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

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

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.

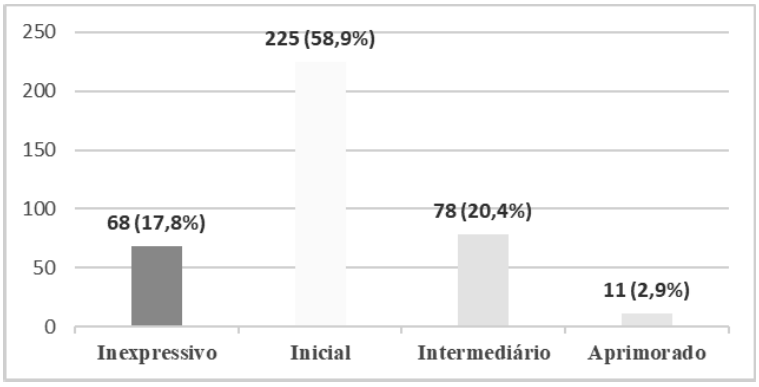
7. A Lei 13.709/2018, inspirada no Regulamento Geral de Proteção de Dados (do inglês *General Data Protection Regulation* – GDPR) da União Europeia (EU), define diretrizes sobre o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica, com o intuito de proteger os direitos fundamentais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

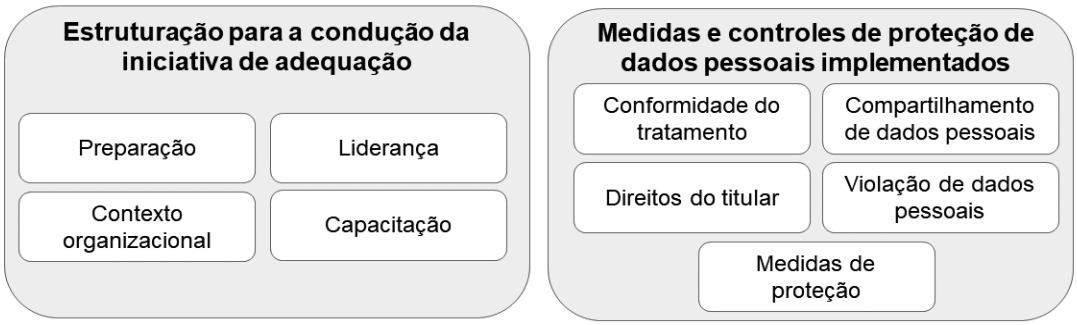


11. A relevância do tema é notória, conforme detalha o relatório precedente. Mesmo após a aprovação da LGPD, o Brasil tem sido vítima de graves ataques que resultaram no vazamento de dados pessoais. Pode-se destacar a divulgação pela imprensa do vazamento de dados de mais de 200 milhões de brasileiros 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.

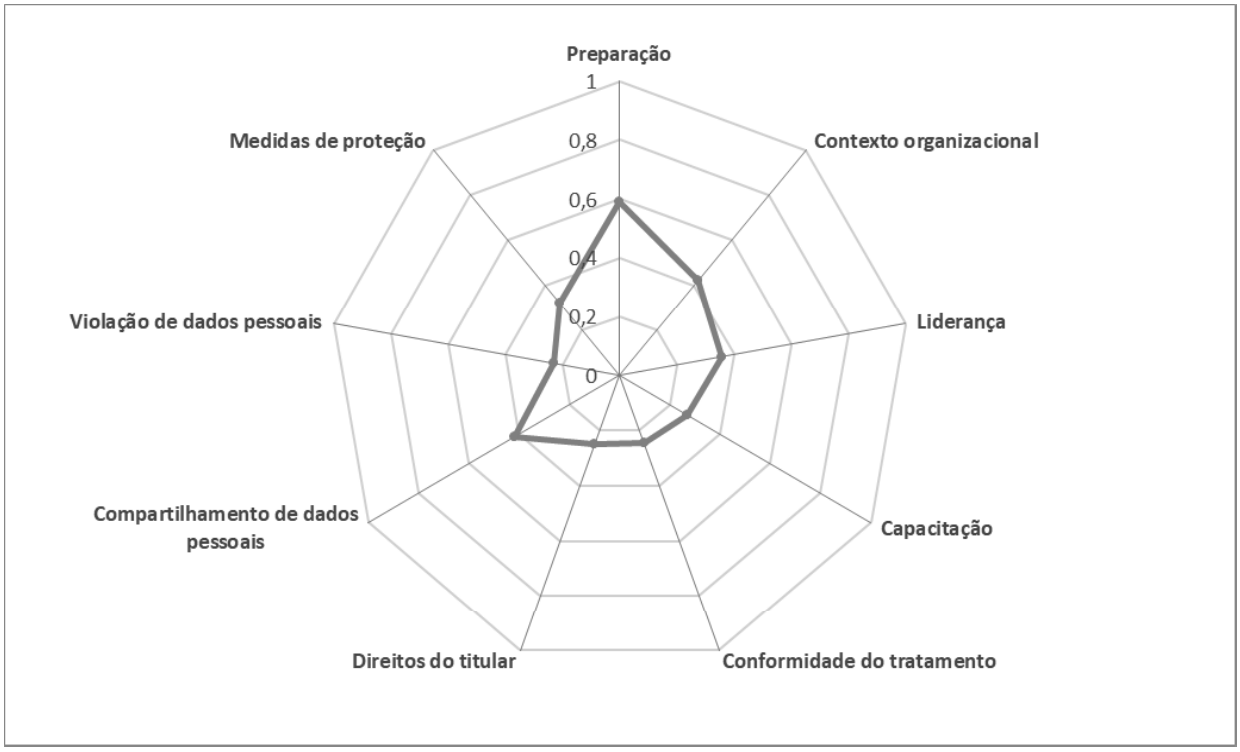
46. A partir do cálculo desse indicador, foram definidos quatro níveis de adequação à LGPD: "Inexpressivo" (indicador menor ou igual a 0,15), "Inicial (indicador maior do que 0,15 e menor ou igual a 0,5), "Intermediário" (indicador maior do que 0,5 e menor ou igual a 0,8) e "Aprimorado" (indicador maior 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 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.

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

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.*

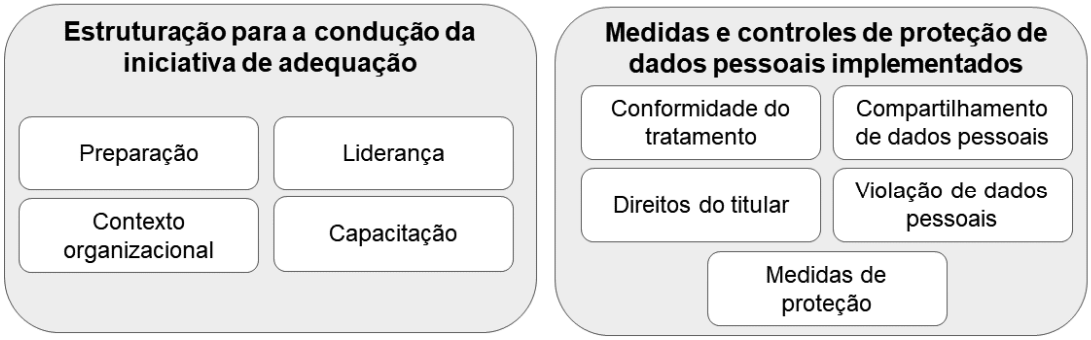
20. *As perguntas do questionário tiveram como referência a própria LGPD e a norma técnica ABNT NBR ISO/IEC 27701:2019 (extensão da ABNT NBR ISO/IEC 27.001 e da ABNT NBR ISO/IEC 27.002 para gestão da privacidade da informação – Requisitos e diretrizes). Também foram consultadas boas práticas oriundas 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.*

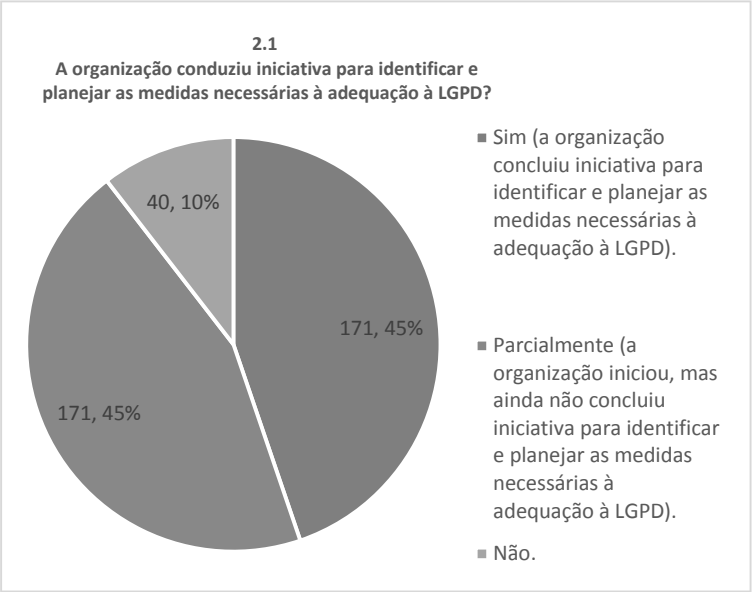
37. *Em consonância com o disposto no art. 50, § 2º, inciso I, da LGPD, o controlador poderá implementar programa de governança em privacidade que seja, entre outros aspectos, adaptado à estrutura, à escala e ao volume das operações, bem como à sensibilidade dos dados pessoais tratados.*

