cada medida:

Tabela 2: NÍVEIS DE IMPLEMENTAÇÃO A SEREM APLICADOS EM CADA MEDIDA

Nível de Implementação	Descrição	Pontuação
Adota em maior parte ou totalmente	Há decisão formal ou plano aprovado, e a medida na organização é implementada integralmente em mais de 50% ou em todos os: - ativos no caso de medida de segurança da informação; ou - processos/serviços no caso de medida de privacidade.	1
Adota em menor parte	Há decisão formal ou plano aprovado, e a medida na organização é implementada integralmente em menos de 50% dos: - ativos no caso de medida de segurança da informação; ou - processos/serviços no caso de medida de privacidade.	0,75
Adota parcialmente	Há decisão formal ou plano aprovado, e a medida na organização é implementada parcialmente em mais de 50% ou em todos os: - ativos no caso de medida de segurança da informação; ou - processos/serviços no caso de medida de privacidade.	0,5
Há decisão formal ou plano aprovado para implementar	Há decisão formal ou plano aprovado, porém não há na organização implementação ou está parcialmente implementado em menos de 50% dos: - ativos no caso de medida de segurança da informação; ou - processos/serviços no caso de medida de privacidade.	0,25
A organização não adota essa medida	Não há qualquer decisão formal ou plano aprovado, tampouco implementação da medida.	0
Não se aplica	A medida não se aplica em nenhum ativo no caso de medida de segurança da informação ou processo/serviço no caso de medida de privacidade, por entendimento dos gestores ou considerando alguma particularidade do contexto de atuação da organização. A não aplicabilidade deverá seguir de uma motivação baseada em uma análise de riscos.	-

Considera-se que ativos de informação são meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização.

Importante ressaltar que, para avaliar o nível de implementação das medidas dos controles de Privacidade, devem ser considerados os serviços ou produtos que realizam

o tratamento de dados pessoais e/ou dados pessoais sensíveis.

Os níveis de implementação aplicáveis ao Controle 0 – Estrutura Básica de Gestão em Segurança da Informação e Privacidade consistem numa resposta binária de “Sim” ou “Não”.

O avaliador deverá selecionar um dos níveis de implementação listados na tabela a seguir para cada medida:

Tabela 3: NÍVEIS DE IMPLEMENTAÇÃO A SEREM APLICADOS NAS MEDIDAS DO CONTROLE 0

Nível de Implementação	Descrição	Pontuação
Sim	O papel ou instrumento foi devidamente instituído na organização.	1
Não	O papel ou instrumento não foi devidamente instituído na organização.	0

6.3.2 *Capacidade: Avaliação e seleção do nível de capacidade por controle*

Diferentemente do nível de implementação, que foca em aspectos quantitativos, o nível de capacidade foca no aspecto qualitativo, e tem como objetivo avaliar o nível de efetividade da adequação de um controle. Além disso, a avaliação é realizada por controle, e não por medida.

O avaliador deverá considerar um dos níveis de capacidade a seguir para cada controle:

Tabela 4: NÍVEIS DE CAPACIDADE POR CONTROLE

Nível de Capacidade	Descrição	Índice
0	Ausência de capacidade para a implementação das medidas do controle, ou desconhecimento sobre o atendimento das medidas.	0
1	O controle atinge mais ou menos seu objetivo, por meio da aplicação de um conjunto incompleto de atividades que podem ser caracterizadas como iniciais ou intuitivas (pouco organizadas).	20
2	O controle atinge seu objetivo por meio da aplicação de um conjunto básico, porém completo, de atividades que podem ser caracterizadas como realizadas.	40
3	O controle atinge seu objetivo de forma muito mais organizada utilizando os recursos organizacionais. Além disso, o controle é formalizado por meio de uma política institucional, específica ou como parte de outra maior.	60
4	O controle atinge seu objetivo, é bem definido e suas medidas são implementadas continuamente por meio de um processo decorrente da política formalizada.	80

Nível de Capacidade	Descrição	Índice
5	O controle atinge seu objetivo, é bem definido, suas medidas são implementadas continuamente por meio de um processo e seu desempenho é mensurado quantitativamente por meio de indicadores.	100

6.3.3 *Maturidade: Obtenção do nível de maturidade por controle*

A maturidade é obtida por meio da relação entre a avaliação quantitativa e a qualitativa, ou seja, considerando os níveis de implementação atribuídos às medidas e os níveis de capacidade atribuídos aos controles.

Dessa forma, considerando as avaliações realizadas nas etapas 1 e 2, as pontuações correspondentes dos níveis de implementação e os índices correspondentes aos níveis de capacidade deverão ser aplicados na seguinte fórmula:

$$iMC = \frac{\left(\frac{\sum PMC}{QMC - QMNAC}\right)}{2} * \left(1 + \frac{iNCC}{100}\right) \quad (1)$$

Onde:
$iMC = indicador\ de\ maturidade\ por\ controle$
$PMC = somatório\ das\ pontuações\ das\ medidas\ avaliadas\ no\ controle$
$QMC = quantidade\ de\ medidas\ do\ controle$
$QMNAC = quantidade\ de\ medidas\ não\ aplicáveis\ do\ controle$
$iNCC = índice\ do\ nível\ de\ capacidade\ do\ controle$

Além de obter o valor numérico do indicador de maturidade (iMC) por controle, este poderá ser enquadrado em uma faixa de nível de maturidade, considerando a tabela a seguir:

Tabela 5: RELAÇÃO ENTRE O INDICADOR E O NÍVEL DE MATURIDADE POR CONTROLE

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

6.3.4 *iSeg & iPriv: Obtenção do iSeg e/ou iPriv*

Após calculada a maturidade de todos os controles de segurança da informação ou de privacidade, os valores dos indicadores de maturidade por controle devem ser aplicados às fórmulas a seguir:

Fórmula de avaliação do iSeg

$$iSeg = \frac{(iMC_0 * 4) + \sum_{i=1}^{18} iMC_i}{22} \quad (2)$$

Onde:

$iSeg = indicador\ de\ maturidade\ de\ segurança\ da\ informação$
$i\ =\ número\ do\ controle\ avaliado, considerando\ os\ controles\ de\ 1\ a\ 18\ de\ Segurança$
$iMC = indicador\ de\ maturidade\ por\ controle$

Fórmula de avaliação do iPriv

$$iPriv = \frac{(iMC_0 * 4) + \sum_{i=19}^{31} iMC_i}{17} \quad (3)$$

Onde:

$iPriv = indicador\ de\ maturidade\ de\ privacidade$
$i\ =\ número\ do\ controle\ avaliado, considerando\ os\ controles\ de\ 19\ a\ 31\ de\ Privacidade$
$iMC = indicador\ de\ maturidade\ por\ controle$

Observa-se nas fórmulas que é considerado um indicador de maturidade por controle (iMC) com índice 0 (zero), ou seja, relativo ao Controle 0 – Estrutura Básica de Gestão em Privacidade e Segurança da Informação. Em virtude da importância quanto à instituição dos papéis e instrumentos em conformidade com a PNSI e com a LGPD, esse controle foi tratado separadamente dos demais controles, atribuindo peso 4 para tal. Tal abordagem aplica-se tanto para o iSeg quanto para o iPriv, pelo entendimento de que os papéis são essenciais para a cultura organizacional quanto às duas temáticas, e de que não há privacidade sem segurança da informação.

Assim como o iMC, o iSeg e iPriv utilizam os níveis de maturidade da tabela a seguir:

Tabela 6: RELAÇÃO ENTRE OS INDICADORES DE MATURIDADE EM SEGURANÇA DA INFORMAÇÃO OU PRIVACIDADE E OS NÍVEIS DE MATURIDADE

iSeg / iPriv	Nível de Maturidade
0,00 a 0,29	Inicial
0,30 a 0,49	Básico
0,50 a 0,69	Intermediário
0,70 a 0,89	Em Aprimoramento
0,90 a 1,00	Aprimorado

Nesse cenário, é apresentado a seguir exemplo de avaliação de capacidade e maturidade de segurança com base em simulação para os controles: “Controle 0 – Estrutura Básica de Gestão em Segurança da Informação e Privacidade”; “Controle 05 – Gestão de Contas”; e “Controle 18 – Testes de Invasão”.

Avaliação do Controle 0 – Estrutura Básica de Gestão em Segurança da Informação e Privacidade

Medida	Nível de Implementação	∑ PMC	QMC	QMNAC	Nível de Capacidade	iNCC
Medida 0.1	Atendido (1)	3,00	7	0	**Nível 2**	40
Medida 0.2	Não Atendido (0)					
Medida 0.3	Atendido (1)					
Medida 0.4	Atendido (1)					
Medida 0.5	Não Atendido (0)					
Medida 0.6	Não Atendido (0)					
Medida 0.7	Não Atendido (0)					

Aplicando os valores obtidos na fórmula do indicador de maturidade por controle, obtém-se o seguinte resultado arredondado para duas casas decimais:
{[3,00 / (7-0)] / 2} * (1 + 40/100) = [(3,00 / 7) / 2] * (1 + 40/100) = (0,43 / 2) * (1 + 40/100) = 0,21 * (1 + 40/100) = 0,21 + 0,09 = **0,30**
Dessa forma, **o indicador de maturidade do Controle 0 – Estrutura Básica de Gestão em Segurança da Informação e Privacidade seria 0,30 ou nível de maturidade Básico**

Avaliação do Controle 05 – Gestão de Contas

Medida	Nível de Implementação	∑ PMC	QMC	QMNAC	Nível de Capacidade	iNCC
Medida 5.1	Adota em maior parte ou totalmente (1)	3,00	6	0	**Nível 3**	60
Medida 5.2	Adota em maior parte ou totalmente (1)					
Medida 5.3	Adota em menor parte (0,75)					
Medida 5.4	Há decisão formal ou plano aprovado para implementar (0,25)					
Medida 5.5	A organização não adota essa medida (0)					
Medida 5.6	A organização não adota essa medida (0)					

Aplicando os valores obtidos na fórmula do indicador de maturidade por controle, obtém-se o seguinte resultado arredondado para duas casas decimais:
{[3,00 / (6 - 0)] / 2} * (1 + 60/100) = [(3,00 / 6) / 2] * (1 + 60/100) = (0,50 / 2) * (1 + 60/100) = 0,25 * (1 + 60/100) = 0,25 + 0,15 = **0,40**
Dessa forma, **o indicador de maturidade do Controle 05 – Gestão de Contas seria 0,40 ou nível de maturidade Básico**

Avaliação do Controle 18 – Testes de Invasão

Medida	Nível de Implementação	∑ PMC	QMC	QMNAC	Nível de Capacidade	iNCC
Medida 18.1	Adota em maior parte ou totalmente (1)	4,00	5	1	**Nível 4**	80
Medida 18.2	Adota em maior parte ou totalmente (1)					
Medida 18.3	Adota em maior parte ou totalmente (1)					
Medida 18.4	Adota em maior parte ou totalmente (1)					
Medida 18.5	Não se aplica (-)					

Aplicando os valores obtidos na fórmula do indicador de maturidade por controle, obtém-se o seguinte resultado arredondado para duas casas decimais:
{[4,00 / (5 - 1)] / 2} * (1 + 80/100) = [(4,00 / 4) / 2] * (1 + 80/100) = (1,00 / 2) * (1 + 80/100) = 0,50 * (1 + 80/100) = 0,50 + 0,40 = **0,90**
Dessa forma, **o indicador de maturidade do Controle 18 – Testes de Invasão seria 0,90 ou nível de maturidade Aprimorado**

Nesse contexto, a avaliação do iSeg para o exemplo apresentado acima é destacada abaixo.

Avaliação do iSeg

O iSeg é composto por 19 controles, incluindo o controle 0. No entanto, para fins exemplificativos e didáticos, considera-se que serão avaliados apenas três controles para composição do iSeg, conforme já realizado acima: os controles 0, 5 e 18.

Como demonstrado, após avaliação realizada nos três controles, foram obtidos os seguintes iMC:

Controle 0 – Papéis e Instrumentos: **0,30 ou Básico**

Controle 5 – Gestão de Contas: **0,40 ou Básico**

Controle 18 – Testes de Invasão: **0,90 ou Aprimorado**

Dito isso, aplicam-se os valores na fórmula do iSeg (assumindo que trabalhemos apenas com 3 controles neste exemplo), obtendo-se o seguinte resultado arredondado para duas casas decimais:

iSeg = [(0,30 * 4) + 0,40 + 0,90] / 6 = **0,42**

Ou seja, neste exemplo o indicador de maturidade de segurança da informação (iSeg) teria 0,42 de maturidade, ou nível Básico

A SGD disponibiliza ferramenta que automatiza a implementação deste **Framework**, inclusive os cálculos de maturidade destacado por este capítulo. O capítulo 7 deste Guia apresenta informações sobre a referida ferramenta.

7. FERRAMENTA DE ACOMPANHAMENTO DA IMPLEMENTAÇÃO DO FRAMEWORK

Com a finalidade de facilitar a aplicação e acompanhamento da implementação do **Framework de Privacidade e Segurança da Informação**, a SGD desenvolveu uma ferramenta em formato de planilha na qual poderão ser obtidos e acompanhados indicadores de maturidade de privacidade e segurança da informação do órgão mediante preenchimento de diagnósticos.

Detalhes sobre o uso e funcionalidades da ferramenta podem ser observados no link: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/manual_ferramenta_framework.pdf

8. CONSIDERAÇÕES FINAIS

A transformação digital dos serviços públicos é uma realidade no âmbito das organizações públicas brasileiras, demandando uma estrutura de governança que permeie toda organização, com especial atenção, na elaboração de diretrizes pela alta administração, estratégias de implementação e o efetivo monitoramento da implementação dos controles de privacidade e segurança da informação.

Desse modo, o **framework** visa, principalmente, a auxiliar aos gestores da primeira linha de defesa a identificar precocemente fragilidades nas práticas de privacidade e segurança da informação que possam comprometer o desenvolvimento e execução dos serviços, dos produtos e dos processos de trabalhos internos que colaboram para o alcance dos objetivos institucionais.

Extremamente importante ressaltar que o patrocínio da alta administração do representa fator crítico de sucesso para a implementação deste **Framework** na instituição. Desse modo, é fundamental que a alta administração demonstre seu comprometimento com a adoção dos controles e medidas de privacidade e segurança da informação estabelecidos pelo **Framework** por meio de ações que assegurem:

- a estruturação básica de gestão de privacidade e segurança da informação;
- os recursos orçamentários necessários;
- a capacitação dos recursos humanos envolvidos; e
- a implementação do **framework** como parte do programa de governança em privacidade e segurança da informação do órgão ou entidade.

Diante do exposto, a adoção do **Framework de Privacidade e Segurança da Informação** pelas instituições públicas proporcionará benefícios como:

1. ampliação da confiabilidade e da proteção de sistemas informáticos contra os principais ataques que podem resultar em incidentes de segurança;
2. aprimoramento da privacidade e da proteção dos dados pessoais dos cidadãos inseridos nas bases de dados governamentais;
3. aumento da confiança da população na prestação de serviços digitais por parte do governo federal;
4. disseminação da cultura de privacidade e segurança da informação na instituição;

5. criação de uma linguagem comum de controles e de medidas de privacidade e segurança para os órgãos do SISP e demais partes interessadas; e
6. aumento da confiança mútua para compartilhamento de dados entre as instituições públicas devido a evolução dos níveis de maturidade em privacidade e segurança da informação dos ambientes tecnológicos.

Por fim, com a publicação deste Framework, a SGD segue firme no propósito de definir orientações que promovam proteção a dados pessoais e a segurança da informação no âmbito da APF, em articulação com os órgãos responsáveis por políticas públicas.

Fique Atento!

A Secretaria de Governo Digital disponibiliza em seu portal uma série de guias operacionais, que incentiva e auxilia na conformidade de normativos vigentes sobre o tema de privacidade, proteção de dados pessoais e segurança da informação.

Disponível em: Guia Operacionais da SGD

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001:2013**: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança dainformação - Requisitos. Rio de Janeiro, 2013.

_____. **ABNT NBR ISO/IEC 27002:2013**: Tecnologia da informação — Técnicas de segurança — Código de prática para controles desegurança da informação. Rio de Janeiro, 2013.

_____. **ABNT NBR ISO/IEC 27701:2019**: Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes. Rio de Janeiro,2019.

_____. **ABNT NBR ISO/IEC 27184:2021**: Tecnologia da informação - Avisos de privacidade *on-line* e consentimento. Rio de Janeiro,2021.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais**. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 01 jul. 2022.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Decreto nº 9.637, de 26 de dezembro de 2018. **Política Nacional de Segurança da Informação – PNSI**. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm . Acesso em: 01 jul. 2022.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Portaria nº 93, de 26 de setembro de 2019. **Glossário de Segurança da Informação**. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663. Acesso em: 01 jul. 2022.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Instrução Normativa nº 01, de 27 de maio de 2020**. Brasília, DF, GSI/PR, 2020. Disponível em: https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/legislacao/copy_of_IN01_consolidada.pdf. Acesso em: 01 jul. 2022.

BRASIL. Presidência da República. Ministério da Economia. Secretaria de Governo Digital. **Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022**. Brasília, DF, SGD/ME, 2022. Disponível em: https://www.gov.br/governodigital/pt-br/contratacoes/instrucao-normativa-sgd-me-no-1-de-4-de-abril-de-2019. Acesso em: 01 mar. 2023.

BRASIL. Presidência da República. Controladoria-Geral da União. **Instrução Normativa nº 03, de 09 de junho de 2017**. Brasília, DF, CGU, 2017. Disponível em: https://wiki.cgu.gov.br/index.php/Instru%C3%A7%C3%A3o_Normativa_n%C2%BA_3,_de_9_de_junho_de_2017. Acesso em: 01 jul. 2022.

CENTER INTERNET SECURITY. **CIS Controls**, versão 8.0. Maio de 2021. Disponível em: https://www.cisecurity.org/controls. Acesso em: 01 jul. 2022.

CENTER INTERNET SECURITY. **CIS Controls v8 Privacy Companion Guide**, versão 1.0. Janeiro de 2022. Disponível em: https://www.cisecurity.org/insights/white-papers/cis-controls-v8-privacy-companion-guide-portuguese-translation. Acesso em: 01 jul. 2022.

COMITÊ CENTRAL DE GOVERNANÇA DE DADOS - CCGD. **Guia de Boas Práticas LGPD**. Agosto de 2020. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf . Acesso em: 01 jul. 2022.

INTERNATIONAL STANDARD. **ISO/IEC 29100:2011**: Information technology — Security techniques — Privacy framework. Genebra, 2011.

_____. **ISO/IEC 29134:2017**: Information technology – Security techniques – Guidelines for privacy impact assessment. Genebra, 2017.

_____. **ISO 9001:2015**: Quality management systems — Requirements. Genebra, 2015.

_____. **ISO/IEC 29151:2017**: Information technology — Security techniques — Code of practice for personally identifiable information protection. Genebra, 2017.

_____. **ISO/IEC 27018:2014**: Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. Genebra, 2014.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Guia de Aperfeiçoamento da Segurança Cibernética para Infraestrutura Crítica, versão 1.1, 2018. Disponível em: https://www.nist.gov/cyberframework/framework. Acesso em: 01 jul. 2022.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. A estrutura de privacidade do NIST: uma ferramenta para melhorar a privacidade por meio do gerenciamento de riscos corporativos, versão 1.0, 2020. Disponível em: https://www.nist.gov/privacy-framework/privacy-framework. Acesso em: 01 jul. 2022.

_____. **NIST Special Publication 800-53 revisão 5**: Security and Privacy Controls for Information Systems and Organizations. Gaithersburg, 2020. Acesso em: 01 jul. 2022.

BRASIL. Tribunal de Contas da União. **ACÓRDÃO nº 1.109/2021. Plenário**. Relator: Ministro Vital Do Rêgo. Sessão de 12/05/2021. Diário Oficial da União, Brasília, DF, 12 mai. 2021. Disponível em: https://pesquisa.apps.tcu.gov.br/#/. Acesso em: 01 jul. 2022.

BRASIL. Tribunal de Contas da União. **ACÓRDÃO nº 1.768/2022. Plenário**. Relator: Ministro Vital Do Rêgo. Sessão de 03/08/2022. Diário Oficial da União, Brasília, DF, 03 ago. 2022. Disponível em: https://pesquisa.apps.tcu.gov.br/#/. Acesso em: 01 set. 2022.

BRASIL. Tribunal de Contas da União. **ACÓRDÃO nº 1.889/2022. Plenário**. Relator: Ministro Vital Do Rêgo. Sessão de 17/08/2022. Diário Oficial da União, Brasília, DF, 17

ago. 2021. Disponível em: https://pesquisa.apps.tcu.gov.br/#/. Acesso em: 01 set. 2022.

ANEXO I – MODELO DE AVALIAÇÃO DE CRITICIDADE DE SISTEMAS

O modelo de avaliação de criticidade busca identificar qual é o nível de criticidade de cada sistema relevante da organização em razão de sua exposição a riscos de privacidade e segurança da informação.

O modelo adotado é uma adaptação do modelo exposto pelo TCU, por meio do Acórdão 1.889/2020-TCU-Plenário, que tinha como objetivo realizar levantamento de riscos em sistemas informacionais da APF.

Para aplicação deste modelo, considera-se os seguintes conceitos:

a) **Sistema de Informação** se trata de um "conjunto de elementos materiais ou intelectuais, colocados à disposição dos usuários, em forma de serviços ou bens, que possibilitam a agregação dos recursos de tecnologia, informação e comunicações de forma integrada", conforme definição do Glossário de Segurança da Informação GSI/PR.

   Um sistema de informação também pode ser entendido como o conjunto de softwares em uso, eventualmente embarcados em hardware específico, que apoiam processos de negócio, que resultem direta ou indiretamente em serviços aos cidadãos, mediante a conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar, disseminar e fazer uso de informações. Este entendimento foi utilizado pelo TCU em seu Acórdão, e está compatível com a definição do Glossário de Segurança da Informação;

b) **Sistemas relevantes** - são aqueles que possuem significativo grau de importância para a organização. Para classificar um sistema como relevante, podem ser utilizados critérios como lista de precedência para ser posto a funcionar em caso de desastre/recuperação e opinião dos gestores ou da equipe de TI, tratamento de dados pessoais ou dados pessoais sensíveis, entre outros.

c) **Criticidade** de um sistema pode ser entendida como uma medida de exposição a riscos em razão dos impactos decorrentes de falhas e indisponibilidades do sistema e de suas vulnerabilidades;

d) **Impacto** é a consequência de um incidente de segurança da informação (indisponibilidade ou comprometimento da integridade ou da

confidencialidade) ou de uma falha decorrente de defeitos em um sistema. Exemplo: impedimento do funcionamento de atividade finalística da organização; e

e) **Vulnerabilidade** - pode ser entendida como uma suscetibilidade do sistema ou do ambiente em que ele opera de ter sua disponibilidade, integridade ou confidencialidade comprometida.

Os impactos e as vulnerabilidades associados ao sistema ou ao ambiente em que ele opera são fatores relevantes a serem considerados na classificação dos sistemas relevantes, uma vez que possuem potencial lesivo à organização, ao cidadão ou à sociedade como um todo, sendo necessária a utilização de um fator de ponderação para cada um dos parâmetros de avaliação, visando a refletir a importância relativa dos parâmetros quando comparados.

A aplicação do modelo será realizada pela própria organização, por meio do método CSA, os responsáveis serão o Gestor de Tecnologia da Informação e Comunicação e o Proprietário do Ativo (Gestor do sistema/do negócio/da política pública).

O processo inicia com a identificação dos sistemas relevantes, considerando a definição exposta anteriormente. Cada sistema relevante deverá ter seus impactos e vulnerabilidades identificadas, individualmente, aplicando-os ao cálculo para obtenção do nível de criticidade.

Para avaliação dos impactos associados ao sistema relevante, considera-se a tabela a seguir e os respectivos pesos, bem como as possíveis respostas para cada impacto:

- Sim – 1 ponto
- Não – 0 ponto

Tabela 7: IMPACTOS ASSOCIADOS AO SISTEMA RELEVANTE

#	Descrição do Impacto	Peso
1	Perda de vidas humanas ou dano grave para a saúde humana	20,0%
2	Danos ambientais graves	15,0%
3	Degradação significativa na prestação de serviço essencial ao cidadão	6,0%

#	Descrição do Impacto	Peso
4	Danos financeiros significativos à Administração Pública (própria organização ou outro órgão/entidade) ou aos cidadãos	6,0%
5	Danos significativos à reputação ou à credibilidade da organização	2,5%
6	Impedimento do funcionamento de atividade finalística da organização	6,0%
7	Degradação significativa da produtividade dos servidores/funcionários da organização que utilizam ou dependem do sistema	2,5%
8	Degradação significativa do funcionamento de atividades ou processos com características multi-institucionais e que envolvam diferentes esferas da administração ou dos poderes	6,0%
9	Conhecimento não autorizado de informações que possa acarretar dano à soberania e à integridade territorial nacionais; a planos e operações militares; a sistemas, instalações, programas, projetos, planos ou operações de interesse da defesa nacional; às relações internacionais do país; a programas econômicos; e a assuntos diplomáticos e de inteligência (informações secretas ou ultrassecretas)	10,0%
10	Exposição indevida de dados pessoais sensíveis e que possa causar dano ao titular	6,0%
11	Efeito negativo na execução da política econômica do Brasil (fiscal, monetária e cambial)	10,0%
12	Degradação significativa do funcionamento de atividades ou serviços relacionados às infraestruturas críticas do Brasil (definidas na Política Nacional de Segurança de Infraestruturas Críticas)	10,0%

Para avaliação das vulnerabilidades associadas ao sistema relevante, considera-se a tabela a seguir e os respectivos pesos, bem como as possíveis respostas para cada vulnerabilidade:

- Questões 16 e 20:
  a) Não – 0 ponto
  b) Sim, menos da metade do sistema/módulo – 0,33 ponto
  c) Sim, mais da metade do sistema/módulo – 0,66 ponto
  d) Sim, totalmente – 1 ponto.
- Demais questões:
  a) Não – 1 ponto
  b) Sim, menos da metade do sistema/módulo – 0,66 ponto
  c) Sim, mais da metade do sistema/módulo – 0,33 ponto
  d) Sim, totalmente – 0 ponto

Tabela 8: VULNERABILIDADES ASSOCIADAS AO SISTEMA RELEVANTE

#	Descrição da Vulnerabilidade	Peso
13	O sistema está coberto por solução de continuidade de serviços de TI (alta disponibilidade, recuperação de desastres e planos de contingência)	10,0%
14	O sistema é suportado por equipe de respostas a incidentes	8,0%
15	As vulnerabilidades e os riscos de TI relacionados ao sistema e à infraestrutura que o sustenta estão identificados, classificados, analisados e tratados	20,0%
16	O sistema possui tecnologia obsoleta ou desatualizada (hardware e software)	5,0%
17	O sistema está hospedado em sala segura ou sala cofre	10,0%
18	O sistema ou a infraestrutura que o suporta estão cobertos por processo de gestão de patches de segurança	8,0%
19	São realizados testes de invasão ou auditorias de segurança no sistema ou na infraestrutura que o sustenta	10,0%
20	O sistema é alvo de frequentes ataques	8,0%
21	O sistema possui controles para a proteção dos dados e do código (criptografia, backup, controle de acesso, trilhas de auditoria etc.)	16,0%
22	O sistema e a infraestrutura que o suporta estão incluídos em processo de gestão de ativos de TI - ITAM (*IT Asset Management*)	5,0%

É importante ressaltar que os tipos de impacto e vulnerabilidade dispostos nas tabelas devem ser considerados apenas para fins desta avaliação de criticidade de sistemas.

Considerando a avaliação dos impactos e vulnerabilidades, e as pontuações obtidas pela multiplicação entre o valor das respostas e o respectivo peso, aplica-se a seguinte fórmula:

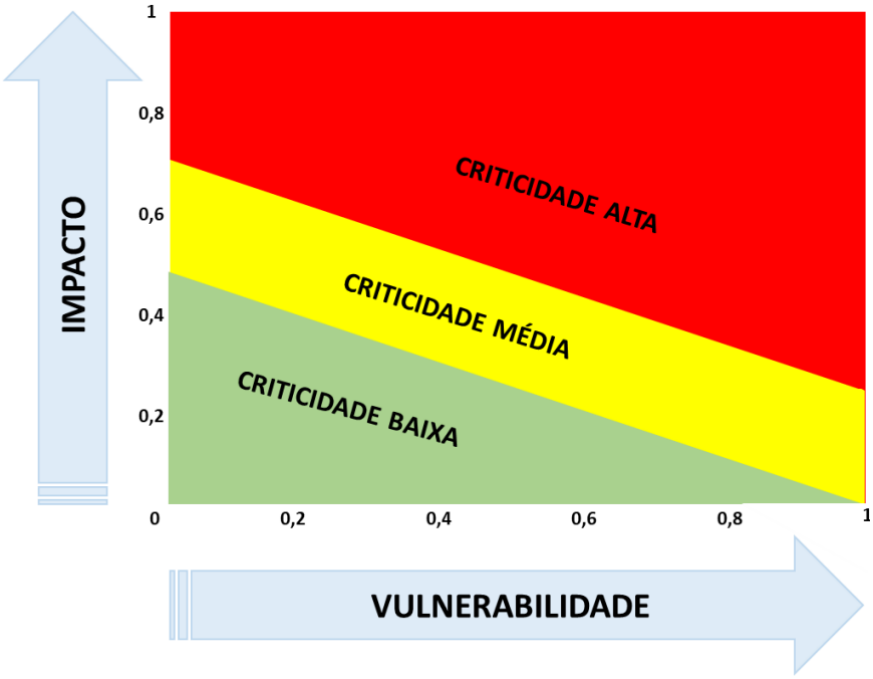
Tabela 9: NOTAS DE IMPACTO, VULNERABILIDADES E CRITICIDADE

Nota de Impacto (I)	I = Soma (pontuação de cada parâmetro de impacto x peso do parâmetro) Nota máxima = 1,00
Nota de Vulnerabilidade (V)	V = Soma (pontuação de cada parâmetro de vulnerabilidade x peso do parâmetro) Nota máxima = 1,00
Nota de Criticidade (NC)	NC = (2 x I) + V

Destaque-se que, para efeito de cálculo da nota de criticidade dos sistemas, a nota final da dimensão impacto para cada sistema foi multiplicada por dois, de forma a considerar a importância dos parâmetros nela agrupados e com potencial de afetar diretamente as estratégias e necessidades das organizações que os utilizam.

Conforme as notas obtidas, os sistemas foram classificados em três faixas de criticidade: alta, média e baixa. O resultado da nota de criticidade dos sistemas, classificados de acordo com impacto e a vulnerabilidade de cada um, podem ser dispostos graficamente tal como indicado na figura a seguir:

Figura 7: FAIXAS DE CRITICIDADE - VULNERABILIDADE x IMPACTO



A definição das faixas utilizou as seguintes premissas:

a) Um sistema com nota de impacto maior que 0,7 (de um total possível de 1), mesmo que não apresente vulnerabilidades conhecidas, deve ser objeto de um olhar prioritário e será considerado de alta criticidade (sistema crítico);

b) Um sistema com nota de impacto entre 0,5 e 0,7 (de um total possível de 1), mesmo que não apresente vulnerabilidades conhecidas, será considerado, no mínimo, como de média criticidade; e

c) Considerando-se que a criticidade é calculada como o dobro da nota impacto somado à nota de vulnerabilidade, as regiões de criticidade alta, média e baixa são separadas por retas de criticidade constante. Dessa

forma, a reta que separa as regiões de alta e média criticidade se caracteriza pela criticidade igual a 1,4 (num extremo, tem-se impacto de 0,7 e vulnerabilidade nula; no outro extremo, o impacto é de 0,2 e a vulnerabilidade é máxima). Já a reta que separa as regiões de média e baixa criticidade se caracteriza pela criticidade igual a 1 (num extremo, tem-se impacto de 0,5 e vulnerabilidade nula; no outro, o impacto é nulo e a vulnerabilidade, máxima).

Com a finalidade de facilitar a avaliação de criticidade dos sistemas relevantes, a SGD disponibiliza a título de sugestão para aqueles órgãos que não possuam uma metodologia própria, uma ferramenta em formato de planilha estruturada onde deverá ser respondido um diagnóstico com perguntas sobre as vulnerabilidades e os possíveis impactos no sistema caso haja um comprometimento.

Detalhes sobre o uso e funcionalidades da ferramenta podem ser observados no link: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/manual_ferramenta_framework.pdf

ANEXO II – NORMATIVOS DO GSI

GSI			
INSTRUÇÃO NORMATIVA	Instrução Normativa GSI Nº 1 - 27 de maio de 2020.	Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.	https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-1-de-27-de-maio-de-2020-258915215
	Instrução Normativa GSI Nº 2 - 24 de julho de 2020.	Altera a Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.	https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-2-de-24-de-julho-de-2020-268684700
	Instrução Normativa GSI Nº 2 - 5 de fevereiro de 2013	Dispõe sobre o Credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal.	https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=18/02/2013&jornal=1&pagina=5&totalArquivos=120
	Instrução Normativa GSI Nº 3 - 28 de maio de 2021	Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.	https://www.in.gov.br/en/web/dou/-/instrucao-normativa-gsi/pr-n-3-de-28-de-maio-de-2021-322963172
	Instrução Normativa GSI Nº 3 - 6 de março de 2013	Dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal.	https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=2&data=14/03/2013
	Instrução Normativa GSI Nº 4 - 26 de março de 2020	Dispõe sobre os requisitos mínimos de Segurança Cibernética que devem ser adotados no estabelecimento das redes 5G.	https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-4-de-26-de-marco-de-2020-250059468
	Instrução Normativa GSI Nº 5 - 31 de agosto de 2021	Dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal.	https://in.gov.br/en/web/dou/-/instrucao-normativa-n-5-de-30-de-agosto-de-2021-341649684
	Instrução Normativa GSI Nº 6 - 23 de dezembro de 2021	Estabelece diretrizes de segurança da informação para o uso seguro de mídias sociais nos órgãos e nas entidades da administração pública federal.	https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-6-de-23-de-dezembro-de-2021-370081858

GSI			
NORMA COMPLEMENTAR	NC nº 05 /IN01/DSIC/GSIPR, e seu anexo	Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal.	https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=17/08/2009&jornal=1&pagina=8&totalArquivos=108
	NC nº 08 /IN01/DSIC/GSIPR	Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal.	https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=24/08/2010&jornal=1&pagina=1&totalArquivos=144
	NC nº 09 /IN01/DSIC/GSIPR	**(Revisão 02)** Estabelece orientações específicas para o uso de recursos criptográficos em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal (APF), direta e indireta. (Publicada no DOU Nº 134, de 16 Jul 2014 - Seção 1)	https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=16/07/2014&jornal=1&pagina=4&totalArquivos=84
	NC nº 12 /IN01/DSIC/GSIPR	Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.	https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=10/02/2012&jornal=1&pagina=3&totalArquivos=264
	NC nº 17 /IN01/DSIC/GSIPR	Estabelece Diretrizes nos contextos de atuação e adequações para Profissionais da Área de Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF).	https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=10/04/2013&jornal=1&pagina=5&totalArquivos=160
	NC nº 18 /IN01/DSIC/GSIPR	Estabelece as Diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF).	https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=10/04/2013&jornal=1&pagina=6&totalArquivos=160
	NC nº 20 /IN01/DSIC/GSIPR	(Revisão 01) Estabelece as Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. (Publicada no DOU Nº 242, de 15 Dez 2014 - Seção 1)	https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=4&data=15/12/2014
	NC nº 21 /IN01/DSIC/GSIPR	Estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta.	https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=10/10/2014&jornal=1&pagina=5&totalArquivos=224
	NC nº 01/IN02/NSC/GSIPR, e seus anexos (Anexo A e Anexo B)	Disciplina o Credenciamento de Segurança de Pessoas Naturais, Órgãos e Entidades Públicas e Privadas para o Tratamento de Informações Classificadas. (Publicada no DOU Nº 123, de 28 de junho de 2013 - Seção 1)	https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=28/06/2013&jornal=1&pagina=5&totalArquivos=144

ANEXO III – TABELA DE CONTROLE e MEDIDAS DE ESTRUTURAÇÃO BÁSICA EM PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

CONTROLE 0: ESTRUTURAÇÃO BÁSICA DE GESTÃO EM PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

ID	FUNÇÃO NIST	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS
0.1	------	O órgão nomeou um Gestor de Tecnologia da Informação e Comunicação?	O Gestor de Tecnologia da Informação e Comunicação, dentre outras atribuições, nos termos da Portaria nº 778, de 4 de abril de 2019, responsável por planejar, implementar e melhorar continuamente os controles de privacidade e segurança da informação em soluções de tecnologia da informação e comunicações, considerando a cadeia de suprimentos relacionada à solução.	Portaria nº 778, de 4 de abril de 2019
0.2	------	O órgão nomeou um Gestor de Segurança da Informação?	O Gestor de Segurança da Informação, dentre outras atribuições, nos termos da Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional, da Presidência da República - GSI/PR, responsável por planejar, implementar e melhorar continuamente os controles de segurança da informação em ativos de informação.	Art. 15, inciso I da Instrução Normativa GSI nº 1, de 27 de maio de 2020
0.3	------	O órgão nomeou um Responsável pela Unidade de Controle Interno?	O Responsável pela Unidade de Controle Interno, atuará no apoio, supervisão e monitoramento das atividades desenvolvidas pela primeira linha de defesa prevista pela Instrução Normativa CGU nº 3, de 9 de junho de 2017.	Instrução Normativa CGU nº 3, de 9 de junho de 2017

CONTROLE 0: ESTRUTURAÇÃO BÁSICA DE GESTÃO EM PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

ID	FUNÇÃO NIST	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS
0.4	------	O órgão instituiu um Comitê de Segurança da Informação?	Instituir um Comitê de Segurança da Informação ou estrutura equivalente, para deliberar sobre os assuntos relativos à Política Nacional de Segurança da Informação.	Art. 15, inciso II da Instrução Normativa GSI nº 1, de 27 de maio de 2020
0.5	------	O órgão instituiu uma Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR?	Instituir e implementar Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR, que constituirá a rede de equipes, integrada pelos órgãos e pelas entidades da administração pública federal, coordenada pelo Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo do Gabinete de Segurança Institucional da Presidência da República.	Art. 15, inciso IV da Instrução Normativa GSI nº 1, de 27 de maio de 2020
0.6	------	O órgão elaborou uma Política de Segurança da Informação - POSIN?	É obrigatório a todos os órgãos e as entidades da administração pública federal possuir uma Política de Segurança da Informação - POSIN, implementada a partir da formalização e aprovação por parte da autoridade máxima da instituição, com o objetivo de estabelecer diretrizes, responsabilidades, competências e subsídios para a gestão da segurança da informação.	Art. 9º da Instrução Normativa GSI nº 1, de 27 de maio de 2020
0.7	GOVERNAR-P	O órgão nomeou um Encarregado pelo Tratamento de Dados Pessoais?	O Encarregado pelo Tratamento de Dados Pessoais, dentre outras atribuições, nos termos do art. 41, §2º, da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD), responsável por conduzir o diagnóstico de privacidade, bem como orientar, no que couber, os	Art. 5º, inciso VIII e Art. 41 da Lei Geral de Proteção de Dados Pessoais nº 13.709, de 14 de agosto de 2018

CONTROLE 0: ESTRUTURAÇÃO BÁSICA DE GESTÃO EM PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

ID	FUNÇÃO NIST	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS
			gestores proprietários dos ativos de informação, responsáveis pelo planejamento, implementação e melhoria contínua dos controles de privacidade em ativos de informação que realizem o tratamento de dados pessoais ou dados pessoais sensíveis.	