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.*

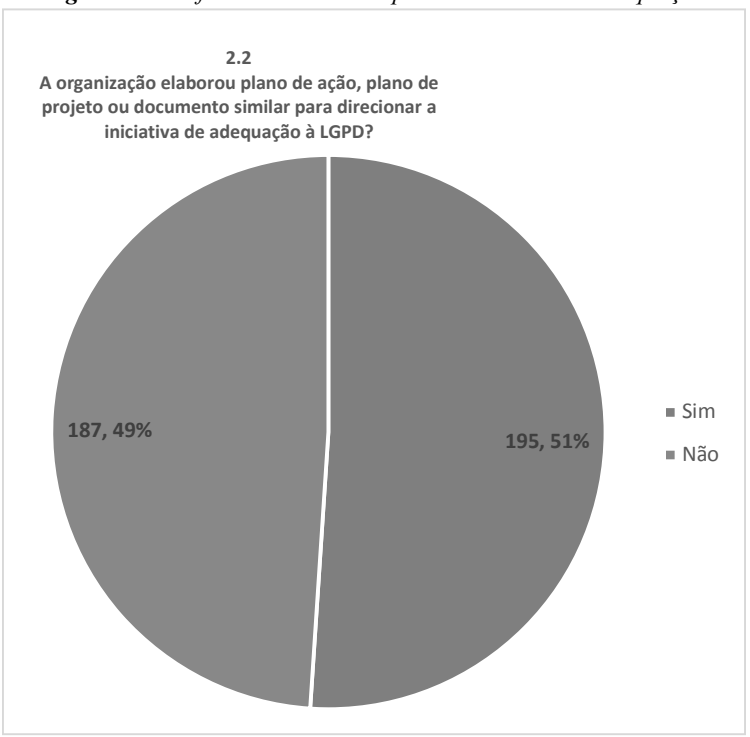
2.1.1.2 Plano de ação

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

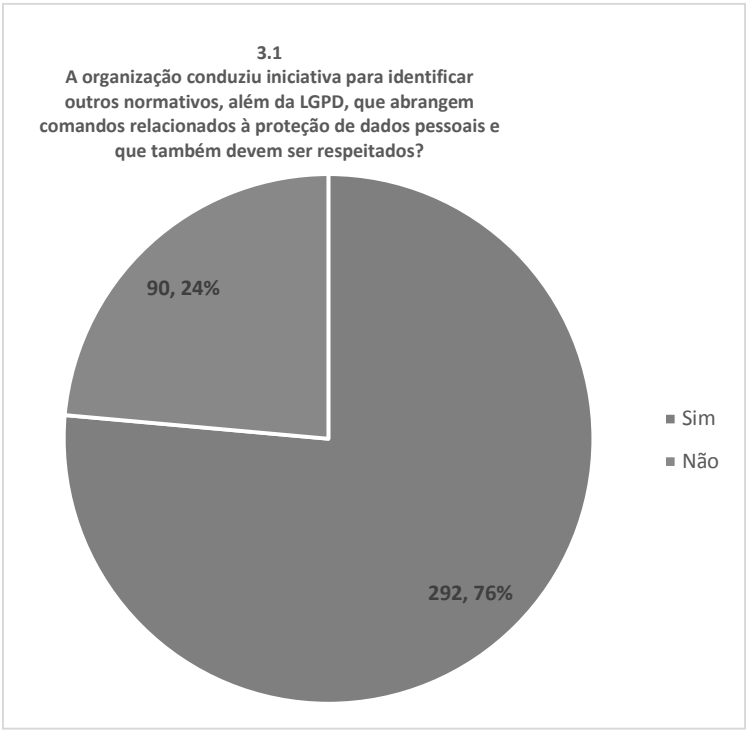
49. *A questão 3.1 do questionário buscou avaliar se as organizações conduziram iniciativa para identificar outros normativos, além da LGPD, que abrangem o tratamento de dados pessoais e que também devem ser respeitados.*

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.*

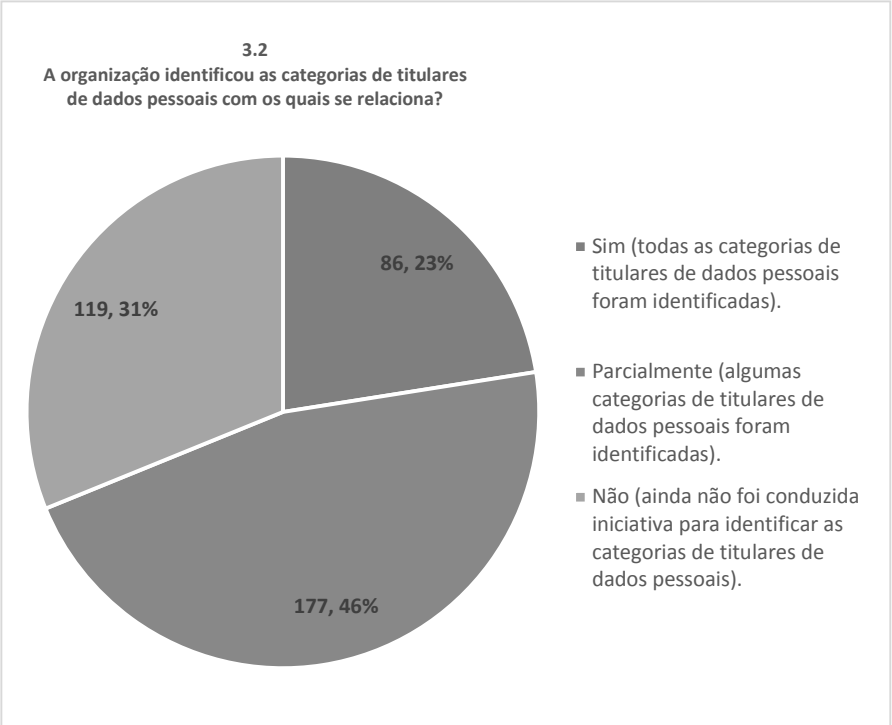
2.1.2.2 <u>Categorias de titulares de dados pessoais</u>

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.*

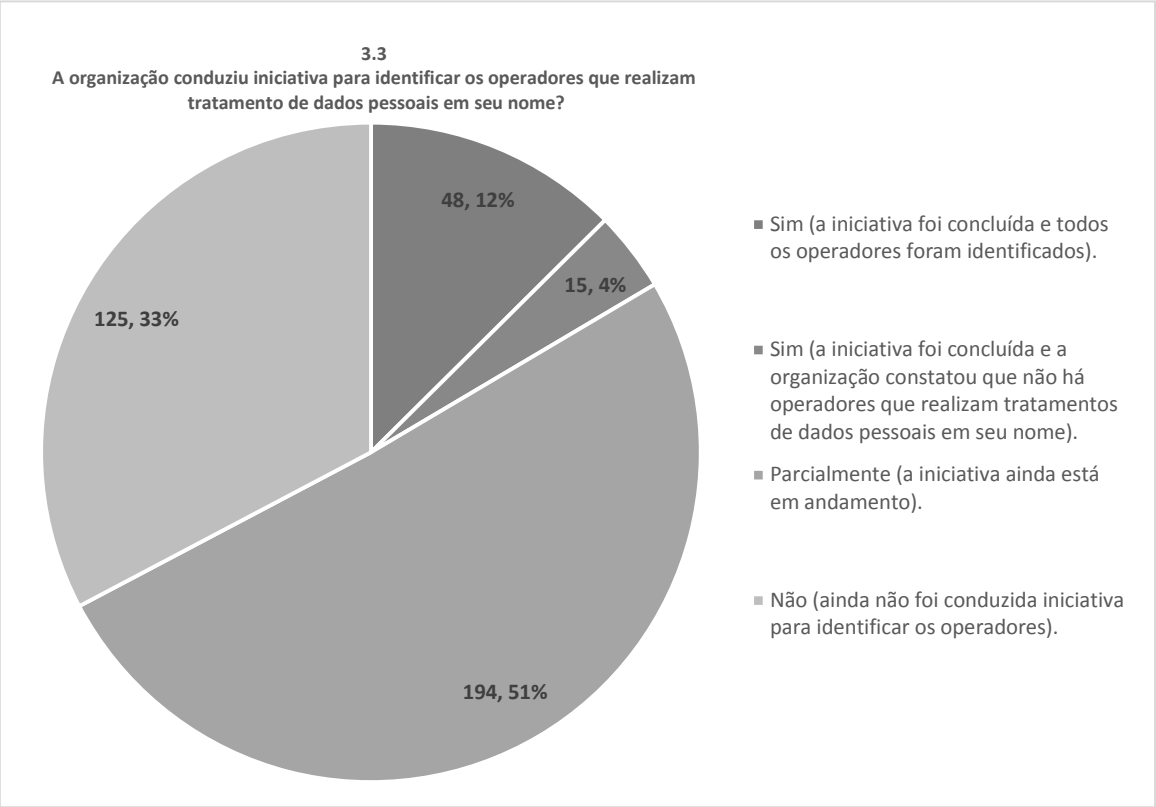
2.1.2.3 <u>Operadores</u>

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*



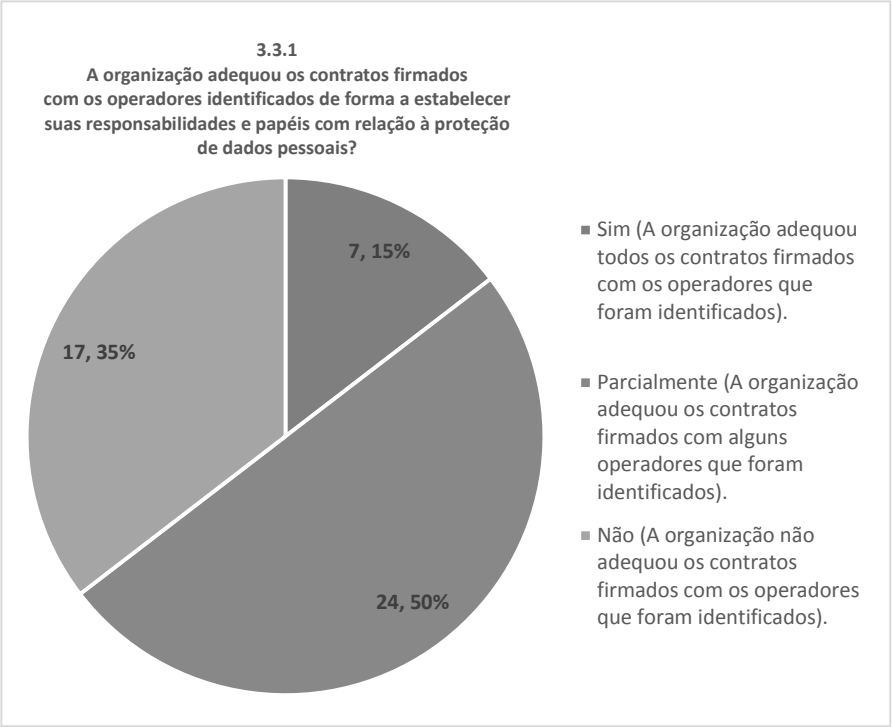
62. *O cenário é preocupante, pois a identificação dos operadores é um ponto chave para a efetividade da proteção dos dados pessoais, uma vez que realizam tratamento de dados em nome das organizações. Além disso, cumpre frisar que o operador responde solidariamente pelos danos causados pelo tratamento 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.*

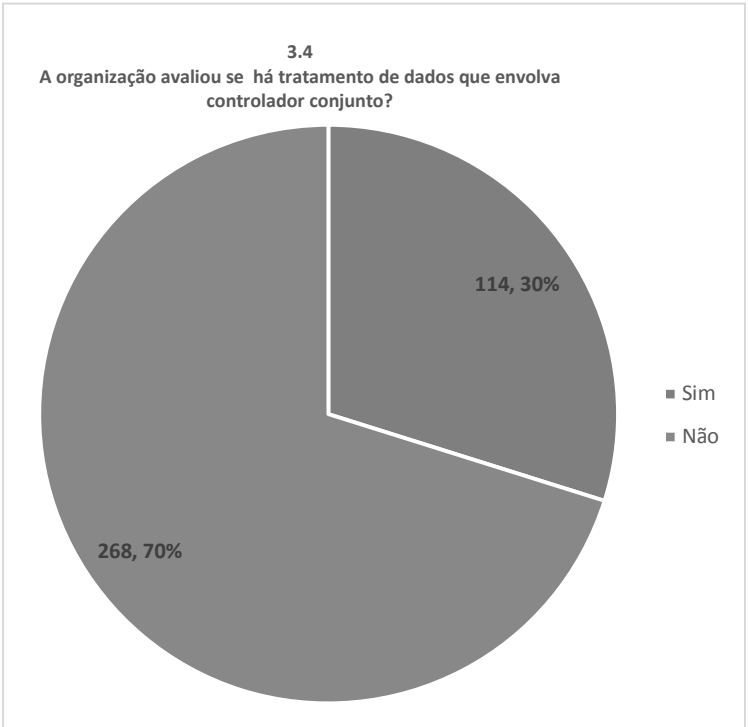
74. *Conforme explorado no tópico anterior, o controlador é a pessoa natural ou jurídica, de direito público ou privado a quem competem as decisões referentes ao tratamento de dados pessoais (LGPD, art. 5º, inciso VI). Por sua vez, de acordo com o item 3.1 da ABNT NBR ISO/IEC 27701:2019, o controlador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