ANEXO IV – TABELA DE CONTROLES e MEDIDAS DE CIBERSEGURANÇA

CIBERSEGURANÇA CONTROLE 1: INVENTÁRIO E CONTROLE DE ATIVOS INSTITUCIONAIS

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
1.1	1.1	IDENTIFICAR	O órgão estabelece e mantém um inventário detalhado de ativos institucionais?	Estabelecer e manter um inventário preciso, detalhado e atualizado de todos os ativos institucionais com potencial para armazenar ou processar dado. Certificar de que o inventário registrará o endereço de rede (se estático), endereço de hardware, nome da máquina, etc. Deverá incluir ativos conectados à infraestrutura física, virtual, e remota e aqueles dentro de ambientes de nuvem. Necessário incluir também ativos mesmo que não estejam sob controle do órgão. Revisar e atualizar o inventário semestralmente ou com mais frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020 IN nº 3/2021 IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 12 /IN01/.DSIC/GSIPR	1, 2, 3
1.2	1.4	IDENTIFICAR	O órgão usa o Dynamic Host Configuration Protocol DHCP para Atualizar o Inventários de Ativos?	Utilizar o registro (logs) do Dynamic Host Configuration Protocol (DHCP) em todos os servidores DHCP ou utilizar uma ferramenta de gerenciamento de endereços IP para atualizar o inventário de ativos de hardware da instituição.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR	2, 3
1.3	1.3	DETECTAR	O órgão usa uma ferramenta de descoberta ativa?	Identificar ativos conectados à rede institucional através de uma ferramenta de descoberta ativa. Configurar para que essa descoberta seja executada diariamente ou com mais frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR	2, 3
1.4	1.5	DETECTAR	O órgão usa ferramenta de Descoberta Passiva?	Utilizar uma ferramenta de descoberta passiva para identificar dispositivos conectados à rede da instituição e automaticamente atualizar o inventário de ativos de hardware da instituição.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR	3
1.5	1.2	RESPONDER	O órgão endereça ativos não autorizados?	Assegurar que exista um processo semanal para lidar com ativos não autorizados. Optar por remover o ativo da rede, negar que o ativo se conecte remotamente à rede ou colocar o ativo em quarentena.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR	1, 2, 3

CIBERSEGURANÇA CONTROLE 2: INVENTÁRIO E CONTROLE DE ATIVOS DE SOFTWARE

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
2.1	2.1	IDENTIFICAR	O órgão estabelece e mantém um inventário de software?	Estabelecer e manter um inventário detalhado de todos os softwares licenciados instalados em ativos. Revisar e atualizar o inventário de software semestralmente ou com mais frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020 IN nº 3/2021	1, 2, 3
2.2	2.2	IDENTIFICAR	O órgão assegura que o software autorizado seja atualmente suportado?	Garantir que apenas aplicações ou sistemas operacionais atualmente suportados pelo fabricante sejam adicionados ao inventário de softwares autorizados. Softwares não suportados devem ser indicados no sistema de inventário. Revisar o inventário de software para verificar o suporte do software pelo menos uma vez por mês ou com mais frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	1,2,3
2.3	2.5	PROTEGER	O órgão possui lista de permissões de Software autorizado?	Utilizar controles técnicos em todos os ativos para garantir que apenas software autorizado seja executado. Reavaliar semestralmente ou com mais frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	2, 3
2.4	2.6	PROTEGER	O órgão possuí lista de permissões de bibliotecas autorizadas?	Utilizar controles técnicos para garantir que apenas bibliotecas autorizadas (tais como *.dll, *.ocx, *.so, etc) tenham permissão para serem carregadas nos processos em execução. Impedir que bibliotecas não autorizadas sejam carregadas nos processos. Reavaliar semestralmente ou com mais frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	2,3
2.5	2.7	PROTEGER	O órgão possuí lista de permissões de Scripts autorizados?	Utilize controles técnicos como assinaturas digitais e controle de versão para garantir que apenas scripts autorizados e assinados digitalmente (tais como *.ps1, *.py, macros etc.) tenham permissão para serem executados. Bloqueie a execução de scripts não autorizados. Reavalie semestralmente ou com mais frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	3
2.6	2.4	DETECTAR	O órgão utiliza ferramentas automatizadas de inventário de software?	Utilizar ferramentas de inventário de software, quando possível, em toda a organização para automatizar a descoberta e documentação do software instalado.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	2, 3

CIBERSEGURANÇA CONTROLE 2: INVENTÁRIO E CONTROLE DE ATIVOS DE SOFTWARE

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
2.7	2.3	RESPONDER	O órgão endereça o software não autorizado?	Assegurar que o software não autorizado seja retirado de uso em ativos institucionais ou receba uma exceção documentada. Revisar mensalmente ou com mais frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	1,2,3

CIBERSEGURANÇA CONTROLE 3: PROTEÇÃO DE DADOS

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
3.1	3.1	IDENTIFICAR	O órgão estabelece e mantém um processo de gestão de dados?	Estabelecer e manter um processo de gestão de dados. No processo, tratar a sensibilidade dos dados, o proprietário dos dados, o manuseio dos dados, os limites de retenção de dados e os requisitos de descarte, com base em padrões de sensibilidade e retenção para a organização. Revisar e atualizar a documentação anualmente ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida de segurança.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020 IN nº 4/2020 IN nº 5/2021 IN nº 6/2021 NC 08 /IN01/DSIC/GSIPR NC 20 /IN01/DSIC/GSIPR	1, 2, 3
3.2	3.2	IDENTIFICAR	O órgão estabelece e mantém um inventário de dados?	Estabelecer e manter um inventário de dados, com base no processo de gestão de dados do órgão. No mínimo inventariar os dados sensíveis. Reavaliar e atualizar o inventário anualmente.	Art. 6º, inciso VII Art. 14, Art. 16, Art. 37 Art. 46 Art. 47, Art. 49 Art. 50	IN nº 1/2020 IN nº 5/2021 IN nº 6/2021 NC 08 /IN01/DSIC/GSIPR NC 20 /IN01/DSIC/GSIPR	1, 2, 3
3.3	3.7	IDENTIFICAR	O órgão estabelece e mantém um esquema de classificação de dados?	Estabelecer e manter um esquema geral de classificação de dados para o órgão, podendo ser “Sensíveis”, “Confidencial” e “Público. Revisar e atualizar o esquema de classificação anualmente ou quando ocorrerem mudanças significativas que possam impactar essa medida de segurança.	Art. 6º, inciso VII Art. 14, Art. 37, Art. 46, Art. 47, Art. 49 Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 20 /IN01/DSIC/GSIPR NC 01/IN02/NSC/GSIPR, e seus anexos (Anexo A e Anexo B)	2, 3
3.4	3.8	IDENTIFICAR	O órgão documenta os Fluxos de Dados?	Documentar o fluxo de dados, contendo fluxos de dados do provedor de serviços, devendo ser baseada no processo de gestão de dados do órgão. Revisar e atualizar a documentação anualmente ou quando ocorrerem mudanças significativas que possam impactar essa medida de segurança.	Art. 6º, inciso VII Art. 14, Art. 16, Art. 37 Art. 46 Art. 47, Art. 49 Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 20 /IN01/DSIC/GSIPR	2, 3

CIBERSEGURANÇA CONTROLE 3: PROTEÇÃO DE DADOS

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
3.5	3.3	PROTEGER	O órgão configura listas de controle de acessos a dados?	Aplicar listas de controle de acesso a dados, também conhecidas como permissões de acesso, a sistemas de arquivos, banco de dados e aplicações locais e remotos.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020 IN nº 4/2020 IN nº 5/2021 IN nº 6/2021 NC 08 /IN01/DSIC/GSIPR NC 20 /IN01/DSIC/GSIPR	1, 2, 3
3.6	3.4	PROTEGER	O órgão aplica retenção de dados?	Reter os dados de acordo com o processo de gestão de dados da organização. A retenção deve incluir prazos mínimos e máximos.	Art. 6º, inciso VII Art. 14, Art. 16, Art. 37, Art. 46, Art. 47, Art. 49, Art. 50	IN nº 3/2013 IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 09 /IN01/DSIC/GSIPR NC 20 /IN01/DSIC/GSIPR	1, 2, 3
3.7	3.5	PROTEGER	O órgão descarta dados com segurança?	Descartar os dados com segurança, conforme processo de gestão de dados da organização. Certificar que o processo e método de descarte sejam compatíveis com a sensibilidade dos dados.	Art. 6º, inciso VII Art, 16, Art. 37, Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020 IN nº 2/2013 IN nº 5/2021 IN nº 6/2021 NC 08 /IN01/DSIC/GSIPR NC 20 /IN01/DSIC/GSIPR	1, 2, 3
3.8	3.6	PROTEGER	O órgão criptografa dados em dispositivos de usuário final?	Criptografar os dados em dispositivos de usuário final que contenham dados sensíveis.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020 IN nº 5/2021 IN nº 6/2021 NC 08 /IN01/DSIC/GSIPR NC 20 /IN01/DSIC/GSIPR	1, 2, 3

CIBERSEGURANÇA CONTROLE 3: PROTEÇÃO DE DADOS

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
3.9	3.9	PROTEGER	O órgão criptografa dados em mídia removível?	Criptografar os dados em removível.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 3/2013 IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 09 /IN01/DSIC/GSIPR NC 20 /IN01/DSIC/GSIPR	2, 3
3.10	3.10	PROTEGER	O órgão criptografa dados sensíveis em trânsito?	Criptografar dados sensíveis em trânsito. Exemplos: Transport Layer Security (TLS) e Open Secure Shell (Open SSH)	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 3/2013 IN nº 4/2020 IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 09 /IN01/DSIC/GSIPR NC 20 /IN01/DSIC/GSIPR	2, 3
3.11	3.11	PROTEGER	O órgão criptografa dados sensíveis em repouso?	Criptografar dados sensíveis em repouso em servidores, aplicações e banco de dados que contenham dados sensíveis.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 3/2013 IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 09 /IN01/DSIC/GSIPR NC 20 /IN01/DSIC/GSIPR	2, 3
3.12	3.12	PROTEGER	O órgão segmenta o processamento e o armazenamento de dados com base na sensibilidade?	Segmentar o processamento e armazenamento de dados com base na sensibilidade dos dados. Não processar dados sensíveis em ativos institucionais destinados a dados de menor sensibilidade.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 20 /IN01/DSIC/GSIPR	2, 3
3.13	3.13	PROTEGER	O órgão implanta uma solução de prevenção contra perda de dados?	Implementar uma ferramenta automatizada, de prevenção de perda de dados (DLP) baseada em host para identificar todos os dados sensíveis armazenados, processados ou transmitidos por meio de ativos institucionais.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 IN nº 6/2021 NC 08 /IN01/DSIC/GSIPR NC 20 /IN01/DSIC/GSIPR	3

CIBERSEGURANÇA CONTROLE 3: PROTEÇÃO DE DADOS

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
3.14	3.14	DETECTAR	O órgão registra o acesso a dados sensíveis?	Registrar o acesso a dados sensíveis, incluindo modificação e descarte.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 20 /IN01/DSIC/GSIPR	3

CIBERSEGURANÇA CONTROLE 4: CONFIGURAÇÃO SEGURA DE ATIVOS INSTITUCIONAIS E SOFTWARE

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
4.1	4.1	PROTEGER	O órgão estabelece e mantém um processo de configuração segura?	Estabelecer e manter um processo de configuração segura para ativos corporativos (dispositivos de usuário final, incluindo portáteis e móveis; dispositivos não computacionais/IoT; e servidores) e software (sistemas operacionais e aplicações). Revisar e atualizar a documentação anualmente ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida de segurança.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 4/2020 IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 12 /IN01/DSIC/GSIPR	1, 2, 3
4.2	4.2	PROTEGER	O órgão estabelece e mantém um processo de configuração segura para a Infraestrutura de Rede?	Estabelecer e manter um processo de configuração segura para dispositivos de rede. Revisar e atualizar a documentação anualmente ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida de segurança.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 4/2020 NC 08 /IN01/DSIC/GSIPR	1, 2, 3
4.3	4.3	PROTEGER	O órgão configura o bloqueio automático de sessão nos ativos?	Configurar o bloqueio automático de sessão nos ativos após um período definido de inatividade. Para sistemas operacionais de uso geral, o período não deve exceder 15 minutos. Para dispositivos móveis de usuário final, o período não deve exceder 2 minutos.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR	1,2,3
4.4	4.4	PROTEGER	O órgão implementa e gerencia um firewall nos servidores?	Implementar e gerenciar um firewall nos servidores, onde houver suporte.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR NC 12 /IN01/DSIC/GSIPR	1, 2, 3
4.5	4.5	PROTEGER	O órgão implementa e gerencia um firewall nos dispositivos de usuário final?	Implementar e gerenciar um firewall baseado em host ou uma ferramenta de filtragem de porta nos dispositivos de usuário final, com uma regra de negação padrão que bloqueia todo o tráfego, exceto os serviços e portas que são explicitamente permitidos.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR	1, 2, 3
4.6	4.6	PROTEGER	O órgão gerencia com segurança os ativos coorporativos e softwares?	Gerenciar com segurança os ativos e software. Exemplos de implementações incluem gestão de configuração por meio de *version controlled-infrastructure-as-code* e acesso a interfaces administrativas por meio de protocolos de rede seguros.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR	1, 2, 3

CIBERSEGURANÇA CONTROLE 4: CONFIGURAÇÃO SEGURA DE ATIVOS INSTITUCIONAIS E SOFTWARE

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
4.7	4.7	PROTEGER	O órgão gerencia contas padrão nos ativos coorporativos e software?	Gerenciar contas padrão nos ativos e software, como root, administrador e outras contas de fornecedores pré-configuradas.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 4/2020 IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR	1, 2, 3
4.8	4.8	PROTEGER	O órgão desinstala ou desativa serviços desnecessários nos ativos e software?	Desinstalar ou desativar serviços desnecessários nos ativos e software, como serviço de compartilhamento de arquivo não utilizado, módulo de aplicação web ou função de serviço.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR	2, 3
4.9	4.9	PROTEGER	O órgão configura servidores DNS confiáveis nos ativos?	Implementar configuração de ativos para usar servidores DNS controlados pelo órgão e/ou servidores DNS confiáveis acessíveis externamente.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR	2, 3
4.10	4.11	PROTEGER	O órgão impõe a capacidade de limpeza remota nos dispositivos portáteis do usuário final?	Limpar remotamente os dados institucionais de dispositivos portáteis de usuário final de propriedade da organização quando for considerado apropriado, como dispositivos perdidos ou roubados, ou quando um indivíduo não trabalha mais no órgão.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR	2, 3
4.11	4.12	PROTEGER	O órgão separa os Espaços de Trabalho nos dispositivos móveis?	Certificar de que a separação de espaços de trabalho seja usada nos dispositivos móveis de usuário final, ou seja, separar aplicações e dados institucionais de aplicações e dados pessoais nos dispositivos, onde houver suporte.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR	3
4.12	4.10	RESPONDER	O órgão impõe o bloqueio automático de dispositivos nos dispositivos portáteis do usuário final?	Impor bloqueio automático de dispositivos quando houver um número pré-definido de tentativas de autenticação com falha,	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 12 /IN01/DSIC/GSIPR	2,3

CIBERSEGURANÇA CONTROLE 5: GESTÃO DE CONTAS

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
5.1	5.1	IDENTIFICAR	O órgão estabelece e mantém um inventário de contas?	Estabelecer e manter um inventário de todas as contas gerenciadas na organização. O inventário deve incluir contas de usuário e administrador. Validar se todas as contas ativas estão autorizadas, trimestralmente ou com mais frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 2/2013 NC 01/IN02/NSC/GSIPR, e seus anexos (Anexo A e Anexo B)	1, 2, 3
5.2	5.5	IDENTIFICAR	O órgão estabelece e mantém um inventário de contas de serviço?	Estabelecer e manter um inventário de contas de serviço. O inventário, no mínimo, deve conter o departamento proprietário, data de revisão e propósito. Realizar análises de contas de serviço para validar se todas as contas ativas estão autorizadas, em uma programação recorrente, no mínimo trimestralmente ou com mais frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	N/A	2, 3
5.3	5.2	PROTEGER	O órgão usa senhas exclusivas?	Usar senhas exclusivas para todos os ativos institucionais. Contas que usam MFA (Autenticação multifator) no mínimo senhas de 8 caracteres e uma senha de 14 caracteres para contas que não usam o MFA.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 2/2013	1, 2, 3
5.4	5.4	PROTEGER	O órgão restringe privilégios de administrador a contas de administrador dedicadas?	Restringir os privilégios de administrador a contas de administrador dedicados nos ativos institucionais. Realizar atividades gerais de computação, como navegação na Internet, e-mail e uso do pacote de produtividade, a partir da conta primária não privilegiada do usuário.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	N/A	1, 2, 3
5.5	5.6	PROTEGER	O órgão centraliza a gestão de contas?	Centralizar a gestão de contas por meio de serviço de diretório ou de identidade.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	N/A	2, 3
5.6	5.3	RESPONDER	O órgão desabilita contas inativas?	Excluir ou desabilitar quaisquer contas inativas após um período de 45 dias de inatividade.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 2/2013	1,2,3

CIBERSEGURANÇA CONTROLE 6: GESTÃO DO CONTROLE DE ACESSO

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
6.1	6.6	IDENTIFICAR	O órgão estabelece e mantém um inventário de sistemas de autenticação e autorização?	Estabelecer e manter um inventário dos sistemas de autenticação e autorização da organização, incluindo aqueles hospedados no site local ou em um provedor de serviços remoto. Revisar e atualizar o inventário anualmente ou com mais frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020 IN nº 2/2013 IN nº 5/2021 NC 01/IN02/NSC/GSIPR, e seus anexos (Anexo A e Anexo B)	2, 3
6.2	6.1	PROTEGER	O órgão estabelece um Processo de Concessão de Acesso?	Estabelecer e seguir um processo, de preferência automatizado, para conceder acesso aos ativos institucionais mediante nova contratação, concessão de direitos ou mudança de função de um usuário.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020 IN nº 2/2013 IN nº 5/2021 NC 01/IN02/NSC/GSIPR, e seus anexos (Anexo A e Anexo B)	1, 2, 3
6.3	6.2	PROTEGER	O órgão estabelece um Processo de Revogação de Acesso?	Estabelecer e seguir um processo, de preferência automatizado, para revogar o acesso aos ativos institucionais, por meio da desativação de contas imediatamente após o encerramento, revogação de direitos ou mudança de função de um usuário. Desativar contas, em vez de excluí-las, pode ser necessário para preservar as trilhas de auditoria.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 01/IN02/NSC/GSIPR, e seus anexos (Anexo A e Anexo B)	1, 2, 3

CIBERSEGURANÇA CONTROLE 6: GESTÃO DO CONTROLE DE ACESSO

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
6.4	6.3	PROTEGER	O órgão exige MFA para aplicações expostas externamente?	Exigir que todas as aplicações corporativas ou de terceiros expostas externamente apliquem o MFA. Impor o MFA por meio de um serviço de diretório ou provedor de SSO é uma implementação satisfatória desta medida de segurança.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 01/IN02/NSC/GSIPR, e seus anexos (Anexo A e Anexo B)	1, 2, 3
6.5	6.4	PROTEGER	O órgão exige MFA para acesso remoto à rede?	Exigir MFA para acesso remoto à rede.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 01/IN02/NSC/GSIPR, e seus anexos (Anexo A e Anexo B)	1, 2, 3
6.6	6.5	PROTEGER	O órgão exige MFA para acesso administrativo?	Exigir MFA para todas as contas de acesso administrativo, em todos os ativos institucionais, sejam gerenciados no site local ou por meio de um provedor terceirizado.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020 IN nº 5/2021 IN nº 6/2021 01/IN02/NSC/GSIPR, e seus anexos (Anexo A e Anexo B)	1, 2, 3

CIBERSEGURANÇA CONTROLE 6: GESTÃO DO CONTROLE DE ACESSO

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
6.7	6.7	PROTEGER	O órgão centraliza o controle de acesso?	Centralizar o controle de acesso para todos os ativos institucionais por meio de um serviço de diretório ou provedor de SSO	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 2/2013 IN nº 5/2021 NC 12 /IN01/DSIC/GSIPR NC 01/IN02/NSC/GSIPR, e seus anexos (Anexo A e Anexo B)	2, 3
6.8	6.8	PROTEGER	O órgão define e mantém o controle de acesso baseado em funções?	Definir e manter o controle de acesso baseado em funções, determinando e documentando os direitos de acesso necessários para cada função dentro da organização para cumprir com sucesso suas funções atribuídas. Realizar análises de controle de acesso de ativos institucionais para validar se todos os privilégios estão autorizados, em uma programação recorrente, uma vez por ano ou com maior frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020 IN nº 2/2013 IN nº 5/2021 NC 12 /IN01/DSIC/GSIPR NC 01/IN02/NSC/GSIPR, e seus anexos (Anexo A e Anexo B)	3

CIBERSEGURANÇA CONTROLE 7: GESTÃO CONTÍNUA DE VULNERABILIDADES

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
7.1	7.5	IDENTIFICAR	O órgão realiza varreduras automatizadas de vulnerabilidade em ativos institucionais internos?	Realizar varreduras automatizadas de vulnerabilidade em ativos institucionais internos trimestralmente ou com mais frequência. Realizar varreduras autenticadas e não autenticadas, usando uma ferramenta compatível com o SCAP(Security Content Automation Protocol).	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 4/2020	2, 3
7.2	7.6	IDENTIFICAR	O órgão realiza varreduras automatizadas de vulnerabilidade em ativos institucionais expostos externamente?	Executar varreduras de vulnerabilidade automatizadas de ativos institucionais expostos externamente usando uma ferramenta de varredura de vulnerabilidade compatível com o SCAP. Executar varreduras mensalmente ou com mais frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	2, 3
7.3	7.1	PROTEGER	O órgão estabelece e mantém um processo de gestão de vulnerabilidade?	Estabelecer e manter um processo de gestão de vulnerabilidade documentado para ativos institucionais. Revisar e atualizar a documentação anualmente ou quando ocorrerem mudanças significativas na organização	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	1, 2, 3
7.4	7.3	PROTEGER	O órgão executa a gestão automatizada de patches do sistema operacional?	Realizar atualizações do sistema operacional em ativos institucionais por meio da gestão automatizada de patches mensalmente ou com mais frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	1,2,3
7.5	7.4	PROTEGER	O órgão executa a gestão automatizada de patches de aplicações?	Realizar atualizações de aplicações em ativos institucionais por meio da gestão automatizada de patches mensalmente ou com mais frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	1,2,3
7.6	7.2	RESPONDER	O órgão estabelece e mantém um processo de remediação?	Estabelecer e manter uma estratégia de remediação baseada em risco documentada em um processo de remediação, com revisões mensais ou mais frequentes.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	1, 2, 3
7.7	7.7	RESPONDER	O órgão corrige vulnerabilidades detectadas?	Corrigir as vulnerabilidades detectadas no software por meio de processos e ferramentas mensalmente, ou com mais frequentemente, com base no processo de correção.	Art. 6º, inciso VII Art. 46, Art. 47,	------	2,3

CIBERSEGURANÇA CONTROLE 7: GESTÃO CONTÍNUA DE VULNERABILIDADES

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
					Art. 49, Art. 50		

CIBERSEGURANÇA CONTROLE 8: GESTÃO DE REGISTROS DE AUDITORIA

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
8.1	8.1	PROTEGER	O órgão estabelece e mantém um processo de gestão de log de auditoria?	Estabelecer e manter um processo de gestão de log de auditoria que defina os requisitos de log da organização. Tratar da coleta, revisão e retenção de logs de auditoria para ativos institucionais. Revisar e atualizar a documentação anualmente ou quando ocorrerem mudanças significativas.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020 IN nº 4/2020 IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 21 /IN01/DSIC/GSIPR	1, 2, 3
8.2	8.3	PROTEGER	O órgão garante o armazenamento adequado do registro de auditoria?	Certificar de que os destinos dos logs mantenham armazenamento adequado para cumprir o processo de gestão de log de auditoria da organização	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 21 /IN01/DSIC/GSIPR	1,2,3
8.3	8.4	PROTEGER	O órgão padroniza a sincronização de tempo?	Padronizar a sincronização de tempo. Configurar pelo menos duas fontes de tempo sincronizadas nos ativos institucionais.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 21 /IN01/DSIC/GSIPR	2,3
8.4	8.10	PROTEGER	O órgão retém os logs de auditoria?	Reter os logs de auditoria em ativos institucionais por no mínimo 90 dias.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 21 /IN01/DSIC/GSIPR	2, 3
8.5	8.2	DETECTAR	O órgão coleta logs de auditoria?	Coletar logs de auditoria. Certificar de que o log, de acordo com o processo de gestão de log de auditoria da organização, tenha sido habilitado em todos os ativos.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 21 /IN01/DSIC/GSIPR	1, 2, 3

CIBERSEGURANÇA CONTROLE 8: GESTÃO DE REGISTROS DE AUDITORIA

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
8.6	8.5	DETECTAR	O órgão coleta logs de auditoria detalhados?	Configurar o log de auditoria detalhado para ativos institucionais contendo dados sensíveis. Incluir a origem do evento, data, nome de usuário, carimbo de data/hora, endereços de origem, endereços de destino e outros elementos úteis que podem ajudar em uma investigação forense.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 21 /IN01/DSIC/GSIPR	2, 3
8.7	8.6	DETECTAR	O órgão coleta logs de auditoria de consulta DNS?	Habilitar o registro de log de consulta do servidor DNS (Domain Name System) para detectar pesquisas de nomes de host para domínios maliciosos conhecidos.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 21 /IN01/DSIC/GSIPR	2, 3
8.8	8.7	DETECTAR	O órgão coleta logs de auditoria de requisição de URL?	Coletar logs de auditoria de requisição de URL em ativos institucionais, quando apropriado e suportado.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 21 /IN01/DSIC/GSIPR	2, 3
8.9	8.8	DETECTAR	O órgão coleta logs de auditoria de linha de comando?	Habilitar o log de auditoria sobre ferramentas de linha de comando, tais como Microsoft Powershell e Bash.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 21 /IN01/DSIC/GSIPR	2, 3
8.10	8.9	DETECTAR	O órgão centraliza os logs de auditoria?	Centralizar a coleta e retenção de logs de auditoria nos ativos institucionais.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 21 /IN01/DSIC/GSIPR	2, 3
8.11	8.11	DETECTAR	O órgão conduz revisões de log de auditoria?	Realizar análises de logs de auditoria para detectar anomalias ou eventos anormais que possam indicar uma ameaça potencial. Realizar revisões semanalmente ou com mais frequência.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 21 /IN01/DSIC/GSIPR	2, 3
8.12	8.12	DETECTAR	O órgão coleta logs do provedor de serviços?	Coletar logs do provedor de serviços. Exemplos de implementações incluem coleta de eventos de autenticação e autorização, eventos de criação e de descarte de dados e eventos de gestão de usuários.	Art. 6º, inciso VII Art. 46, Art. 47,	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 21 /IN01/DSIC/GSIPR	3

CIBERSEGURANÇA CONTROLE 8: GESTÃO DE REGISTROS DE AUDITORIA

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
					Art. 49, Art. 50		

CIBERSEGURANÇA CONTROLE 9: PROTEÇÕES DE E-MAIL E NAVEGADOR WEB

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
9.1	9.1	PROTEGER	O órgão garante o uso apenas de navegadores e clientes de e-mail suportados plenamente?	Certificar de que apenas navegadores e clientes de e-mail suportados plenamente tenham permissão para executar na organização, usando apenas a versão mais recente dos navegadores e clientes de e-mail fornecidos pelo fornecedor.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020	1,2,3
9.2	9.2	PROTEGER	O órgão usa serviços de filtragem de DNS?	Usar os serviços de filtragem de DNS em todos os ativos institucionais para bloquear o acesso a domínios mal-intencionados conhecidos.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020	1, 2, 3
9.3	9.3	PROTEGER	O órgão mantém e impõe filtros de URL baseados em rede?	Impor e atualizar filtros de URL baseados em rede para limitar um ativo institucional de se conectar a sites potencialmente maliciosos ou não aprovados.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020	2, 3
9.4	9.4	PROTEGER	O órgão restringe extensões de cliente de e-mail e navegador desnecessárias ou não autorizadas?	Restringir, seja desinstalando ou desabilitando, quaisquer plug-ins de cliente de e-mail ou navegador, extensões e aplicações complementares não autorizados ou desnecessários.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020	2, 3
9.5	9.5	PROTEGER	O órgão implementa o DMARC?	Para diminuir a chance de e-mails forjados ou modificados de domínios válidos, implemente a política e verificação DMARC, começando com a implementação dos padrões Sender Policy Framework (SPF) e DomainKeys Identified Mail (DKIM)	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020	2,3
9.6	9.6	PROTEGER	O órgão bloqueia tipos de arquivo desnecessários?	Bloquear tipos de arquivo desnecessários que tentem entrar no gateway de e-mail do órgão.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020	2,3
9.7	9.7	PROTEGER	O órgão implanta e mantém proteções antimalware de servidor de e-mail?	Implantar e manter proteção antimalware de servidores de e-mail, como varredura de anexos e/ou sandbox.	Art. 6º, inciso VII Art. 46, Art. 47,	IN nº 1/2020	3

CIBERSEGURANÇA CONTROLE 9: PROTEÇÕES DE E-MAIL E NAVEGADOR WEB

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
					Art. 49, Art. 50		

CIBERSEGURANÇA CONTROLE 10: DEFESAS CONTRA MALWARE

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
10.1	10.1	PROTEGER	O órgão instala e mantém um software antimalware?	Instalar e manter um software anti-malware em todos os ativos cibernéticos da organização.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR	1, 2, 3
10.2	10.2	PROTEGER	O órgão configura atualizações automáticas de assinatura antimalware?	Realizar a configuração de atualizações automáticas para as assinaturas anti-malware em todos os ativos cibernéticos da organização.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR	1, 2, 3
10.3	10.3	PROTEGER	O órgão desabilita a execução e reprodução automática para mídias removíveis?	Configurar os dispositivos para a não execução e reprodução automática de mídias removíveis.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR	1,2,3
10.4	10.5	PROTEGER	O órgão habilita funções antiexploração?	Habilitar funcionalidades "anti-exploits" tais como Data Execution Prevention (DEP) ou Address Space Layout Randomization (ASLR) que estejam disponíveis no sistema operacional, ou implantar ferramentas apropriadas que possam ser configuradas para aplicar proteções sobre um conjunto mais amplo de aplicações e executáveis.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR	2,3
10.5	10.6	PROTEGER	O órgão gerencia o software antimalware de maneira centralizada?	Utilizar software anti-malware gerenciado centralmente para monitorar e defender continuamente cada uma das estações de trabalho e servidores da organização.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR	2, 3
10.6	10.4	DETECTAR	O órgão configura a varredura antimalware automática de mídia removível?	Configure o software anti-malware para verificar automaticamente a mídia removível.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR	2, 3

CIBERSEGURANÇA CONTROLE 10: DEFESAS CONTRA MALWARE

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
10.7	10.7	DETECTAR	O órgão utiliza software antimalware baseado em comportamento?	Utilizar software anti-malware que consiga monitorar e identificar comportamentos fora do comum dos equipamentos da organização.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR	2,3

CIBERSEGURANÇA CONTROLE 11: RECUPERAÇÃO DE DADOS

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
11.1	11.3	PROTEGER	O órgão protege os dados de recuperação?	Garantir que os dados de recuperação sejam protegidos adequadamente por meio de segurança física ou criptografia quando são armazenados, bem como quando são movidos pela rede. Isso inclui backups remotos e serviços em nuvem. Devem ser estabelecidos controles que garantam que os dados de recuperação sejam equivalentes aos dados originais.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 3/2021	1, 2, 3
11.2	11.1	RECUPERAR	O órgão estabelece e mantém um processo de recuperação de dados?	Estabelecer e manter um processo de recuperação de dados. Tal processo deve descrever em seu escopo as atividades de recuperação de dados, priorização da recuperação e a atividade de segurança dos dados de backup. Periodicamente, deve ser realizada uma revisão e/ou atualização deste processo, assim como em casos específicos quando ocorrerem mudanças significativas na organização que venham impactar a organização de forma significativa.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 3/2013 NC 09 /IN01/DSIC/GSIPR	1, 2, 3
11.3	11.2	RECUPERAR	O órgão executa backups automatizados?	Garantir que todos os dados dos sistemas tenham cópias de segurança (backups) realizadas automaticamente e de forma regular.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	1, 2, 3
11.4	11.4	RECUPERAR	O órgão estabelece e mantém uma instância isolada de dados de recuperação?	Criar e manter pelo menos uma instância isolada dos dados de recuperação. Alguns exemplos deste tipo de implementação são controle de versão de destinos de backup por meio de sistemas e serviços off-line (backup off-line, não acessível por meio de uma conexão de rede), em nuvem, ou em datacenter separado do site local.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	1, 2, 3
11.5	11.5	RECUPERAR	O órgão testa os dados de recuperação?	Realizar o teste de integridade dos dados na mídia de backup regularmente, executando um processo de restauração de dados para garantir que o backup esteja funcionando corretamente.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	2, 3

CIBERSEGURANÇA CONTROLE 12: GESTÃO DA INFRAESTRUTURA DE REDE

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
12.1	12.4	IDENTIFICAR	O órgão elabora e mantém diagramas de arquitetura?	Elaborar e manter diagramas e demais documentações da arquitetura de rede da organização. A revisão destas documentações deve ser realizada de forma periódica ou quando ocorrerem mudanças que possam impactar tais artefatos.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 4/2020	2, 3
12.2	12.1	PROTEGER	O órgão garante que a infraestrutura de rede está atualizada?	Garantir que a infraestrutura de rede da organização esteja sempre atualizada. Deve ser realizada uma revisão das versões de software de forma periódica, ou quando for identificada uma vulnerabilidade que eleve o risco da organização.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	1,2,3
12.3	12.2	PROTEGER	O órgão garante níveis de segurança para a arquitetura de rede?	Garantir que a arquitetura de rede se mantenha segura. É interessante buscar implementar políticas de segurança como segmentação de rede, privilégio mínimo e níveis básicos de disponibilidade.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 4/2020	2, 3
12.4	12.3	PROTEGER	O órgão gerencia a infraestrutura de rede e segurança?	Implementar e gerenciar com segurança a infraestrutura de rede da organização.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	2,3
12.5	12.5	PROTEGER	O órgão centraliza a autenticação, autorização e auditoria de rede (AAA)?	Implementar a centralização de (AAA) de rede.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 4/2020	2, 3
12.6	12.6	PROTEGER	O órgão utiliza protocolos de comunicação e gestão de rede seguros?	Implementar protocolos de comunicação e rede seguros.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 4/2020	2,3

CIBERSEGURANÇA CONTROLE 12: GESTÃO DA INFRAESTRUTURA DE REDE

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
12.7	12.7	PROTEGER	O órgão garante que os dispositivos remotos utilizem uma VPN e se conectem em uma infraestrutura AAA segura da organização?	Fazer com que os usuários se autentiquem em serviços de autenticação e VPN gerenciados pela organização antes de acessar os dispositivos e recursos da organização.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	2, 3
12.8	12.8	PROTEGER	O órgão utiliza e mantém recursos cibernéticos dedicados para todo o trabalho administrativo?	Habilitar a coleta de Netflow e registros de log em cada um dos dispositivos existentes para a execução de tarefas administrativas, utilize e mantenha recursos cibernéticos dedicados, estes devem estar fisicamente ou logicamente separados e seguros. É importante que tais recursos sejam segmentados da rede primária da organização, e não deve ser permitido o acesso a rede externa da organização. fronteiras da rede.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	3

CIBERSEGURANÇA CONTROLE 13: MONITORAMENTO E DEFESA DA REDE

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
13.1	13.4	PROTEGER	O órgão realiza filtragem de tráfego entre os segmentos de rede?	Realize a filtragem de tráfego entre os segmentos de rede.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 12 /IN01/DSIC/GSIPR	2, 3
13.2	13.5	PROTEGER	O órgão aplica o gerenciamento de controle de acesso em ativos remotos?	Aplique o gerenciamento de controle de acesso em ativos que se conectam remotamente a organização. Determine a quantidade de acesso aos recursos da organização utilizando softwares antimalware devidamente atualizados, processos de configuração segura de ativos e certifique-se que os sistemas operacionais e demais aplicações estejam sempre atualizados.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 12 /IN01/DSIC/GSIPR	2,3
13.3	13.7	PROTEGER	O órgão implanta soluções para prevenção de intrusão baseada em host?	Implante uma solução para prevenção de intrusão baseada em host e ativos institucionais, preferencialmente com suporte do fornecedor.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 12 /IN01/DSIC/GSIPR	3
13.4	13.8	PROTEGER	O órgão implanta soluções para prevenção de intrusão de rede?	Implante uma solução para prevenção de intrusão baseada em rede, preferencialmente com suporte do fornecedor.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 12 /IN01/DSIC/GSIPR	3
13.5	13.9	PROTEGER	O órgão implanta controle de acesso a nível de porta?	Implante o controle de acesso em nível de porta. Tal controle utiliza o protocolo 802.1x ou soluções semelhantes como certificados, também podem ser utilizadas ferramentas para autenticação de usuário e/ou dispositivo.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 12 /IN01/DSIC/GSIPR	3
13.6	13.10	PROTEGER	O órgão realiza a filtragem de camada de aplicação?	Realize a filtragem de camada de aplicação. Exemplos de implementações são proxy de filtragem, firewall desta camada ou gateway.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 4/2020 IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 12 /IN01/DSIC/GSIPR	3

CIBERSEGURANÇA CONTROLE 13: MONITORAMENTO E DEFESA DA REDE

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
13.7	13.1	DETECTAR	O órgão centraliza alertas de eventos de segurança?	Centralize os alertas de eventos de segurança em ativos institucionais para que a organização consiga realizar a correlação e análise do log. Uma boa prática é o uso de um SIEM que inclua alertas de correlação de eventos definidos pelo fornecedor. Outra boa prática é a adoção de uma plataforma de análise de log configurada com aletas de correlação relevantes para a segurança cibernética.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 12 /IN01/DSIC/GSIPR	2, 3
13.8	13.2	DETECTAR	O órgão implanta soluções de detecção e intrusão baseada em host?	Implante soluções para detecção de intrusão baseada em host em ativos institucionais	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 12 /IN01/DSIC/GSIPR	2, 3
13.9	13.3	DETECTAR	O órgão implanta soluções de detecção e intrusão baseada em rede?	Implante soluções para detecção de intrusão de rede em ativos institucionais	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 12 /IN01/DSIC/GSIPR	2, 3
13.10	13.6	DETECTAR	O órgão coleta logs de fluxo e tráfego de rede?	Realize a coleta dos logs de fluxo e tráfego de rede com o objetivo de checar e alertar sobre dispositivos de rede que estejam com comportamento que fujam do padrão. em sua necessidade de acesso como parte de suas responsabilidades.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 12 /IN01/DSIC/GSIPR	2, 3
13.11	13.11	DETECTAR	O órgão ajusta limites de alertas de eventos de segurança?	Ajuste periodicamente os limites dos alertas de eventos de segurança.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 4/2020 IN nº 5/2021 NC 08 /IN01/DSIC/GSIPR NC 12 /IN01/DSIC/GSIPR	3

CIBERSEGURANÇA CONTROLE 14: CONSCIENTIZAÇÃO E TREINAMENTO DE COMPETÊNCIAS SOBRE SEGURANÇA

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
14.1	14.1	PROTEGER	O órgão implanta e mantém um programa de conscientização de segurança?	Criar programa de conscientização de segurança para que todos os membros da força de trabalho o realizem regularmente com o objetivo de garantir que eles entendam e exibam os conhecimentos e comportamentos necessários para ajudar a garantir a segurança da instituição. O programa de conscientização de segurança da instituição deve ser comunicado de maneira contínua e envolvente.	Art. 6º, inciso VII Art. 46, Art. 49, Art. 50	IN nº 6/2021 NC 08 /IN01/DSIC/GSIPR NC 17 /IN01/DSIC/GSIPR NC 18 /IN01/DSIC/GSIPR	1, 2, 3
14.2	14.2	PROTEGER	O órgão treina colaboradores para reconhecer ataques de engenharia social?	Treinar os colaborares sobre como identificar diferentes formas de ataques de engenharia social, como phishing, golpes de telefone e chamadas realizadas por impostores.	Art. 6º, inciso VII Art. 46, Art. 49, Art. 50	IN nº 6/2021 NC 08 /IN01/DSIC/GSIPR NC 17 /IN01/DSIC/GSIPR NC 18 /IN01/DSIC/GSIPR	1, 2, 3
14.3	14.3	PROTEGER	O órgão treina os colaboradores nas melhores práticas de autenticação?	Treinar os colaboradores sobre a importância de habilitar utilizar as melhores práticas de autenticação segura como MFA (Multi-factor Authentication – Autenticação de múltiplos fatores), composição de senha e gestão de credenciais.	Art. 6º, inciso VII Art. 46, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR NC 17 /IN01/DSIC/GSIPR NC 18 /IN01/DSIC/GSIPR	1, 2, 3
14.4	14.4	PROTEGER	O órgão treina os colaboradores nas Melhores Práticas de Tratamento de Dados?	Treinar os membros da força de trabalho sobre como identificar e armazenar, transferir, arquivar e destruir informações sensíveis (incluindo dados pessoais) adequadamente. Isto também inclui o treinamento sobre práticas recomendadas de mesa e tela limpas, (não deixar senhas expostas nas mesas de trabalho e bloquear a tela da estação de trabalho ao se ausentar), apagar quadros físicos e virtuais após reuniões e armazenar dados e ativos com segurança.	Art. 6º, inciso VII Art. 46, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR NC 17 /IN01/DSIC/GSIPR NC 18 /IN01/DSIC/GSIPR	1, 2, 3
14.5	14.5	PROTEGER	O órgão treina os colaboradores sobre as causas da exposição não intencional de dados?	Treinar os membros da força de trabalho para estarem cientes das causas de exposições de dados não intencionais, como perder seus dispositivos móveis ou enviar e-mail para a pessoa errada devido ao preenchimento automático de e-mail.	Art. 6º, inciso VII Art. 46, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR NC 17 /IN01/DSIC/GSIPR NC 18 /IN01/DSIC/GSIPR	1, 2, 3

CIBERSEGURANÇA CONTROLE 14: CONSCIENTIZAÇÃO E TREINAMENTO DE COMPETÊNCIAS SOBRE SEGURANÇA

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
14.6	14.6	PROTEGER	O órgão treina os colaboradores sobre como Reconhecer e Relatar incidentes de Segurança?	Treinar os colaboradores para serem capazes de identificar os indicadores mais comuns de um incidente e serem capazes de relatar tal incidente.	Art. 6º, inciso VII Art. 46, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR NC 17 /IN01/DSIC/GSIPR NC 18 /IN01/DSIC/GSIPR	1, 2, 3
14.7	14.7	PROTEGER	O órgão treina os colaboradores sobre como identificar e comunicar se os seus ativos institucionais estão desatualizados em relação a segurança?	Treine os colaboradores para entender como verificar e relatar patches de software desatualizados ou quaisquer falhas em ferramentas e processos automatizados. É importante incluir nesse treinamento a etapa de notificação do pessoal de TI sobre quaisquer falhas em processos e ferramentas automatizadas que estejam ocorrendo.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR NC 17 /IN01/DSIC/GSIPR NC 18 /IN01/DSIC/GSIPR	1,2,3
14.8	14.8	PROTEGER	O órgão treina os colaboradores sobre os perigos de se conectar e transmitir dados institucionais em redes inseguras?	Treine os colaboradores sobre os perigos de se conectar e transmitir dados em redes inseguras para atividades corporativas. Se a organização tiver funcionários remotos, o treinamento deve incluir orientação para garantir que todos os usuários configurem com segurança sua infraestrutura de rede doméstica.	Art. 6º, inciso VII Art. 46, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR NC 17 /IN01/DSIC/GSIPR NC 18 /IN01/DSIC/GSIPR	1, 2, 3
14.9	14.9	PROTEGER	O órgão conduz treinamento de competências e conscientização de segurança para funções específicas?	Para colaboradores que atuem em funções específicas, realize o treinamento de conscientização de segurança e de competências específicas para estas funções. Exemplos de implementações incluem cursos de administração de sistema seguro para profissionais de TI, treinamento de conscientização e prevenção de vulnerabilidades para desenvolvedores de aplicações da web do OWASP e treinamento avançado de conscientização de engenharia social para funções de níveis estratégico da organização	Art. 6º, inciso VII Art. 46, Art. 49, Art. 50	NC 08 /IN01/DSIC/GSIPR NC 17 /IN01/DSIC/GSIPR NC 18 /IN01/DSIC/GSIPR	2, 3

CIBERSEGURANÇA CONTROLE 15: GESTÃO DE PROVEDOR DE SERVIÇOS

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
15.1	15.1	IDENTIFICAR	O órgão cria e gerencia o inventário de provedores de serviços?	Crie e gerencie o inventário de provedores de serviços. Este inventário deve listar todos os provedores de serviços da organização, incluir classificações, e conter contatos institucionais para cada provedor de serviço. Deve ser realizada uma revisão e/ou atualização deste inventário anualmente ou quando ocorrerem mudanças significativas do provedor que venham impactar a organização de forma significativa.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 4/2020 IN nº 5/2021	1, 2, 3
15.2	15.2	IDENTIFICAR	O órgão cria e gerencia uma política de gestão de provedores de serviços?	Crie e gerencie uma política de gestão de provedores de serviços. Faça com que tal política trate de classificação, inventário, avaliação, monitoramento e descomissionamento de prestadores e provedores de serviço da organização. Deve ser realizada uma revisão e/ou alteração desta política periodicamente, em casos específicos quando ocorrerem mudanças significativas na organização que venham impactar a organização de forma significativa.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 4/2020 IN nº 5/2021	2, 3
15.3	15.3	IDENTIFICAR	O órgão classifica provedores de serviços?	Realize a classificação de provedores de serviços. Para que seja realizada a classificação podem ser levadas em consideração uma ou mais característica do provedor, como a sensibilidade dos dados e informações que este provedor opera/gerencia, volume destes dados e informações, regulamentações aplicáveis, requisitos de disponibilidade e classificação de risco. Deve ser realizada uma revisão e/ou alteração desta classificação periodicamente, em casos específicos quando ocorrerem mudanças significativas na organização que venham impactar a organização e forma significativa.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021	2, 3
15.4	15.5	IDENTIFICAR	O órgão avalia provedores de serviços?	Realizar a avaliação de provedores de serviços da organização. O escopo da avaliação deve levar em consideração as diretrizes contidas na política de gestão de provedores de serviços além de classificações e relatórios de avaliação padronizados, questionários, e processos rigorosos aplicáveis. A avaliação de provedores de serviço deve ser realizada de forma periódica e na medida em que novos contratos estipulados ou renovados.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 3/2013 IN nº 4/2020 IN nº 5/2021 NC 09 /IN01/DSIC/GSIPR	3

CIBERSEGURANÇA CONTROLE 15: GESTÃO DE PROVEDOR DE SERVIÇOS

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
15.5	15.4	PROTEGER	O órgão garante que os contratos dos provedores de serviços contenham requisitos mínimos de segurança?	Fazer com que os contratos do provedor de serviços contenham requisitos de segurança, alguns exemplos destes requisitos de segurança são, requisitos mínimos de segurança do software, resposta a incidentes de segurança, criptografia e descarte de dados. Tais requisitos mínimos devem ser concisos com a política de gestão de provedores da organização. Deve ser realizada uma revisão dos contratos de provedores de forma periódica com o objetivo de atualizar e garantir que os requisitos de segurança estão sendo cumpridos.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 4/2020 IN nº 5/2021	2, 3
15.6	15.7	PROTEGER	O órgão encerra de forma segura o contrato com o provedor de serviços?	Realizar de forma segura o encerramento de contrato de provedores e prestadores de serviço. Algumas ações que possam ser utilizadas para realizar o encerramento de contratos ou desligamento de prestadores são, desativação de contas de usuário e serviço utilizadas durante o contrato, encerramento de fluxo de dados e descarte seguros de dados e informações corporativas em sistemas dos provedores de serviço.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 4/2020 IN nº 5/2021	3
15.7	15.6	DETECTAR	O órgão monitora provedores de serviço?	Realizar a monitoração de provedores de acordo com a política de gestão dos provedores de serviços. Tal monitoração pode incluir a avaliação periódica do provedor, monitoração de artefatos entregues pelo provedor	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 5/2021	3

CIBERSEGURANÇA CONTROLE 16: SEGURANÇA DE APLICAÇÕES

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
16.1	16.1	PROTEGER	O órgão estabelece e mantém um processo de desenvolvimento de aplicações?	Estabelecer e manter um processo de desenvolvimento de aplicações seguro. Este processo deve tratar de itens como padrões de design seguro de aplicações (Security by Design), práticas de codificação seguras, treinamentos para desenvolvedores, gestão de vulnerabilidades, segurança de código de terceiros e procedimentos de teste de segurança de aplicação. Deve ser realizada uma revisão e/ou alteração deste processo periodicamente, em casos específicos ou quando ocorrerem mudanças na organização que venham impactá-la de forma significativa.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	---	2, 3
16.2	16.2	PROTEGER	O órgão estabelece e mantém um processo para aceitar e endereçar vulnerabilidades de software?	Estabelecer e manter um processo de aceitação e tratamento de informações sobre vulnerabilidades de software, incluindo mecanismos para que entidades externas contatem o grupo de segurança da instituição. É importante que o processo inclua itens como: Política de tratamento de vulnerabilidades identificadas e relatadas, equipe ou profissional responsável por analisar os relatórios de vulnerabilidade e um processo de entrada, atribuição, correção e testes de correção. Como parte deste processo, é importante rastrear as vulnerabilidades, classificar a gravidade e atribuir métricas capazes de medir o tempo de identificação, análise e correção das vulnerabilidades. Deve ser realizada uma revisão e/ou alteração deste processo periodicamente, em casos específicos ou quando ocorrerem mudanças na organização que venham impactá-la de forma significativa.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	---	2, 3
16.3	16.3	PROTEGER	O órgão executa análise de causa raiz em vulnerabilidades de segurança?	Executar a análise de causa raiz em vulnerabilidades de segurança. A análise da causa raiz é a tarefa capaz de avaliar os problemas subjacentes que criam vulnerabilidades no código da aplicação e permite que as equipes de desenvolvimento vão além de apenas corrigir vulnerabilidades individuais conforme elas surgem.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	---	2,3

CIBERSEGURANÇA CONTROLE 16: SEGURANÇA DE APLICAÇÕES

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
16.4	16.4	PROTEGER	O órgão estabelece e gerencia um inventário de componentes de software de terceiros?	Estabelecer e gerenciar um inventário atualizado de componentes de terceiros usados no desenvolvimento, geralmente chamados de “lista de materiais”, bem como componentes programados para uso futuro. Este inventário deve incluir quaisquer riscos que cada componente de terceiros possa representar a organização. Deve ser realizada uma revisão e/ou alteração deste inventário periodicamente, com o objetivo de identificar quaisquer mudanças ou atualização nesses componentes e validar a compatibilidade do mesmo.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	---	2, 3
16.5	16.5	PROTEGER	O órgão usa componentes de software de terceiros atualizados e confiáveis?	Utilizar apenas componentes de terceiros atualizados e confiáveis. Quando possível, escolher bibliotecas e estruturas pré-estabelecidas e comprovadas que forneçam a segurança adequada. É importante adquirir tais componentes de fornecedores e fontes confiáveis ou realizar a avaliação de vulnerabilidades do software antes de usar/adquirir.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 3/2013 IN nº 5/2021 NC 09 /IN01/DSIC/GSIPR	2,3
16.6	16.6	PROTEGER	O órgão estabelece e mantém um processo para a classificação de severidade de vulnerabilidades?	Estabelecer e manter um processo para a classificação de gravidade de vulnerabilidades capaz de facilitar a priorização na medida em que as vulnerabilidades descobertas são corrigidas. Esse processo deve incluir a definição de um nível mínimo de aceitabilidade de segurança para a liberação de código ou aplicações. A classificação de gravidade deve trazer uma forma sistemática de triagem de vulnerabilidades que venha a melhorar a gestão de riscos e ajuda a garantir que os bugs mais graves sejam priorizados. Revise o processo o e a classificação de vulnerabilidade periodicamente.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	---	2, 3
16.7	16.7	PROTEGER	O órgão usa modelos de configurações de segurança padrão para infraestrutura de aplicações?	Utilizar modelos de configuração de segurança padrão (Segurança by Default) recomendados pela equipe de segurança em componentes de infraestrutura de aplicações. Isso inclui servidores subjacentes, bancos de dados e servidores web e se aplica a contêineres de nuvem, componentes de Platform as a Service (PaaS) e componentes de Security as a Service (SaaS). Não permita que o software desenvolvido internamente enfraqueça as configurações de segurança da organização.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	---	2,3

CIBERSEGURANÇA CONTROLE 16: SEGURANÇA DE APLICAÇÕES

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
16.8	16.8	PROTEGER	O órgão separa sistemas de produção e não produção?	Manter ambientes separados para sistemas de produção e não produção.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	---	2,3
16.9	16.9	PROTEGER	O órgão treina desenvolvedores em conceitos de segurança de aplicações e codificação segura?	Garantir que todos os responsáveis pelo desenvolvimento de software recebam treinamento para escrever código seguro para seu ambiente de desenvolvimento e responsabilidades específicas. O treinamento deve incluir princípios gerais de segurança e práticas padrão de segurança para aplicações. O treinamento deve ser realizado periodicamente, é interessante estabelecer uma cultura de segurança entre os desenvolvedores.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	---	2,3
16.10	16.10	PROTEGER	O órgão aplica princípios de design seguro em arquiteturas de aplicações?	Aplicar princípios de design seguro em arquiteturas de aplicações. Os princípios de design seguro incluem o conceito de privilégio mínimo e aplicação de mediação para validar cada operação que o usuário faz, promovendo o conceito de “nunca confiar nas entradas do usuário”. Os exemplos incluem garantir que a verificação explícita de erros seja realizada e documentada para todas as entradas, incluindo tamanho, tipo de dados e intervalos ou formatos aceitáveis. O design seguro também significa minimizar a superfície de ataque da infraestrutura da aplicação, como desligar portas e serviços desprotegidos, remover programas e arquivos desnecessários e renomear ou remover contas padrão.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	---	2,3
16.11	16.11	PROTEGER	O órgão aproveita os módulos ou serviços controlados para componentes de segurança de aplicações?	Aproveitar módulos ou serviços controlados para componentes de segurança da aplicação, como gestão de identidade, criptografia e auditoria de logs. O uso de recursos para plataforma em funções críticas de segurança deve reduzir a carga de trabalho dos desenvolvedores e minimizará a probabilidade de erros de design ou implementação. Os sistemas operacionais modernos fornecem mecanismos eficazes para identificação, autenticação e autorização e disponibilizam esses mecanismos para as aplicações. Use apenas algoritmos de criptografia padronizados, atualmente aceitos e amplamente revisados. Os sistemas operacionais também fornecem	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	---	2,3

CIBERSEGURANÇA CONTROLE 16: SEGURANÇA DE APLICAÇÕES

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
				mecanismos para criar e manter logs de auditoria seguros.			
16.12	16.12	PROTEGER	O órgão implementa verificações de segurança em nível de código?	Utilizar ferramentas de análise estáticas e dinâmicas dentro do ciclo de vida da aplicação para verificar se as práticas de codificação seguras estão sendo utilizadas na organização.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	---	3
16.13	16.13	PROTEGER	O órgão realiza teste de invasão de aplicação?	Realizar testes de invasão em aplicações. Para aplicações críticas, o teste de invasão autenticado é mais adequado para localizar vulnerabilidades de codificação e de negócios do que a varredura de código e o teste de segurança automatizado. O teste de invasão depende da habilidade do testador para manipular manualmente uma aplicação como um usuário autenticado e não autenticado.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	---	3
16.14	16.14	PROTEGER	O órgão realiza a modelagem de ameaças?	Realizar a modelagem de ameaças. A modelagem de ameaças é o processo de identificar e abordar as falhas de design de segurança da aplicação em um desenho, antes que o código seja criado. É conduzido por profissionais especialmente treinados que avaliam o design da aplicação e medem os riscos de segurança para cada ponto de entrada e nível de acesso. O objetivo é mapear a aplicação, a arquitetura e a infraestrutura de uma forma estruturada para entender todos os pontos fracos.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	---	3

CIBERSEGURANÇA CONTROLE 17: GESTÃO DE RESPOSTA A INCIDENTES

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
17.1	17.1	RESPONDER	O órgão designa os colaboradores para gerenciar o tratamento de incidentes?	Designar os responsáveis para gerenciar o processo de tratamento de incidentes da organização. A equipe de gestão é responsável pela coordenação e documentação dos esforços de resposta e recuperação a incidentes, esta equipe pode formada por colaboradores internos, terceirizados ou pode contar com os dois tipos de colaborares. Casos em que a equipe for composta somente por funcionários terceirizados, a organização deve designar pelo menos um colaborador interno para supervisionar qualquer ação terceirizada.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020 IN nº 2/2020 IN nº 3/2021 NC 05 /IN01/DSIC/GSIPR, e seu anexo NC 08 /IN01/DSIC/GSIPR	1, 2, 3
17.2	17.2	RESPONDER	O órgão estabelece e mantém informações de contato para relatar incidentes de segurança?	Estabelecer e manter as informações de contato das pessoas que precisam ser informadas sobre os incidentes de segurança. Os contatos podem incluir funcionários internos, fornecedores terceirizados, policiais, provedores de seguros cibernéticos, agências governamentais relevantes, parceiros do Information Sharing and Analysis Center (ISAC) ou outras partes interessadas. Verifique os contatos periodicamente para garantir que as informações estejam atualizadas.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 3/2021 IN nº 4/2020 NC 05 /IN01/DSIC/GSIPR, e seu anexo	1, 2, 3
17.3	17.3	RESPONDER	O órgão estabelece e mantém um processo institucional para relatar incidentes?	Estabelecer e manter um processo institucional para a colaborares relatarem incidentes de segurança. O processo inclui cronograma de relatórios, pessoal responsável por para relatar, mecanismo para relatar e as informações mínimas a serem relatadas. É importante certificar que o processo está publicamente disponível para todos os colaboradores da organização. Deve ser realizada uma revisão periódica deste processo ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida de segurança.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 3/2021 IN nº 4/2020 NC 05 /IN01/DSIC/GSIPR, e seu anexo NC 08 /IN01/DSIC/GSIPR	1, 2, 3
17.4	17.4	RESPONDER	O órgão estabelece e mantém um processo de resposta a incidente?	Estabelecer e manter um processo de resposta a incidentes que aborde funções e responsabilidades, requisitos de conformidade e um plano de comunicação. Realize a revisão deste processo de forma periódica ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida de segurança.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 3/2021 IN nº 4/2020 NC 05 /IN01/DSIC/GSIPR, e seu anexo NC 08 /IN01/DSIC/GSIPR	2, 3

CIBERSEGURANÇA CONTROLE 17: GESTÃO DE RESPOSTA A INCIDENTES

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
17.5	17.5	RESPONDER	O órgão atribui funções e responsabilidades?	Atribuir funções e responsabilidades chave para resposta a incidentes, incluindo equipe jurídica, TI, segurança da informação, instalações, relações s públicas, recursos humanos, equipe de resposta a incidentes, conforme aplicável. Realize a revisão deste processo de forma periódica ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida de segurança. Realize a revisão desta medida de forma periódica ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida de segurança.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 3/2021 NC 05 /IN01/DSIC/GSIPR, e seu anexo NC 08 /IN01/DSIC/GSIPR	2, 3
17.6	17.6	RESPONDER	O órgão define mecanismos de comunicação durante a resposta a incidente?	Determinar quais mecanismos primários e secundários serão usados para relatar um incidente e se comunicar durante um incidente de segurança. Os mecanismos podem incluir ligações, e-mails ou cartas. Lembre-se de que certos mecanismos, como e-mails, podem ser afetados durante um incidente de segurança. Realize a revisão desta medida de forma periódica ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida de segurança.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 3/2021 IN nº 4/2020 NC 05 /IN01/DSIC/GSIPR, e seu anexo NC 08 /IN01/DSIC/GSIPR	2, 3
17.7	17.7	RECUPERAR	O órgão conduz exercícios de resposta a incidentes regularmente?	Planejar e conduzir exercícios e cenários rotineiros de resposta a incidentes para a equipe envolvida na resposta a incidentes, de forma a manter a conscientização e tranquilidade no caso de resposta a ameaças reais. Os exercícios devem testar os canais de comunicação, tomada de decisão e recursos técnicos da equipe de resposta a incidentes, contemplando a utilização das ferramentas e dados disponíveis.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 3/2021 NC 05 /IN01/DSIC/GSIPR, e seu anexo NC 08 /IN01/DSIC/GSIPR	2, 3
17.8	17.8	RECUPERAR	O órgão realiza análises pós-incidente?	Realizar análises pós-incidente. As análises pós-incidente ajudam a prevenir a recorrência do incidente por meio da identificação de lições aprendidas e ações de acompanhamento.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 3/2021 NC 05 /IN01/DSIC/GSIPR, e seu anexo NC 08 /IN01/DSIC/GSIPR	2, 3

CIBERSEGURANÇA CONTROLE 17: GESTÃO DE RESPOSTA A INCIDENTES

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
17.9	17.9	RECUPERAR	O órgão estabelece e mantém limites de incidentes de segurança?	Estabelecer e manter limites de incidentes de segurança, incluindo, no mínimo, a diferenciação entre um incidente e um evento. Os exemplos podem incluir: atividade anormal, vulnerabilidade de segurança, ameaça de segurança, violação de dados, incidente de privacidade etc. Realize a revisão desta medida de forma periódica ou quando ocorrerem mudanças significativas na organização que possam impactar esta medida de segurança.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	IN nº 1/2020 IN nº 2/2020 IN nº 3/2021 NC 05 /IN01/DSIC/GSIPR, e seu anexo NC 08 /IN01/DSIC/GSIPR	3

CIBERSEGURANÇA CONTROLE 18: TESTES DE INVASÃO

ID	ID CIS	FUNÇÃO NIST CSF	MEDIDA	DESCRIÇÃO DA MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS GSI	GRUPOS DE IMPLEMENTAÇÃO
18.1	18.1	IDENTIFICAR	O órgão elabora e mantém um programa de teste de invasão?	Estabelecer um programa para testes de invasão adequado ao tamanho, complexidade e maturidade da organização. O programa de teste de invasão deve levar em consideração o escopo do teste como rede, aplicação web, API, controles de instalações físicas e etc.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	2, 3
18.2	18.2	IDENTIFICAR	O órgão realiza testes de invasão externos periódicos?	Conduzir testes de invasão e externos regularmente. A teste de invasão externo deve ser reconhecido pela organização e deve ser capaz de detectar informações exploráveis que possam impactar a segurança da organização. Tal teste deve ser realizado por profissionais qualificados.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	2, 3
18.3	18.5	IDENTIFICAR	O órgão realiza testes de invasão internos periódicos?	Realize testes de invasão internos periódicos com base nos requisitos do programa de testes de invasão.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	3
18.4	18.3	PROTEGER	O órgão corrige os resultados dos testes de invasão?	Corrigir as descobertas do teste de invasão com base na política da organização para o escopo e a priorização de correção de vulnerabilidades.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	2, 3
18.5	18.4	PROTEGER	O órgão valida as medidas de segurança?	Validar as medidas de segurança após cada teste de invasão. Se necessário, modificar os conjuntos de regras e recursos para detectar as técnicas usadas durante o teste.	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	------	3

ANEXO V – TABELA DE CONTROLES e MEDIDAS DE PRIVACIDADE

PRIVACIDADE CONTROLE 19: INVENTÁRIO E MAPEAMENTO

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	REFERÊNCIAS NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
19.1	IDENTIFICAR-P	A organização documenta os sistemas, serviços e processos que tratam dados pessoais?	Art. 37	ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)	NIST ID.IM-P1	1, 2, 3
19.2	IDENTIFICAR-P	O órgão mapeia os agentes de tratamento (controlador, co-controladores e operadores) responsáveis pelo processamento de dados pessoais?	Art. 37	ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)	NIST ID.IM-P2	1, 2, 3
19.3	IDENTIFICAR-P	O órgão documenta as fases do tratamento em que o operador atua?	Art. 37	ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)	NIST ID.IM-P2 NIST ID.IM-P4	1, 2, 3
19.4	IDENTIFICAR-P	O órgão mapeia os fluxos ou ações do tratamento de dados pessoais?	Art. 37	ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)	NIST ID.IM-P8	1, 2, 3
19.5	IDENTIFICAR-P	O órgão mapeia o escopo (abrangência ou área geográfica) dos tratamentos de dados pessoais?	Art. 37	ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)	N/A	1, 2, 3
19.6	IDENTIFICAR-P	O órgão documenta a natureza (fonte) dos dados pessoais tratados?	Art. 37	ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)	N/A	1, 2, 3
19.7	IDENTIFICAR-P	A organização registra as bases legais que fundamentam as atividades de tratamento de dados pessoais e dados pessoais sensíveis?	Art. 7º Art. 11 Art. 23 Art. 37	ABNT NBR ISO/IEC 27701:2019 (item 7.2.2) ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)	N/A	1, 2, 3
19.8	IDENTIFICAR-P	O órgão inventaria as categorias dos dados pessoais e dados pessoais sensíveis objetos dos tratamentos realizados?	Art. 37	ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)	NIST ID.IM-P6	1, 2, 3
19.9	IDENTIFICAR-P	O órgão registra o tempo de retenção de dados pessoais tratados conforme a finalidade de cada processamento?	Art. 37	ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)	NIST ID.IM-P4	1, 2, 3
19.10	IDENTIFICAR-P	O órgão inventaria as categorias dos titulares de dados pessoais utilizados no tratamento?	Art. 37	ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)	NIST ID.IM-P3	1, 2, 3
19.11	IDENTIFICAR-P	O órgão registra os compartilhamentos de dados pessoais realizados com operadores terceiros e outras instituições conforme Art. 26 e 27 da LGPD, incluindo quais dados pessoais foram divulgados, a quem e com que finalidade?	Art. 26 Art. 27 Art. 37	ABNT NBR ISO/IEC 29151:2017 (item A.7.4) ABNT NBR ISO/IEC 27701:2019 (item 7.5.3 e 7.5.4)	NIST CM.AW-P4	1, 2, 3

PRIVACIDADE CONTROLE 19: INVENTÁRIO E MAPEAMENTO

ID	FUNÇÃO NIST PF	MEDIDA	LGPD	REFERÊNCIAS ISO	NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
				ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)		
19.12	IDENTIFICAR-P	O órgão mapeia os ambientes (ex: interno, nuvem, terceiros, etc) em que os dados pessoais objetos dos tratamentos são processados?	Art. 37	ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)	NIST ID.IM-P7	1, 2, 3
19.13	IDENTIFICAR-P	O órgão registra as transferências internacionais de dados pessoais realizadas conforme o Capítulo V da LGPD, incluindo quais dados pessoais foram divulgados e a quem?	Capítulo V Art. 37	ABNT NBR ISO/IEC 27701:2019 (item 7.5.3 e 7.5.4) ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)	N/A	1, 2, 3
19.14	IDENTIFICAR-P	O órgão mapeia os contratos estabelecidos/firmados com terceiros operadores responsáveis pelos tratamentos de dados pessoais?	Art. 37 Art. 39	ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)	N/A	1, 2, 3

PRIVACIDADE CONTROLE 20: FINALIDADE E HIPÓTESES LEGAIS

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
20.1	IDENTIFICAR-P	O órgão identifica as finalidades específicas antes da realização dos tratamentos de dados pessoais?	Art. 6º, I e II Art. 23	ABNT NBR ISO/IEC 27701:2019 (item 7.2.1)	NIST ID.IM-P5	1, 2, 3
20.2	IDENTIFICAR-P	O órgão identifica as hipóteses de tratamento antes da realização dos processamentos de dados pessoais?	Art. 7º Art. 11	ABNT NBR ISO/IEC 27701:2019 (item 7.2.1)	N/A	1, 2, 3
20.3	IDENTIFICAR-P	A organização identifica as bases legais que fundamentam as atividades de tratamento de dados pessoais e dados pessoais sensíveis antes da realização do tratamento?	Art. 7º Art. 11 Art. 23	ABNT NBR ISO/IEC 27701:2019 (item 7.2.2)	N/A	1, 2, 3
20.4	CONTROLAR-P	O órgão prioritariamente realiza tratamento de dados pessoais apenas para o atendimento de finalidade específica, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público?	Art. 23	ISO/IEC 29151:2017 (item A.4.1)	N/A	1, 2, 3
20.5	CONTROLAR-P	O órgão trata dados pessoais sensíveis para executar políticas públicas previstas apenas em leis e regulamentos?	Art. 11, inciso II, alíneas a, b	N/A	N/A	1, 2, 3
20.6	CONTROLAR-P	O órgão ao realizar tratamento de dados pessoais sensíveis baseado na hipótese de tutela da saúde, restringe o tratamento exclusivamente a profissionais de saúde, serviços de saúde ou autoridade sanitária?	Art. 11, inciso II, alínea f	N/A	N/A	1, 2, 3
20.7	CONTROLAR-P	O órgão adota mecanismos para assegurar que a divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa, em nenhuma hipótese, revele dados pessoais?	Art. 13, § 1º	N/A	N/A	1, 2, 3
20.8	CONTROLAR-P	O órgão, ao realizar estudos em saúde pública, trata os dados pessoais exclusivamente dentro da instituição, mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico, e estritamente para a finalidade de realização de estudos e pesquisas?	Art. 13	N/A	N/A	1, 2, 3
20.9	CONTROLAR-P	O órgão mantém processo contínuo de gerenciamento das hipóteses legais de tratamento, incluindo o desenvolvimento de capacidades para cumprimento de obrigações decorrentes da definição da hipótese legal de tratamento, tais como: gerenciamento do consentimento, elaboração de Avaliação de Legitimo Interesse, etc?	Art. 7° Art. 8° Art. 10 Art. 11 Art. 12 Art. 13	N/A	N/A	1, 2, 3

PRIVACIDADE CONTROLE 20: FINALIDADE E HIPÓTESES LEGAIS

ID	FUNÇÃO NIST PF	MEDIDA	LGPD	REFERÊNCIAS ISO	NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
20.10	CONTROLAR-P	O órgão, ao realizar compartilhamento de dados pessoais, adota medidas que assegurem a compatibilidade do propósito geral da finalidade original informada ao titular?	Art. 6, inciso I	N/A	N/A	1, 2, 3
20.11	CONTROLAR-P	O órgão ao coletar cookies identifica, no banner de segundo nível, as hipóteses legais utilizadas, de acordo com cada finalidade/categoria de cookie, utilizando o consentimento como principal hipótese legal, exceção feita aos cookies estritamente necessários, que podem se basear no legítimo interesse ou, se for caso, cumprimento de obrigações ou atribuições legais?	Art. 6º, inciso VI; Art. 7° Art. 9º Art. 11 Art. 18	ISO/IEC 29184 (item 5.3.15)	NIST CM.AW-P1	1, 2, 3
20.12	CONTROLAR-P	O órgão ao coletar cookies permite, no banner de segundo nível, a obtenção do consentimento específico de acordo com as categorias identificadas, observados o disposto na LGPD?	Art. 8º Art. 14 Art. 18	ISO/IEC 29184 (item 5.4.1) ISO/IEC 29151 (item A.3)	NIST CM.AW-P1 NIST CM.AW-P8 NIST CT.PO-P1	1, 2, 3
20.13	CONTROLAR-P	O órgão mantém o fornecimento do serviço quando os titulares de dados pessoais se recusam a fornecer o consentimento para cookies não necessários?	Art. 7º Art. 8º Art. 9º Art. 11	ISO/IEC 29151 (item A.3)	NIST CM.AW-P8 NIST CT.PO-P1	1, 2, 3
20.14	CONTROLAR-P	O tratamento de dados pessoais de crianças e adolescentes é realizado no seu melhor interesse com base em hipótese legal prevista pela LGPD e, no que couber, conforme preconizado pelo art. 14 da LGPD?	Art. 7º Art. 11 Art. 14 Art. 23	ABNT NBR ISO/IEC 27701:2019 (item 7.2.2)	N/A	1, 2, 3