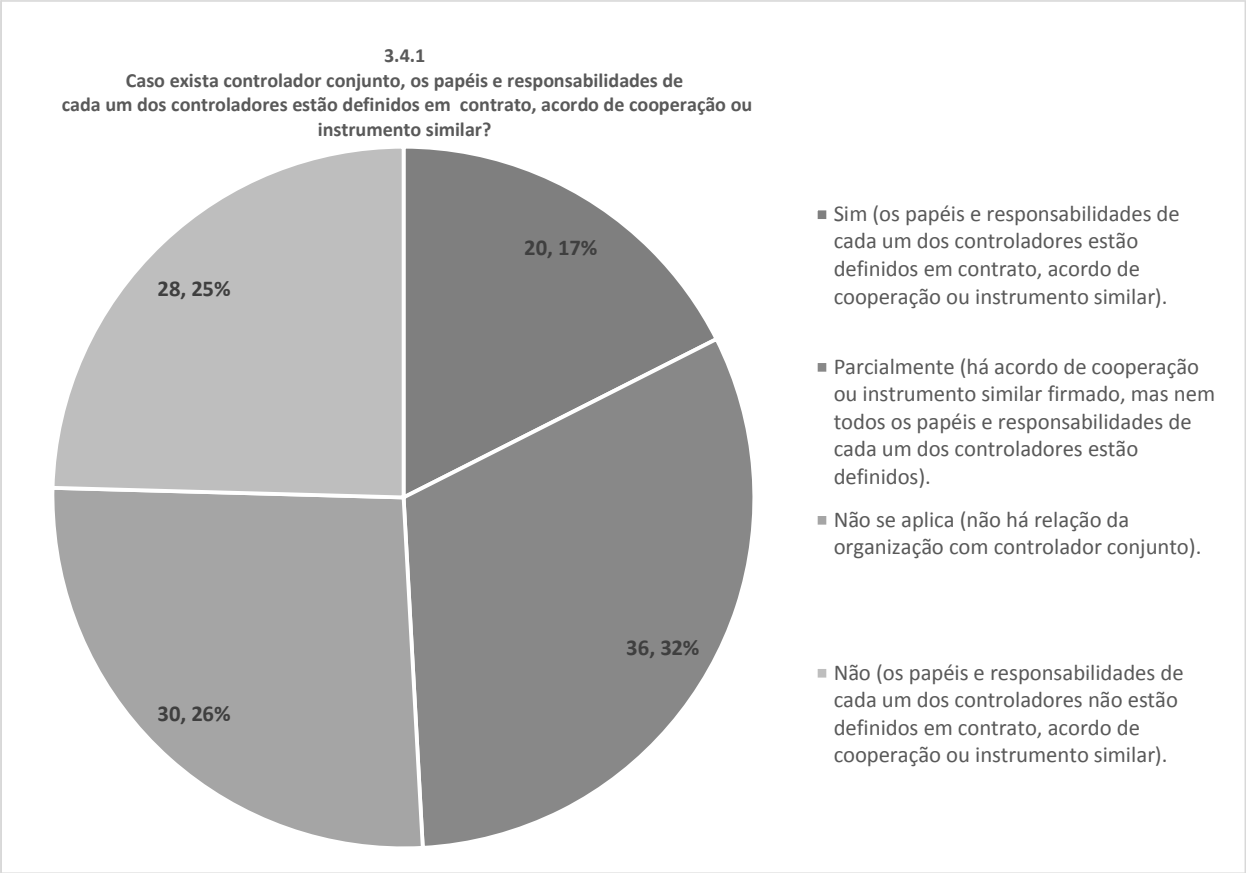


78. *Para melhor avaliar este quesito, caso a organização informasse que avaliou se havia a ocorrência de tratamento de dados pessoais com o envolvimento de controlador conjunto, era exibida*

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.*

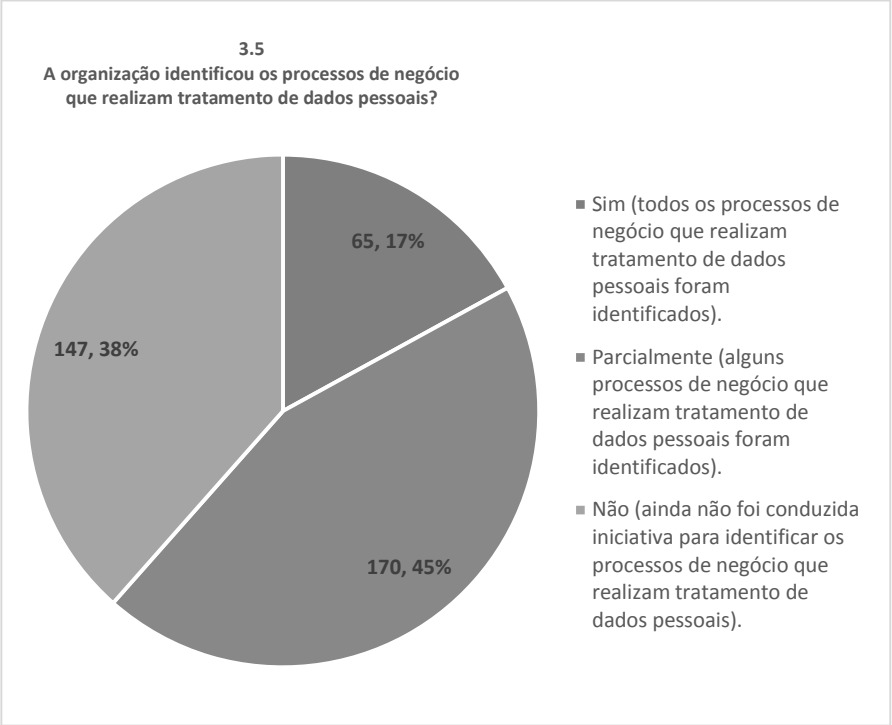
2.1.2.5 Processos que realizam tratamento de dados pessoais

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*



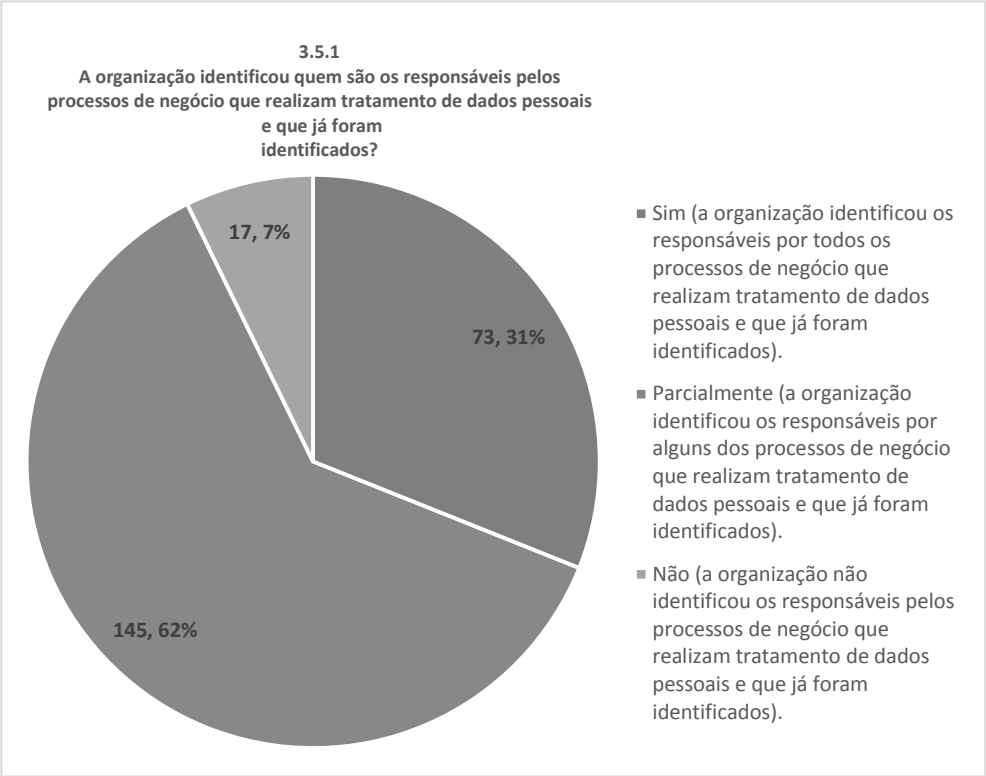
86. *A identificação dos processos que realizam tratamento de dados pessoais é uma das tarefas elementares em um projeto de adequação, pois é a partir dessa identificação que é possível avaliar os riscos inerentes a cada processo e identificar informações relevantes como: o propósito do tratamento, a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