PRIVACIDADE CONTROLE 21: GOVERNANÇA

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	REFERÊNCIAS NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
21.1	GOVERNAR-P	O órgão adota medidas para adequar seus processos e atividades relacionadas ao tratamento de dados pessoais às legislações/normativos de privacidade e proteção de dados vigentes?	Art. 50 § 2º inciso I	ABNT NBR ISO/IEC 27701:2019 (item 5.2.1) ABNT NBR ISO/IEC 27701:2019 (item 5.4)	NIST GV.PO-P	1, 2, 3
21.2	GOVERNAR-P	O órgão já elaborou e divulgou o seu Programa Institucional de Privacidade de Dados, conforme estabelecido no art.50 da LGPD?	Art. 50, § 2º, inciso I	ABNT NBR ISO/IEC 27701:2019 (item 5)	NIST GV.PO-P2	1, 2, 3
21.3	GOVERNAR-P	As funções e responsabilidades dos colaboradores envolvidos nos tratamentos de dados pessoais são claramente estabelecidas e comunicadas?	Art. 50	N/A	NIST GV.PO-P3 NIST GV.AT-P1 NIST GV.AT-P2 NIST GV.AT-P3 NIST GV.AT-P4	1, 2, 3
21.4	GOVERNAR-P	O órgão disponibiliza para o encarregado os recursos necessários para implementação da LGPD e acesso direto à alta administração?	Art. 50	ISO/IEC 29151 (item A.11.1)	N/A	1, 2, 3
21.5	GOVERNAR-P	O órgão determina as responsabilidades e respectivos papéis para o tratamento de dados pessoais com o(s) controlador(es) conjunto(s) envolvido(s)?	Art. 50	ABNT NBR ISO/IEC 27701:2019 (item 7.2.7)	NIST GV.PO-P3	2, 3
21.6	GOVERNAR-P	O órgão divulga a seus colaboradores internos e externos as políticas e procedimentos operacionais relacionados à proteção de dados pessoais?	Art. 50	ISO/IEC 29151 (item A.11.1, f)	NIST GV.PO-P1 NIST GV.PO-P4	1, 2, 3
21.7	GOVERNAR-P	Os requisitos legais, regulatórios e contratuais relativos à privacidade são compreendidos e direcionados por meio regras de boas práticas e de governança publicadas pela instituição?	Art. 50	N/A	NIST GV.PO-P5	1, 2, 3
21.8	GOVERNAR-P	No âmbito das operações de tratamento de dados pessoais, existe uma tolerância ao risco organizacional definida, claramente expressa e informada às partes interessadas do órgão?	Art. 50	N/A	NIST GV.RM-P2 NIST GV.RM-P3	2, 3
21.9	GOVERNAR-P	Foram definidos indicadores que serão utilizados para medir os resultados e desempenho do órgão na implementação do Programa Institucional de Privacidade de Dados?	Art. 50	N/A	NIST GV.MT-P	2, 3

PRIVACIDADE CONTROLE 21: GOVERNANÇA

ID	FUNÇÃO NIST PF	MEDIDA	LGPD	REFERÊNCIAS ISO	NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
21.10	GOVERNAR-P	O órgão instituiu uma equipe que realiza o monitoramento das vulnerabilidades técnicas dos serviços que tratam dados pessoais?	Art. 46	ABNT NBR ISOIEC 27701:2019 (item 6.9.6.1)	NIST PR.PO-P10	2, 3

PRIVACIDADE CONTROLE 22: POLÍTICAS, PROCESSOS E PROCEDIMENTOS

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	REFERÊNCIAS NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
22.1	GOVERNAR-P	A organização revisou e adequou a Política de Segurança da Informação ou instrumento similar à LGPD?	Art. 6º, inciso VII Art. 46 Art. 50 § 2º, inciso I, alíneas “a” e “d"	ABNT NBR ISO/IEC 27701:2019 (itens 5.3.2 e 6.2)	NIST PR.PO-P NIST GV.MT-P2	1, 2, 3
22.2	GOVERNAR-P	Há uma política vigente ou documento equivalente que dispõe sobre diretrizes de proteção de dados pessoais?	Art. 6º Art. 46 Art. 50, § 2º, inciso I, alíneas “a” e “d”	ABNT NBR ISO/IEC 29151:2017 (Item A.2) ABNT NBR ISO/IEC 27701:2019 (item 6.2)	NIST PR.PO-P	1, 2, 3
22.3	GOVERNAR-P	As políticas, processos e procedimentos de gerenciamento de risco de privacidade do tratamento de dados pessoais são identificados, estabelecidos, avaliados, gerenciados e acordados pelas partes interessadas organizacionais, e seu progresso medido e comunicado?	Art. 6, X Art. 38 Art. 46 Art. 50, § 2º, inciso I, alíneas 'a'; 'd'; 'f'	N/A	NIST ID.DE-P1 NIST GV.MT-P4	2, 3
22.4	GOVERNAR-P	Os instrumentos convocatórios (editais licitatórios) estão adequados à LGPD?	Art. 39 Art. 50	ISO/IEC 29151:2017 (Item 15.1.2)	NIST GV.PO-P5	1, 2, 3
22.5	GOVERNAR-P	O órgão fornece um processo para monitorar as leis e políticas de privacidade com o objetivo de identificar alterações que afetem o programa de proteção de dados pessoais?	Art. 50, § 2º, inciso I, alínea “h”	ISO/IEC 29151 (item A.13)	NIST GV.MT-P3	1, 2, 3
22.6	CONTROLAR-P	A instituição estabelece um processo formal para a concessão de direitos de acesso privilegiado para o processamento de dados pessoais?	Art. 6º, inciso VIII Art. 46 Art. 47 Art. 49	ISO/IEC 29151:2017 (item 9.2.4)	NIST CT.PO-P1	1, 2, 3
22.7	CONTROLAR-P	O órgão estabelece procedimento ou metodologia para assegurar que os princípios da LGPD estão sendo respeitados desde a fase de concepção do produto ou do serviço até a sua execução (Privacy by Design)?	Art. 6º Art. 46 § 2º Art. 47 Art. 49	ISO/IEC 29151:2017 (Item 14.2.10) ABNT NBR ISO/IEC 27701:2019 (item 7.4)	NIST GV.PO-P2 NIST CT.DM-P10	1, 2, 3
22.8	CONTROLAR-P	A instituição implementa processos para que o tratamento dos dados pessoais seja preciso, completo, atualizado, adequado e relevante para a finalidade de uso?	Art. 6º, inciso I, II e V Art. 23, inciso I	ISO/IEC 29151:2017 (item A.8)	N/A	1, 2, 3
22.9	CONTROLAR-P	O órgão estabelece políticas, procedimentos e adota mecanismos documentados para o descarte de dados pessoais?	Art. 50	ISO/IEC 29151 (item A.7.1, A.7.2)	NIST CT.PO-P2	2, 3

PRIVACIDADE CONTROLE 22: POLÍTICAS, PROCESSOS E PROCEDIMENTOS

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	REFERÊNCIAS NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
22.10	CONTROLAR-P	A organização adequou seu Plano de Resposta a Incidentes (ou documento similar) à LGPD de forma a tratar violações relativas à privacidade dos titulares de dados pessoais?	Art. 50, § 2º, inciso I, alínea "g"	ABNT NBR ISO/IEC 27701:2019 (item 6.13)	NIST PR.PO-P7	1, 2, 3
22.11	CONTROLAR-P	A organização estabeleceu procedimentos para comunicar à Autoridade Nacional de Proteção de Dados e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares?	Art. 48 Art. 50, § 2º, inciso I, alínea "g"	ABNT NBR ISO/IEC 27701:2019 (6.13.1.5)	N/A	1, 2, 3
22.12	CONTROLAR-P	O órgão revisa periodicamente as políticas, processos, planos e procedimentos de proteção de dados pessoais?	Art. 50, § 2º, inciso I, alínea "h"	ISO/IEC 29151 (item 5.1.3)	NIST GV.MT-P2 NIST GV.MT-P3	2, 3

PRIVACIDADE CONTROLE 23: CONSCIENTIZAÇÃO E TREINAMENTO

ID	FUNÇÃO NIST PF	MEDIDA	LGPD	REFERÊNCIAS ISO	NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
23.1	GOVERNAR-P	O órgão implementa e mantêm uma estratégia abrangente de treinamento e conscientização a fim de garantir que a força de trabalho compreenda sobre suas responsabilidades e procedimentos de proteção de dados pessoais?	Art. 50	ISO/IEC 29151 (item A.11.5 a)	GV.AT-P	1, 2, 3
23.2	GOVERNAR-P	O plano de desenvolvimento de pessoas do órgão contempla treinamento adequado sobre a temática de privacidade e de proteção de dados pessoais?	Art. 50	ISO/IEC 29151 (item A.11.5 a)	GV.AT-P	1, 2, 3
23.3	GOVERNAR-P	As ações de treinamento e conscientização realizadas pela instituição visam a manter os colaboradores atualizados sobre os desenvolvimentos no ambiente regulatório, contratual e tecnológico que possam afetar a conformidade de privacidade da organização?	Art. 50	ISO/IEC 29151 (item A.11.5 c)	GV.AT-P	1, 2, 3
23.4	GOVERNAR-P	O órgão executa regularmente (por exemplo, anual) ou conforme necessário (por exemplo, após um incidente) treinamento básico e direcionado de proteção de dados pessoais conforme as funções das pessoas envolvidas com o tratamento?	Art. 50	ISO/IEC 29151 (item A.11.5 c)	GV.AT-P	1, 2, 3

PRIVACIDADE CONTROLE 24: MINIMIZAÇÃO DE DADOS

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
24.1	CONTROLAR-P	O órgão avalia e classifica os dados pessoais a serem coletados em obrigatórios e opcionais a fim de priorizar somente a coleta dos dados obrigatórios para a prestação do serviço?	Art. 18	ISO/IEC 29151 (item A.5 e A.6)	NIST CT.DP-P	2, 3
24.2	CONTROLAR-P	O órgão restringe ao máximo a coleta de dados de forma que seja suficiente para atender a finalidade específica do tratamento?	Art. 18, inciso IV	ISO/IEC 29151 (item A.5 e A.6)	NIST CT.DP-P	1, 2, 3
24.3	CONTROLAR-P	O órgão, ao realizar o tratamento de dados pessoais, aplica o princípio da minimização de dados para restringir a quantidades de dados pessoais ao estritamente necessário para atendimento da finalidade específica?	Art. 6º - III Art. 18, inciso IV	ISO/IEC 29151:2017 (Item A.5 e A.6) ABNT NBR ISO/IEC 27701:2019 (item 7.4.1)	NIST CT.DP-P	1, 2, 3
24.4	CONTROLAR-P	O órgão adota medidas para assegurar que as configurações de privacidade sejam aplicadas por padrão (Privacy by Default) nos serviços fornecidos?	Art. 6º - III Art. 46, § 2º	ABNT NBR ISO/IEC 27701:2019 (item 7.4)	N/A	2, 3
24.5	CONTROLAR-P	O órgão adota o princípio 'need-to-how', em que deve ser dado acesso apenas aos dados pessoais necessários para o desempenho das funções dos colaboradores?	Art. 46	ISO/IEC 29151 (item A.6)	NIST CT.DP-P	2, 3
24.6	CONTROLAR-P	O órgão adota como padrão, sempre que possível, interações e transações que não envolvam a identificação dos titulares?	Art. 7º Art. 11 Art. 12 Art. 13 Art. 16 Art. 18	ISO/IEC 29151 (item A.5 e A.6)	NIST CT.DP-P1 NIST CT.DP-P2	3
24.7	CONTROLAR-P	O órgão adota mecanismos para limitar a vinculação dos dados pessoais coletados?	Art. 7º Art. 11 Art. 12 Art. 13 Art. 16 Art. 18	ISO/IEC 29151 (item A.5 e A.6)	NIST CT.DP-P1 NIST CT.DP-P2	3
24.8	CONTROLAR-P	As referências de atributos são substituídas por valores de atributos? Por exemplo, para o atributo "aniversário", um valor de atributo poderia ser "1/12/1980" e uma referência de atributo seria "nascido em dezembro".	Art. 6º, inciso VII Art. 46 Art. 47 Art. 49	N/A	NIST CT.DP-P5	3

PRIVACIDADE CONTROLE 24: MINIMIZAÇÃO DE DADOS

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
24.9	CONTROLAR-P	Os dados pessoais utilizados em ambiente de TDH (teste, desenvolvimento e homologação) passam por um processo de anonimização?	Art. 6º, inciso VII Art. 12, § 3º Art. 46 Art. 47 Art. 49	ISO/IEC 29151:2017 (Item 12.1.5)	NIST CT.DP-P	2, 3
24.10	CONTROLAR-P	O órgão realiza revisão periódica dos dados pessoais tratados para que continuem a ser o mínimo necessários para cumprir com a finalidade?	Art. 6º, inciso I, II e III Art. 18	ISO/IEC 29151 (item A.5 e A.6)	NIST CT.DP-P	3
24.11	CONTROLAR-P	O órgão determina e desidentifica os dados pessoais que necessitam ser anonimizados de acordo com o tratamento e exigências estabelecidas por leis aplicáveis?	Art. 7º Art. 11 Art. 12 Art. 13 Art. 16 Art. 18	ISO/IEC 29151 (item A.5 e A.6)	NIST CT.DP-P	2, 3
24.12	CONTROLAR-P	Ao fornecer a base de informações para órgãos de pesquisa ou para realização de estudos em saúde pública, os dados pessoais são, sempre que possível, anonimizados ou pseudoanonimizados?	Art. 7º, inciso IV Art. 11, inciso II alínea c Art. 13	ISO/IEC 29151:2017 (item A.6)	NIST CT.DP-P	1, 2, 3
24.13	CONTROLAR-P	O órgão ao coletar cookies disponibiliza botão de fácil visualização, no banner de primeiro e de segundo nível, que permita rejeitar todos os cookies não-necessários?	Art. 6º, incisos III VI Art. 8º Art. 9º Art. 18	ISO/IEC 29184 (item 5.4.6) ABNT NBR ISO/IEC 27701:2019 (item 7.4.1) ISO/IEC 29151 (item A.5 e A.6)	CM.AW-P1 CM.AW-P2	1, 2, 3
24.14	CONTROLAR-P	O órgão ao coletar cookies desativa, no banner de primeiro nível, cookies baseados no consentimento por padrão (opt-in)?	Art. 6º, incisos III e VI Art. 8º Art. 9º Art. 18	ABNT NBR ISO/IEC 27701:2019 (item 7.4.1)	CM.AW-P1 CM.AW-P2	1, 2, 3
24.15	CONTROLAR-P	O órgão ao coletar cookies classifica os cookies em categorias no banner de segundo nível?	Art. 6º, inciso VI; Art. 8º Art. 9º Art. 18	ISO/IEC 29184 (item 5.4.6) ISO/IEC 29151 (item A.5 e A.6)	CM.AW-P1 CM.AW-P2	1, 2, 3

PRIVACIDADE CONTROLE 25: GESTÃO DO TRATAMENTO

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS			GRUPOS DE IMPLEMENTAÇÃO
			LGPD	ISO	NIST - PF	
25.1	CONTROLAR-P	O órgão configura os sistemas para registrar a data em que os dados pessoais são coletados, criados, atualizados, excluídos ou arquivados?	Art. 50	ISO/IEC 29151 (item A.7)	NIST CT.DM-P8	2, 3
25.2	CONTROLAR-P	O órgão limita a quantidade de processamento sobre os dados pessoais sob sua custódia?	Art. 6º, inciso III	ISO/IEC 29151 (item A.7)	NIST CT.DM-P	1, 2, 3
25.3	CONTROLAR-P	O órgão define e documenta os objetivos da minimização do tratamento sobre os dados pessoais sob sua custódia?	Art. 6º, inciso III	ABNT NBR ISO/IEC 27701:2019 (item 7.4.4)	NIST CT.DM-P	3
25.4	CONTROLAR-P	Os dados são mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral?	Art. 25	N/A	NIST ID.DE-P4	1, 2, 3
25.5	CONTROLAR-P	Há procedimentos para garantir que quando há o término do tratamento de dados do titular no órgão, este segue as hipóteses previstas no artigo 15 da LGPD?	Art. 15	N/A		1, 2, 3
25.6	CONTROLAR-P	A instituição utiliza técnicas ou métodos apropriados para garantir exclusão ou destruição segura de dados pessoais (incluindo originais, cópias e registros arquivados), de modo a impedir sua recuperação?	Art. 6º, inciso VII Art. 46 Art. 47 Art. 49	ISO/IEC 29151:2017 (item 8.3.3, A.7.1 "b" e A.7.2) ABNT NBR ISO/IEC 27701:2019 (itens 7.4.6, 7.4.8, 8.4.1 e 8.4.2)	NIST CT.PO-P2 NIST CT.DM-P4 NIST CT.DM-P5	2, 3
25.7	CONTROLAR-P	A organização avalia se os dados pessoais são retidos (armazenados) durante o tempo estritamente necessário para cumprir com as finalidades de tratamento de dados pessoais que foram identificadas?	Art. 6º, inciso I e III Art. 16	ABNT NBR ISO/IEC 27701:2019 (item 7.4.7) ISO/IEC 29151:2017 (item A.7.1 a)	N/A	1, 2, 3
25.8	CONTROLAR-P	O órgão implementa no serviço a detecção da expiração do período de retenção e aviso automático de que deve ser avaliada a possibilidade de exclusão dos dados pessoais após o cumprimento das finalidades?	Art. 6º Art. 15 Art. 16	ISO/IEC 29151 (item A.7.1)	NIST CT.DM-P	3
25.9	CONTROLAR-P	O órgão bloqueia e adota medidas de proteção para isentar de processamento adicional os dados pessoais quando os propósitos informados ao titular são atingidos, mas a retenção for exigida pelas leis aplicáveis?	Art. 6º Art. 15 Art. 16	ISO/IEC 29151 (item A.7.1)	NIST CT.DM-P	3

PRIVACIDADE CONTROLE 26: ACESSO E QUALIDADE

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
26.1	CONTROLAR-P	Há um canal de comunicação ativo, seguro e autenticado com um ponto de contato para receber e responder a reclamações e requisições do titular sobre o tratamento de dados pessoais?	Art. 41, § 2º, inciso I Art. 46	ISO/IEC 29151:2017 (Item A.10.3)	NIST CM.PO-P	1, 2, 3
26.2	CONTROLAR-P	O órgão adota meios para verificar a validade e exatidão das solicitações de correção realizadas por parte do titular de dados pessoais?	Art. 6º Art. 18 Art. 19	ISO/IEC 29151 (item A.8 e)	NIST CT.DM-P NIST CT.PO-P2	2, 3
26.3	CONTROLAR-P	O órgão fornece meios para que o titulares de dados pessoais possam solicitar as correções dos dados pessoais ou contestar a exatidão e integridade dos dados pessoais com direito a confirmação de recebimento da solicitação?	Art. 6º Art. 18 Art. 19	ISO/IEC 29151 (item A.10.1)	NIST CT.DM-P NIST CT.PO-P2	1, 2, 3
26.4	CONTROLAR-P	O órgão fornece, na medida do possível, as respostas ao titular de dados pessoais de forma equivalente àquela em que a solicitação foi realizada?	Art. 6º Art. 18 Art. 19	ISO/IEC 29151 (item A.10.1)	NIST CT.DM-P NIST CT.PO-P2	2, 3
26.5	CONTROLAR-P	O órgão adota mecanismos de rastreamento para garantir que todas as petições e reclamações recebidas dos titulares de dados pessoais sejam analisadas e tratadas adequadamente em tempo hábil?	Art. 6º Art. 18 Art. 19	ISO/IEC 29151 (item A.10.3)	NIST CT.DM-P NIST CT.PO-P2	1, 2, 3
26.6	CONTROLAR-P	São utilizados padrões técnicos, principalmente os definidos pela ANPD, que facilitem o controle pelos titulares dos seus dados pessoais?	Art. 51	N/A	N/A	2, 3
26.7	CONTROLAR-P	O órgão implementa meios práticos para permitir que os titulares gerenciem os seus dados pessoais, de forma simples, rápida e eficiente, e que não acarrete atrasos indevidos ou custo ao titular?	Art. 6º Art. 18 Art. 19	ISO/IEC 29151 (item A.10.1)	NIST CT.DM-P NIST CT.PO-P2	2, 3
26.8	CONTROLAR-P	O órgão confirma, na medida do possível, a exatidão, relevância e integridade dos dados pessoais na coleta?	Art. 6º Art. 18 Art. 19	ISO/IEC 29151 (item A.8)	NIST CT.DM-P NIST CT.PO-P2	3

PRIVACIDADE CONTROLE 26: ACESSO E QUALIDADE

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	REFERÊNCIAS NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
26.9	CONTROLAR-P	A instituição implementa medidas que visam a garantir e maximizar a exatidão, qualidade e completude dos dados pessoais coletados?	Art. 6º, inciso V Art. 18, inciso III	ISO/IEC 29151:2017 (item A.8 g)	NIST CT.PO-P2 NIST CT.DM-P	1, 2, 3
26.10	CONTROLAR-P	O órgão revisa periodicamente e corrige, conforme necessário, os dados pessoais imprecisos ou desatualizados?	Art. 6º, inciso V Art. 18, inciso III	ISO/IEC 29151 (item A.8 f)	NIST CT.DM-P NIST CT.PO-P2	2, 3
26.11	COMUNICAR-P	O órgão fornece informações ao titular de dados pessoais sobre o andamento de suas solicitações?	Art. 6º, inciso VI; Art. 8º Art. 9º Art. 18	ISO/IEC 29151 (item A.10.1 h)	N/A	2, 3
26.12	COMUNICAR-P	O órgão comunica qualquer alteração, correção ou remoção dos dados pessoais para operadores e terceiros com quem os dados pessoais foram compartilhados?	Art. 6º Art. 18 Art. 39	ISO/IEC 29151 (item A.10.2)	NIST CT.DM-P NIST CT.PO-P2 NIST CM.AW.P5	1, 2, 3

PRIVACIDADE CONTROLE 27: COMPARTILHAMENTO, TRANSFERÊNCIA E DIVULGAÇÃO

ID	FUNÇÃO NIST PF	MEDIDA	LGPD	REFERÊNCIAS ISO	NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
27.1	IDENTIFICAR-P	O órgão identifica os compartilhamentos de dados pessoais realizados com operadores terceiros e outras instituições conforme Art. 26 e 27 da LGPD, incluindo quais dados pessoais foram divulgados, a quem, a que horas e com que finalidade?	Art. 26 e 27	N/A	CM.AW-P4	1, 2, 3
27.2	IDENTIFICAR-P	O órgão identifica as transferências internacionais de dados pessoais realizadas conforme o Capítulo V da LGPD, incluindo quais dados pessoais foram divulgados, a quem, a que horas e com que finalidade?	Art. 33 Art. 34 Art. 35 Art. 36	N/A	CM.AW-P4	1, 2, 3
27.3	CONTROLAR-P	O órgão, ao compartilhar dados pessoais, adota um processo de formalização e registro, identificando objeto e finalidade, base legal e duração do tratamento?	Art. 25 Art. 26 Art. 27 Art. 30	N/A	CT.PO-P2	1, 2, 3
27.4	CONTROLAR-P	O órgão solicita descrição formal das medidas de proteção de dados pessoais adotadas pelas entidades com quem compartilha dados pessoais?	Art. 25 Art. 26 Art. 27 Art. 30	N/A	CT.PO-P2	2, 3
27.5	CONTROLAR-P	O órgão observa o disposto pelo art. 33-36 da LGPD para a realização de transferência internacional de dados pessoais?	Art. 33 Art. 34 Art. 35 Art. 36	ABNT NBR ISO/IEC 29151:2017 (item A.13.2) ABNT NBR ISO/IEC 27701:2019 (item 7.5.1, 7.5.2, 8.5.1 e 8.5.2)	N/A	1, 2, 3

PRIVACIDADE CONTROLE 28: SUPERVISÃO EM TERCEIROS

ID	FUNÇÃO NIST PF	MEDIDA	LGPD	REFERÊNCIAS ISO	NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
28.1	CONTROLAR-P	O órgão estabelece as funções e responsabilidades do operador envolvido no tratamento de dados pessoais, principalmente a notificação em caso de violação de dados pessoais?	Art. 39	ISO/IEC 29151 (item A.11.3 c)	NIST GV.PO-P4 NIST GV.PO-P5 NIST GV.AT-P4	1, 2, 3
28.2	CONTROLAR-P	São estabelecidos acordos de confidencialidade, termos de responsabilidade ou termos de sigilo com operadores de dados pessoais controlados pelos órgãos?	Art. 39	ISO/IEC 29151:2017 (Item 13.2.5)	NIST GV.PO-P4 NIST GV.PO-P5	1, 2, 3
28.3	CONTROLAR-P	O órgão estabelece no contrato que o operador não processe os dados pessoais para finalidades que divergem da finalidade principal informada pelo controlador?	Art. 23 Art. 39	ABNT NBR ISO/IEC 27701:2019 (item 8.2.2)	NIST GV.PO-P4 NIST GV.PO-P5 NIST GV.AT-P4	1, 2, 3
28.4	CONTROLAR-P	O órgão determina por contrato o assunto e o prazo do serviço a ser prestado, a extensão, a forma e a finalidade do tratamento de dados pessoais pelo operador, bem como os tipos de dados pessoais processados?	Art. 39	ISO/IEC 29151 (item A.11.3 d)	NIST GV.PO-P4 NIST GV.PO-P5 NIST GV.AT-P4	1, 2, 3
28.5	CONTROLAR-P	O órgão documenta no contrato de nível de serviço os requisitos de proteção de dados pessoais que os operadores de dados pessoais devem atender?	Art. 39	ISO/IEC 29151 (item A.11.3 a)	NIST GV.PO-P4 NIST GV.PO-P5 NIST GV.AT-P4	2, 3
28.6	CONTROLAR-P	O órgão adota meios para garantir que os sistemas do operador de dados pessoais tenham mecanismos de proteção de dados implementados?	Art. 39	ABNT NBR ISO/IEC 27701:2019 (item 7.2.6)	NIST GV.PO-P4 NIST GV.AT-P4	3
28.7	CONTROLAR-P	O órgão instrui ao operador que implemente meios práticos para permitir que os titulares exerçam seu direito de gerenciamento dos dados pessoais?	Art. 6º, incisos IV e V Art. 8º § 5º Art. 9º § 2º Art. 18 Art. 39	ABNT NBR ISO/IEC 27701:2019 (item 7.3.4, 7.3.5, 7.3.6, 7.3.9 e 8.3)	NIST GV.PO-P4 NIST GV.AT-P4	2, 3
28.8	CONTROLAR-P	O órgão exige do operador o cumprimento de todas as cláusulas estipuladas em contrato sobre divulgação de dados pessoais, a menos que proibido por lei?	Art. 39	ISO/IEC 29151 (item A.7.3 e A.11.3 g) ABNT NBR ISO/IEC 27701:2019 (item 8.5.4 e 8.5.5)	NIST GV.PO-P4 NIST GV.PO-P5 NIST GV.AT-P4	1, 2, 3
28.9	CONTROLAR-P	O órgão exige que o operador o informe sobre assuntos envolvendo o tratamento de dados pessoais para que o controlador esteja em conformidade com suas obrigações, principalmente em casos de solicitações juridicamente vinculativas para divulgação de dados pessoais, violação de dados pessoais, sobre alterações relevantes ao serviço?	Art. 39 Art. 44 Art. 45	ISO/IEC 29151 (item A.11.3 i) ABNT NBR ISO/IEC 27701:2019 (item 8.2.4, 8.2.5 e 8.5.4)	NIST GV.PO-P4 NIST GV.PO-P5 NIST GV.AT-P4	1, 2, 3

PRIVACIDADE CONTROLE 28: SUPERVISÃO EM TERCEIROS

ID	FUNÇÃO NIST PF	MEDIDA	LGPD	REFERÊNCIAS ISO	NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
28.10	CONTROLAR-P	O órgão especifica as condições sob as quais o operador deve devolver ou descartar com segurança os dados pessoais após a conclusão do serviço, rescisão de qualquer contrato ou de outra forma mediante solicitação do controlador?	Art. 15 Art. 16 Art. 39 Art. 46	ISO/IEC 29151 (item A.11.3 e) ABNT NBR ISO/IEC 27701:2019 (item 7.4.8 e 8.4.2)	NIST GV.PO-P NIST GV.AT-P4 NIST CT.PO-P2	3
28.11	CONTROLAR-P	O órgão especifica no contrato entre controlador e operador sobre o uso de subcontratados para processar dados pessoais?	Art. 39	ISO/IEC 29151 (item A.7.5) ABNT NBR ISO/IEC 27701:2019 (item 8.5.6, 8.5.7 e 8.5.8)	NIST GV.PO-P4 NIST GV.PO-P5 NIST GV.AT-P4	2, 3
28.12	CONTROLAR-P	O órgão monitora e inspeciona a implementação dos requisitos estabelecidos nas cláusulas contratuais pelos operadores?	Art. 39	ISO/IEC 29151 (item A.11.3 b)	NIST GV.PO-P4 NIST GV.PO-P5 NIST GV.AT-P4	2, 3
28.13	CONTROLAR-P	O órgão realizou revisão das cláusulas contratuais em vigência com os operadores terceiros para adequá-los à LGPD?	Art. 39	ISO/IEC 29151:2017 (Item 15.1.2, A.7.5 e A.11.3) ABNT NBR ISO/IEC 27701:2019 (item 7.2.6)	NIST GV.PO-P5 NIST GV.PO-P4 NIST GV.AT-P4	1, 2, 3

PRIVACIDADE CONTROLE 29: ABERTURA, TRANSPARÊNCIA E NOTIFICAÇÃO

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
29.1	CONTROLAR-P	O órgão adota meios para apresentar as informações de tratamento de dados pessoais de forma clara para que possam ser compreendidas por uma pessoa que não esteja familiarizada com as tecnologias da informação, internet ou jargões jurídicos?	Art. 6º, inciso VI; Art. 8º, § 1º Art. 9º Art. 18, inciso I, VII e VIII	ISO/IEC 29151 (item A.9.1 e) ABNT NBR ISO/IEC 27701:2019 (item 7.3.3)	NIST CM.AW-P1 NIST CM.AW-P2	1, 2, 3
29.2	CONTROLAR-P	O órgão adota meios para disponibilizar a política de privacidade em local de fácil acesso, antes ou no momento do tratamento de dados pessoais, sem a necessidade de o titular ter que solicitá-lo especificamente?	Art. 6º, inciso VI; Art. 8º Art. 9º Art. 18	ISO/IEC 29151 (item A.9.1)	NIST CM.AW-P1 NIST CM.AW-P2	2, 3
29.3	CONTROLAR-P	O órgão adota algum mecanismo, sempre que possível, para comprovar que o titular de dados pessoais obteve acesso à política de privacidade fornecida?	Art. 6º, inciso VI; Art. 8º Art. 9º Art. 18	ISO/IEC 29151 (item A.9.1 i)	NIST CM.AW-P1 NIST CM.AW-P2	1, 2, 3
29.4	CONTROLAR-P	O órgão revisa a política de privacidade, cookies e outras aplicáveis ao tratamento de dados pessoais, antes ou assim que possível, para refletir mudanças realizadas no tratamento?	Art. 6º, inciso VI; Art. 8º, § 1º Art. 9º Art. 18, inciso I, VII e VIII	ISO/IEC 29151 (item A.9.1 c)	NIST CM.AW-P1 NIST CM.AW-P2	1, 2, 3
29.5	COMUNICAR-P	O órgão destaca na Política de Privacidade informações sobre os dados pessoais que a organização coleta e a(s) finalidade(s) do tratamento para a qual a coleta é realizada, hipóteses e bases legais?	Art. 6º, inciso VI; Art. 8º Art. 9º Art. 18	ISO/IEC 29151 (item A.9.1) ABNT NBR ISO/IEC 27701:2019 (item 7.3.2)	NIST CM.AW-P1 NIST CM.AW-P2	1, 2, 3
29.6	COMUNICAR-P	A identidade e as informações de contato do encarregado estão divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador?	Art. 41, § 1º	ABNT NBR ISO/IEC 27701:2019 (item 6.3.1)	NIST CM.PO-P1 NIST CM.PO-P2	1, 2, 3
29.7	COMUNICAR-P	O órgão fornece informações aos titulares sobre como é realizado o tratamento de dados pessoais, tais como o período de retenção dos dados pessoais coletados, entre outras ações de tratamento?	Art. 6º, inciso VI; Art. 8º Art. 9º Art. 18	ISO/IEC 29151 (item A.9.1 a) ABNT NBR ISO/IEC 27701:2019 (item 7.3.2)	NIST CM.AW-P1 NIST CM.AW-P2	1, 2, 3
29.8	COMUNICAR-P	Os titulares de dados são informados quando há alterações na forma de tratamento dos dados pessoais?	Art. 6º, inciso VI; Art. 8º Art. 9º	ISO/IEC 29151:2017 (item A.9.1)	NIST CM.AW-P1 NIST CM.AW-P5	1, 2, 3
29.9	COMUNICAR-P	O órgão fornece orientações ao titular sobre a forma e meios utilizados de gerenciamento aos dados pessoais?	Art. 6º, inciso VI; Art. 8º Art. 9º Art. 18	ISO/IEC 29151 (item A.9)	NIST CM.AW-P1 NIST CM.AW-P2	2, 3

PRIVACIDADE CONTROLE 29: ABERTURA, TRANSPARÊNCIA E NOTIFICAÇÃO

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	REFERÊNCIAS NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
				ABNT NBR ISO/IEC 27701:2019 (item 7.3.2)		
29.10	COMUNICAR-P	O órgão informa se a organização compartilha dados pessoais com entidades externas, os dados pessoais compartilhados e a finalidade para tal compartilhamento?	Art. 6º, inciso VI; Art. 8º **Art. 9º, inciso V** Art. 18	ISO/IEC 29151 (item A.9.1 a) ABNT NBR ISO/IEC 27701:2019 (item 7.3.2)	NIST CM.AW-P1 NIST CM.AW-P2 NIST CM.AW-P4	1, 2, 3
29.11	COMUNICAR-P	O órgão fornece informações sobre a proteção e descarte seguro dos dados pessoais coletados?	Art. 6º, inciso VI; Art. 8º Art. 9º Art. 18	**ISO/IEC 29151 (item A.9.1 a)** ABNT NBR ISO/IEC 27701:2019 (item 7.3.2)	NIST CM.AW-P1	2, 3
29.12	COMUNICAR-P	O órgão fornece, quando solicitado por instituição competente, informações relativas a violações de privacidade dos titulares, juntamente com quaisquer ações associadas que o solicitante possa tomar para mitigar os riscos adicionais decorrentes da violação?	Art. 48	**ISO/IEC 29151 (item A.9.2 j)**	NIST CM.AW-P1	1, 2, 3

PRIVACIDADE CONTROLE 30: AVALIAÇÃO DE IMPACTO, MONITORAMENTO E AUDITORIA

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	REFERÊNCIAS NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
30.1	GOVERNAR-P	O órgão observa o conteúdo mínimo a ser inserido no Relatório de Impacto à Proteção de Dados Pessoais - RIPD conforme o disposto no Art. 38, parágrafo único da LGPD?	Art. 5º XVII Art. 38	ABNT NBR ISO/IEC 29134:2017 (Item 5, 6 e 7 e Anexos A,B,C e D) ABNT NBR ISOIEC 27701:2019 (5.6.2, 5.6.3 e 7.2.5)	NIST ID.RA-P NIST CM.AW-P1	1, 2, 3
30.2	GOVERNAR-P	O órgão estabelece processo para avaliar o impacto na privacidade ao fornecer serviços que tratam dados pessoais?	Art. 4º, § 3º Art. 10, § 3º Art. 32 Art. 38 Art. 46 Art. 47 Art. 49 Art 50, inciso I alínea d	ISO/IEC 29151 (item A.11.2)	NIST ID.RA-P NIST GV.MT-P	1, 2, 3
30.3	GOVERNAR-P	A organização avalia os riscos dos processos de tratamento de dados pessoais que foram identificados?	Art. 4º, § 3º Art. 10, § 3º Art. 32 Art. 38 Art. 46 Art. 47 Art. 49 Art 50, inciso I alínea d	ISO/IEC 29134:2017 (item 6.4.4)	NIST ID.RA-P	1, 2, 3
30.4	GOVERNAR-P	O órgão documenta os riscos de privacidade oriundos da avaliação de impacto à Proteção de Dados Pessoais?	Art. 10, § 3º Art. 32 Art. 38 Art. 46 Art. 47 Art. 49 Art 50, inciso I alínea d	ISO/IEC 29151 (item A.11.2)	NIST ID.RA-P	1, 2, 3
30.5	GOVERNAR-P	O órgão documenta as medidas de proteção de dados pessoais adotadas para mitigação do impacto à Proteção de Dados Pessoais?	Art. 10, § 3º Art. 32 Art. 38 Art. 46 Art. 47 Art. 49 Art 50, inciso I alínea d	ISO/IEC 29151 (item A.11.2)	NIST ID.RA-P	1, 2, 3