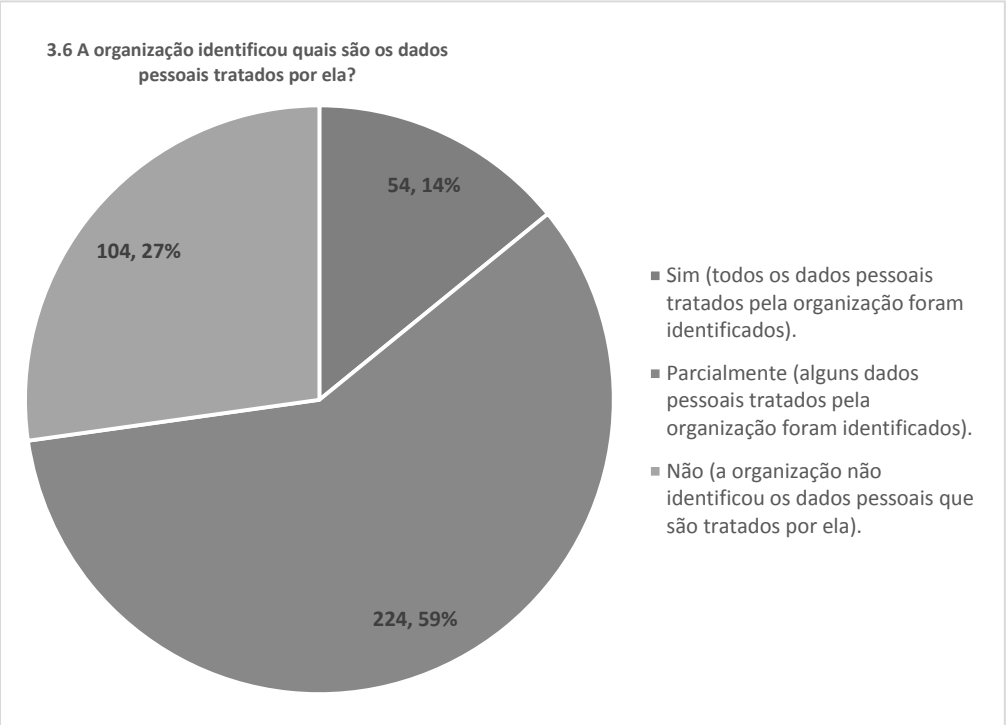
2.1.2.6 <u>Dados pessoais tratados</u>

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*

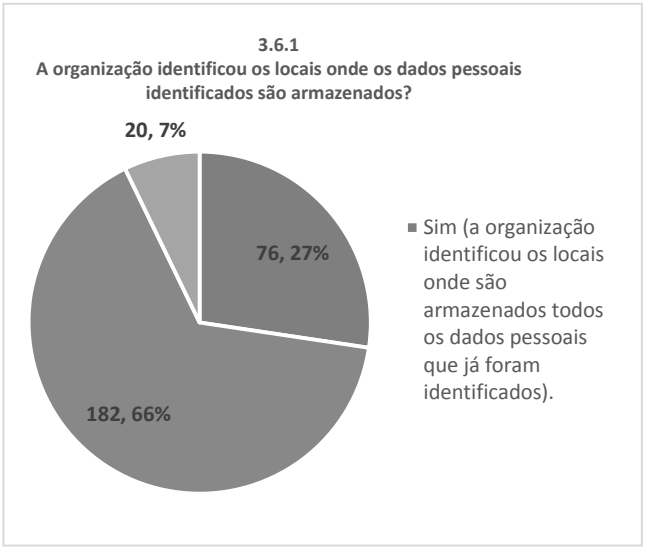


95. *Não basta saber quais dados pessoais são tratados pela organização, é necessário saber onde se encontram. Os dados pessoais podem ser armazenados em diferentes dispositivos, como: ativos de TI (e.g.: servidores de banco de dados, nuvem, dispositivo USB, storage e fita de backup) e arquivos físico (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.*

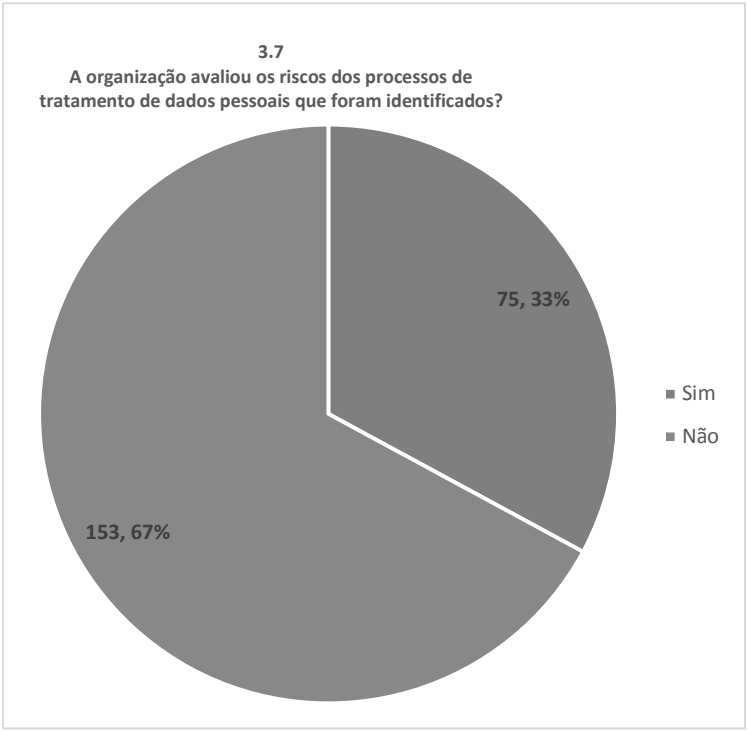
2.1.2.7 Riscos dos processos de tratamento de dados pessoais

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.*

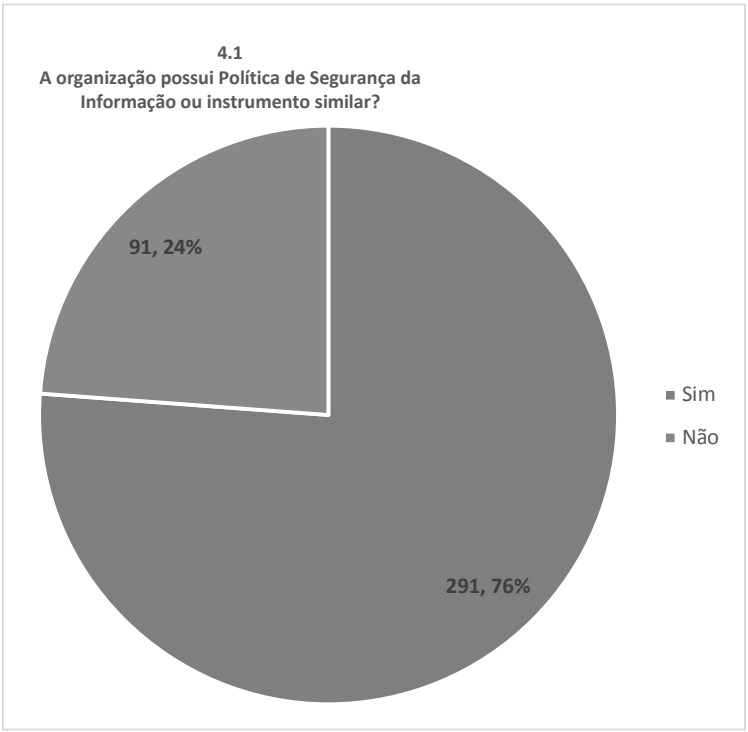
2.1.3.1 Política de Segurança da Informação

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.*

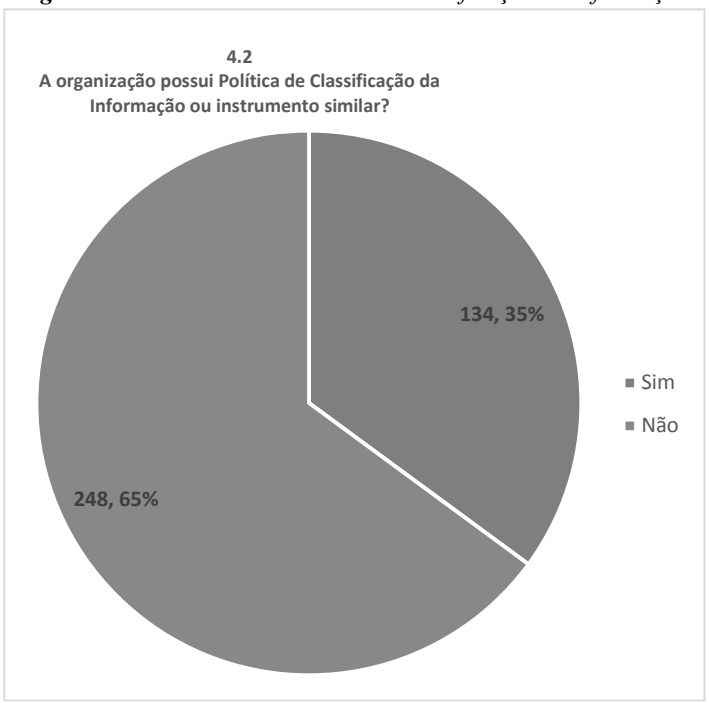
2.1.3.2 <u>Política de Classificação da Informação</u>

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*

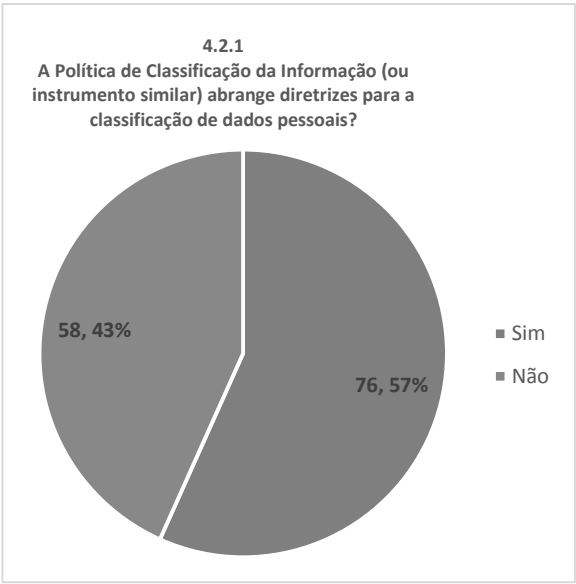


119. *Semelhante ao citado no capítulo anterior, a Política de Classificação da Informação é mencionada desde a primeira versão da norma ABNT ISO/IEC 27002 e deveria ser contemplada em mais organizações.*

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*



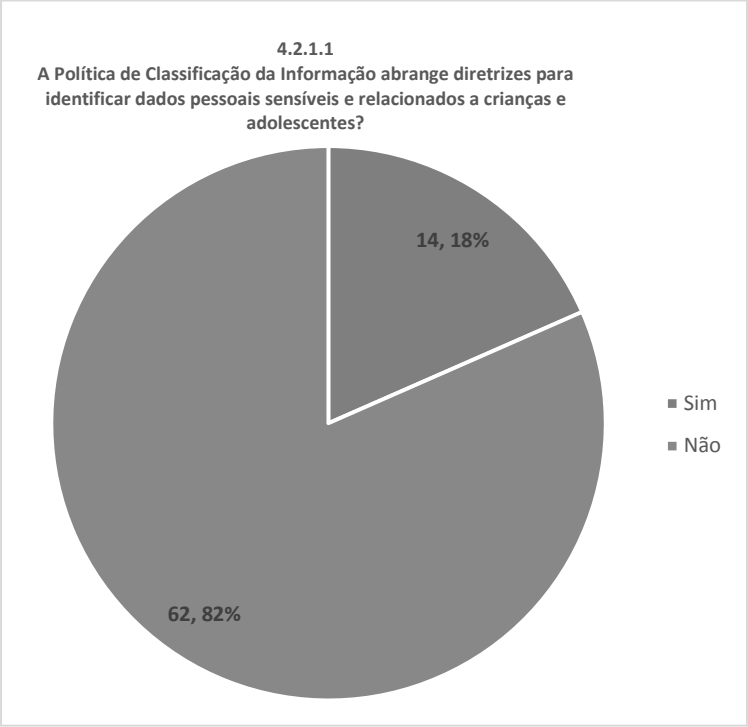
122. *As organizações que ainda não atualizaram a política para contemplar a classificação de dados pessoais devem providenciar tal alteração.*

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

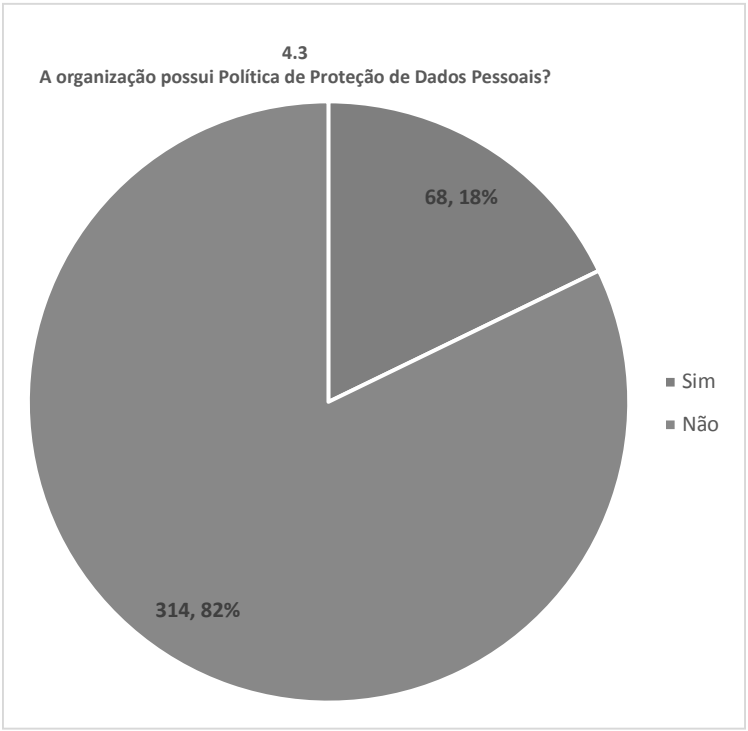
129. *A questão 4.3 do questionário buscou avaliar se as organizações possuíam Política de Proteção de Dados Pessoais ou instrumento similar.*

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*

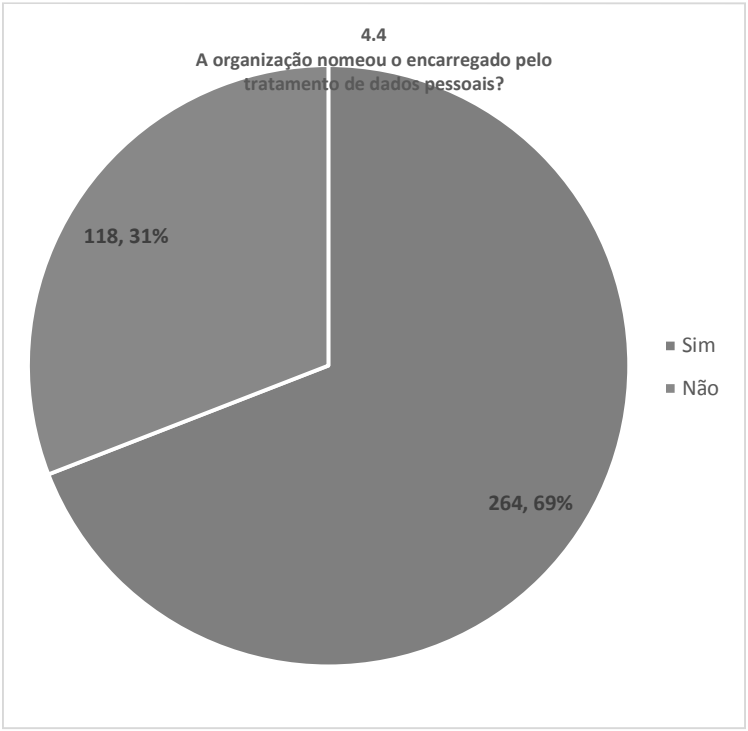
uma pessoa responsável pelo cargo, diferentemente do papel do controlador, que deve ser a própria organização.

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*

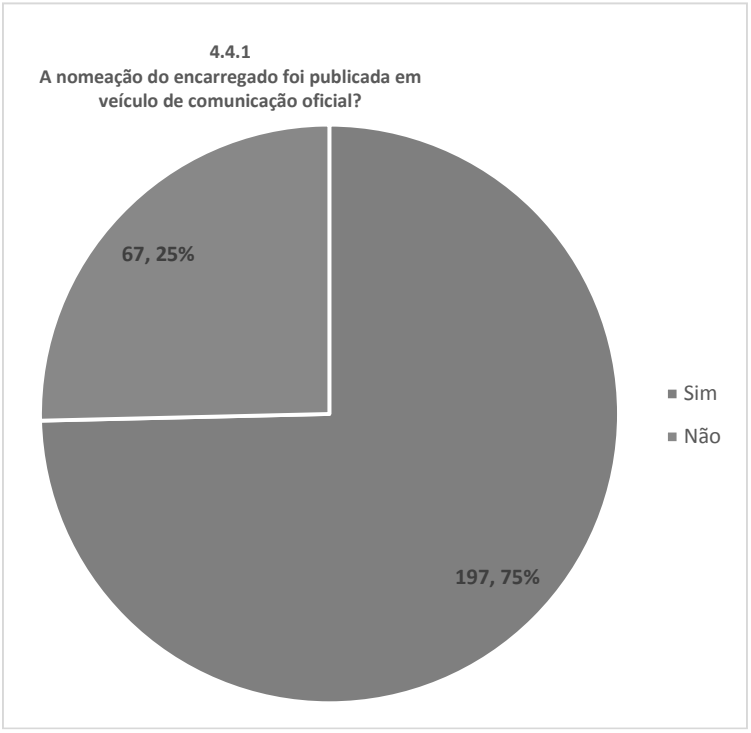
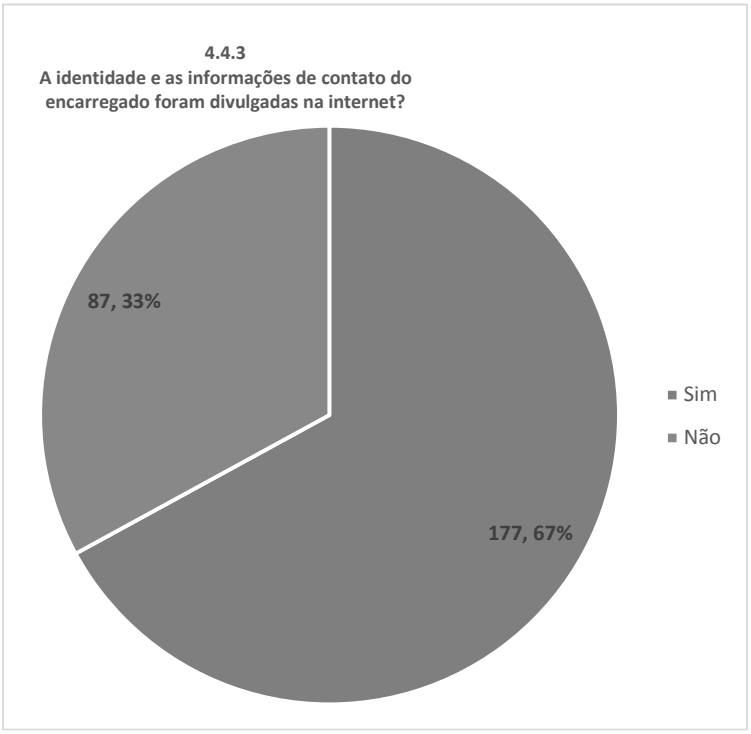


Figura 22 *- Divulgação de informações do encarregado na internet*

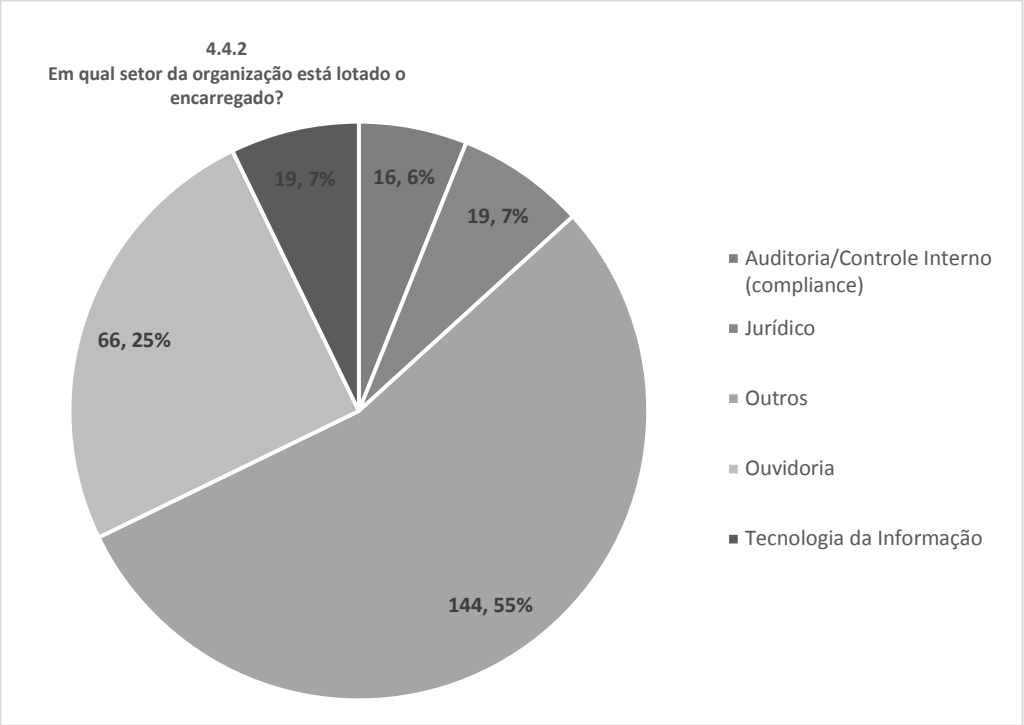


141. *Por fim, caso a organização informasse que designou o encarregado, também foi exibida a subquestão 4.4.2 para verificar em qual setor estaria lotada a pessoa designada. Esse questionamento foi realizado porque, conforme descrito no item 6.3.1.1 da ABNT NBR ISO/IEC 27701:2019, o encarregado deve 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

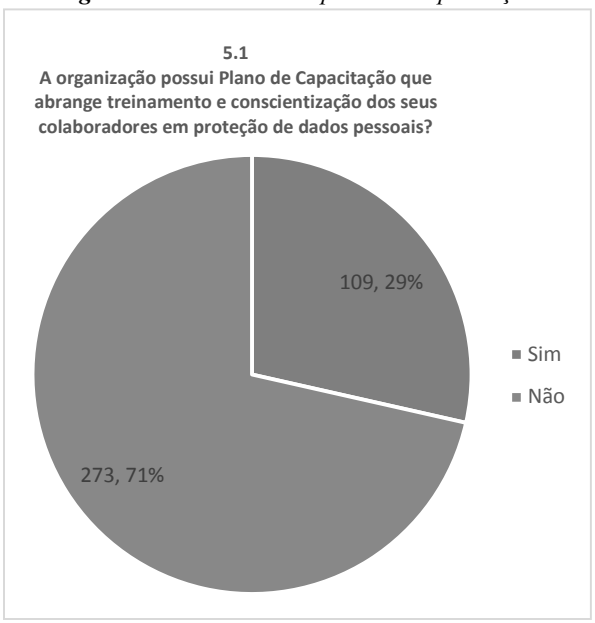
154. *A questão 5.1 do questionário buscou verificar se as organizações elaboraram Plano de Capacitação para direcionar o treinamento e a conscientização dos colaboradores em proteção de dados pessoais.*