PRIVACIDADE CONTROLE 30: AVALIAÇÃO DE IMPACTO, MONITORAMENTO E AUDITORIA

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	REFERÊNCIAS NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
30.6	GOVERNAR-P	O órgão realiza e documenta os resultados de uma avaliação de impacto à Proteção de Dados Pessoais?	Art. 10, § 3º Art. 32 Art. 38 Art. 46 Art. 47 Art. 49 Art 50, inciso I alínea d	ISO/IEC 29151 (item A.11.2)	NIST ID.RA-P	1, 2, 3
30.7	GOVERNAR-P	O órgão desenvolve, divulga (no que couber) e atualiza relatórios (por exemplo, relatórios sobre violações, investigações, auditorias), a fim de demonstrar responsabilidade e conformidade com leis e regulamentos de proteção de dados pessoais?	Art. 10, § 3º Art. 32 Art. 38 Art. 46 Art. 47 Art. 49 Art 50, inciso I alínea d	ISO/IEC 29151 (item A.11.6)	NIST ID.RA-P	3
30.8	CONTROLAR-P	O órgão monitora e audita regularmente as operações de tratamento de dados pessoais, especialmente aquelas envolvendo dados pessoais sensíveis, para garantir que estejam em conformidade com as leis, regulamentos e termos contratuais aplicáveis?	Art. 10, § 3º Art. 32 Art. 38 Art. 46 Art. 47 Art. 49 Art 50, inciso I alínea d	ISO/IEC 29151 (item A.11.4 a)	NIST GV.MT-P	2, 3
30.9	CONTROLAR-P	Os controles de proteção de dados pessoais são monitorados e auditados periodicamente para garantir que as operações que envolvam dados pessoais estejam em conformidade com normas e regulamentos internos e externos, quando aplicável, a organização?	Art. 6º, incisos VII, VIII e X Art. 39 Art. 46 Art. 47 Art. 49 Art. 50, inciso I alínea d	ISO/IEC 29151 (item A.11.4 b)	NIST GV.PO-P NIST GV.MT-P NIST ID.DE-P5	3
30.10	CONTROLAR-P	O órgão implementa medidas apropriadas para monitorar e auditar periodicamente os controles de privacidade e a eficácia da política de privacidade interna (política de proteção de dados pessoais) da instituição?	Art. 10, § 3º Art. 32 Art. 38 Art. 46 Art. 47 Art. 49 Art 50, inciso I alínea d	ISO/IEC 29151 (item A.11.4)	NIST GV.PO-P NIST GV.MT-P	3

PRIVACIDADE CONTROLE 30: AVALIAÇÃO DE IMPACTO, MONITORAMENTO E AUDITORIA

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
30.11	CONTROLAR-P	O órgão assegura que as auditorias sejam conduzidas por partes qualificadas e independentes (internas ou externas à organização)?	Art. 10, § 3º Art. 32 Art. 38 Art. 46 Art. 47 Art. 49 Art 50, inciso I alínea d	ISO/IEC 29151 (item A.11.4 c)	NIST GV.PO-P NIST GV.MT-P	3
30.12	CONTROLAR-P	O órgão produz um relatório anual detalhando as ações tomadas para conformidade e um resumo das ações pendentes?	Art. 10, § 3º Art. 32 Art. 38 Art. 46 Art. 47 Art. 49 Art 50, inciso I alínea d	ISO/IEC 29151 (item A.13.1 a)	NIST GV.PO-P NIST GV.MT-P	3

PRIVACIDADE CONTROLE 31: SEGURANÇA APLICADA A PRIVACIDADE

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	REFERÊNCIAS NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
31.1	PROTEGER-P	A organização adota medidas de segurança, técnicas e administrativas, testadas e avaliadas, aptas a proteger dados pessoais de acordo com os resultados de uma avaliação de riscos ou impacto de proteção de dados pessoais?	Art. 6º, inciso VII Art. 44 Art. 46 Art. 47 Art. 48, §1° inciso VI Art. 49	ISO/IEC 29151 (item A.12 “c” e “e”)	NIST PR. P	1, 2, 3
31.2	PROTEGER-P	O órgão submete os controles de privacidade e segurança da informação adotados a revisão e reavaliação periódicas resultantes da avaliação de impacto na privacidade?	Art. 46 Art. 47 Art. 49 Art. 50	ISO/IEC 29151 (item A.12 f)	NIST PR.PO-P NIST PR.AC-P NIST PR.DS-P NIST PR.MA-P NIST PR.PT-P	2, 3
31.3	PROTEGER-P	A organização implementa processo para registro, cancelamento e provisionamento de usuários em sistemas que realizam tratamento de dados pessoais?	Art. 6º, inciso VII Art. 46 Art. 47 Art. 49	ABNT NBR ISO/IEC 27701:2019 (itens 6.6.2.1 e 6.6.2.2) ISO/IEC 29151:2017 (item 9.2.2 e 9.2.3)	NIST PR.AC-P1 NIST PR.AC-P4 NIST PR.AC-P6	1, 2, 3
31.4	PROTEGER-P	A instituição considera o princípio do privilégio mínimo na concessão de direitos de acesso para o processamento de dados pessoais?	Art. 6º, inciso VII Art. 46 Art. 47 Art. 49	ISO/IEC 29151:2017 (item 9.2.3)	NIST PR.AC-P4	1, 2, 3
31.5	PROTEGER-P	Meios fortes de autenticação são providos para o processamento dos dados pessoais, em especial os dados sensíveis (dados de saúde e demais dados previstos pelo art.5º, II da LGPD)?	Art. 6º, inciso VII Art. 46 Art. 47 Art. 49	ISO/IEC 29151:2017 (item 9.2.3)	NIST PR.AC-P	2, 3
31.6	PROTEGER-P	O acesso físico aos dados e dispositivos é gerenciado?	Art. 6º, inciso VII Art. 46 Art. 47 Art. 49 Art. 50	N/A	NIST PR.AC-P2	1, 2, 3
31.7	PROTEGER-P	O compartilhamento ou transferência de dados pessoais é realizado por meio de um canal criptografado e de cifra recomendada pelos sítios especializados de segurança (Exemplo: https://www.ssllabs.com/ssltest/)?	Art. 6º, inciso VII Art. 30, Art. 34, inciso IV Art. 46, Art. 47, Art. 49, Art. 50	ISO/IEC 29151:2017 (item 13.2.2)	NIST PR.DS-P2	2, 3

PRIVACIDADE CONTROLE 31: SEGURANÇA APLICADA A PRIVACIDADE

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	REFERÊNCIAS NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
31.8	PROTEGER-P	Os dados pessoais armazenados/retidos possuem controles de integridade permitindo identificar se os dados foram alterados sem permissão?	Art. 6º, inciso VII Art. 46, Art. 47, Art. 49, Art. 50	ISO/IEC 29151:2017 (item A.12 a)	NIST PR.DS-P6	2, 3
31.9	PROTEGER-P	O órgão adota mecanismos para restauração de dados pessoais?	Art. 46, Art. 47, Art. 49, Art. 50	ISO/IEC 27018 (item A.10.3) ABNT NBR ISO/IEC 27701:2019 (item 6.9.3.1)	NIST PR.PO-P NIST PR.DS-P NIST PR.PT-P	1, 2, 3
31.10	PROTEGER-P	O órgão restringe e controla a impressão de documentos que contenha dados pessoais encaminhados para as impressoras corporativas?	Art. 46, Art. 47, Art. 49, Art. 50	ISO/IEC 27018 (item A.10.2)	NIST PR.PT-P	1, 2, 3
31.11	PROTEGER-P	O órgão descarta materiais impressos de forma segura?	Art. 46, Art. 47, Art. 49, Art. 50	ISO/IEC 27018 (item A.10.7)	NIST PR.PO-P NIST PR.DS-P	1, 2, 3
31.12	PROTEGER-P	As medidas de mitigação de riscos resultantes do RIPD são consideradas no processo de desenvolvimento de sistemas?	Art. 32 Art. 38 Art. 46 Art. 47 Art. 49	ISO/IEC 29151:2017 (item 14.1.2) ABNT NBR ISO/IEC 27701:2019 (item 5.6.2 e 7.2.5)	NIST ID.RA-P NIST GV.MT-P1 NIST PR.DS-P	2, 3
31.13	PROTEGER-P	A manutenção e reparação dos ativos organizacionais são realizadas e registradas, com ferramentas aprovadas e controladas?	Art. 6º, inciso VII Art. 46 Art. 50	N/A	NIST PR.MA-P1	2, 3
31.14	PROTEGER-P	A manutenção remota dos ativos organizacionais é aprovada, registrada e executada de forma a impedir o acesso não autorizado?	Art. 6º, inciso VII Art. 46 Art. 50	N/A	NIST PR.MA-P2	2, 3

PRIVACIDADE CONTROLE 31: SEGURANÇA APLICADA A PRIVACIDADE

ID	FUNÇÃO NIST PF	MEDIDA	REFERÊNCIAS LGPD	REFERÊNCIAS ISO	NIST - PF	GRUPOS DE IMPLEMENTAÇÃO
31.15	PROTEGER-P	A organização ao realizar registros de eventos (logs), considerando o princípio de minimização de dados, grava o acesso ao dado pessoal, incluindo por quem, quando, qual titular de dados pessoais foi acessado e quais mudanças (se houver alguma) foram feitas (adições, modificações ou exclusões), como um resultado do evento?	Art. 6º, inciso VII Art. 46 Art. 47 Art. 49 Art. 50	ABNT NBR ISO/IEC 27701:2019 (item 6.9.4.1)	NIST CT.DM-P8	3
31.16	PROTEGER-P	A organização monitora proativamente a ocorrência de eventos que podem ser associados à violação de dados pessoais?	Art. 48 Art. 50, § 2º, inciso I, alínea “g”	ABNT NBR ISO/IEC 27701:2019 (itens 6.13.1.4 e 6.13.1.5)	NIST PR.DS-P5	2, 3
31.17	PROTEGER-P	A organização possui sistema para o registro de incidentes de segurança da informação que envolvem violação de dados pessoais?	Art. 46 Art. 47 Art. 49 Art. 50, § 2º, inciso I, alínea “g”	ABNT NBR ISO/IEC 27701:2019 (item 6.13.1.1)	NIST PR.PO-P7	1, 2, 3
31.18	PROTEGER-P	A organização comunica à Autoridade Nacional de Proteção de Dados sobre a ocorrência de incidente de segurança e proteção de dados pessoais?	Art. 48	N/A	NIST CMAW-P7	1, 2, 3

ANEXO VI – MUDANÇAS DAS VERSÕES

Este anexo tem a finalidade de fornecer os destaques das mudanças inseridas nesta versão do Guia do Framework de Privacidade e Segurança da Informação.

Mudanças da Versão 1.1.3

A mudança inserida nesta versão em comparação com a anterior visa a ajustar a fórmula do Indicador de Maturidade por Controle (iMC), conforme descrito na página 84, em alinhamento ao estabelecido na Ferramenta do Framework disponibilizada aos órgãos para diagnóstico e avaliação da maturidade em Privacidade e Segurança da Informação.

Importante destacar que o ajuste desta fórmula nesta versão do presente Guia não impacta nos resultados dos indicadores de maturidade obtidos nos ciclos de implementações já realizados uma vez que a fórmula ajustada já estava implementada na ferramenta.

Ademais, os exemplos apresentados imediatamente após a referida expressão foram adaptados de acordo com as alterações mencionadas.

Mudanças da Versão 1.1.2

A mudança inserida nesta versão em comparação com a anterior visa a padronizar o termo “**Unidade de Controle Interno**” em alinhamento ao estabelecido pela Portaria SGD/MGI nº 852/2023 que dispõe sobre o PPSI.

Além disso, foi atualizada a Figura 5 com o objetivo de contemplar as medidas do controle 0 que trata da Estruturação Básica de Gestão em Privacidade e Segurança da Informação.

Mudanças da Versão 1.1.1

A mudança inserida nesta versão em comparação com a anterior visa o ajuste da redação da medida 31.2, conforme destaque em negrito apresentado a seguir:

- O órgão submete os controles **de privacidade e segurança da informação adotados** a revisão e reavaliação periódicas **resultantes da avaliação de impacto na privacidade**?

Mudanças da Versão 1.1

As mudanças inseridas nesta versão em comparação com a anterior visam principalmente a revisão das referências das medidas de privacidade constantes do Anexo V, mais especificamente as referências ABNT NBR ISO/IEC 27701, ISO/IEC 29151, ISO/IEC 27018, ISO/IEC 29134, ABNT NBR ISO/IEC 29184.

Além disso, foram realizados ajustes como as remoções das seguintes citações: termo “operador” na página 20 e na medida 0.7 do Controle 0 (Anexo III); e termos “primário” e “secundário” nas medidas 0.1 e 0.2 do Controle 0 (Anexo III).

Por fim, o termo “autoridade máxima de Tecnologia da Informação” foi substituído em todo o Guia pelo termo “Gestor de Tecnologia da Informação e Comunicação” em alinhamento ao estabelecido pela Portaria SGD/MGI nº 852/2023.


ANPD
GUIA ORIENTATIVO
Tratamento de dados pessoais pelo Poder Público
VERSÃO 2.0 | JUN / 2023

ANPD Autoridade Nacional de Proteção de Dados

GUIA ORIENTATIVO

Tratamento de dados pessoais pelo Poder Público

Versão 2.0

Cristiane Landerdahl
Isabela Maiolino
Jeferson Dias Barbosa
Lucas Borges de Carvalho

Brasília, DF
2023

Presidente da República Luiz Inácio Lula da Silva

Autoridade Nacional de Proteção de Dados

Diretor-Presidente Waldemar Gonçalves Ortunho Junior

Diretores Arthur Pereira Sabbat
Joacil Basilio Rael
Miriam Wimmer
Nairane Farias Rabelo Leitão

Equipe de elaboração Cristiane Landerdahl
Isabela Maiolino
Jeferson Dias Barbosa
Lucas Borges de Carvalho

Projeto gráfico e editoração André Scofano

Versão 1.0
Publicação digital (janeiro / 2022)
Versão 2.0
Publicação impressa, 200 exemplares (junho / 2023)
Publicação digital (junho / 2023)

ANPD
Autoridade Nacional de Proteção de Dados
SCN, Qd. 6, Conj. A,
Ed. Venâncio 3000, Bl. A, 9º andar
Brasília, DF · Brasil · 70716-900
www.anpd.gov.br

Sumário

Apresentação

O tratamento de dados pessoais pelo Poder Público possui muitas peculiaridades, que decorrem, em geral, da necessidade de compatibilização entre o exercício de prerrogativas estatais típicas e os princípios, regras e direitos estabelecidos na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018 – LGPD).

Diante desse cenário, o desafio posto é o de estabelecer parâmetros objetivos, capazes de conferir segurança jurídica às operações com dados pessoais realizadas por órgãos e entidades públicos. Trata-se de assegurar a celeridade e a eficiência necessárias à execução de políticas e à prestação de serviços públicos com respeito aos direitos à proteção de dados pessoais e à privacidade.

Entre outros aspectos relevantes, muitos órgãos e entidades públicos têm questionado a Autoridade Nacional de Proteção de Dados (ANPD) sobre (i) o âmbito de incidência da LGPD e a aplicação de seus conceitos básicos ao setor público; (ii) a adequada interpretação das bases legais que autorizam o tratamento de dados pessoais; (iii) os requisitos e as formalidades a serem observados nas hipóteses de uso compartilhado de dados pessoais; e (iv) a relação entre as normas de proteção de dados pessoais e o acesso à informação pública.

Considerando essas questões, o presente Guia Orientativo busca delinear parâmetros que possam auxiliar entidades e órgãos públicos nas atividades de adequação e de implementação da LGPD. As orientações apresentadas constituem um primeiro passo no processo de delimitação das interpretações sobre a LGPD aplicáveis ao Poder Público. Por isso, a versão publicada ficará aberta a comentários e contribuições de forma contínua, com o fim de atualizar o Guia oportunamente, à medida que novas regulamentações e entendimentos forem estabelecidos, a critério da ANPD. As sugestões podem ser enviadas para a Ouvidoria da ANPD, por meio da *Plataforma Fala.BR* (https://falabr.cgu.gov.br/).

Cumpre enfatizar que não é objeto deste Guia a definição de conceitos básicos previstos na LGPD. Em caso de dúvida, sugere-se consultar a página de documentos e publicações[1] da ANPD, na qual estão disponíveis orientações mais específicas sobre esses conceitos, a exemplo do Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado[2].

O Guia inicia com uma breve explanação sobre a LGPD, o conceito de Poder Público e as competências da ANPD. A seguir, são apresentadas orientações sobre as bases legais mais comuns e os mais relevantes princípios que devem nortear o tratamento de dados pessoais por entidades e órgãos públicos. Na parte final, serão abordadas duas operações específicas de tratamento de dados pessoais pelo Poder Público: o compartilhamento e a divulgação de dados pessoais, sempre sob o enfoque da conformidade do tratamento com a LGPD. Os Anexos I e II trazem, respectivamente, um sumário das recomendações apresentadas na análise dos dois casos específicos mencionados.

A LGPD, o Poder Público e as competências da ANPD

A LGPD foi promulgada em 2018 e tem como objetivo regulamentar o tratamento de dados pessoais para garantir o livre desenvolvimento da personalidade e a dignidade da pessoa humana. Para isso, a lei estabelece uma série de regras a serem seguidas pelos agentes de tratamento, incluindo o Poder Público.

O termo "Poder Público" é definido pela LGPD de forma ampla e inclui órgãos ou entidades dos entes federativos (União, Estados, Distrito Federal e Municípios) e dos três Poderes (Executivo, Legislativo e Judiciário), inclusive das Cortes de Contas e do Ministério Público[3]. Assim, os tratamentos de dados pessoais realizados por essas entidades e órgãos públicos devem observar as disposições da LGPD, ressalvadas as exceções previstas no art. 4º da lei[4].

Também se incluem no conceito de Poder Público: (i) os serviços notariais e de registro (art. 23, § 4º); e (ii) as empresas públicas e as sociedades de economia mista (art. 24), neste último caso, desde que (ii.i.) não estejam atuando em regime de concorrência; ou (ii.ii) operacionalizem políticas públicas, no âmbito da execução destas.

A LGPD visa, ainda, assegurar que dados pessoais sejam utilizados de forma transparente e com fins legítimos, ao mesmo tempo garantindo

os direitos dos titulares. Especificamente em relação ao Poder Público, a LGPD (art. 55–J, XI e XVI) prevê que a ANPD pode solicitar informe específico sobre o âmbito, a natureza dos dados e demais detalhes envolvidos na operação, bem como realizar auditorias sobre o tratamento de dados pessoais. O art. 52, § 3°, estabelece quais sanções podem ser aplicadas às entidades e aos órgãos públicos, com expressa exclusão das penalidades de multa simples ou diária previstas na LGPD.

Importante ressaltar que a ANPD é o órgão central de interpretação da LGPD e do estabelecimento de normas e diretrizes para sua implementação, no que se inclui a deliberação administrativa, em caráter terminativo, sobre a interpretação da lei e sobre as suas próprias competências e casos omissos (art. 55–K, parágrafo único; art. 55–J, XX). Além disso, a autoridade nacional detém competência exclusiva para aplicar as sanções administrativas previstas na LGPD, com prevalência de suas competências sobre outras correlatas de entidades e órgãos da administração pública no que se refere à proteção de dados pessoais (art. 55–K).

Assim, a ANPD possui competência originária, específica e uniformizadora no que concerne à proteção de dados pessoais e à aplicação da LGPD, previsão legal que deve ser interpretada de forma a se compatibilizar com a atuação de outros entes públicos que possam eventualmente tratar sobre o tema. A esse respeito, a LGPD (art. 55–J, § 3º) estabelece que a ANPD deve atuar em coordenação e articulação com outros órgãos e entidades públicos, visando assegurar o cumprimento de suas atribuições com maior eficiência e promover o adequado funcionamento dos setores regulados[5].

Importante ressaltar, por fim, que o servidor público que infrinja a LGPD também é passível de responsabilização administrativa pessoal e autônoma, conforme o art. 28 do Decreto Lei n° 4.657, de 4 de setembro de 1942 (Lei de Introdução às normas do Direito Brasileiro). Dessa

forma, tratar dados pessoais indevidamente, como, por exemplo, vendendo banco de dados, alterando ou suprimindo cadastros de forma inadequada ou usando dados pessoais para fins ilegítimos pode levar à responsabilização do servidor público que praticou o ato ilegal.

Bases legais

Uma das principais providências a serem tomadas antes de realizar o tratamento de dados pessoais é a de identificar a base legal aplicável. O tratamento de dados pessoais pelo Poder Público deve se amparar em uma das hipóteses previstas no art. 7º ou, no caso de dados sensíveis, no art. 11 da LGPD. Esses dispositivos devem ser interpretados em conjunto e de forma sistemática com os critérios adicionais previstos no art. 23, que complementam e auxiliam a interpretação e a aplicação prática das bases legais no âmbito do Poder Público, conforme será demonstrado.

Considerando os questionamentos encaminhados à ANPD e as peculiaridades do tratamento de dados pessoais pelo Poder Público, bem como o previsto na Agenda Regulatória do biênio 2021–2022[6], a análise a seguir será limitada às seguintes bases legais: consentimento, legítimo interesse, cumprimento de obrigação legal e regulatória e execução de políticas públicas.

Consentimento

Conforme a definição legal (art. 5º, XII, LGPD), o consentimento é a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade

determinada". Adicionalmente, no caso de dados sensíveis, o consentimento deve ser fornecido "de forma específica e destacada, para finalidades específicas" (art. 11, I, LGPD).

Assim, a autorização do titular deve ser intencional e ele deve saber exatamente para que fim seus dados serão tratados, sendo vedada a autorização tácita e para finalidades genéricas. Além disso, o consentimento pressupõe uma escolha efetiva entre autorizar e recusar o tratamento dos dados pessoais, incluindo a possibilidade de revogar o consentimento a qualquer momento.

Diante dessas características, em muitas ocasiões, o consentimento não será a base legal mais apropriada para o tratamento de dados pessoais pelo Poder Público, notadamente quando o tratamento for necessário para o cumprimento de obrigações e atribuições legais. Nesses casos, o órgão ou a entidade exerce prerrogativas estatais típicas, que se impõem sobre os titulares em uma relação de desbalanceamento de forças, na qual o cidadão não possui condições efetivas de se manifestar livremente sobre o uso de seus dados pessoais.

Não obstante, o consentimento poderá eventualmente ser admitido como base legal para o tratamento de dados pessoais pelo Poder Público. Para tanto, a utilização dos dados não deve ser compulsória e a atuação estatal não deve, em regra, basear-se no exercício de prerrogativas estatais típicas, que decorrem do cumprimento de obrigações e atribuições legais.

Assim, a utilização da base legal do consentimento no âmbito do tratamento de dados pessoais pelo Poder Público pressupõe assegurar ao titular a efetiva possibilidade de autorizar ou não o tratamento de seus dados, sem que de sua manifestação de vontade resultem restrições significativas à sua condição jurídica ou ao exercício de direitos fundamentais.

EXEMPLO 1

Matrícula de estudante em universidade pública

Universidade pública solicita de novos estudantes o fornecimento de dados pessoais necessários para fins de cadastro e matrícula. O procedimento é realizado online e, para prosseguir para as etapas seguintes, com a escolha de disciplinas e horários, o estudante deve "aceitar" as condições estipuladas para o tratamento de seus dados. Essas condições são descritas de forma genérica, com a indicação de que os dados poderão ser utilizados para "fins educacionais e outros correlatos". Uma mensagem indica que, caso não fornecido o consentimento, a matrícula não será concluída e o estudante não terá acesso ao curso e a serviços como os de assistência estudantil e empréstimo de livros na biblioteca.

No exemplo citado, o consentimento eventualmente obtido será nulo, pois: (i) os estudantes não possuem condições efetivas de aceitar ou recusar o tratamento de seus dados pessoais, haja vista o caráter compulsório do tratamento realizado pela universidade; e (ii) a autorização é fornecida para uma finalidade genérica. Com o objetivo de adequar as suas práticas ao disposto na LGPD, a universidade deve fornecer informações claras e precisas sobre a finalidade específica do tratamento, identificando outra base legal mais apropriada para a hipótese, que não o consentimento. Ainda, em atenção ao princípio da necessidade, não devem ser solicitados mais dados do que o necessário para atingir as finalidades informadas ao titular.

EXEMPLO 2

Inscrição em evento acadêmico

Estudante realiza inscrição para participar de um evento organizado por uma universidade pública. O procedimento é realizado online, ocasião em que são solicitadas informações básicas de cadastro, como

nome e número de matrícula, este para o fim específico de concessão da gratuidade da inscrição, benefício exclusivo para estudantes. Adicionalmente, o estudante tem a opção de fornecer e-mail, caso queira "receber informações de outros eventos organizados pela universidade". Uma mensagem esclarece que o fornecimento do e-mail é facultativo e a recusa não impede a participação no evento. Ademais, as informações sobre os outros eventos são rotineiramente divulgadas na página da universidade na Internet.

Na hipótese, o consentimento é a base legal apropriada para a coleta do e-mail do estudante, podendo ser considerado válido, haja vista a finalidade específica informada ao titular, bem como a existência de condições efetivas para a livre, informada e inequívoca manifestação de vontade.

Legítimo interesse

A base legal do legítimo interesse autoriza o tratamento de dados pessoais de natureza não sensível quando necessário ao atendimento de interesses legítimos do controlador ou de terceiros, "exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais" (art. 7º, IX). Trata-se, portanto, de base legal não aplicável ao tratamento de dados pessoais sensíveis.

Por ser uma base legal mais flexível, sua adoção deve ser precedida de uma avaliação em que seja demonstrada a proporcionalidade entre, de um lado, os interesses do controlador ou de terceiro para a utilização do dado pessoal e, de outro, os direitos e as legítimas expectativas do titular. Além disso, deve-se considerar que, conforme o art. 18, § 2º, o titular tem o direito de se opor ao tratamento realizado com base no legítimo interesse, em caso de descumprimento dos requisitos previstos na LGPD.

De forma similar ao que ocorre com o consentimento, a aplicação do legítimo interesse é limitada no âmbito do setor público. Em particular, a sua utilização não é apropriada quando o tratamento de dados pessoais é realizado de forma compulsória ou quando for necessário para o cumprimento de obrigações e atribuições legais do Poder Público.

Nessas situações, não há como se realizar, propriamente, uma ponderação entre as expectativas dos titulares e os supostos interesses estatais, visto que estes, por definição legal ou regulamentar, conforme o caso, tendem a estabelecer restrições aos direitos individuais nele envolvidos. Isto é, a própria legislação estabelece essa ponderação, ao fixar as condições a serem observadas para a realização do tratamento de dados pessoais. Por isso, é recomendável que, em geral, órgãos e entidades públicos evitem recorrer ao legítimo interesse, preferindo outras bases legais, a exemplo de execução de políticas públicas e cumprimento de obrigação legal, para fundamentar os tratamentos de dados pessoais que realizam nessas condições.

Não obstante, o legítimo interesse poderá eventualmente ser admitido como base legal para o tratamento de dados pessoais pelo Poder Público. Para tanto, a utilização dos dados não deve ser compulsória ou, ainda, a atuação estatal não deve se basear no exercício de prerrogativas estatais típicas, que decorrem do cumprimento de obrigações e atribuições legais. Nesse contexto, torna-se efetivamente possível realizar uma ponderação entre, de um lado, os interesses legítimos do controlador ou de terceiro e, de outro, as expectativas legítimas e os direitos dos titulares[7].

Exemplo 3

Segurança da informação

Entidade pública realiza tratamento de dados pessoais de seus servidores com a finalidade de garantir a segurança dos sistemas de infor-

mação utilizados, como, por exemplo, para viabilizar a autenticação de usuários e prevenir que softwares maliciosos possam criar vulnerabilidades na rede interna.

Considerando que o tratamento não está associado ao exercício de prerrogativas estatais típicas, é possível recorrer à base legal do legítimo interesse. Nesse caso, devem ser observados os requisitos previstos na LGPD, em particular a necessidade de ponderação entre os interesses da entidade pública e os direitos e as expectativas legítimas dos titulares. É necessário, ainda, que sejam adotadas medidas para garantir a transparência do tratamento de dados pessoais baseado no legítimo interesse.

Cumprimento de obrigação legal ou regulatória

Conforme o art. 7º, II, da LGPD, o tratamento de dados pessoais pelo Poder Público poderá ser realizado "para o cumprimento de obrigação legal ou regulatória pelo controlador". A mesma hipótese está prevista no art. 11, II, *a*, que rege o tratamento de dados sensíveis.

De forma geral, a aplicação desses dispositivos será efetuada em dois contextos normativos distintos, que se diferenciam em razão da espécie de norma jurídica que estabelece a obrigação a ser cumprida. É o caso, em especial, das normas de conduta e das normas de organização [8].

Na primeira hipótese, a obrigação legal decorre de uma norma de conduta, isto é, uma regra que disciplina um comportamento, em geral estabelecendo um fato ou uma hipótese legal, com uma possível consequência jurídica em caso de descumprimento. Caso o responsável não cumpra a obrigação legal (como, por exemplo, a divulgação da agenda de compromissos públicos de autoridades, conforme art.

11 da Lei nº 12.813/2013), poderá ser objeto das penalidades administrativas previstas na legislação[9].

Nessas situações, o tratamento de dados pessoais é necessário para atender a uma regra específica, ou seja, uma determinação legal expressa ou uma obrigação de natureza regulatória estabelecida por um órgão regulador. Não há, por isso, um vínculo necessário e direto entre o tratamento de dados e o exercício de atribuições e competências legais do controlador.

Já na segunda hipótese, a obrigação legal decorre de normas de organização, assim entendidas as normas que estruturam órgãos e entidades e estabelecem suas competências e atribuições[10]. Nesse contexto normativo, o tratamento de dados pessoais é parte essencial do exercício de prerrogativas estatais típicas, uma vez que necessário para viabilizar a própria execução das atribuições, competências e finalidades públicas da entidade ou do órgão público.

Assim, diferentemente das normas de conduta, que estabelecem obrigações de forma direta e expressa, prevendo uma consequência específica em caso de descumprimento, as normas de organização estabelecem obrigações que estão associadas, de forma mais geral, ao próprio cumprimento e à execução de atribuições legais típicas da entidade ou do órgão público responsável pelo tratamento de dados pessoais.

Vale ressaltar que essa interpretação do conceito de obrigação legal, conforme previsto no art. 7º, II, e no art. 11, II, *a*, da LGPD, é reforçada pelo disposto no art. 23 da mesma lei, segundo o qual o tratamento de dados pessoais no setor público deverá ser realizado "com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público", observando-se o interesse público e o atendimento da finalidade pública do controlador.

EXEMPLO 4

Canal de TV

Assembleia Legislativa pretende lançar canal de TV próprio. Para tanto, entre outros requisitos, o órgão regulador determinou a apresentação de dados pessoais de parlamentares e servidores responsáveis pela direção do canal, sob pena de ter o pedido de outorga indeferido.

O tratamento dos dados pessoais pela Assembleia Legislativa é legítimo, uma vez que, nos termos do art. 7º, II, da LGPD, vincula-se diretamente ao cumprimento de normas de conduta, no caso, obrigações regulatórias definidas pelo órgão regulador competente, em conformidade com a legislação aplicável.

EXEMPLO 5

Processo legislativo

Assembleia Legislativa trata dados pessoais contidos em documentos relacionados ao processo legislativo, tais como atas de reunião, pareceres e projetos de lei. Os dados pessoais em questão se referem, entre outros, a parlamentares, servidores públicos, membros da sociedade civil e especialistas ouvidos em audiências públicas.

O tratamento dos dados pessoais é legítimo, na medida em que diretamente vinculado ao cumprimento de obrigações e à execução de competências típicas do órgão legislativo, que decorrem de normas de organização previstas na Constituição Estadual, em conformidade com a base legal prevista no art. 7º, II, e com o disposto no art. 23, da LGPD.

EXEMPLO 6

Agência reguladora

Uma agência reguladora trata dados pessoais de seus servidores públicos com a finalidade específica de realizar o pagamento de salários e benefícios previdenciários, como pensões e aposentadorias. Essas obrigações estão expressamente previstas na legislação que dispõe sobre o regime jurídico dos servidores. A mesma agência reguladora tem a atribuição legal de fiscalizar prestadoras de um determinado serviço público. Para cumprir essa competência geral de fiscalização, conforme estipulado na lei que dispõe sobre a sua estrutura e funcionamento, a agência reguladora trata dados pessoais, como, por exemplo, aqueles provenientes de reclamações de usuários do serviço.

Embora atendam a finalidades distintas, em ambos os casos o tratamento dos dados pessoais pela agência reguladora se fundamenta na hipótese de cumprimento de obrigação legal, nos termos do art. 7º, II, da LGPD.

Execução de políticas públicas

O inciso III do art. 7º da LGPD estabelece que a "administração pública" pode realizar "o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres". Por sua vez, em relação aos dados sensíveis, o art. 11, II, *b*, refere-se ao "tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos".

A aplicação dessa base legal por entidades e órgãos públicos pressupõe a adequada compreensão sobre os principais termos utilizados

nos artigos da LGPD acima citados. Com esse intuito, destacamos a seguir orientações práticas sobre a interpretação dos seguintes conceitos: (i) administração pública; e (ii) políticas públicas.

(I) ADMINISTRAÇÃO PÚBLICA

O conceito de "administração pública" deve ser delimitado a partir da definição de Poder Público, conforme já exposta neste Guia. Assim, abrange tanto órgãos e entidades do Poder Executivo quanto dos Poderes Legislativo e Judiciário, inclusive das Cortes de Contas e do Ministério Público, desde que estejam atuando no exercício de funções administrativas.

De fato, embora a função administrativa seja típica do Poder Executivo, órgãos dos demais Poderes também a exercem em determinadas circunstâncias. Ou seja, ao lado de suas funções típicas, tais como as de legislar e aplicar a lei, órgãos dos Poderes Legislativo e Judiciário também exercem atividades administrativas. É o que ocorre, por exemplo, quando são firmados convênios ou acordos de cooperação técnica com outros órgãos públicos ou entidades sem fins lucrativos visando ao atendimento de alguma finalidade pública. Como explica José dos Santos Carvalho Filho:

> A Administração Pública, sob o ângulo subjetivo, não deve ser confundida com qualquer dos Poderes estruturais do Estado, sobretudo o Poder Executivo, ao qual se atribui usualmente a função administrativa. Para a perfeita noção de sua extensão é necessário pôr em relevo a função administrativa em si, e não o Poder em que é ela exercida. Embora seja o Poder Executivo o administrador por excelência, nos Poderes Legislativo e Judiciário há numerosas tarefas que constituem atividade administrativa, como é o caso, por exemplo, das que se referem à organização interna dos seus serviços e dos seus servidores. Desse modo, todos os órgãos e

> agentes que, em qualquer desses Poderes, estejam exercendo função administrativa, serão integrantes da Administração Pública[11].

Portanto, com base nessa definição de administração pública, pode-se afirmar que a base legal referida nos artigos 7º, III e 11, II, b, da LGPD, é aplicável a órgãos e entidades dos três Poderes e entes federativos, inclusive das Cortes de Contas e do Ministério Público, desde que estejam atuando no exercício de suas funções administrativas, com vistas à execução de políticas públicas.

(II) POLÍTICAS PÚBLICAS

O conceito de políticas públicas não é definido na LGPD, não tendo sido editada regulamentação da ANPD sobre o tema até o presente momento. Assim, recomenda-se que sejam consideradas as definições usuais do termo, conforme a praxe administrativa e as orientações a seguir apresentadas.

Nesse sentido, devem ser considerados, ao menos, dois aspectos. O primeiro é a existência de ato formal que institui a política pública, o que pode ocorrer mediante ato normativo (lei ou regulamento) ou por ajustes contratuais (contratos, convênios e instrumentos congêneres).

Ressalte-se que o art. 11, I, *b*, da LGPD, não fez referência às políticas públicas instituídas em ajustes contratuais. Por isso, no caso de tratamento de dados sensíveis pelo Poder Público, a base legal é mais restrita, uma vez que limitada a políticas públicas previstas em "leis e regulamentos".

Quanto ao aspecto material, uma política pública envolve, em geral, a definição de um programa ou ação governamental específico, a ser executado por uma entidade ou por um órgão público. Nessa linha, Maria Paula Dallari Bucci destaca que, "como tipo ideal, a política pú-

blica deve visar a realização de objetivos definidos, expressando a seleção de prioridades, a reserva de meios necessários à sua consecução e o intervalo de tempo em que se espera o atingimento dos resultados"[12].

Assim, considerando os elementos expostos, recomenda-se que o conceito de política pública seja interpretado de forma ampla, de modo a abranger qualquer programa ou ação governamental, definido em instrumento formal, isto é, lei, regulamento ou ajuste contratual, conforme o caso, cujo conteúdo inclui, em regra, objetivos, metas, prazos e meios de execução.

Por fim, também na hipótese de execução de política pública deve ser observado o disposto no art. 23 da LGPD, em especial a exigência de que o tratamento seja realizado para o atendimento da finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

EXEMPLO 7

Política de controle do tabagismo

Secretaria de Saúde realiza tratamento de dados pessoais de pessoas fumantes, atendidas em hospitais públicos, para fins de planejamento e execução de política pública de controle do tabagismo e prevenção e tratamento do câncer de pulmão. A política foi estabelecida em norma infralegal, da qual constam, entre outros elementos, objetivos, competências e meios de financiamento. Os dados pessoais são tratados pela própria Secretaria de Saúde e, eventualmente, compartilhados com a autarquia responsável por executar programa de orientação e auxílio a pessoas que desejam parar de fumar. Por envolver dados sensíveis, o tratamento dos dados pessoais é realizado com base no art. 11, II, b, da LGPD.

A finalidade é específica de execução de política pública, estabelecida em regulamento, em conformidade com a LGPD.

Princípios

A observância dos princípios (art. 6º, LGPD) constitui parte essencial do tratamento de dados pessoais. Seguindo os propósitos deste Guia, serão apresentadas a seguir orientações não exaustivas, com foco nas peculiaridades do setor público, considerando os seguintes princípios: finalidade; adequação; necessidade; transparência; e livre acesso. Como regra geral, os princípios devem ser interpretados em conjunto e de forma sistemática com as disposições do Capítulo IV da LGPD (arts. 23 a 30), no qual se encontram normas específicas direcionadas ao Poder Público.

Finalidade e adequação

De acordo com o princípio da finalidade (art. 6º, I), o tratamento dos dados pessoais deve ser realizado para "propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades." Adicionalmente, no âmbito do setor público, o tratamento de dados pessoais deve atender a uma "finalidade pública", conforme previsto no art. 23 da LGPD.

Portanto, o tratamento de dados pessoais pelo Poder Público deve estar sempre associado a uma finalidade pública, que seja: (i) legítima,

isto é, lícita e compatível com o ordenamento jurídico, além de amparada em uma base legal, que autorize o tratamento; (ii) específica, de maneira que a partir da finalidade seja possível delimitar o escopo do tratamento e estabelecer as garantias necessárias para a proteção dos dados pessoais; (iii) explícita, isto é, expressa de uma maneira clara e precisa; e (iv) informada, isto é, disponibilizada em linguagem simples e de fácil compreensão e acesso ao titular dos dados.

Além disso, o princípio da finalidade estabelece uma limitação ao tratamento posterior dos dados pessoais. Assim, eventual uso secundário dos dados pessoais somente pode ser realizado para uma finalidade que seja compatível com a finalidade original do tratamento dos dados pessoais. Em sentido similar, o princípio da adequação (art. 6º, II) impõe a observância da compatibilidade entre o tratamento dos dados pessoais e as finalidades que são informadas ao titular, observado o contexto em que é realizado. Dessa forma, o tratamento do dado deve ser compatível com o propósito informado ao titular.

Essa determinação possui elevada importância prática, em especial nos casos de tratamento posterior de dados publicamente disponíveis e de uso compartilhado de dados pessoais pelo Poder Público.

Em relação aos dados disponíveis publicamente, a LGPD autoriza o seu tratamento, desde que observadas a finalidade, a boa-fé e o interesse público que justificaram a sua disponibilização (art. 7º, § 3º). Além disso, o tratamento posterior para novas finalidades somente poderá ser realizado se "observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei" (art. 7º, § 7º).

No caso de uso compartilhado de dados pessoais pelo Poder Público, entre outras regras, o art. 26 da LGPD exige que sejam atendidas "finalidades específicas de execução de políticas públicas e atribuição le-

gal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei".

Diante do que estabelece a LGPD e tendo em vista a experiência internacional em torno do assunto[13], recomenda-se a avaliação da compatibilidade entre a finalidade original e a do uso secundário dos dados pessoais. Essa avaliação deve levar em consideração os seguintes aspectos: (i) o contexto e as circunstâncias relevantes do caso concreto; (ii) a existência de conexão fática ou jurídica entre a finalidade original e a que fundamenta o tratamento posterior; (iii) a natureza dos dados pessoais, adotando-se posição de maior cautela quando abrangidos dados sensíveis; (iv) as expectativas legítimas dos titulares e os possíveis impactos do tratamento posterior sobre seus direitos; e (v) o interesse público e a finalidade pública específica do tratamento posterior, bem como o seu vínculo com as competências legais dos órgãos ou entidades envolvidos, nos termos do art. 23 da LGPD.

Exemplo 8

Política pública de vacinação

A Secretaria de Saúde de um município coleta dados de casos confirmados de uma doença infecciosa para fins de desenho, implementação e monitoramento de uma política pública de vacinação. Os dados são compartilhados com um órgão de pesquisa, para a finalidade específica de realização de estudos em saúde pública.

Neste caso, o tratamento posterior dos dados é compatível com a finalidade original da coleta, em conformidade com o princípio da finalidade. Por se tratar de dados sensíveis, relativos à saúde, o órgão deve ter cautela ao compartilhá-los ou divulgá-los, sempre observando o art. 13 e o Capítulo IV da LGPD. Nesse sentido, é preferível que o compartilhamento dessas informações inclua, sempre que possível, a pseudonimização ou a anonimização dos dados.

Necessidade

O princípio da necessidade estabelece que o tratamento deve ser limitado ao "mínimo necessário para a realização de suas finalidades", abrangendo apenas os "dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados" (art. 6º, III LGPD). O princípio da necessidade impõe, portanto, que a coleta se atenha à menor quantidade possível de dados para o alcance da finalidade proposta. Da mesma forma, esse princípio desaconselha o próprio tratamento de dados pessoais quando a finalidade que se almeja pode ser atingida por outros meios menos gravosos ao titular de dados.

No que tange a esse princípio, entidades e órgãos públicos devem verificar se as informações usualmente coletadas de cidadãos – a exemplo de cópias de documentos de identidade ou de dados solicitados em formulários-padrão – são, efetivamente, necessárias para as finalidades para as quais serão utilizadas, não se admitindo a prática de coleta indistinta de dados pessoais, em particular de dados para os quais não se tenha identificado uma finalidade específica e legítima para o tratamento. Mesmo após a coleta de dados pessoais, o princípio da necessidade ainda é importante no sentido de avaliar a necessidade de outros tratamentos, como o armazenamento e processamento.

É importante, ainda, que entidades do Poder Público exerçam cautela em eventuais tratamentos discriminatórios injustificados que possam ocorrer em decorrência do tratamento de dados pessoais desnecessários.

EXEMPLO 9

Dados coletados para elaboração de contrato administrativo

A Secretaria de Educação de um Município contrata, por licitação, uma empresa para fornecer merenda nas escolas. Para firmar o contrato

com a Secretaria, tanto o representante da empresa quanto o servidor público que assinará o contrato fornecem os seus dados, como nome, profissão, CPF, RG, estado civil e endereço residencial. Para atender a outros dispositivos legais e dar publicidade à contratação da empresa, o contrato é divulgado no sítio eletrônico da Secretaria de Educação.

É possível que dados como estado civil e endereço residencial não sejam necessários para a identificação dos responsáveis pela contratação e para viabilizar o exercício do controle social sobre a atividade do órgão público. Assim, a fim de limitar o tratamento ao mínimo necessário para a realização de suas finalidades, o ideal é não coletar esses tipos de dados.

Transparência e livre acesso

O princípio da transparência (art. 6º, VI) garante ao titular a disponibilização de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento de seus próprios dados pessoais e os seus respectivos agentes de tratamento. De forma similar, o princípio do livre acesso (art. 6º, IV) garante aos titulares consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais. Assim, enquanto o princípio da transparência impõe obrigações de cunho geral e que demandam uma postura ativa do agente de tratamento, que tem o dever de disponibilizar as informações exigidas pela lei, independentemente de solicitação do titular; o princípio do livre acesso, por sua vez, enfatiza a necessidade de o agente de tratamento disponibilizar mecanismos efetivos para que o titular possa solicitar e ter acesso facilitado e gratuito a determinadas informações referentes ao tratamento de seus dados pessoais. Esses princípios também são essenciais para garantir o direito fundamental de todos os indivíduos à informação administrativa.

Em conformidade com o que estabelecem os princípios da transparência e do livre acesso, o art. 9º da LGPD delimita as informações que devem ser disponibilizadas aos titulares, entre as quais: (i) forma, duração e finalidade específica do tratamento; (ii) identificação e informações de contato do controlador; (iii) informações sobre o uso compartilhado de dados e a finalidade; (iv) responsabilidades dos agentes que realizarão o tratamento; e (v) direitos do titular, com menção explícita aos direitos contidos no art. 18. Além dessas informações, deve ser objeto de divulgação a identidade e as informações de contato do encarregado (art. 41, § 1º).

Em complemento a essas disposições gerais, a LGPD prevê o dever de publicidade em relação aos tratamentos realizados pelo Poder Público. Nesse sentido, os órgãos e entidades devem fornecer "informações claras e atualizadas sobre a previsão legal, finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades", nos termos do art. 23, I. Tais informações devem estar em meios de fácil acesso, preferencialmente em sítios eletrônicos. Nos termos do art. 23, § 1º, da LGPD, a ANPD poderá dispor sobre as formas de publicidade das operações de tratamento[14].

Demonstrando a importância da publicidade no setor público, o art. 25 da LGPD prevê também que os dados devem ser mantidos "em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas", visando, entre outras finalidades, "à disseminação e ao acesso das informações pelo público em geral", sem, contudo, que deixem de ser observados os princípios que asseguram a proteção dos dados pessoais e a privacidade dos seus titulares.

As informações exigidas pela LGPD devem ser disponibilizadas de forma clara, adequada e ostensiva, em linguagem simples e acessível, de modo a assegurar o efetivo conhecimento do titular a respeito das ati-

vidades de tratamento realizadas pelo controlador, bem como sobre os seus direitos e a forma de exercê-los. Nesse sentido, constitui uma boa prática a disponibilização dessas informações na página eletrônica do órgão ou entidade responsável, da qual podem constar seções específicas relacionadas à "Lei Geral de Proteção de Dados Pessoais" e documentos como política de privacidade ou equivalente.

EXEMPLO 10

Princípio da transparência no setor público

Uma pessoa tem seus dados coletados pela recepção de um órgão público para fins de segurança patrimonial e dos servidores. Para atender a outros dispositivos legais e dar publicidade a atos do órgão, caso essa pessoa realize uma reunião com uma autoridade, seu nome poderá ser divulgado na agenda pública da autoridade, salvo eventual restrição legal.

Em geral, essa pessoa deverá ser informada das finalidades que justificam a coleta e o tratamento, incluindo a de que parte ou a totalidade deles poderá ser divulgada para atender normas específicas que tratem de divulgação de agenda pública. Entre outras possibilidades, essas informações podem constar da política de privacidade ou documento equivalente, disponibilizado na página do órgão público na internet.

Compartilhamento de dados pessoais pelo Poder Público

O compartilhamento de dados pessoais é a operação de tratamento pela qual órgãos e entidades públicos conferem permissão de acesso ou transferem uma base de dados pessoais a outro ente público ou a entidades privadas visando ao atendimento de uma finalidade pública. De forma mais específica, a LGPD utiliza o termo "uso compartilhado de dados", que é definido como a "comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados."

O uso compartilhado de dados é um mecanismo relevante para a execução de atividades típicas e rotineiras do Poder Público, a exemplo de pagamento de servidores e prestação de serviços públicos. A LGPD reconhece essa relevância ao estabelecer, em seu art. 25, que os dados devem ser mantidos "em formato interoperável e estruturado para o uso compartilhado", visando, entre outras finalidades, "à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral".

Não obstante, assim como ocorre com as demais operações de tratamento, o uso compartilhado de dados pessoais deve ser realizado em conformidade com a LGPD, notadamente com os princípios, as bases legais, garantia dos direitos dos titulares e outras regras específicas aplicáveis ao Poder Público. Além de conferir maior previsibilidade, transparência e segurança jurídica ao uso compartilhado de dados, a observância dessas disposições legais constitui peça-chave para a promoção de uma relação de confiança com os titulares e para a adequada gestão de riscos pelos controladores, inclusive para evitar a ocorrência de abusos e desvios de finalidades[15].

Com esse intuito, a título de orientação a entidades e órgão públicos, são indicados a seguir os principais requisitos que devem ser observados nos processos de compartilhamento de dados pessoais pelo Poder Público. Importante ressaltar que esses requisitos expressam diretrizes gerais, que decorrem da própria LGPD, podendo ser ajustados ou complementados com parâmetros e requisitos adicionais de acordo com o contexto e as peculiaridades de cada caso concreto.

(a) Formalização e registro

O uso compartilhado de dados pessoais pelo Poder Público deve ser formalizado, seja em atenção às normas gerais que regem os procedimentos administrativos, seja em atenção à obrigatoriedade de registro das operações de tratamento, conforme disposto no art. 37 da LGPD. Para tanto, recomenda-se a instauração de processo administrativo, do qual constem os documentos e as informações pertinentes, incluindo análise técnica e jurídica, conforme o caso, que exponham a motivação para a realização do compartilhamento e a sua aderência à legislação em vigor.

Além disso, recomenda-se que o compartilhamento seja estabelecido em ato formal, a exemplo de contratos, convênios ou instrumentos

congêneres firmados entre as partes. Outra possibilidade é a expedição de decisão administrativa pela autoridade competente, que autorize o acesso aos dados e estabeleça os requisitos definidos como condição para o compartilhamento[16].

Especialmente nos casos em que o órgão ou a entidade pública compartilha dados pessoais com frequência, sugere-se avaliar a conveniência de editar ato normativo interno, a exemplo de portarias e instruções normativas, com o objetivo de, além de proporcionar o devido formalismo, conferir maior padronização e celeridade a essas operações. O ato normativo pode, por exemplo, definir competências e estabelecer procedimentos, prazos e requisitos essenciais a serem observados nos processos de compartilhamento.

(b) Objeto e finalidade

Independentemente da opção adotada para a formalização e registro, os dados pessoais, objeto de compartilhamento, devem ser indicados de forma objetiva e detalhada, limitando-se ao que for estritamente necessário para as finalidades do tratamento, em conformidade com o princípio da necessidade.

Por sua vez, a finalidade deve ser específica, com a indicação precisa, por exemplo, de qual iniciativa, ação ou programa será executado ou, ainda, de qual atribuição legal será cumprida mediante o compartilhamento dos dados pessoais. Nessa linha, o art. 26 da LGPD estabelece que "o uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei." Finalidades descritas de forma genérica ou indeterminada contrariam as disposições da LGPD, além de

precedentes firmados pelo Supremo Tribunal Federal (STF) em casos similares[17].

Deve ficar claro, em suma, quais dados pessoais serão compartilhados, bem como por que e para que serão compartilhados. Por exemplo, o ato formal pode prever que "serão compartilhados com a Entidade Pública X os dados pessoais que constam da base de dados do Órgão Público Y, consistentes em nome, CPF e endereço residencial, para a finalidade específica de realização de cadastro e identificação de cidadãos aptos ao recebimento do benefício social de que trata a Lei nº XYZ".

Por fim, em qualquer hipótese, deve ser avaliada a compatibilidade entre a finalidade original da coleta e a finalidade do compartilhamento dos dados, conforme as orientações constantes deste Guia.

(c) Base legal

O terceiro requisito a ser atendido para o uso compartilhado de dados pessoais pelo Poder Público é a definição da base legal, conforme art. 7º ou, no caso de dados sensíveis, art. 11 da LGPD, nos termos das orientações apresentadas neste Guia. Recomenda-se, nesse sentido, que o ato que autoriza ou formaliza o compartilhamento contenha expressa indicação da base legal utilizada.

(d) Duração do tratamento

O tratamento de dados pessoais é um processo com duração definida, após o qual, em regra, os dados pessoais devem ser eliminados, observados as condições e os prazos previstos em normas específicas que regem a gestão de documentos e arquivos. Vale ressaltar que o

art. 16 da LGPD estabelece hipóteses gerais em que é autorizada a conservação de dados pessoais.

A delimitação do período de duração do uso compartilhado dos dados também é relevante para o fim de reavaliação periódica do instrumento que autorizou o compartilhamento, incluindo a possibilidade de sua adequação a novas disposições legais e regulamentares ou a previsão de novas medidas de segurança, de acordo com as tecnologias disponíveis.

Portanto, o instrumento que autoriza ou formaliza o compartilhamento deve estabelecer, de forma expressa, o período de duração do uso compartilhado dos dados, além de esclarecer, conforme o caso, se há a possibilidade de conservação ou se os dados devem ser eliminados após o término do tratamento.

(e) Transparência e direitos dos titulares

Os atos que regem e autorizam o compartilhamento de dados pessoais devem prever as formas de atendimento ao princípio da transparência (art. 6º, VI), assegurando a disponibilização de informações claras, precisas e facilmente acessíveis aos titulares sobre a realização do compartilhamento e sobre como exercer seus direitos, conforme as orientações apresentadas neste Guia. Constitui uma boa prática divulgar, na página eletrônica dos órgãos e das entidades responsáveis, as informações pertinentes, nos termos do art. 23, I, da LGPD.

Adicionalmente, recomenda-se que sejam delimitadas as obrigações das partes no que se refere: (i) à divulgação das informações exigidas pela LGPD; e (ii) às responsabilidades e aos procedimentos a serem observados visando ao atendimento de solicitações apresentadas pelos titulares.

(f) Prevenção e segurança

Também é importante que sejam estabelecidas as medidas de segurança, técnicas e administrativas, que serão adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (art. 6º, VII, e 46, da LGPD). Estas medidas, que devem ser proporcionais aos riscos às liberdades civis e aos direitos fundamentais dos cidadãos envolvidos no caso concreto, deverão estar previstas nos atos que regem e autorizam o compartilhamento dos dados.

(g) Outros requisitos

Além dos indicados acima, pode ser necessário atender a outros requisitos, que decorram das peculiaridades do caso concreto ou de determinações provenientes de normas específicas.

É o caso de eventual novo compartilhamento ou transferência posterior dos dados, a ser efetuado pelo recebedor dos dados no âmbito do próprio setor público ou para entes do setor privado. Entre outras possibilidades, o instrumento que rege o uso compartilhado dos dados pode vedar a realização de novo compartilhamento ou, ainda, autorizá-lo sob determinadas condições, observadas as normas aplicáveis. Por exemplo, no caso de dados pessoais disponibilizados para a realização de estudos em saúde pública, a LGPD veda que o órgão de pesquisa responsável transfira os dados a terceiro (art. 13, § 2º).

Outro ponto a ser considerado é a definição sobre eventual ônus financeiro decorrente da operação. O ato que rege o compartilhamento pode, se for o caso, indicar a remuneração a ser paga ou, simplesmente, prever que não haverá transferência de recursos financeiros na hipótese, conforme as disposições legais aplicáveis.

Por sua vez, nos casos de uso compartilhado de dados pessoais entre entes públicos e entidades privadas, é necessário observar os requisitos adicionais e específicos indicados no art. 26, § 1º e no art. 27 da LGPD. Em especial, deve-se considerar que eventual transferência de dados pessoais para entidades privadas somente será admitida se amparada em uma das seguintes hipóteses: (i) nos casos de execução descentralizada da atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado; (ii) nos casos de dados acessíveis publicamente; (iii) quando houver previsão legal ou a transferência for respaldada em contratos e instrumentos congêneres; ou (iv) na hipótese de a transferência objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades.

A elaboração de relatório de impacto à proteção de dados pessoais pode auxiliar a motivação da decisão a ser proferida pela autoridade competente, além de fortalecer a sua conformidade com a legislação de proteção de dados pessoais. A avaliação quanto à necessidade de elaboração do documento deve considerar as peculiaridades do caso concreto, em particular, a existência de riscos às liberdades civis e aos direitos fundamentais dos cidadãos, observado o disposto nos art. 5º, XVII e no art. 38 da LGPD.

Por fim, em muitos casos pode ser necessário identificar as funções e responsabilidades dos agentes de tratamento envolvidos no uso compartilhado de dados pessoais. Em caso de compartilhamento de dados entre controlador e operador, por exemplo, podem ser detalhadas as instruções e as condições que devem ser observadas pelo operador ao realizar o tratamento dos dados pessoais, conforme art. 39 da LGPD.

EXEMPLO 11

Compartilhamento de dados de servidores com entidade financeira

Uma autarquia federal trata dados pessoais de seus servidores, como nome, telefone e e-mail para fins de gestão de pessoas. Uma entidade financeira privada solicita ao setor de recursos humanos dessa autarquia os dados de contato dos servidores para oferecer empréstimo consignado.

O pedido foi negado pela autoridade competente, com base em análise técnica e jurídica, que concluiu pela impossibilidade de realização do compartilhamento dos dados, tendo em vista: (i) a incompatibilidade entre a finalidade original da coleta e a finalidade proposta para o compartilhamento; (ii) a inexistência de base legal válida a amparar o uso compartilhado dos dados, em particular a inexistência de consentimentos dos titulares, de obrigação legal ou de qualquer vínculo com a execução de políticas públicas na hipótese; e (iii) a vedação prevista no art. 26, § 1º, da LGPD e o não enquadramento do caso em uma das exceções previstas nos incisos do mesmo dispositivo.

Divulgação de dados pessoais

No setor público, o processo de adequação às disposições da LGPD tem suscitado muitas dúvidas a respeito dos parâmetros a serem observados para a disponibilização pública de informações pessoais. De forma geral, a análise dessas situações envolve uma ponderação entre direitos: de um lado, o direito à privacidade e o direito à proteção de dados pessoais e, de outro, o direito de todos os indivíduos à informação sobre as atividades do Poder Público. Este último se traduz, por exemplo, na divulgação, com base no interesse público, de informações relativas à execução de políticas públicas e ao exercício de competências legais pelos órgãos e entes públicos que permitam aos cidadãos o exercício do controle social sobre as atividades do Poder Público. Frequentemente, todavia, para atender ao princípio da publicidade, o Estado é obrigado a divulgar dados pessoais.

Enquanto o primeiro conjunto de direitos demanda uma posição de cautela e de análise de riscos a respeito da divulgação de informações pessoais, o segundo espelha a determinação legal de que a publicidade é a regra, admitindo-se o sigilo apenas em hipóteses excepcionais, nos termos da Lei de Acesso à Informação (Lei nº 12.527, de 17 de novembro de 2011 – LAI)[18].

Não obstante, o tratamento de dados pessoais pelo Poder Público, incluindo a divulgação pública de dados pessoais, deve ser realizado em conformidade com as disposições da LGPD. Mais especificamente, devem ser observadas as normas que garantem a proteção integral dos dados pessoais, a autodeterminação informativa[19] e o respeito à privacidade dos titulares durante todo o ciclo do tratamento.

Desde a realização da coleta até o fim da atividade realizada com os dados pessoais, conforme o caso, entidades e órgãos públicos devem, pelo menos, observar os princípios previstos na lei, verificar a base legal aplicável ao tratamento, garantir os direitos dos titulares e adotar medidas de prevenção e segurança, a fim de evitar a ocorrência de incidentes.

Nesse contexto, o cumprimento da LGPD demanda de entidades e órgãos públicos uma análise mais ampla, que não se limita à atribuição de sigilo ou de publicidade a determinados dados pessoais – este nem mesmo é o escopo da LGPD. Em termos práticos, considerando o reforço protetivo trazido pela LGPD ao titular de dados, é necessário realizar uma avaliação sobre os riscos e os impactos para os titulares dos dados pessoais bem como sobre as medidas mais adequadas para mitigar possíveis danos decorrentes do tratamento de dados pessoais.

Dados pessoais sensíveis (art. 5º, II, LGPD), por exemplo, estão submetidos a uma proteção jurídica especial, o que implica adotar maior cautela quando for necessário realizar o tratamento de dados pessoais dessa natureza. Nessa linha, pode ser mencionada a vedação de serem revelados dados pessoais sensíveis por ocasião da divulgação de resultados de estudos em saúde pública (art. 13, § 1º, LGPD).

Os princípios da finalidade, adequação e necessidade também impõem limites ao tratamento de dados pessoais. Em atenção a esses princípios, entidades e órgãos públicos devem verificar se as informações coletadas são, efetivamente, adequadas e necessárias para o

atendimento das finalidades para as quais serão utilizadas, não podendo haver, desses dados, uso incompatível com as finalidades que justificaram sua coleta ou a sua obtenção. Muitas vezes, a coleta indiscriminada de dados pessoais é o ponto principal a ser considerado, de modo que, ao invés de eventual e posterior atribuição de sigilo, a proteção será mais efetiva com a própria dispensa da coleta ou com a eliminação da informação.

Em outras situações, nas quais a coleta seja necessária e não seja cabível a eliminação dos dados, podem ser adotadas medidas de mitigação de risco, que fortalecem e tornam mais segura a possibilidade de divulgação dos dados pessoais, haja vista a diminuição de seu potencial lesivo aos direitos dos titulares. Eventualmente, essas medidas podem ser descritas em relatório de impacto à proteção de dados pessoais, documento do controlador que "contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco" (art. 5º, XVII; 38, parágrafo único).

Uma possível salvaguarda a ser adotada é a limitação da divulgação àqueles dados efetivamente necessários para se alcançar os propósitos legítimos e específicos em causa, observados o contexto do tratamento e as expectativas legítimas dos titulares. Nesse sentido, em cumprimento à decisão proferida pelo STF, a divulgação da remuneração individualizada de servidores públicos federais é realizada sem a apresentação completa de números como o CPF e a matrícula do servidor. A restrição de acesso a essas informações mitiga os riscos aos titulares de dados pessoais, sem, no entanto, comprometer a finalidade de garantia de transparência e de controle social sobre as despesas públicas. O contexto e as expectativas legítimas dos titulares também são relevantes, na medida em que se entende, como uma decorrência natural do exercício da atividade pública, que determina-

das informações pessoais dos servidores se submetam ao escrutínio da sociedade.[20]

Em atenção aos princípios da segurança, da prevenção e da responsabilização e prestação de contas, órgãos e entidades públicas devem adotar medidas técnicas e administrativas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, observado o disposto nos arts. 46 a 49 da LGPD. No mesmo sentido, conforme o art. 50, § 1º, constitui boa prática realizar o tratamento de dados pessoais levando em consideração a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes do tratamento de dados. Entre outras medidas, sempre que possível, os dados pessoais devem ser pseudonimizados ou anonimizados.

Por isso, mesmo nos casos de divulgação pública de dados pessoais, é recomendável que órgãos e entidades públicos avaliem a possibilidade de adoção de medidas técnicas e administrativas capazes de mitigar riscos e prevenir a ocorrência de danos aos titulares. Essas medidas adicionais se justificam, pois, em conformidade com os princípios acima referidos, a LGPD estabelece ampla proteção aos dados pessoais, inclusive para aqueles cujo acesso é público, seja por força de lei ou por manifestação de vontade do titular, conforme se extrai de seu art. 7º, §§ 3º, 4º e 7º.

Da mesma forma, em algumas situações, a simples atribuição de sigilo aos dados pessoais pode ser uma medida insuficiente para a sua proteção efetiva. Daí que, em razão da gravidade dos riscos envolvidos em um tratamento e a fim de evitar a ocorrência de incidentes de segurança, pode ser necessária a adoção de mecanismos adicionais de proteção. É o que ocorre, por exemplo, nos casos de estudos em saúde pública, em relação aos quais o art. 13 da LGPD prevê a adoção de medidas adicionais de prevenção e segurança para o tratamento

de dados sensíveis, tais como o seu armazenamento em ambiente controlado e seguro, bem como, sempre que possível, a sua anonimização ou pseudonimização.

Finalmente, a própria transparência a respeito dos tratamentos de dados realizados e a efetiva garantia de direitos aos titulares devem ser considerados como fatores relevantes para diminuir o uso indevido de dados pessoais. Afinal, a possibilidade de o interessado apresentar um requerimento ao órgão público responsável, relatando eventual violação a seus direitos, pode viabilizar a correção de erros, bem como a implementação de medidas como a anonimização, o bloqueio ou a eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD (art. 18, IV).

EXEMPLO 12

Perfil socioeconômico de servidores públicos

A equipe responsável pela implementação da LGPD em um órgão público municipal identificou que o Departamento de Recursos Humanos solicita de novos servidores o preenchimento de uma ficha cadastral e de um formulário denominado "perfil socioeconômico". Deste último, constam dados sensíveis, tais como informações sobre origem racial, convicção religiosa e filiação a sindicato. A equipe verificou que o formulário foi utilizado há alguns anos para subsidiar uma pesquisa efetuada em convênio com uma instituição de ensino local. Porém, mesmo após o fim do convênio, o formulário continuou sendo utilizado como parte do cadastro de novos servidores. Além disso, foi identificado que não é atribuída restrição de acesso aos processos administrativos nos quais estas e outras informações funcionais dos servidores são anexadas. A justificativa apresentada para tanto foi a de que o nome do servidor é excluído dos documentos tornados públicos. No entanto, a equipe constatou que a reindentificação do servidor correspondente poderia ser facilmente realizada, mediante, por exemplo, simples cruzamento

com outras informações disponibilizadas na própria página eletrônica do órgão.

Diante de tais fatos, e seguindo a orientação da equipe responsável, a administração do órgão adotou as seguintes providências, visando à conformidade com a LGPD: (i) imediata interrupção da coleta dos dados socioeconômicos de novos servidores, em atenção aos princípios da necessidade e da finalidade; (ii) eliminação das informações socioeconômicas até então coletadas, haja vista a inexistência, na hipótese, de obrigação legal de armazenamento, e que a finalidade foi alcançada e os dados pessoais deixaram de ser necessários e pertinentes; e (iii) atribuição de sigilo aos documentos que contêm informações funcionais dos servidores do órgão. Em acréscimo, a equipe ainda avalia, junto à alta administração do órgão, a possibilidade de definir normas internas mais restritas de controle de acesso aos dados funcionais de seus servidores, além da adoção de técnicas de pseudonimização.

EXEMPLO 13

Currículo de candidatos a órgão consultivo

Entidade pública municipal recebe candidaturas de interessados em integrar órgão consultivo na qualidade de representante de organizações da sociedade civil ou de sindicatos de empresas ou de trabalhadores. Durante o processo seletivo, os currículos dos candidatos são disponibilizados na internet. Informações pessoais de candidatos de processos anteriores também permanecem disponíveis na página da entidade. Um candidato que, há alguns anos, participou do mesmo processo seletivo, solicitou que seu currículo fosse retirado da página eletrônica da entidade.

Seguindo orientação da área técnica e da jurídica, a autoridade competente acatou o pedido. Assim, o currículo do titular e os de

outras pessoas na mesma situação foram retirados da página da entidade na internet. Além disso, a entidade municipal passou a adotar a prática de limitar a divulgação dos currículos apenas durante o período do processo seletivo, mitigando, dessa forma, os riscos decorrentes da exposição pública dos titulares. Para tanto, considerou-se que, embora determinada por lei municipal, a divulgação dos dados pessoais dos candidatos tem por objetivo viabilizar o exercício do controle social, mediante, por exemplo, eventual impugnação de candidatura. Assim, após a conclusão do processo, com a designação dos novos membros do órgão consultivo, a finalidade legal é alcançada, não mais se justificando a disponibilização dos currículos em transparência ativa.

Notas

Apresentação ▸ p.5–6

[1] Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes. ▸ p.6

[2] Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. ▸ p.6

A LGPD, o Poder Público e as competências da ANPD ▸ p.7–9

[3] O art. 1º da LGPD é expresso quanto à aplicação da lei às pessoas jurídicas de direito público. O parágrafo único do mesmo artigo esclarece que as normas gerais contidas na LGPD "são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios". Já o art. 23, ao regulamentar o tratamento de dados pessoais pelo Poder Público, menciona as "pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação)". Este dispositivo, por sua vez, se refere aos "órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público". ▸ p.7

[4] O art. 4º, III, excepciona parcialmente a aplicação da LGPD aos tratamentos de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais. Os §§ 1º a 4º do mesmo artigo estabelecem que, nessas hipóteses, que serão regidas por legislação específica, devem ser observados o devido processo legal e os princípios gerais de proteção e os direitos do titular previstos na LGPD. Além disso, é atribuída à ANPD a competência para emitir opiniões técnicas e recomendações, bem como para solicitar a elaboração de relatório de impacto à proteção de dados pessoais. É vedado o tratamento de dados pessoais nessas hipóteses por pessoa jurídica de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à ANPD. A lei estabelece, ainda, que em nenhum caso a totalidade de tais dados pessoais poderá ser tratada por pessoa jurídica de direito privado, salvo por aquela que possua capital integralmente constituído pelo Poder Público. ▸ p.7

[5] Conforme o Parecer nº 00018/2021/GAB/ASJUR-ANPD/CGU/AGU (NUP 0130.000035/2021-97), sobre a abrangência da competência da ANPD. ▸ p.8

Bases legais ▸ p.10–21

[6] A agenda regulatória da ANPD, publicada pela Portaria nº 11, de 27 de janeiro de 2021, prevê a publicação de um Guia de boas práticas sobre "hipóteses legais de tratamento de dados pessoais", atividade prevista para ser iniciada no segundo semestre de 2022. ▸ p.10

[7] No âmbito da União Europeia, o Regulamento Geral sobre a Proteção de Dados (RGPD) estabelece que a base legal do legítimo interesse não é aplicável ao tratamento de dados pessoais realizado por autoridades públicas quando estas agem no cumprimento de suas atribuições legais (Considerando 47; art. 6º, 1, f). Com base nessa disposição regulamentar, autoridades de proteção de dados europeias admitem o excepcional recurso ao legítimo interesse apenas quando o tratamento estiver associado a outras finalidades, fora do escopo das atribuições legais típicas da autoridade pública. Nesse sentido são as orientações sobre o tema disponibilizadas pela ICO (disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/) e pela CNIL (disponível em: https://www.cnil.fr/fr/les-bases-legales/choisir-base-legale). ▸ p.14

[8] Um terceiro tipo de obrigação pode decorrer de "normas-objetivo" ou "normas programáticas", que estabelecem objetivos e metas a serem alcançados por entidades e órgãos públicos. Nestes casos, porém, a ação estatal costuma ser materializada por meio da definição e execução de políticas públicas, base legal específica, objeto de comentário na próxima seção. ▸ p.15

[9] As normas de conduta "são aquelas destinadas a reger, diretamente, as relações sociais e o comportamento das pessoas. Normas de conduta [...] preveem um fato e a ele atribuem um efeito jurídico. São concebidas na forma de um juízo hipotético: se ocorrer *F*, então *E*. Por exemplo: em se verificando o fato gerador, será devido o tributo; se o contrato for violado, a parte responsável deverá pagar uma indenização." BARROSO, L. R. **Curso de direito constitucional contemporâneo**. São Paulo: Saraiva, 2009, p. 192. ▸ p.16

[10] Segundo Luís Roberto Barroso, as normas de organização "contêm uma prescrição objetiva, uma ordem para que alguma coisa seja feita de determinada maneira. Não contêm um juízo hipotético, mas um mandamento taxativo. Em lugar de disciplinarem condutas, as normas de organização, também chamadas de normas de *estrutura*,

instituem órgãos, atribuem competências, definem procedimentos". BARROSO, L. R., *ob. cit.*, p. 193. Em sentido similar, para Miguel Reale, o que caracteriza uma norma de organização "é a *obrigação objetiva de algo que deve ser feito*, sem que o dever enunciado fique subordinado à ocorrência de um fato previsto, do qual possam ou não resultar determinadas consequências." (grifo conforme o original). **Lições preliminares de direito**. 25ª ed. São Paulo: Saraiva, 2001, p. 87-88. ▸ p.16

[11] CARVALHO FILHO, J. S. **Manual de direito administrativo**. 28ª ed. São Paulo: Atlas, 2015, p. 12. Ainda segundo o autor, a função administrativa visa à "gestão dos interesses coletivos", sendo definida de forma residual, isto é, "onde não há criação de direito novo [função legislativa] ou solução de conflitos de interesses na via própria (judicial), a função exercida, sob o aspecto material, é a administrativa" *Idem*, p. 5. ▸ p.20

[12] BUCCI, M. P. O conceito de política pública em direito. In: BUCCI, M. P. **Políticas públicas**: reflexões sobre o conceito jurídico. São Paulo: Saraiva, 2006, p. 39. ▸ p.21

Princípios ▸ p.22–28

[13] Em sentido similar ao proposto, ver o art. 6º, 4, do Regulamento Geral sobre a Proteção de Dados, da União Europeia. ▸ p.24

[14] Em sentido similar, a Lei nº 14.129/2021 estabeleceu obrigações específicas relativas à publicidade das operações de tratamento de dados pessoais: "art. 25. As Plataformas de Governo Digital devem dispor de ferramentas de transparência e de controle do tratamento de dados pessoais que sejam claras e facilmente acessíveis e que permitam ao cidadão o exercício dos direitos previstos na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais). §1º As ferramentas previstas no caput deste artigo devem: I - disponibilizar, entre outras, as fontes dos dados pessoais, a finalidade específica do seu tratamento pelo respectivo órgão ou ente e a indicação de outros órgãos ou entes com os quais é realizado o uso compartilhado de dados pessoais, incluído o histórico de acesso ou uso compartilhado, ressalvados os casos previstos no inciso III do caput do art. 4º da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais); II - permitir que o cidadão efetue requisições ao órgão ou à entidade controladora dos seus dados, especialmente aquelas previstas no art. 18 da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais). §2º A Autoridade Nacional de Proteção de Dados (ANPD) poderá editar normas complementares para regulamentar o disposto neste artigo. ▸ p.27

Compartilhamento de dados pessoais pelo Poder Público ▸ p.29–36

[15] Conforme os princípios de boas práticas para a ética de dados no setor público, divulgados pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE), as decisões e as ações do Poder Público relativas ao tratamento de dados pessoais devem buscar "[...] prevenir, evitar ou, pelo menos, limitar a ocorrência de danos intencionais a indivíduos, a grupos sociais e à sociedade [...]. Para alcançar esse objetivo, os governos devem realizar uma efetiva gestão ética dos dados, incluindo os de indivíduos e comunidades, ao longo de todo o seu ciclo de valor, visando ao fortalecimento das instituições democráticas e do Estado de Direito (por exemplo, no que concerne à privacidade e à proteção de dados pessoais). Isso ajudaria a ampliar a legitimidade do uso e do tratamento de dados pelos governos, inclusive no que concerne à entrega de políticas e serviços centrados no ser humano" [tradução livre]. OCDE. Good Practice Principles for Data Ethics in the Public Sector, 2020, p. 5. Disponível em: https://www.oecd.org/digital/digital-government/good-practice-principles-for-data-ethics-in-the-public-sector.htm. Acesso: 10 dez. 2021. ▸ p.30

[16] Nesse sentido, o Decreto nº 10.046/2019 adotou a sistemática de dispensar a celebração de convênio, acordo de cooperação técnica ou instrumentos congêneres para a efetivação de compartilhamento de dados entre órgãos e entidades da administração pública federal (art. 5º). Em alternativa, definiu-se que nos casos de dados categorizados como "restritos" ou "específicos", o compartilhamento deve observar, respectivamente, as regras estabelecidas pelo Comitê Central de Governança de Dados (art. 12) ou decisão administrativa do gestor dos dados, que conceda a permissão de acesso e defina os requisitos definidos como condição para o compartilhamento (art. 14). ▸ p.31

[17] No julgamento da Ação Direta de Inconstitucionalidade nº 6387, em 24 de abril de 2020, o STF considerou inconstitucional a Medida Provisória (MP) nº 954, de 17 de abril de 2020, que obrigava as prestadoras de serviços de telecomunicações a compartilhar dados de seus usuários com o IBGE para fins de "produção estatística oficial". Conforme exposto no voto da Ministra Rosa Weber, relatora da ação, a norma "não delimita o objeto da estatística a ser produzida, nem a finalidade específica, tampouco a amplitude. Igualmente não esclarece a necessidade de disponibilização dos dados nem como serão efetivamente utilizados [...]. Nessa linha, ao não definir propriamente como e para que serão utilizados os dados coletados, a MP n. 954/2020 não

oferece condições para avaliação da sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades." ▸ p.32

Divulgação de dados pessoais ▸ p.37–43

[18] Os critérios de divulgação de informações pessoais estão previstos, por exemplo, no art. 31 da LAI. No âmbito da administração pública federal, a Controladoria-Geral da União e a Comissão Mista de Reavaliação de Informações são os órgãos competentes para deliberar, com base na LAI, sobre recursos interpostos em casos de negativa de acesso à informação determinada por órgão ou entidade pública federal, nos termos dos arts. 23 e 24 do Decreto nº 7.724, de 16 de maio de 2012. ▸ p.37

[19] A autodeterminação informativa é um dos fundamentos da disciplina legal da proteção de dados pessoais (art. 2º, II, LGPD) e consiste em garantir ao titular os meios necessários ao exercício do controle sobre seus próprios dados pessoais. ▸ p.38

[20] Conforme decidido pelo STF, "a remuneração dos agentes públicos constitui informação de interesse coletivo ou geral", aplicando-se à hipótese o princípio constitucional da publicidade administrativa, que "propicia o controle da atividade estatal até mesmo pelos cidadãos." A Corte entendeu, ainda, que os riscos pessoais decorrentes da divulgação são atenuados com "a proibição de se revelar o endereço residencial, o CPF e a CI de cada servidor". Por fim, em atenção ao contexto e às expectativas dos titulares envolvidos, a decisão menciona que "os dados objeto de divulgação em causa dizem respeito a agentes públicos mesmos; ou, na linguagem da própria Constituição, agentes estatais agindo nessa qualidade". Suspensão de Liminar nº 623/DF, Ministro Ayres Britto, 10 de julho de 2012. ▸ p.40

Anexo I

Uso compartilhado de dados pessoais pelo Poder Público

Requisito	Recomendação
Formalização e registro	▸ Instauração de processo administrativo; ▸ Análise técnica e jurídica; ▸ Decisão administrativa ou celebração de contrato, convênio ou instrumento congênere; ▸ Edição de ato normativo interno.
Objeto e finalidade	▸ Descrição dos dados pessoais de forma objetiva e detalhada; ▸ Indicação de finalidade específica; ▸ Avaliação da compatibilidade entre a finalidade original e a finalidade do compartilhamento.
Base legal	▸ Indicação da base legal utilizada.
Duração do tratamento	▸ Definição do período (duração) do uso compartilhado dos dados, de forma fundamentada, e esclarecimento sobre a possibilidade de conservação ou a necessidade de eliminação após o término do tratamento.
Transparência e direitos dos titulares	▸ Divulgação das informações pertinentes na página eletrônica dos órgãos e das entidades responsáveis; ▸ Divulgação de maneira que as informações sobre dados pessoais tratados pela entidade sejam de fácil compreensão; ▸ Definição de responsabilidades e de procedimentos relativos ao atendimento de solicitações de titulares.