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.*

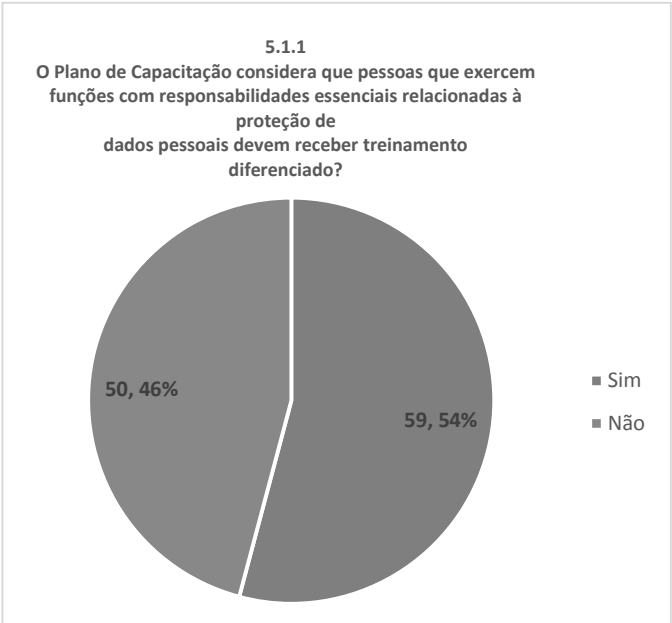
Figura 24 *- Existência de plano de capacitação*



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*



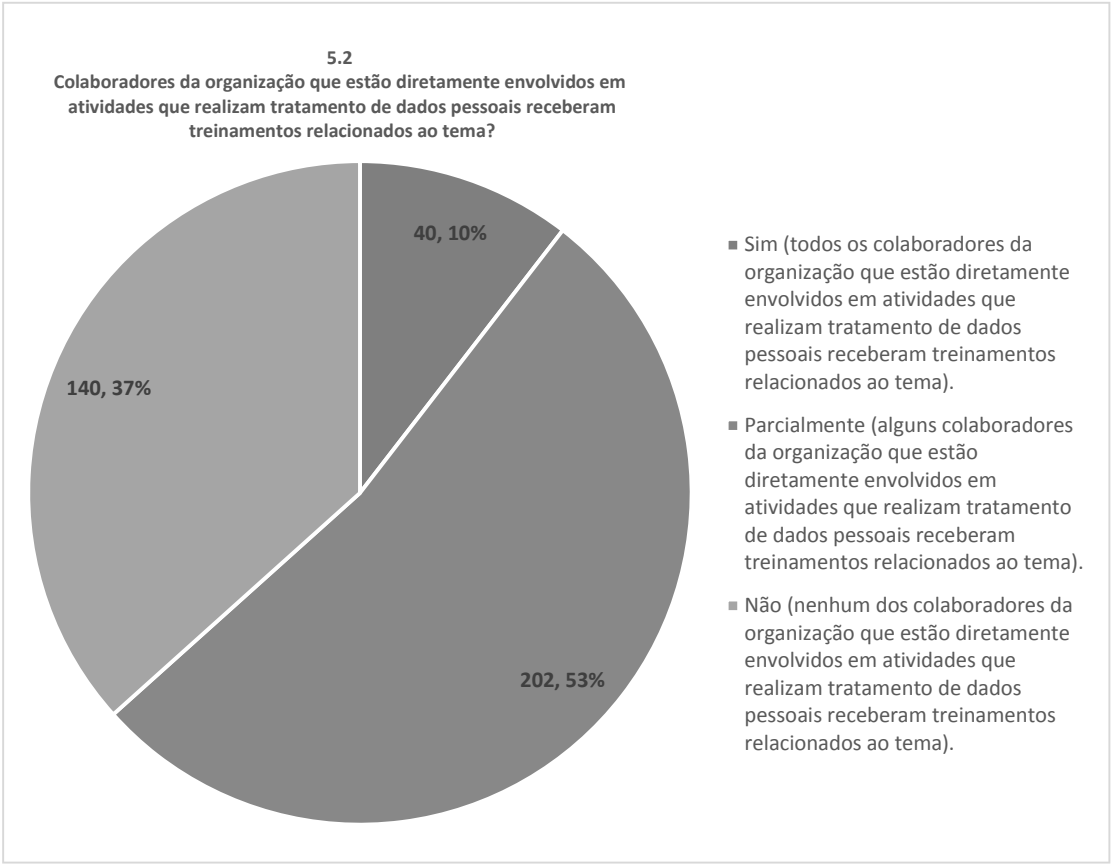
160. *O resultado demonstra a necessidade de as organizações planejarem, com cuidado, o treinamento e a conscientização dos seus colaboradores.*

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

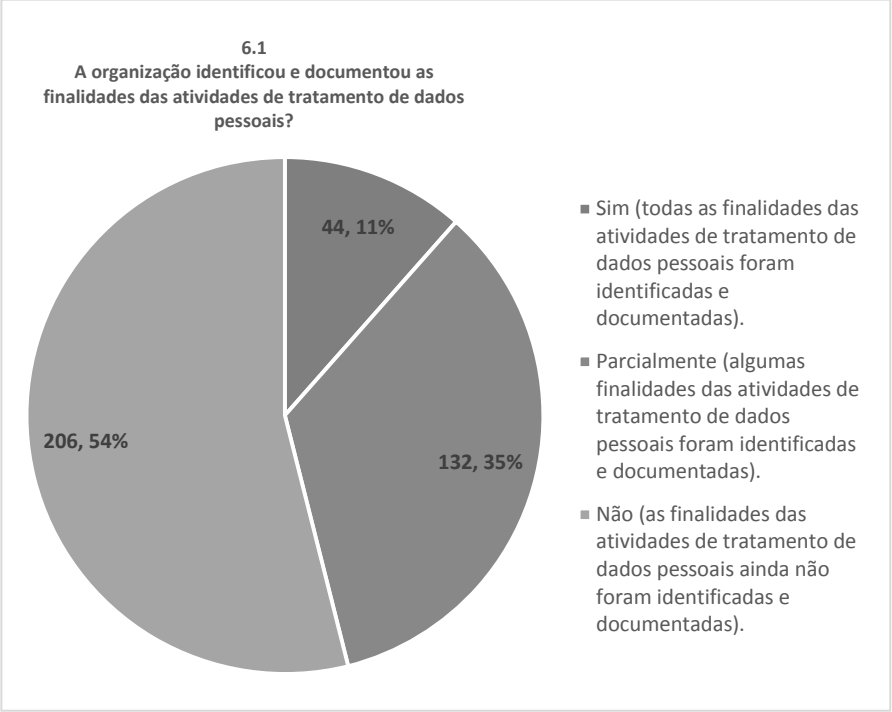
167. *A questão 6.1 do questionário buscou verificar se as organizações identificaram e documentaram as finalidades das atividades de tratamento de dados pessoais.*

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*

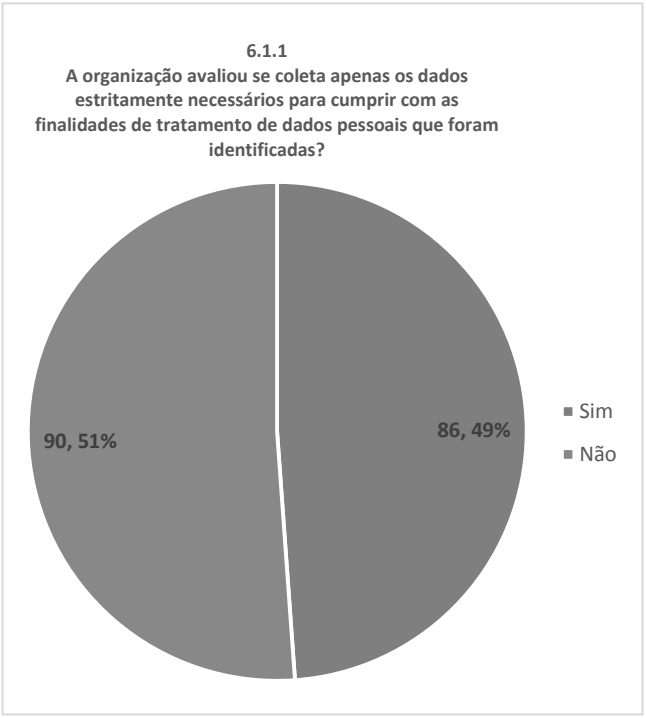
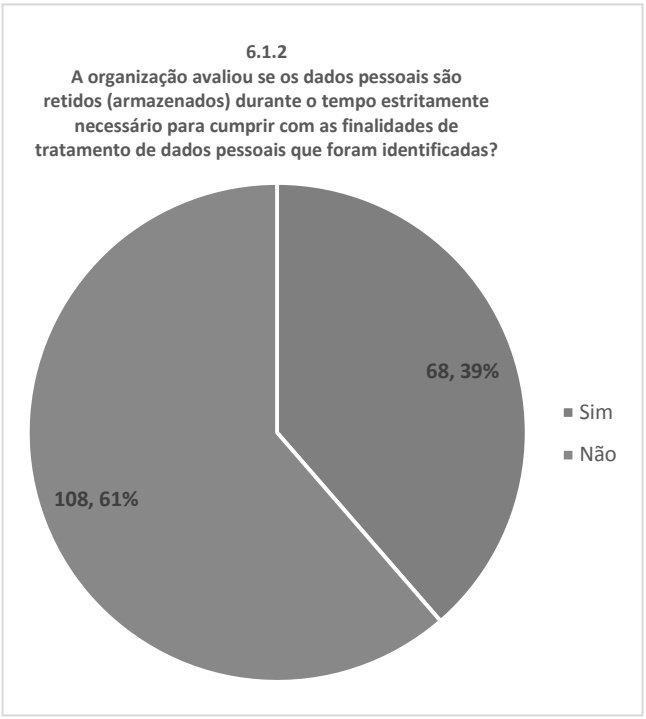


Figura 29 *- Avaliação quanto ao tempo em que os dados pessoais são retidos*



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

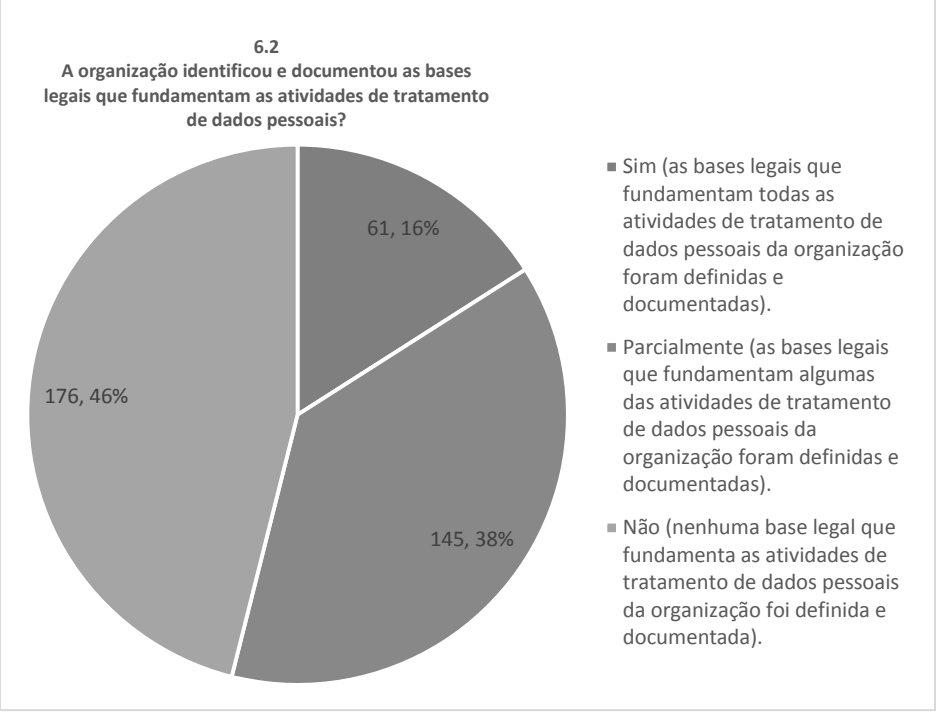
176. *A questão 6.2 do questionário buscou avaliar se as organizações identificaram e documentaram as bases legais que fundamentam as atividades de tratamento de dados pessoais.*