Prevenção e segurança	▸ Descrição das medidas técnicas e administrativas adotadas para proteger os dados pessoais de incidentes de segurança.
Outros requisitos (avaliação conforme o caso concreto)	▸ Autorização ou vedação para novo compartilhamento ou transferência posterior dos dados pessoais; ▸ Ônus financeiro; ▸ Requisitos específicos para compartilhamento de dados pessoais com entidades privadas (art. 26, § 1º e art. 27, LGPD); ▸ Elaboração de relatório de impacto à proteção de dados pessoais, caso necessário; ▸ Identificar as funções e responsabilidades dos agentes de tratamento.

Anexo II

Cuidados a serem observados quando da divulgação de dados pessoais pelo Poder Público

Parâmetro	Recomendação
A coleta do dado pessoal é necessária e adequada para a finalidade do tratamento?	▸ Verificar a possibilidade de dispensa da coleta ou de eliminação dos dados pessoais, tendo em vista a sua efetiva necessidade para o alcance das finalidades do tratamento; ▸ Verificar se há formas de atingir a finalidade almejada sem o tratamento de dados pessoais e de maneira menos gravosa para o titular de dados.
A divulgação envolve dados pessoais sensíveis?	▸ Em caso afirmativo, o tratamento deve ser efetuado com maior cautela, observando-se normas específicas, como os dispositivos da LGPD relativos a estudos em saúde pública.
Quais medidas de mitigação de risco para o titular de dados podem ser adotadas?	▸ Elaboração de relatório de impacto à proteção de dados pessoais, caso necessário; ▸ Medidas de prevenção e segurança, a exemplo de anonimização ou pseudonimização dos dados pessoais sempre que isso não comprometa o exercício do controle social; ▸ Limitação da divulgação àqueles dados necessários para alcançar a finalidade pretendida, observados o contexto, a finalidade e as expectativas legítimas dos titulares; ▸ Transparência do tratamento; e ▸ Garantia de direitos dos titulares.

www.anpd.gov.br

Guia de Elaboração de Inventário de Dados Pessoais

PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI)

Versão 2.0

Brasília, março de 2023

GUIA DE ELABORAÇÃO DE INVENTÁRIO DE DADOS PESSOAIS

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS

Esther Dweck

Ministra

SECRETARIA DE GOVERNO DIGITAL

Rogério Souza Mascarenhas

Secretário de Governo Digital

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Leonardo Rodrigo Ferreira

Diretor de Privacidade e Segurança da Informação

COORDENAÇÃO-GERAL DE PROTEÇÃO DE DADOS

Loriza Andrade Vaz de Melo

Coordenadora-Geral de Proteção de Dados

Equipe Técnica de Elaboração

Denis Marcelo Oliveira

Julierme Rodrigues da Silva

Loriza Andrade Vaz de Melo

Luiz Henrique do Espírito Santo Andrade

Tássio Correia da Silva

Wellington Francisco Pinheiro de Araújo

Equipe Técnica de Revisão - Versão 2.0

Bruno Pierre Rodrigues de Sousa

Francisco Magno Felix Nobre

Ivaldo Jeferson De Santana Castro

Julierme Rodrigues da Silva

Leonard Keyzo Yamaoka Batista

Rafael Da Silva Ribeiro

Raphael César Estevão

Rogério Vinícius Matos Rocha

Histórico de Versões

Data	Versão	Descrição	Autor
23/09/2020	1.0	Primeira versão do Guia de Elaboração de Inventário de Dados Pessoais.	Equipe Técnica de Elaboração
26/04/2021	1.1	Atualização do link com a tabela de temporalidade das atividades meio do Poder Executivo (Portaria 47/2020 do CONARQ).	Equipe Técnica de Elaboração
31/03/2023	2.0	Atualização para alinhamento com o Guia do Framework de Privacidade e Segurança da Informação, conforme destacado no Anexo II.	Equipe Técnica de Revisão

SUMÁRIO

AVISO PRELIMINAR E AGRADECIMENTOS

O presente Guia, especialmente recomendado e dirigido aos órgãos e às entidades da Administração Pública Federal - APF, visa a auxiliar na Elaboração de um Inventário de Dados Pessoais, em atendimento ao previsto no art. 37 da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), que determina que a Administração Pública, ao prestar diversos serviços que tratam dados pessoais à sociedade, deve manter registro das operações de tratamento realizadas sobre os dados que estão sob sua custódia. Adicionalmente, a Elaboração de um Inventário de Dados Pessoais visa a atender, além da LGPD, a outros normativos vigentes sobre o tema de privacidade e segurança da informação.

Este documento é de autoria exclusiva da Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos e tem como referência fundamental o Guia do Framework de Privacidade e Segurança da Informação baseado em diversas publicações e documentos técnicos já existentes que são utilizados amplamente por profissionais da área de privacidade e segurança da informação. Destacam-se as publicações do *Center for Internet Security* (CIS), da *International Organization for Standardization* (ISO), do *National Institute of Standards and Technology* (NIST) e de Autoridades de Proteção de Dados. Com o objetivo de facilitar a difusão de conhecimentos sobre privacidade e segurança da informação, tais referências, quando escritas em línguas estrangeiras, foram traduzidas para o português pela equipe técnica da Diretoria de Privacidade e Segurança da Informação da Secretaria de Governo Digital.

Nesse cenário, a Secretaria de Governo Digital enfatiza que:

a) não representa, tampouco se manifesta em nome do CIS, da ISO e do NIST e vice-versa;
b) não se manifesta em nome de autoridades de privacidade e segurança da informação;
c) não é coautora das publicações internacionais abordadas;
d) não assume nenhuma responsabilidade administrativa, técnica ou jurídica por usos ou interpretações inadequadas, fragmentados ou parciais do presente guia; e

e) caso o leitor deseje se certificar de que atende integralmente os requisitos das publicações das instituições mencionadas, deverá consultar diretamente as fontes oficiais de informação ofertadas por elas, que foram listadas na seção “Referências Bibliográficas” deste documento.

Finalmente, um agradecimento especial deve ser registrado ao CIS, à ISO, às autoridades de proteção de dados referenciadas, ao NIST e aos profissionais de privacidade e segurança da informação consultados, por suas valiosas contribuições para a comunidade e para elaboração **deste documento**.

Este Guia será atualizado frequentemente, de acordo com as novas diretrizes determinadas pelas autoridades em privacidade e segurança da informação ou segundo eventuais alterações que ocorram nos normativos vigentes relacionados a privacidade e segurança da informação e outras referências utilizadas **neste documento**.

INTRODUÇÃO

Este Guia tem por finalidade apresentar orientações com o intuito de auxiliar os órgãos e entidades da Administração Pública Federal, direta, autárquica e fundacional a realizar o levantamento e registro dos dados pessoais tratados no âmbito institucional.

O Controle 19 do Guia do Framework de Privacidade e Segurança da Informação (p. 60) estabelece que:

Controle 19: Inventário e Mapeamento – *As operações de tratamento de dados pessoais por sistemas, produtos, processos ou serviços devem ser identificadas e inventariadas.*

O presente Guia serve como um modelo prático a ser utilizado para auxiliar na adoção do Controle 19 do Guia do Framework de Privacidade e Segurança da Informação[1] v1 e respectivas evoluções desta versão (1.1, 1.2 etc.) elaborado e publicado pela SGD. As medidas do Controle 19 que estão contempladas por este Guia são: 19.1, 19.2, 19.3, 19.4, 19.5, 19.6, 19.7, 19.8, 19.9, 19.10, 19.11, 19.12, 19.13 e 19.14.

Um modo de manter os registros das operações de tratamento de dados pessoais é manter um inventário ou uma lista das atividades de tratamento que a organização realiza. O Inventário de Dados Pessoais representa o documento primordial para documentar o tratamento de dados pessoais realizados pela instituição em alinhamento ao previsto pelo art. 37 da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD):

> *"Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse."*

O inventário consiste em uma excelente forma de fazer um balanço do que o órgão e entidade faz com os dados pessoais, identificando quais dados pessoais são tratados, onde estão e que operações são realizadas com eles.

[1] < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf >. Acesso em 03/02/2023.

GUIA DE ELABORAÇÃO DO INVENTÁRIO DE DADOS PESSOAIS

As orientações relativas à elaboração do Inventário de Dados Pessoais foram estruturadas em três capítulos:

- O Capítulo 1 destaca sua composição;
- O Capítulo 2 trata sobre como elaborá-lo; e
- O Capítulo 3 aborda a elaboração de uma listagem geral dos serviços/processos de negócios que tratam dados pessoais.

1 O INVENTÁRIO DE DADOS PESSOAIS

1.1 O que é

O **Inventário de Dados Pessoais – IDP** consiste no registro das operações de tratamento dos dados pessoais realizados pela instituição (LGPD. Art. 37).

De uma forma geral, esse registro mantido pelo **IDP** envolve descrever informações em relação ao tratamento de dados pessoais realizado pelo órgão ou entidade como:

- atores envolvidos (agentes de tratamento e o encarregado);
- finalidade (o que a instituição faz com o dado pessoal);
- hipótese (arts. 7º e 11 da LGPD);
- previsão legal;
- dados pessoais tratados pela instituição;
- categoria dos titulares dos dados pessoais;
- tempo de retenção dos dados pessoais;
- instituições com as quais os dados pessoais são compartilhados;
- transferência internacional de dados (art. 33 LGPD); e
- medidas de segurança atualmente adotadas.

O **IDP** representa um documento importante de governança de dados pessoais e de subsídio para avaliação de impacto à proteção de dados pessoais com vistas a verificar a conformidade da instituição no que se refere ao preconizado pela LGPD.

1.2 Estruturação

A estrutura do **IDP** apresentado neste documento é inspirado nos modelos propostos pelas autoridades de proteção de dados da França[2], Bélgica[3] e Inglaterra[4].

[2] < https://www.cnil.fr/sites/default/files/atoms/files/record-processing-activities.ods>. Acesso em 06/07/2020.
[3] < https://www.autoriteprotectiondonnees.be/publications/modele-de-registe-des-activites-de-traitement.xls >. Acesso em 06/07/2020.
[4] < https://ico.org.uk/media/for-organisations/documents/2172937/gdpr-documentation-controller-template.xlsx >. Acesso em 06/07/2020.

O **inventário** foi estruturado em formato de planilha eletrônica, disponível no link < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/template_inventario_dados_pessoais.xlsx >.

A planilha eletrônica que representa o template do **IDP** é composta por 4 divisões denominadas:

- "1-Orientações" – orientações gerais sobre preenchimento do template;
- "2-Lista Inventário" – lista geral dos serviços/processos de negócio institucionais que realizam o tratamento de dados pessoais;
- "3-Template" – modelo de inventário de dados pessoais a ser elaborada para cada serviço/processo de negócio da instituição; e
- "4-Listas" – apresenta uma sugestão de informações para preenchimento do inventário de dados com valores padronizados. A lista não é exaustiva e por isso pode ser ajustada de acordo com a realidade de cada instituição.

O próximo capítulo descreve o processo de elaboração do **IDP** com base divisão denominada "3-Template" constante da planilha eletrônica mencionada no início desta seção.

1.3 Inventário de Dados Pessoais, RIPD e Conformidade

O **IDP** consiste no registro das operações de tratamento dos dados pessoais realizados pela instituição. Ele proporciona uma espécie de "fotografia" do atual cenário do tratamento de dados pessoais do serviço/processo de negócio.

As informações contidas no **IDP** fornecem subsídios para a elaboração do RIPD, o qual é um instrumento fundamental para avaliação da conformidade do tratamento de dados pessoais em relação à LGPD, bem como de análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de riscos adotados.

Ao finalizar a elaboração do **IDP**, caso a instituição identifique, por exemplo, a necessidade de minimização dos dados pessoais tratados ou incompatibilidades de adequação à finalidade do tratamento de dados, **não há objeções, caso opte por sanar imediatamente no serviço/processo de negócio essas não conformidades antes da**

elaboração do RIPD. Todavia, **após realizar tal ação é indicado que seja gerado nova versão do IDP**, refletindo o novo cenário de tratamento de dados pessoais.

2 COMO ELABORAR O INVENTÁRIO DE DADOS PESSOAIS

De acordo com o art. 37 da LGPD, o "controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem (...)". O inventário de dados pessoais vem atender precisamente essa determinação da Lei 13.709/2018 no que se refere à manutenção de registro do levantamento do tratamento de dados pessoais realizados pela instituição.

O formulário de **IDP** apresentado neste documento constitui uma **sugestão para auxiliar os órgãos e entidades, que exercem papel de controlador de dados pessoais,** na elaboração de inventário de dados pessoais. Dessa forma, e caso seja considerado pertinente pela instituição, o modelo de **IDP** pode ser adaptado para se adequar a cada contexto particular. A figura a seguir destaca as fases de elaboração do inventário.

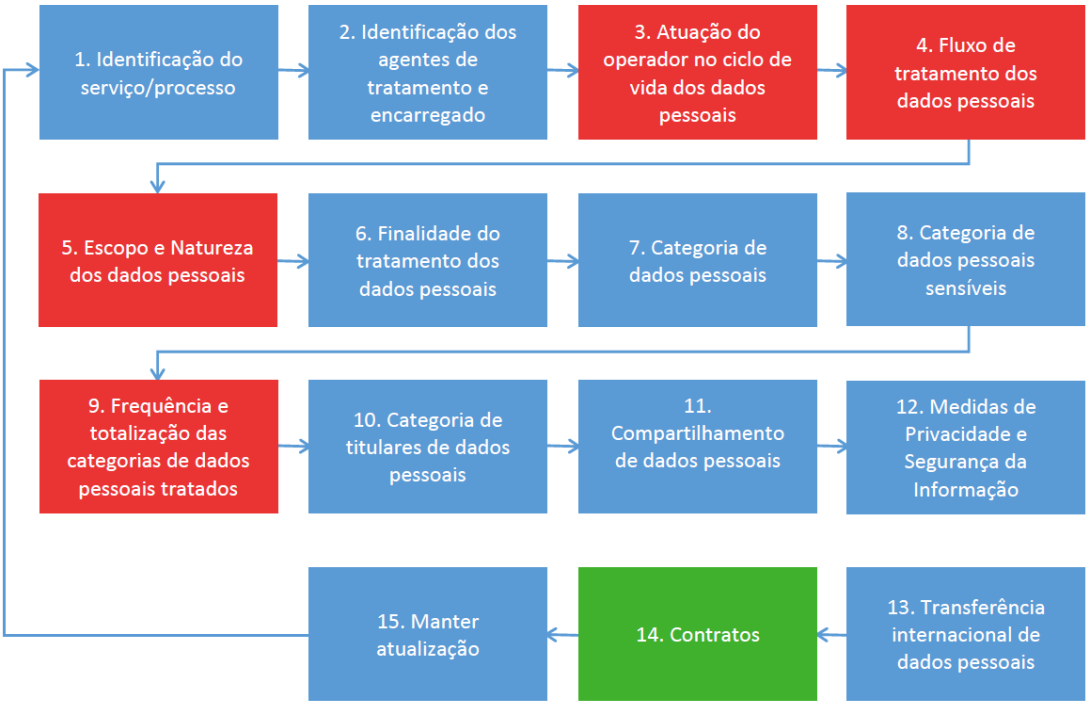


Figura 1 Fases de elaboração do Inventário de Dados Pessoais

As fases acima destacadas **em azul** representam os elementos mínimos para o **IDP,** as destacadas **em laranja** representam levantamento complementar no inventário de informações que auxiliarão a elaboração do Relatório de Impacto de Proteção de Dados

Pessoais - RIPD[5] (CCGD, 2020) e a destacada em **verde** corresponde à identificação inicial de contrações a serem avaliadas na análise de adequação contratual. Importante ressaltar que todas as informações do **IDP** subsidiarão o RIPD.

Usar o modelo proposto por este Guia não é obrigatório. A instituição pode documentar as atividades de tratamento de dados pessoais da sua organização de muitas maneiras diferentes, desde modelos básicos até pacotes de software especializados. A forma como o órgão mantém sua documentação dependerá de fatores como o tamanho da instituição, o volume de dados pessoais tratados e a complexidade das operações de tratamento.

Além da proteção de dados, os órgãos e entidades muitas vezes estão sujeitos a vários outros regulamentos que têm suas próprias obrigações de documentação, especialmente em setores como seguros e finanças. Se a organização está sujeita a tais requisitos regulamentares, então é provável que já exista uma estrutura de governança de dados estabelecida em vigor que suporta seus procedimentos de documentação existentes; pode até se sobrepor aos requisitos de manutenção de registros da LGPD. Nesse caso, a LGPD não proíbe de combinar e incorporar a documentação de suas atividades de tratamento de dados pessoais com as práticas existentes de inventário de dados. Mas deve-se ter cuidado para garantir que pode cumprir os requisitos do art. 37 da LGPD, se necessário, ajustando sua estrutura de governança de dados para inventariar os dados pessoais.

As próximas seções descrevem o processo de elaboração do **IDP**, **cujo modelo tratado por este Capítulo deve ser elaborado para cada serviço/processo de negócio da instituição**.

2.1 Identificação do serviço/processo

O modelo de **IDP** proposto neste Guia adota a estratégia de inventariar os dados pessoais por serviço e/ou processo de negócio realizado pelo órgão ou entidade (Figura 2).

[5] Informações sobre o RIPD podem ser obtidas na seção 2.5 do Guia de Boas Práticas LGPD, disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf>

1 - Identificação dos serviços / processo de negócio de tratamento de dados pessoais	
1.1 - Nome do serviço / Processo de negócio	
1.2 - Nº Referência / ID	
1.3 - Data de Criação do Inventário	
1.4 - Data Atualização do Inventário	

Figura 2 Seção 1 da guia "3-Templates" da planilha eletrônica do Inventário de Dados Pessoais (seção 1.2 deste Guia)

A opção de inventariar por serviço possibilita que a instituição realize o levantamento dos dados pessoais tratados pelos serviços divulgado no portal gov.br (https://www.gov.br/pt-br/servicos).

Cumpre destacar que os dados pessoais de todos os serviços devem ser inventariados, mesmo os serviços que, porventura, não são digitais.

O **IDP** também possibilita o inventário de dados pessoais por processo de negócio. Essa opção visa contemplar processos ou rotinas internas como, por exemplo, processo interno de gestão de pessoas (servidores, empregados públicos, etc.) da instituição.

Com a finalidade facilitar a identificação do serviço ou processo inventariado, o item 1.2 da Figura 2 deve ser preenchido com um número de referência ou um ID para identificação da atividade de tratamento de dados pessoais relacionada ao serviço/ processo de negócio. **Exemplos de números de referência:** 0001, 0002, etc. **Exemplo de ID adotando Sigla do Serviço informado no campo "Nome do serviço/ Processo de Negócio:** AVA, CRRA e etc. Essa etapa é finalizada com o preenchimento das datas de criação e de última atualização do inventário de dados pessoais do serviço/processo de negócio.

2.2 Identificação dos agentes de tratamento e encarregado

Esta fase envolve identificar os agentes de tratamento (controlador e operador) e o encarregado no **IDP** (art. 5º da LGPD), destacando nome, endereço, CEP, telefone e e-mail (Figura 3).

2 - Agentes de Tratamento e Encarregado	Nome	Endereço	CEP	Telefone	E-mail
2.1 - Controlador					

2.2 - Encarregado					
2.3 - Operador					

Figura 3 Seção 2 da guia "3-Templates" da planilha eletrônica do Inventário de Dados Pessoais (seção 1.2 deste Guia)

Explicações sobre controlador, operador e encarregado podem ser conferidas na seção 1.1 do Guia de Boas Práticas LGPD (CCGD, 2020).

2.3 Atuação do operador no ciclo de vida do tratamento do dado pessoal

O ciclo de vida do tratamento do dado pessoal envolve as fases de: coleta, retenção, processamento, compartilhamento e eliminação.

Constatar em que fase do ciclo de vida do tratamento do dado pessoal o operador atua (Figura 4) é essencial para compreensão de quais operações de tratamento são realizadas por ele e quais ativos organizacionais estão envolvidos nesse tratamento.

3 - Fases do Ciclo de Vida do Tratamento Dados Pessoais	Coleta	Retenção	Processamento	Compartilhamento	Eliminação
3.1 - Em qual fase do ciclo de vida o Operador atua					

Figura 4 Seção 3 da guia "3-Templates" da planilha eletrônica do Inventário de Dados Pessoais (seção 1.2 deste Guia)

Uma vez identificados os ativos, é necessário analisá-los para verificar quais medidas técnicas de segurança estão efetivamente implementadas nesses ativos, com vistas a prover a adequada proteção aos dados pessoais de que trata a LGPD. As medidas de segurança resultantes dessa análise serão descritas na fase “Medidas de Segurança” descrita na seção 2.12 deste Guia.

Orientações sobre ciclo de vida de tratamento de dados pessoais e seu relacionamento com os ativos organizacionais podem ser observadas no Capítulo 3 do Guia de Boas Práticas LGPD (CCGD, 2020).

Esta fase do **IDP** subsidiará um dos elementos que compõem a descrição da natureza do tratamento no RIPD (CCGD, 2020), no que tange ao papel do operador em relação ao tratamento do dado pessoal.

2.4 Fluxo de tratamento dos dados pessoais

Descrever como (de que forma) os dados pessoais são coletados, retidos/armazenados, processados/usados e eliminados (Figura 5).

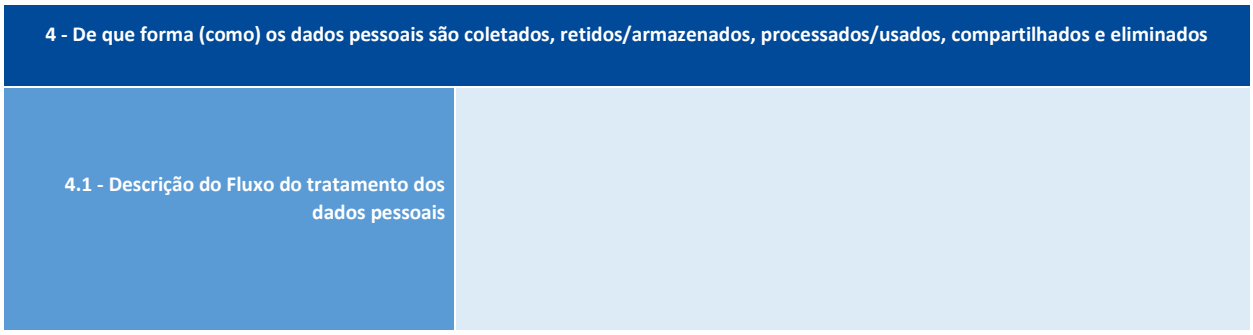


Figura 5 Seção 4 da guia "3-Templates" da planilha eletrônica do Inventário de Dados Pessoais (seção 1.2 deste Guia)

Nessa fase, pode até ser elaborado um desenho com um fluxo de dados.

Abaixo, consta exemplificação de descrição do fluxo de tratamento de dados pessoais do programa fictício de localização de desaparecidos do Departamento de Segurança Pública - DSP.

Exemplo de descrição de fluxo de dados:

1. Os dados pessoais são coletados mediante preenchimento formulário eletrônico do Sistema Nacional pelo titular dos dados pessoais.

2. Os dados são transferidos armazenados nas instalações físicas da Empresa de Processamento e Tecnologia Fictum (operador).

3. A empresa Fictum realiza processamento sobre os dados pessoais e disponibiliza para uso do Departamento de Segurança Pública – DSP (controlador). O DSP disponibiliza os dados pessoais para utilização e consumo do comunicante.

4. O DSP transfere dados de comunicantes e pessoas desaparecidas para a Secretaria de Desenvolvimento Humano desenvolver as ações de apoio psicológico para as famílias dos desaparecidos.

5. Os dados pessoais podem ser eliminados a pedido do titular. Nesse caso, o DSP encaminha essa solicitação para a empresa Fictum executar a eliminação dos dados pessoais da base de dados do Sistema Nacional de Desaparecidos.

2.5 Escopo e Natureza dos dados pessoais

Esta fase contempla identificar dois elementos relevantes do escopo e natureza dos dados pessoais tratados a serem futuramente descritos no RIPD (CCGD, 2020). Esses elementos são, respectivamente, a abrangência e a fonte de dados pessoais (Figura 6).

5 - Escopo e Natureza dos Dados Pessoais	
5.1 - Abrangência da área geográfica do tratamento	
5.2 - Fonte de dados utilizada para obtenção dos dados pessoais	

Figura 6 Seção 5 da guia "3-Templates" da planilha eletrônica do Inventário de Dados Pessoais (seção 1.2 deste Guia)

A abrangência representa o alcance geográfico do tratamento de dados realizado: nacional, estadual, distrital, municipal ou regional.

A fonte de obtenção de dados pessoais, pode ser por exemplo: titular dos dados pessoais, XML, API, etc. A forma de obtenção dos dados pessoais tem influência direta nos mecanismos que devem ser implementadas para assegurar os princípios da qualidade dos dados (LGPD, art. 6º, V) e segurança (LGPD, art. 6º, VII).

Exemplo 1: Se os dados pessoais são obtidos por meio de preenchimento de formulário eletrônico, então a fonte de dados é o titular dos dados pessoais.

Exemplo 2: Fonte de dados que não seja o titular de dados, é importante detalhar a fonte, como por exemplo, API CONSULTA CPF.

2.6 Finalidade do Tratamento dos dados pessoais

Esta fase aborda a identificação de três aspectos fundamentais para respaldar o tratamento dos dados pessoais: a hipótese (arts. 7º e 11) da LGPD, a especificação da finalidade e a previsão legal (Figura 7).

6 - Finalidade do Tratamento de Dados Pessoais	
6.1 - Hipótese de Tratamento	
6.2 - Finalidade	
6.3 - Previsão legal	

6.4 - Resultados pretendidos para o titular de dados	
6.5 - Benefícios esperados para o órgão, entidade ou para a sociedade como um todo	

Figura 7 Seção 6 da guia "3-Templates" da planilha eletrônica do Inventário de Dados Pessoais (seção 1.2 deste Guia)

Orientações sobre base legal (Figura 7, item 6.3) e hipóteses de tratamento (Figura 7, item 6.1) podem ser conferidas, respectivamente, nas seções 1.1 e 2.1 do Guia de Boas Práticas LGPD (CCGD, 2020).

A previsão legal representa informar no item 6.3 da Figura 7 qual Lei, Decreto, normativo ou regulamento que respalda a finalidade do tratamento de dados pessoais realizado.

Exemplo fictício de previsão legal considerando o Programa de Localização de Desaparecidos:

- Decreto nº 8.956, de 25 de janeiro de 2218, institui o Programa de Localização de Desaparecidos.

Nesse momento, cabe ressaltar que os órgãos e entidades da administração pública tem a prerrogativa de tratar os dados pessoais para o exercício de suas competências legais ou execução de políticas públicas sem a necessidade de obter consentimento do titular dos dados pessoais (CCGD, 2020).

A finalidade (Figura 7, item 6.2) é a razão ou motivo pela qual se deseja tratar os dados pessoais. É fundamental estabelecer claramente a finalidade, pois é ela que apresenta a justificativa do tratamento de dados pessoais e fornece os elementos para informar o titular dos dados pessoais (CCGD, 2020).

A conclusão dessa fase compreende descrever em relação à finalidade do tratamento:

- os resultados pretendidos para o titular dos dados pessoais; e
- benefícios esperados para o órgão, entidade ou para a sociedade como um todo.

2.7 Categorias de dados pessoais

Identificar quais são os dados pessoais tratados pelo órgão ou entidade que representa o objetivo central do **IDP**. Inventariar os dados pessoais utilizados pela instituição

possibilitará avaliar se todos os dados pessoais usados são realmente necessários e adequados para realização de suas finalidades (LGPD, art. 6º, III).

A fim de facilitar a identificação dos dados pessoais tradados, o modelo de **IDP elenca uma lista exemplificativa e não exaustiva de 15 categorias de dados pessoais com suas respectivas subcategorias,** para as quais devem ser especificamente descritos os dados pessoais tratados.

A Figura 8 destaca o primeiro tipo de categoria de dados pessoais,"7.1 Dados de Identificação Pessoal", e as colunas a serem preenchidas explicadas a seguir.

7 - Categoria de Dados Pessoais				
7.1 -Dados de Identificação Pessoal	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.1.1 - Informações de identificação pessoal				
7.1.2 - Informações de identificação atribuídas por instituições governamentais				
7.1.3 - Dados de identificação eletrônica				
7.1.4 - Dados de localização eletrônica				

Figura 8 Seção 7 da guia "3-Templates" da planilha eletrônica do Inventário de Dados Pessoais (seção 1.2 deste Guia)

Descrição: descrever de forma específica os dados pessoais tratados (ex.: CPF, nome, etc.) de acordo com as subcategorias listadas no Anexo deste Guia.

Tempo Retenção dos dados: informação sobre quanto tempo o dado pessoal será armazenado. Para definição do tempo de retenção é indicado verificar:

- se existe alguma definição legal de tempo de retenção/guarda/arquivamento de documentos e/ou dos dados tratados pelo órgão e/ou entidade; e

- tabela de temporalidade do CONARQ[6].

[6] Disponível em: < https://www.gov.br/arquivonacional/pt-br/servicos/gestao-de-documentos/orientacao-tecnica-1/codigo-de-classificacao-e-tabela-de-temporalidade-e-destinacao-de-documentos-de-arquivo/copy_of_cod_classif_-e_tab_temp_2019_m_book_digital_25jun2020.pdf >

Fonte de Retenção: em que local o dado pessoal está armazenado/retido. Nesse campo deve ser informado a principal fonte de retenção/armazenamento dos dados para cada categoria de dados pessoais efetivamente tratada pela instituição.

Nome Base de Dados: essa coluna deverá ser preenchida, se a principal fonte de retenção / armazenamento dos dados pessoais for base de dados. Informar o mesmo nome da base de dados registrada no Sistema de Catálogo de Dados[7] mantido pela Secretaria de Governo Digital - SGD. O nome e a descrição da base de dados devem ser atualizados na guia "4-Listas" apresentada na seção 1.2 deste documento. **Necessário destacar que não há obrigatoriedade de se informar o nome da base de dados, caso a instituição não tenha iniciado o citado Catálogo de Dados**.

Se órgão não for iniciar o cadastro do Catálogo de Base de Dados – CBD antes ou concomitante ao **IDP**, então a instituição pode optar por definir o nome e a descrição da base de dados, conforme orientado na guia "4-Listas" mencionada acima. Posteriormente, ao iniciar o CBD, o órgão ou entidade pode aproveitar os nomes e descrições das bases de dados definidos no inventário e informá-los no sistema do CBD.

Compreendido o que significa cada coluna exibida pelo Figura 8, é recomendável que seja realizada a leitura do Anexo deste documento, no qual consta uma tabela com **rol não exaustivo** de categorias, subcategorias e o que deve ser descrito na coluna "Descrição" constante da Figura 8 referentes aos dados pessoais tratados pela instituição. Dessa forma, ao elaborar o **IDP**, **a instituição tem total liberdade para adaptar, remover, incluir categorias, subcategorias e descrição dos dados tratados de acordo com sua realidade institucional.**

Diante do listado no Anexo deste Guia, para cada categoria e subcategoria dos dados pessoais tratados pelo órgão ou entidade, deve-se preencher os dados pessoais efetivamente usados. **A título de exemplificação**, se a instituição trata apenas dados pessoais de CPF e nome, então a coluna "Descrição" da Figura 8 serão preenchidos da seguinte forma:

[7] Para saber mais sobre a iniciativa de Catálogo de Base de Dados da SGD, acesse o link: < https://www.gov.br/governodigital/pt-br/governanca-de-dados/catalogo-de-bases-de-dados >

- na subcategoria “7.1.1 - Informações de identificação pessoal” constaria o dado pessoal “Nome”; e
- na subcategoria “7.1.2 - Informações de identificação atribuídas por instituições governamentais” constaria o dado pessoal “CPF”.

2.8 Categorias de dados pessoais sensíveis

O preenchimento das colunas relativas aos dados pessoais sensíveis da Figura 9 segue a mesma forma explicada na seção 2.7 do Guia.

8 - Categorias de Dados Pessoais Sensíveis	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
8.1 - Dados que revelam origem racial ou ética				
8.2 - Dados que revelam convicção religiosa				
8.3 - Dados que revelam opinião política				
8.4 - Dados que revelam filiação a sindicato				
8.5 - Dados que revelam filiação a organização de caráter religioso				
8.6 - Dados que revelam filiação ou crença filosófica				
8.7 - Dados que revelam filiação ou preferências política				
8.8 - Dados referentes à saúde ou à vida sexual				
8.9 - Dados genéticos				
8.10 - Dados biométricos				

Figura 9 Seção 8 da guia "3-Templates" da planilha eletrônica do Inventário de Dados Pessoais (seção 1.2 deste Guia)

Realizar o inventário de dados pessoais sensíveis é extremamente importante, visto que o uso indevido desses dados pode resultar em algum tipo de discriminação em relação ao titular dos dados pessoais sensíveis. A seção 2.1.3 do Guia de Boas Práticas LGPD (CCGD, 2020) trata das especificidades para o tratamento de dados pessoais sensíveis.

As categorias listadas na Figura 9 representam a lista de dados sensíveis do inciso II do art. 5º da LGPD.

Art. 5º Para os fins desta Lei, considera-se:

> II - dado pessoal sensível: 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;

2.9 Frequência e totalização das categorias de dados pessoais tratados

Nesta fase são identificadas a frequência de tratamento dos dados pessoais e a quantidade de dados pessoais e dados pessoais sensíveis tratados pelo serviço / processo de negócio (Figura 10).

A frequência e totalização das categorias de dados pessoais tratados fornecerão subsídio para o escopo do tratamento de dados pessoais a serem descritos no RIPD (CCGD, 2020).

9 - Frequência e totalização das categorias de dados pessoais tratados	
9.1 - Frequência de tratamento dos dados pessoais	
9.2 - Quantidade de dados pessoais e dados pessoais sensíveis tratados	

Figura 10 Seção 9 da guia "3-Templates" da planilha eletrônica do Inventário de Dados Pessoais (seção 1.2 deste Guia)

A frequência de tratamento de dados pessoais representa a disponibilidade e horário de funcionamento do sistema automatizado ou processo manual que trata os dados pessoais.

Exemplo fictício de descrição da frequência de tratamento de dados pessoais do Sistema Nacional de Desaparecidos - SND:

> O SND está disponível no regime 24x7 (24 horas por dia nos 7 dias da semana) para comunicação (coleta) dos dados dos desaparecimentos e as demais fases e operações de tratamento são realizadas no horário comercial em dias úteis.

Informação sobre o horário em que os dados pessoais são tratados contribui para identificar acessos ou processamentos indevidos dos dados pessoais. Considerando o exemplo acima, se operações específicas de tratamento de dados pessoais somente ocorre em horário comercial e dias úteis, uma ação no sistema fora

desses parâmetros pode indicar que alguma operação suspeita sobre os dados foi realizada.

Totalizar a quantidade de dados pessoais e dados pessoais sensíveis tratados propicia uma visão quantitativa do número de dados pessoais tratados. Essa totalização é muito relevante, pois quantos mais dados pessoais são tratados maior será o potencial impacto aos titulares dos dados pessoais em caso, por exemplo, de vazamentos.

Exemplo de totalização de dados pessoais:

A instituição realiza tratamento de dados pessoais como: idade, sexo, data de nascimento, local de nascimento, estado civil e nacionalidade.

Trata dados pessoais sensíveis de saúde como: CID10 e data do exame médico.

Nesse exemplo a informação a ser preenchida no item 9.2 exibido na Figura 10 é:

São tratados 6 dados pessoais e 2 dados pessoais sensíveis, totalizando 8 dados pessoais tratados pelo serviço.

2.10 Categorias de titulares de dados pessoais

Além de elencar os dados pessoais tratados, é necessário identificar em relação a esses dados (Figura 11): quais são as categorias (tipos) de titulares a quem pertencem os dados pessoais; e se são tratados dados pessoais de crianças/adolescentes, bem como de outro grupo vulnerável.

10 - Categorias dos titulares de dados pessoais	Tipo de Categoria	Descrição
10.1 - Categoria 1		
10.2 - Categoria 2		
10.3 - Trata dados de crianças e adolescentes		
10.4 - Além de crianças e adolescente trata dados de outro grupo vulnerável		

Figura 11 Seção10 da guia "3-Templates" da planilha eletrônica do Inventário de Dados Pessoais (seção 1.2 deste Guia)

Na planilha eletrônica que automatiza o **IDP**, podem ser inseridas quantas categorias de titulares que forem necessárias para o fiel registro dos tipos de titulares de dados pessoais que estão envolvidos pelo tratamento de dados realizado pelo serviço / processo de negócio. **Os tipos de categorias já estão previamente definidos na guia "4-Listas" citada na seção 1.2, mas podem ser alterados e ajustados de acordo com o contexto da instituição**.

A coluna "Descrição" constante da Figura 11, deve ser preenchida se for necessário descrever informações complementares, detalhando a categoria do titular dos dados pessoais.

Exemplo 1: Categoria de titular = Pessoas. Nesse caso, a coluna "Descrição" poderia ser preenchida com "Pessoas com deficiência", "Pessoas de baixa renda", etc.

Exemplo 2: Categoria de titular = Dependentes. Nesse caso, a coluna "Descrição" poderia ser preenchida com "Dependentes para fins de IRRF", "Dependentes de para fins de Plano de Saúde", etc.

No item 10.3 mostrado pela Figura 11, o **IDP** propicia constatar se são tratados dados de crianças e adolescentes. Tal constatação é fundamental no sentido de o órgão ou entidade analisar se são atendidas as determinações do art. 14 da LGPD, tal como o prévio consentimento de pais e responsáveis para o tratamento de dados pessoais de crianças. Considerações sobre esse tema podem ser conferidas na seção 2.1.4 do Guia de Boas Práticas LGPD (CCGD, 2020).

O item 10.4 destacado pela Figura 11, permite identificar se é tratado dado pessoal de algum outro grupo vulnerável como, por exemplo: idosos, população em condição de rua, pessoas com deficiência física ou sofrimento mental etc.

A identificação do tratamento de dados pessoais propiciada pelos itens 10.3 e 10.4 da Figura 11 fornecerão elementos para descrição do contexto de tratamento no RIPD (CCGD, 2020) subsidiando a composição do cenário de riscos para avaliar quais controles e

medidas de segurança devem ser adotados para proteção dos dados de crianças, adolescentes e outros grupos vulneráveis em alinhamento à legislação vigente que os protegem.

2.11 Compartilhamento de dados pessoais

Informar com quais instituições os dados pessoais são compartilhados e para qual finalidade (Figura 12). **Devem ser inseridas quantas linhas forem necessárias para registrar todas as instituições que têm acesso aos dados pessoais via compartilhamento. Caso sejam compartilhados dados pessoais com menos de 4 instituições, indica-se a exclusão das linhas excedentes.**

11 - Compartilhamento de Dados Pessoais	Dados pessoais compartilhados	Finalidade do compartilhamento
11.1 - Nome da Instituição 1		
11.2 - Nome da Instituição 2		
11.3 - Nome da Instituição 3		
11.4 - Nome da Instituição 4		

Figura 12 Seção 11 da guia "3-Templates" da planilha eletrônica do Inventário de Dados Pessoais (seção 1.2 deste Guia)

O início dessa fase é marcado pela indicação do nome da instituição que recebe os dados pessoais compartilhados, deve-se substituir o subitem da seção 11 da Figura 12 pelo nome da instituição.

Exemplos de registro das instituições que recebem dados pessoais por compartilhamento:

Exemplo 1: Compartilhamento com o Ministério da Gestão e da Inovação em Serviços Públicos. Nesse caso, substitua "11.1 - Nome da Instituição 1" por "11.1 - Ministério da Gestão e da Inovação em Serviços Públicos ".

Exemplo 2: Compartilhamento com o Banco Central. Nesse caso, substitua "11.2 - Nome da Instituição 2" por "11. 2 - Banco Central".

Exemplo 3: Compartilhamento com a CGU. Nesse caso, substitua "11.3 - Nome da Instituição 3" por "11.3 - CGU".

Exemplo 4: Compartilhamento com o INSS. Nesse caso, substitua "11.4 - Nome da Instituição 4" por "11. 4 - INSS".

Para cada instituição deve-se informar quais são os dados compartilhados e a finalidade do compartilhamento.

Desse modo, a coluna **"Dados pessoais compartilhados"** referenciada pela Figura 12, é preenchida com os dados pessoais e dados pessoais sensíveis compartilhados com as instituições destinatárias dos dados. No preenchimento dessa coluna utilize, no que couber, as informações descritas nas seções "7 - Categorias de Dados Pessoais" e "8 - Categorias de Dados Pessoais Sensíveis" explicitadas nas seções 2.7 e 2.8 deste Guia. **Se não compartilhar dados com outras instituições, preencha a coluna "Dados pessoais compartilhados" do item "11.1 - Nome da Instituição 1" destacado na Figura 12 com "Não se Aplica".**

Esta fase é finalizada com o preenchimento finalidade do compartilhamento. Nesse caso, **é fundamental atentar que a finalidade do compartilhamento deve ser compatível com a finalidade que embasou o tratamento dos dados pessoais discutida na seção 2.6 deste Guia.**

Se existir incompatibilidade, então esse é um ponto de atenção a ser tratado pela instituição no sentido de existir uma adequação da finalidade do compartilhamento ou até mesmo sua interrupção. Essa situação é um dos pontos de atenção a ser considerado na seção 2.16 deste documento.

2.12 Controles de Privacidade e Segurança da Informação

Esta fase envolve identificar os atuais controles de segurança, técnicos administrativos adotados e a descrição das medidas implementadas (Figura 13) que visam assegurar a integridade dos dados pessoais, minimizando os riscos como, por exemplo, de

perda ou vazamento de dados. **Devem ser inseridas quantas linhas forem necessárias para registrar todos os controles de privacidade e segurança da informação aplicados para proteção de dados pessoais, bem como a descrição das medidas adotadas. Caso sejam implementadas menos de 3 controles, indica-se a exclusão das linhas excedentes.**

Os controles de segurança implementados dependem da sensibilidade dos dados pessoais que são tratados e dos riscos para os titulares de dados no caso de um incidente.

12 – Controles de Privacidade e Segurança da Informação	Tipo de Controle de Privacidade e Segurança da Informação	Descrição da(s) Medida(s)
12.1 - Controle de Privacidade e Segurança da Informação 1		
12.2 - Controle de Privacidade e Segurança da Informação 2		
12.3 - Controle de Privacidade e Segurança da Informação 3		

Figura 13 Seção 12 da guia "3-Templates" da planilha eletrônica do Inventário de Dados Pessoais (seção 1.2 deste Guia)

Na planilha eletrônica que automatiza o **IDP**, podem ser inseridos quantos controles de privacidade e segurança da informação forem necessários para o fiel registro dos tipos de titulares de dados pessoais que estão envolvidos pelo tratamento de dados realizado pelo serviço / processo de negócio. **Os tipos de controles de privacidade segurança da informação da coluna "Tipos de controles de privacidade e segurança da informação" já estão previamente definidos na guia "4-Listas" citada na seção 1.2 e foram selecionados do Guia do Framework de Privacidade e Segurança da Informação, mas podem ser alterados e ajustados de acordo com o contexto da instituição**.

A coluna "Descrição das Medidas" exibida na Figura 13 deve ser preenchida com os identificadores ou a descrição da(s) medida(s) específica(s) adotada(s) para o controle de privacidade e segurança da informação.

Exemplos de controles de privacidade e segurança da informação e descrição de medidas:

Exemplo 1:

Tipo de controle de privacidade e segurança da informação = Proteção de dados.

Descrição da(s) Medida(s) = Descarte seguro de dados; Uso de criptografia em mídia removível, dados sensíveis em trânsito e em repouso; e Adoção de solução de prevenção contra perda de dados.

Exemplo 2:

Tipo de controle de privacidade e segurança da informação = Abertura, Transparência e Notificação.

Descrição da(s) Medida(s) = Disponibilização de política de privacidade em local de fácil acesso, antes ou no momento do tratamento de dados pessoais, sem a necessidade de o titular ter que solicitá-lo especificamente.

2.13 Transferência internacional de dados pessoais

Esta fase do **IDP** envolve destacar as organizações internacionais que recebem dados pessoais por meio de qualquer tipo de transferência ou compartilhamento (Figura 14). **Devem ser inseridas quantas linhas forem necessárias para registrar todas as organizações que têm acesso ao dado pessoal por transferência internacional. Caso exista transferência internacional de dados pessoais com menos de 3 organizações, indica-se a exclusão das linhas excedentes.**

13 - Transferência Internacional de Dados Pessoais	País	Dados pessoais transferidos	Tipo de garantia para transferência
13.1 - Organização 1			
13.2 - Organização 2			
13.3 - Organização 3			

Figura 14 Seção 13 da guia "3-Templates" da planilha eletrônica do Inventário de Dados Pessoais (seção 1.2 deste Guia)

O início dessa fase é marcado pelo registro do nome da organização e país que recebe o dado pessoal por transferência internacional. Deve-se substituir o subitem da seção 13 da Figura 14 pelo nome da organização.

Exemplos de registros das organizações e países que recebem dados pessoais por transferência internacional:

Exemplo 1: Transferência Internacional para a Universidade de Coimbra. Nesse caso, substitua "**13.1 - Nome da Organização 1**" por **"13.1 - Universidade de Coimbra"**. Nesse caso, preencher a coluna **"País"** com **"Portugal"**.

Exemplo 2: Transferência Internacional para o U.S. Department of Agriculture (USDA). Nesse caso, substitua **"13.2 - Nome da Organização 2"** por **"13.2 - U.S. Department of Agriculture (USDA)"**. Nesse caso, preencher a coluna "País" com **"Estados Unidos"**.

Exemplo 3: Transferência Internacional para o Department of Justice - Government of Western Australia. Nesse caso, substitua "**13.3 - Nome da Organização 3"** por **"13.3 - Department of Justice - Government of Western Australia"**. Nesse caso, preencher a coluna "**País"** com **"Austrália".**

Caso o órgão ou entidade não realize transferência internacional de dados pessoais, preencha a coluna "País" do item "13.1 – Nome da Organização 1" destacada na Figura 14 com "Não se Aplica".

Para cada organização que recebe dados por transferência internacional deve-se informar quais são os dados pessoais transferidos e o tipo de garantia para transferência. Desse modo, a coluna **"Dados pessoais transferidos"** referenciada pela Figura 14, é preenchida com os dados pessoais e dados pessoais sensíveis compartilhados com as instituições destinatárias dos dados. No preenchimento dessa coluna utilize, no que couber, as informações descritas nas seções **"7 - Categorias de Dados Pessoais"** e **"8 - Categorias de Dados Pessoais Sensíveis"** explicitadas nas seções 2.7 e 2.8 deste Guia.

A coluna **"Tipo de garantia para transferência"** deve ser preenchida para cada organização que recebe dados pessoais por transferência internacional. **Os tipos de garantia da coluna "Tipo de garantia para transferência" já estão previamente definidos na divisão "4-Listas" citada na seção 1.2, mas podem ser alterados e ajustados de acordo com o contexto da instituição**. A transferência internacional de

dados pessoais somente é permitida para os casos elencados no art. 33 da LGPD, os quais já estão contemplados pelo modelo de **IDP** apresentado neste Guia.

Antes de realizar transferência internacional, é recomendado verificar se o país estrangeiro para o qual o órgão ou entidade está transferindo os dados pessoais detém legislação de proteção de dados e se é reconhecida como adequada pela Autoridade Nacional de Proteção de Dados - ANPD. Caso a legislação do país estrangeiro não seja considerada como adequada pela ANPD, o órgão ou entidade precisará indicar ao país estrangeiro uma das estruturas legais descritas no art. 33 a fim de garantir a proteção dos dados pessoais dos cidadãos brasileiros no exterior.

2.14 Contrato(s)

Nesse momento, identificam-se as contratações de serviços ou soluções de TI que realizam algum tipo de operação de tratamento com os dados pessoais do serviço/processo de negócio (Figura 15). **Devem ser inseridas quantas linhas forem necessárias para destacar todos os contratos que tratam os dados pessoais elencados para o serviço/processo de negócio. Se existir apenas um contrato, então deve-se excluir a linha identificada por "14.2 - Contrato nº 2".**

14 - Contrato(s) de serviços e/ou soluções de TI que trata(m) dados pessoais do serviço/processo de negócio	Nº Processo Contratação	Objeto	E-mail do Gestor do Contrato
14.1 - Contrato nº 1			
14.2 - Contrato nº 2			

Figura 15 Seção 14 da guia "3-Templates" da planilha eletrônica do Inventário de Dados Pessoais (seção 1.2 deste Guia)

Inicialmente, é necessário informar o número de identificação do contrato de serviço ou solução de TI que realiza algum tipo de operação de tratamento com os dados pessoais elencados no inventário, assim, deve-se substituir o subitem da seção 14 da Figura 15 pelo número do contrato.

Exemplos de registros de identificação de contratos de serviços e/ou solução de TI que realizam alguma operação de tratamento sobre os dados pessoais elencados no IDP.

Exemplo 1: Contrato identificado pelo nº 15/2020. Nesse caso, substitua "Contrato nº 1" por "Contrato nº 15/2020".

Exemplo 2: Contrato identificado pelo nº 30/2020. Nesse caso, substitua "Contrato nº 2" por "Contrato nº 30/2020".

Caso não exista contrato de serviço ou solução de TI que realize operação de tratamento com os dados pessoais elencados no inventário, preencha a coluna "Nº Processo de Contratação" do item "14.1 – Contrato nº 1" destacada na Figura 15 com "Não há contrato de serviço ou solução de TI que realize operação de tratamento com os dados pessoais elencados neste inventário".

Após identificar os contratos, é necessário informar o objeto contrato e o e-mail de contato do gestor do contrato.

Dessa forma, a coluna **"Objeto do Contrato"** referenciada pela Figura 15, é preenchida com a especificação do objeto descrita no contrato.

A coluna **"E-mail do Gestor do Contrato"** deve ser preenchida com o e-mail institucional do gestor responsável pelo contrato.

A identificação dos gestores de contratos viabiliza a discussão dos possíveis ajustes contratuais no momento de a instituição realizar a atividade de análise da adequação dos contratos em relação ao preconizado pela LGPD.

A atividade de adequação contratual é abordada no "Guia de Boas Práticas para Especificação de Requisitos de Segurança da Informação em Contratações de Tecnologia da Informação" disponibilizado pela Secretaria de Governo Digital.

2.15 Manter Atualização

O **IDP** não termina com a conclusão de sua elaboração. É extremamente necessário que as informações documentadas no **inventário** sempre reflitam a situação atual do tratamento de dados pessoais do serviço/processo de negócio. Ele é um documento "vivo" que é atualizado quando necessário.

Portanto, indica-se que o **IDP** deva ser revisto e atualizado, no mínimo, anualmente, ou sempre que existir qualquer mudança que afete o tratamento dos dados pessoais do serviço/processo de negócio registrado no inventário.

3 LISTAGEM GERAL DO INVENTÁRIO DOS SERVIÇOS / PROCESSOS DE NÉGOCIO QUE TRATAM DADOS PESSOAIS

Ter uma visão geral de todos os inventários de dados pessoais elaborados para cada serviço/processo de negócio é de suma importância para a instituição. Isso facilita o acompanhamento do andamento das ações de inventário e propicia rápida localização da identificação de um inventário de um serviço/processo inventariado.

Nesse contexto, as próximas seções abordarão o modelo de listagem geral sintética apresentado pela guia "2-Lista Inventário" constante da planilha eletrônica disponível em < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/template_inventario_dados_pessoais.xlsx>. Tal listagem visa elencar os **IDPs** elaborados pelo órgão/entidade.

3.1 Identificação do Controlador e Encarregado

Nesta parte inicial da listagem são identificados o controlador e o encarregado (incisos VI e VII do art. 5º da LGPD), destacando nome, e-mail, endereço, CEP, cidade e telefone (Figura 16).

Controlador	Nome: CEP:	E-mail: Cidade:	Endereço: Telefone:
Encarregado	Nome: CEP:	E-mail: Cidade:	Endereço: Telefone:

Figura 16 Parte inicial da guia "2-Lista Inventário" da planilha eletrônica do Inventário de Dados Pessoais (seção 1.2 deste Guia)

Diferentemente da seção 2.2 deste Guia, na listagem geral não consta a identificação do operador porque pode ocorrer de existir mais de um operador atuando em cada serviço/processo de negócio que trata dados pessoais. Contudo, se a instituição considerar importante constar a informação do operador na listagem geral, então realize esse ou

qualquer outro ajuste no modelo da listagem, de acordo com o mais indicado para sua realidade institucional.

3.2 Listagem geral dos serviços e processos de negócio

Nesta parte final da listagem geral são preenchidas as seguintes colunas para cada serviço/processo de negócio inventariado (Figura 16):

- "Nome do serviço/processo de negócio";
- "Nº Ref / ID";
- "Data de Criação do Inventário";
- "Data de Atualização do Inventário";
- "Finalidade do tratamento dos dados pessoais"; e
- "Trata Dados Pessoais Sensíveis?"

Nome do serviço/processo de negócio	Nº Ref / ID	Data de Criação do Inventário	Data de Atualização do Inventário	Finalidade do tratamento dos dados pessoais	Trata Dados Pessoais Sensíveis?

Figura 17 Parte final do guia "2-Lista Inventário" da planilha eletrônica do Inventário de Dados Pessoais (seção 1.2 deste Guia)

As informações a serem preenchidas nas colunas destacadas pela Figura 16 constam das seções discutidas no capítulo 2 deste Guia. Assim, com a finalidade de destacar a correspondência entre as colunas exibidas pela Figura 16 com o modelo de **IDP** apresentado no Capítulo 2, é apresentada a tabela a seguir.

Coluna da guia "2-Lista Inventario" (Figura 16)	Seção do Capítulo 2 do Guia - item da figura
Nome do serviço/processo de negócio	Seção 2.1 – item 1.1 da Figura 2
Nº Ref / ID	Seção 2.1 – item 1.2 da Figura 2
Data de Criação do Inventário	Seção 2.1 – item 1.3 da Figura 2
Data de Atualização do Inventário	Seção 2.1 – item 1.4 da Figura 2
Finalidade do tratamento dos dados pessoais	Seção 2.6 – item 6.2 da Figura 7

Coluna da guia "2-Lista Inventario" (Figura 16)	Seção do Capítulo 2 do Guia - item da figura
Trata Dados Pessoais Sensíveis?	Seção 2.8 – Item 8.1 até 8.10 da Figura 9 **Preencher com Sim:** se existir pelo menos uma informação de dado sensível estiver preenchida em qualquer das subcategorias do item 8. **Preencher com Não** se nenhuma informação de dado sensível estiver preenchida nas subcategorias do item 8.

Tabela 1 Correspondência da Listagem Geral com o IDP

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais.** Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm >. Acesso em: 04 set. 2020.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS - CNIL. **Record of processing activities.** Disponível em: < https://www.cnil.fr/sites/default/files/atoms/files/record-processing-activities.ods>. Acesso em: 04 set. 2020.

COMITÊ CENTRAL DE GOVERNANÇA DE DADOS - CCGD. **Guia de Boas Práticas LGPD.** Abril 2020. Disponível em: < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf >. Acesso em: 04 set. 2020.

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO DA SECRETARIA DE GOVERNO DIGITAL – DPSI/SGD. **Guia do Framework de Privacidade e Segurança da Informação.** Novembro 2022. Disponível em: < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf >. Acesso em: 06 fev. 2023.

CONSELHO NACIONAL DE ARQUIVOS - CONARQ. **Classificação, Temporalidade e Destinação de documentos de Arquivo Relativo às Atividades-Meio da Administração Pública.** Disponível em: < https://www.gov.br/arquivonacional/pt-br/servicos/gestao-de-documentos/orientacao-tecnica-1/codigo-de-classificacao-e-tabela-de-temporalidade-e-destinacao-de-documentos-de-arquivo/copy_of_cod_classif_-e_tab_temp_2019_m_book_digital_25jun2020.pdf>. Acesso em: 26 abr. 2021.

Information Commissioner's Office - ICO. **Documentation template for controllers.** Disponível em: < https://ico.org.uk/media/for-organisations/documents/2172937/gdpr-documentation-controller-template.xlsx >. Acesso em: 04 set. 2020.

AUTORITÉ DE PROTECTION DES DONNÉES GEGEVENSBESCHERMINGSAUTORITEIT. M**odele de Registe des Activites de Traitement.** Disponível em: <

https://www.autoriteprotectiondonnees.be/publications/modele-de-registe-des-activites-de-traitement.xls >. Acesso em: 04 set. 2020.

ANEXO I

Categorias de Dados Pessoais

As categorias, subcategorias e descrições dos dados pessoais apresentadas na tabela abaixo foram inspiradas no modelo de registro (inventário) proposto pela autoridade de proteção de dados da Bélgica[8].

SUBCATEGORIA	DESCRIÇÃO (Descrever se são tratados dados pessoais sobre:)
CATEGORIA: 7.1 - Dados de Identificação Pessoal	
7.1.1 - Informações de identificação pessoal	Nome, endereço residência, histórico de endereços anteriores, número de telefone fixo residencial, número celular pessoal, e-mail pessoal, etc.
7.1.2 - Informações de identificação atribuídas por instituições governamentais	CPF, RG, número do passaporte, número da carteira de motorista, número da placa, número de registro em conselho profissional, etc.
7.1.3 - Dados de identificação eletrônica	Endereços IP, cookies, momentos de conexão etc.
7.1.4 - Dados de localização eletrônica	Dados de comunicação de torres de celulares (ex: GSM), dados de GPS etc.
CATEGORIA: 7.2 - Dados Financeiros	
7.2.1 - Dados de identificação financeira	Números de identificação, números de contas bancárias, números de cartões de crédito ou débito, códigos secretos.
7.2.2 - Recursos financeiros	Renda, posses, investimentos, renda total, renda profissional, poupança, datas de início e término dos investimentos, receita de investimento, dívidas sobre ativos.
7.2.3 - Dívidas e despesas	Total de despesas, aluguel, empréstimos, hipotecas e outras formas de crédito.
7.2.4 - Situação financeira (Solvência)	Avaliação do rendimento e avaliação de capacidade de pagamento.
7.2.5 - Empréstimos, hipotecas, linhas de crédito	Natureza do empréstimo, valor emprestado, saldo remanescente, data de início, período do empréstimo, taxa de juros, visão geral do pagamento, detalhes sobre as garantias.
7.2.6 - Assistência financeira	Benefícios, assistência, bonificações, subsídios, etc.

[8] < https://www.autoriteprotectiondonnees.be/publications/modele-de-registe-des-activites-de-traitement.xls >. Acesso em 06/07/2020.

SUBCATEGORIA	DESCRIÇÃO (Descrever se são tratados dados pessoais sobre:)
7.2.7 - Detalhes da apólice de seguro	Natureza da apólice de seguro, detalhes sobre os riscos cobertos, valores segurados, período segurado, data de rescisão, pagamentos feitos, recebidos ou perdidos, situação do contrato, etc.
7.2.8 - Detalhes do plano de pensão	Data efetiva do plano de pensão, natureza do plano, data de término do plano, pagamentos recebidos e efetuados, opções, beneficiários, etc.
7.2.9 - Transações financeiras	Valores pagos e a pagar pelo titular dos dados, linhas de crédito concedidas, avais, forma de pagamento, visão geral do pagamento, depósitos e outras garantias, etc.
7.2.10 - Compensação	Detalhes sobre compensações reivindicadas, valores pagos ou outros tipos de compensação, etc.
7.2.11 - Atividades profissionais	Atividades profissionais executadas pelo titular dos dados: natureza da atividade, natureza dos bens ou serviços utilizados ou entregues pela pessoa no registro, relações comerciais, etc.
7.2.12 - Acordos e ajustes	Detalhes sobre acordos ou ajustes comerciais; acordos sobre representação ou acordos legais, etc.
7.2.13 - Autorizações ou consentimentos	Autorizações ou consentimentos realizados pelo titular de dados, etc.
CATEGORIA: 7.3 - Características Pessoais	
7.3.1 - Detalhes pessoais	Idade, sexo, data de nascimento, local de nascimento, estado civil, nacionalidade.
7.3.2 - Detalhes militares	Situação militar, patente militar, distinções militares, etc.
7.3.3 - Situação de Imigração	Detalhes sobre o visto, autorização de trabalho, limitações de residência ou movimentação, condições especiais relacionadas à autorização de residência, etc.
7.3.4 - Descrição Física (informações físicas de uma pessoa com possibilidade de serem visivelmente identificadas.)	Altura, peso, cor do cabelo, cor dos olhos, características distintivas, etc.
CATEGORIA: 7.4 - Hábitos Pessoais	
7.4.1 - Hábitos	Uso de tabaco, uso de álcool, hábito alimentar, dieta alimentar etc.

SUBCATEGORIA	DESCRIÇÃO (Descrever se são tratados dados pessoais sobre:)
7.4.2 - Estilo de vida	Informações sobre o uso de bens ou serviços, comportamento dos titulares dos dados, etc.
7.4.3 - Viagens e deslocamentos	Antigas residências e deslocamentos, visto de viagem, autorizações de trabalho, etc.
7.4.4 - Contatos sociais	Amigos, parceiros de negócios, relacionamentos com pessoas que não sejam familiares próximos; etc.
7.4.5 - Posses	Terra, propriedade ou outros bens.
7.4.6 - Denúncias, incidentes ou acidentes	Informações sobre um acidente, incidente ou denúncia na qual o titular dos dados está envolvido, a natureza dos danos ou ferimentos, pessoas envolvidas, testemunhas, etc.
7.4.7 - Distinções	Distinções civis, administrativas ou militares.
7.4.8 - Uso de mídia	Definição do comportamento de uso de mídias e meios de comunicação.
CATEGORIA: 7.5 - Características Psicológicas	
7.5.1 - Descrição Psicológica	Personalidade ou caráter.
CATEGORIA: 7.6 - Composição Familiar	
7.6.1 - Casamento ou forma atual de coabitação	Nome do cônjuge ou companheiro(a), nome de solteira do cônjuge ou companheira, data do casamento, data do contrato de coabitação, número de filhos, etc.
7.6.2 - Histórico conjugal	Casamentos ou parcerias anteriores, divórcios, separações, nomes de parceiros anteriores.
7.6.3 - Familiares ou membros da família	Detalhes de outros familiares ou membros da família do titular de dados.
CATEGORIA: 7.7 - Interesses de lazer	
7.7.1 - Atividades e interesses de lazer	Hobbies, esportes, outros interesses.
CATEGORIA: 7.8 – Associações	
7.8.1 Associações (exceto profissionais, políticas, em sindicatos ou qualquer outra associação que se enquadre em dados pessoais sensíveis)	Participação em organizações de caridade ou benevolentes, clubes, parcerias, organizações, grupos, etc.
CATEGORIA: 7.9 - Processo Judicial/Administrativo/Criminal	

SUBCATEGORIA	DESCRIÇÃO (Descrever se são tratados dados pessoais sobre:)
7.9.1 - Suspeitas	Suspeitas de violações, conexões conspiratórias com criminosos conhecidos. Inquéritos ou ações judiciais (civis ou criminais) empreendidas por ou contra o titular dos dados, etc.
7.9.2 - Condenações e sentenças	Condenações e sentenças, etc.
7.9.3 - Ações judiciais	Tutela, guarda temporária ou definitiva, interdição, adoção, etc.
7.9.4 - Penalidades Administrativas	Multas, processo disciplinar, advertências, bem como qualquer outro tipo de penalidade ou sanção administrativa prevista em leis, normas e regulamentos.
CATEGORIA: 7.10 - Hábitos de Consumo	
7.10.1 - Dados de bens e serviços	Bens e serviços vendidos, alugados ou emprestados ao titular dos dados.
CATEGORIA: 7.11 - Dados Residenciais	
7.11.1 – Residência	Natureza da residência, propriedade própria ou alugada, duração da residência nesse endereço, aluguel, custos, classificação da residência, detalhes sobre a avaliação, nomes das pessoas que possuem as chaves.
CATEGORIA: 7.12 - Educação e Treinamento	
7.12.1 - Dados acadêmicos/escolares	Diplomas, certificados obtidos, resultados de exames, avaliação do progresso dos estudos, histórico escolar, grau de formação, etc.
7.12.2 Registros financeiros do curso/treinamento	Taxas de inscrição e custos pagos, financiamento, formas de pagamento, registros de pagamento, etc.
7.12.3 - Qualificação e experiência profissional	Certificações profissionais, interesses profissionais, interesses acadêmicos, interesses de pesquisam experiência de ensino, etc.
CATEGORIA: 7.13 - Educação e Treinamento	
7.13.1 - Emprego atual	Empregador, descrição do cargo e função, antiguidade, data de recrutamento, local de trabalho, especialização ou tipo de empresa, modos e condições de trabalho, cargos anteriores e experiência anterior de trabalho no mesmo empregador, etc.

SUBCATEGORIA	DESCRIÇÃO (Descrever se são tratados dados pessoais sobre:)
7.13.2 – Recrutamento	Data de recrutamento, método de recrutamento, fonte de recrutamento, referências, detalhes relacionados com o período de estágio, etc.
7.13.3 - Rescisão de trabalho	Data de rescisão, motivo, período de notificação, condições de rescisão, etc.
7.13.4 – Carreira	Emprego anterior e empregadores, períodos sem emprego, serviço militar, etc.
7.13.5 - Absentismo e disciplina	Registos de absentismo, motivos de ausência, medidas disciplinares, etc.
7.13.6 - Avaliação de Desempenho	Avaliação de desempenho ou qualquer outro tipo de análise de qualificação ou habilidades profissionais, etc.
CATEGORIA: 7.14 -Registros/gravações de vídeo, imagem e voz	
7.14.1 - Vídeo e imagem	Arquivos de vídeos, fotos digitais, fitas de vídeo, etc.
7.14.2 - Imagem de Vigilância	Imagens e/ou vídeos de câmeras de segurança/vigilância (ex: CFTV), etc.
7.14.3 – Voz	Fitas e arquivos digitais de voz, bem como outros registros de gravações de voz, etc.
CATEGORIA: 7.15 -Outros (Especificar)	
7.15.1 - Outros (Especificar)	**Obs.:** Conforme explicado na seção 2.7, a lista não é exaustiva. Assim, pode incluir quantas outras categorias e subcategorias que forem necessárias.

ANEXO II

Mudanças da Versão 2.0

Este anexo tem a finalidade de fornecer os destaques das mudanças inseridas nesta versão do Guia de Elaboração Inventário de Dados Pessoais.

Primeiramente, ressalta-se que as mudanças inseridas nesta versão em comparação com a anterior visam a adequação com o Guia do Framework de Privacidade e Segurança da Informação v1 elaborado e publicado pela SGD em novembro de 2022.

Foram realizadas inclusões de: seção sobre aviso preliminar e agradecimentos; e referência de que controle e medidas do Framework de Privacidade e Segurança da Informação são atendidos pelo Guia de Elaboração do IDP.

Cumpre destacar os 32 Controles de Privacidade e Segurança da Informação trazidos pelo Guia do Framework que foram inseridos na ferramenta em formato de planilha eletrônica, disponível no link < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/template_inventario_dados_pessoais.xlsx>.

A listagem geral dos controles é apresentada na guia "4-Listas" da ferramenta constante da planilha eletrônica disponível em < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/template_inventario_dados_pessoais.xlsx>.

Os 32 novos Controles de Privacidade e Segurança da Informação substituem as antigas 23 Medidas de Segurança trazidas na versão anterior que eram baseadas no Guia de Avaliação de Riscos de Segurança e Privacidade v1 (p. 10 e 11) publicado pela SGD em novembro de 2020.

A Tabela a seguir apresenta os 32 novos controles e as 23 antigas medidas.

Controles de Privacidade e Segurança da Informação (Guia do Framework de Privacidade e Segurança da Informação)	**Medidas de Segurança** (Guia de Avaliação de Riscos de Segurança e Privacidade)
ESTRUTURAÇÃO BÁSICA DE GESTÃO EM PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO	
Controle 0: Estruturação básica de gestão em privacidade e segurança da informação	
CIBERSEGURANÇA / SEGURANÇA	
Controle 1: Inventário e Controle de Ativos Institucionais	Continuidade de Negócio
Controle 2: Inventário e Controle de Ativos de Software	Controles Criptográficos
Controle 3: Proteção de Dados	Controles de Acesso Lógico
Controle 4: Configuração Segura de Ativos Institucionais e Software	Controles de Segurança em Redes, Proteção Física e do Ambiente

Controles de Privacidade e Segurança da Informação (Guia do Framework de Privacidade e Segurança da Informação)	**Medidas de Segurança** (Guia de Avaliação de Riscos de Segurança e Privacidade)
Controle 5: Gestão de Contas	Cópia de Segurança
Controle 6: Gestão do Controle de Acesso	Desenvolvimento Seguro
Controle 7: Gestão Contínua de Vulnerabilidades	Gestão de Capacidade e Redundância
Controle 8: Gestão de Registros de Auditoria	Gestão de Mudanças
Controle 9: Proteções de E-mail e Navegador Web	Gestão de Riscos
Controle 10: Defesas Contra *Malware*	Registro de Eventos, Rastreabilidade e Salvaguarda de Logs
Controle 11: Recuperação de Dados	Segurança Web
Controle 12: Gestão da Infraestrutura de Rede	Resposta a Incidente
Controle 13: Monitoramento e Defesa da Rede	
Controle 14: Conscientização e Treinamento de Competências sobre Segurança	
Controle 15: Gestão de Provedor de Serviços	
Controle 16: Segurança de Aplicações	
Controle 17: Gestão de Resposta a Incidentes	
Controle 18: Testes de Invasão	
PRIVACIDADE	
Controle 19: Inventário e Mapeamento	Abertura, Transparência e Notificação
Controle 20: Finalidade e Hipóteses Legais	*Compliance* com a Privacidade
Controle 21: Governança	Consentimento e Escolha
Controle 22: Políticas, Processos e Procedimentos	Controle de Acesso e Privacidade
Controle 23: Conscientização e Treinamento	Legitimidade e Especificação de Propósito
Controle 24: Minimização de Dados	Limitação de Coleta
Controle 25: Gestão do Tratamento	Minimização de Dados
Controle 26: Acesso e Qualidade	Participação Individual e Acesso
Controle 27: Compartilhamento, Transferência e Divulgação	Precisão e qualidade
Controle 28: Supervisão em Terceiros	Responsabilização
Controle 29: Abertura, Transparência e Notificação	Uso, Retenção e Limitação de Divulgação
Controle 30: Avaliação de Impacto, Monitoramento e Auditoria	
Controle 31: Segurança Aplicada à Privacidade	