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.*

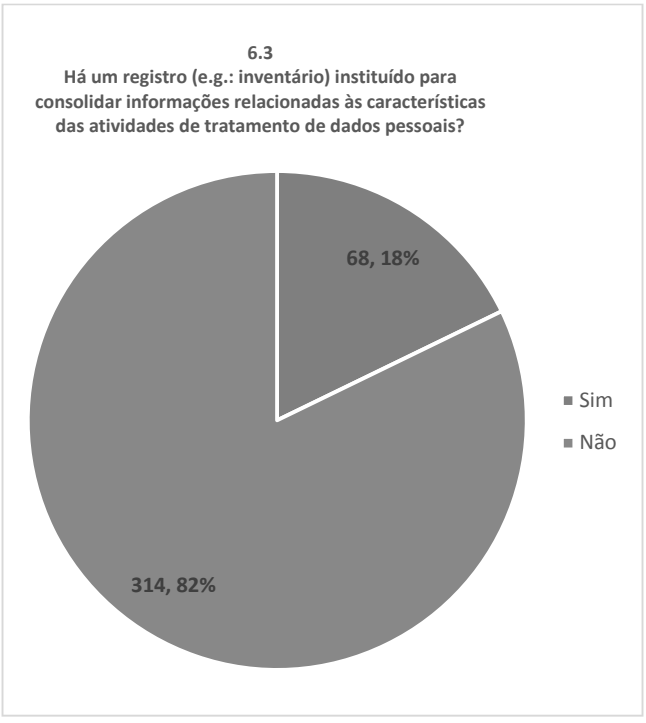
2.1.5.3 Registro das operações de tratamento de dados pessoais

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

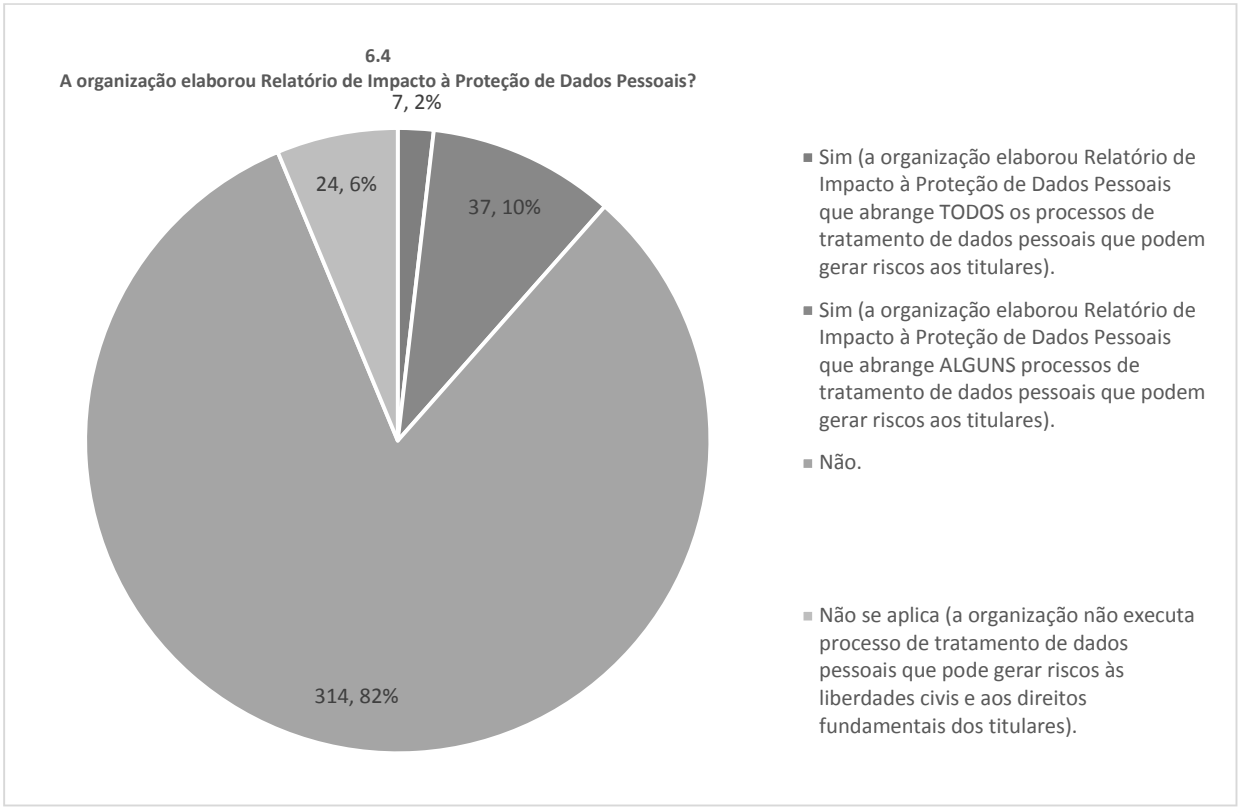
188. *A questão 6.4 do questionário buscou verificar se as organizações elaboraram relatório de impacto à proteção de dados pessoais (RIPD).*

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.*

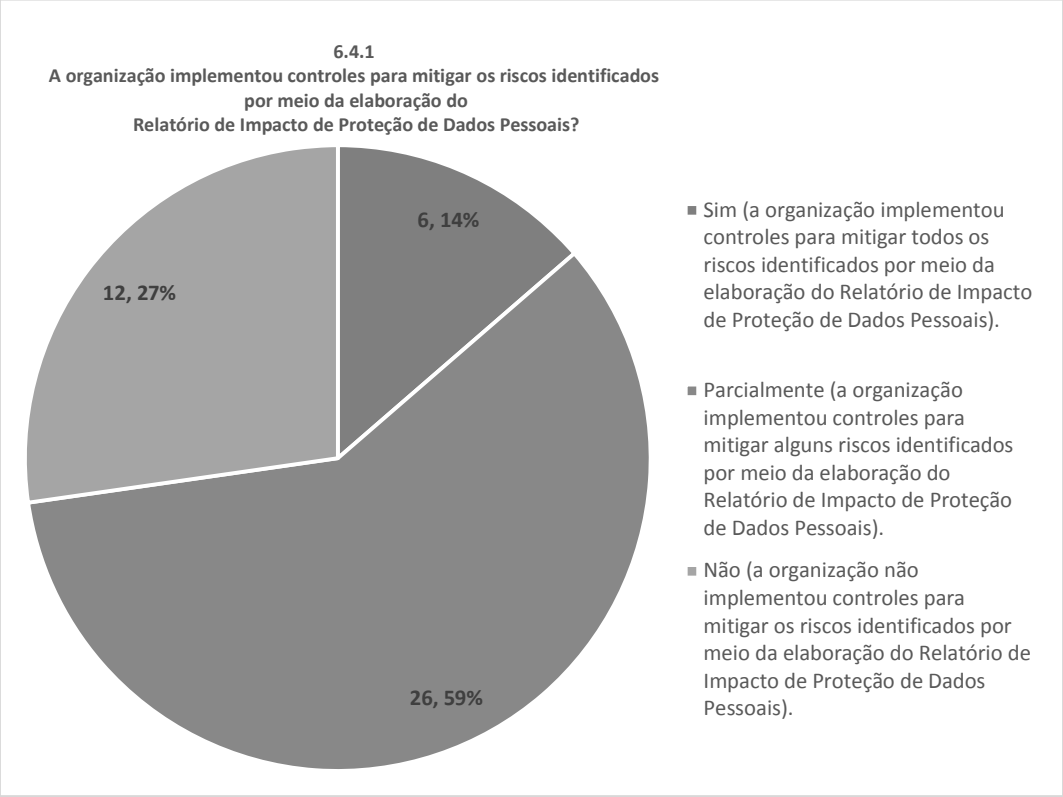
Figura 32 *- Relatório de impacto à proteção de dados pessoais*



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.*

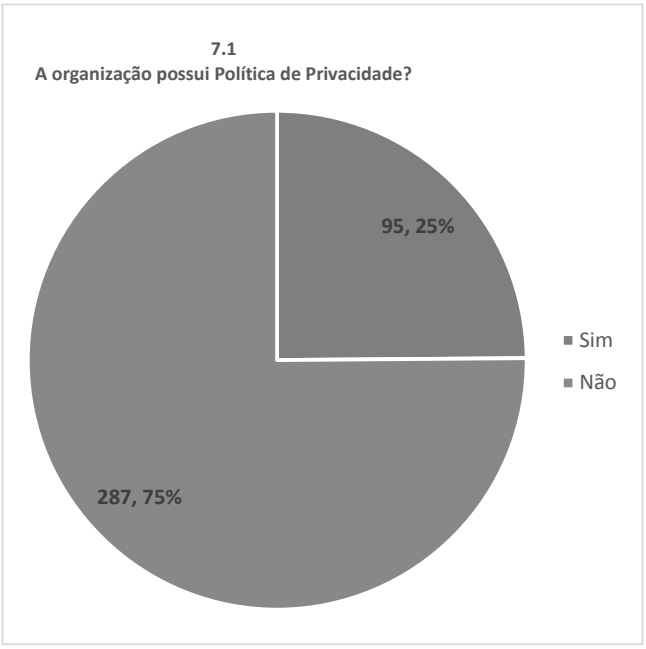
200. *O art. 6º da LGPD enumera, além da boa-fé, dez princípios que as atividades de tratamento de dados pessoais devem observar. Dentre os quais se destacam: o livre acesso, que representa a garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como 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.*

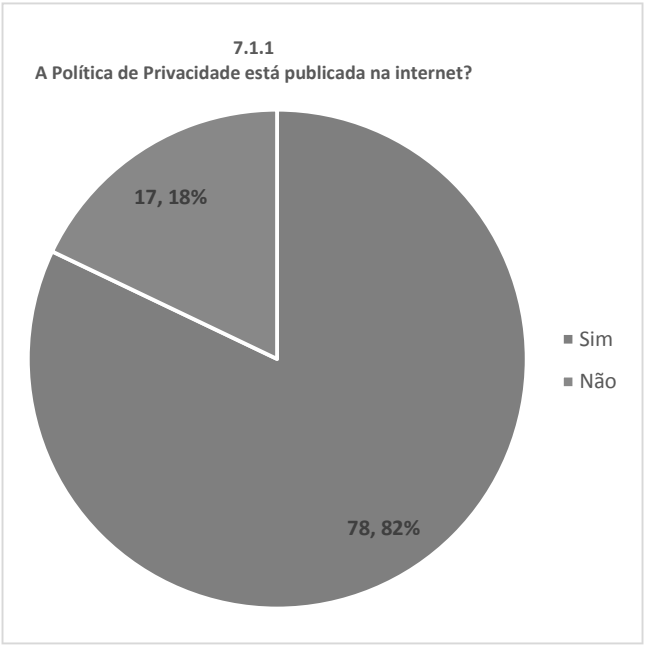
***Figura 34** - Política de privacidade*



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>

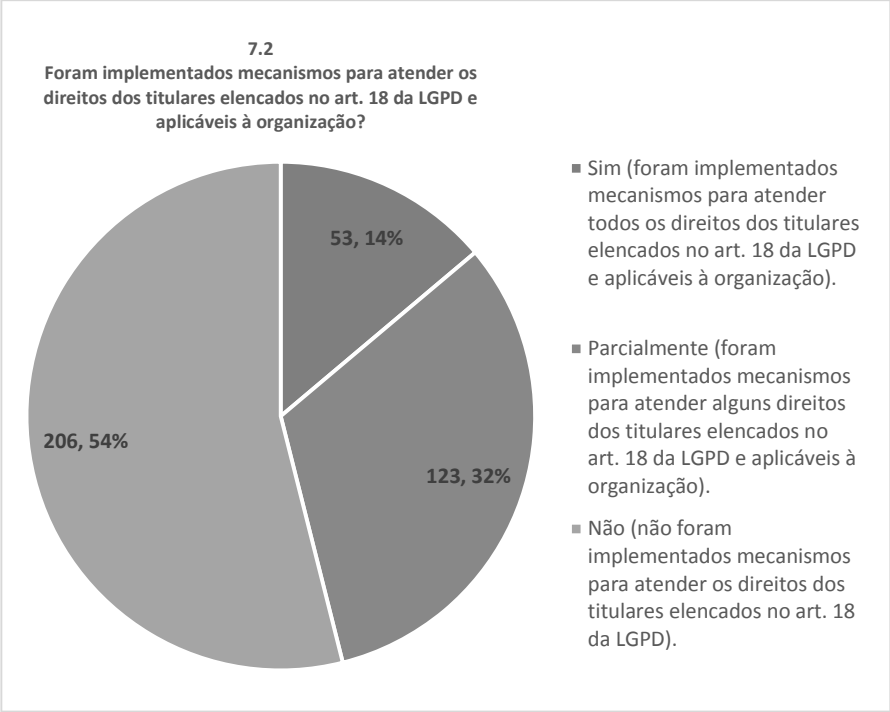
208. *A questão 7.2 buscou verificar se as organizações implementaram mecanismos para atender os direitos dos titulares elencados no art. 18 da LGPD.*

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.*

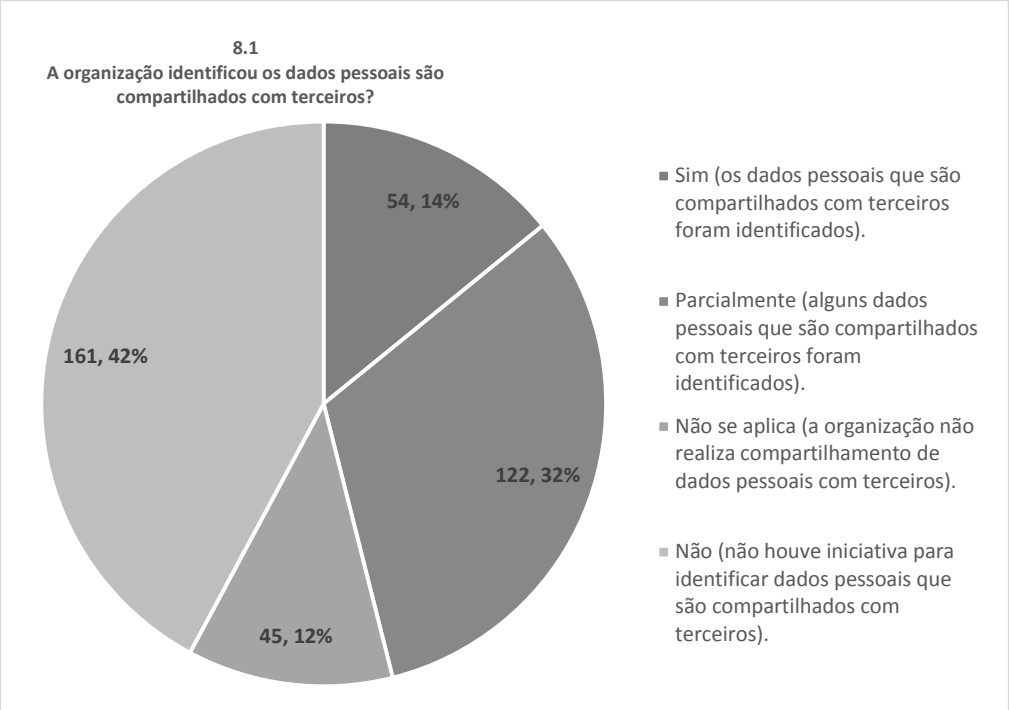
218. *O art. 5º da LGPD traz a seguinte definição (grifou-se):*

> *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.*

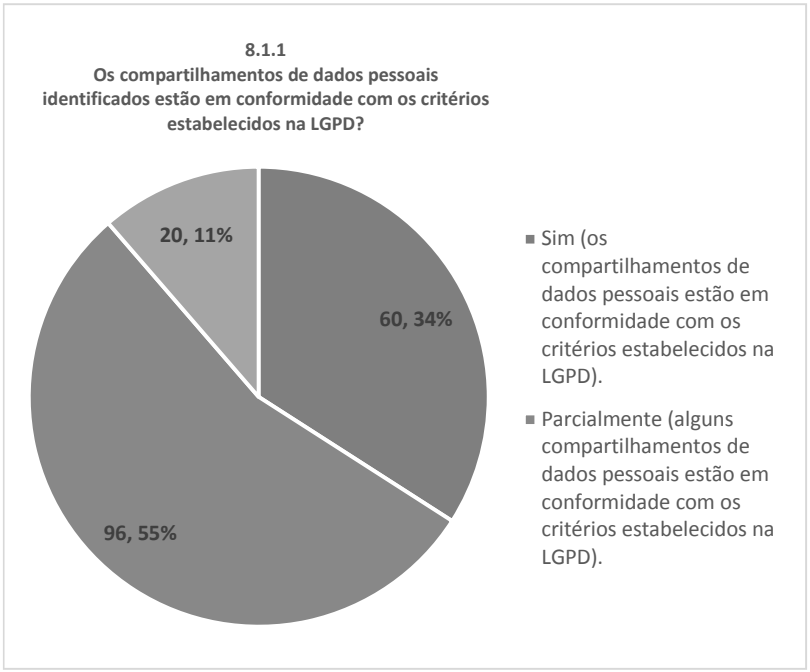
222. *Sob a mesma perspectiva, caso a organização afirmasse que identificou, na totalidade ou em parte, os dados pessoais que são compartilhados com terceiros, eram exibidas as subquestões 8.1.1, 8.1.2 e 8.1.3. A primeira para avaliar se os compartilhamentos identificados estão em conformidade com os 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.*

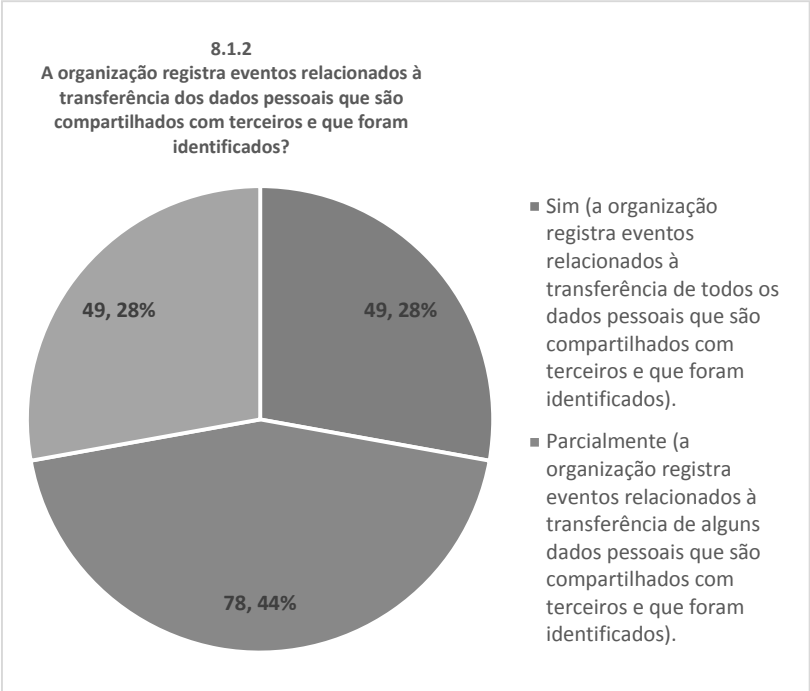
Figura 38 *- Conformidade com a LGPD dos compartilhamentos de dados pessoais*



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*

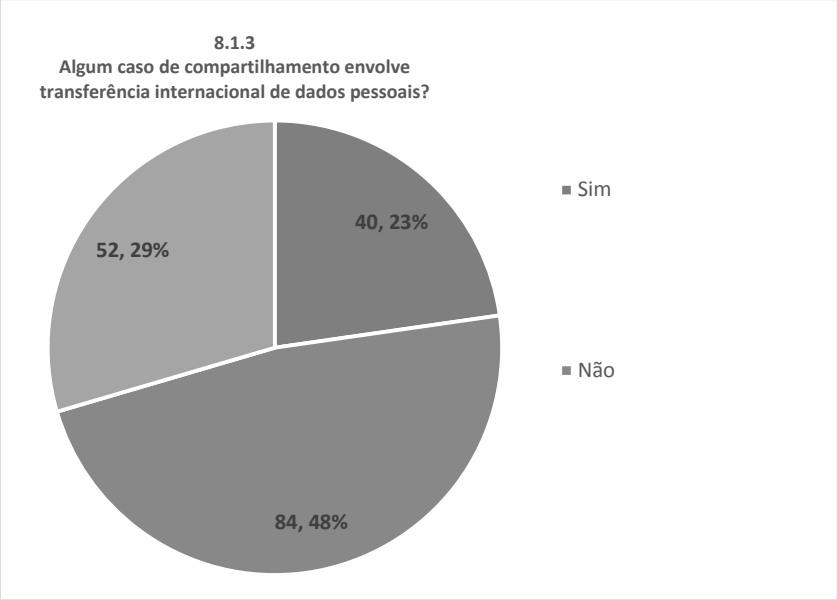


228. *Já em relação à questão 8.1.3, destaca-se que o art. 33 da LGPD relaciona nove casos nos quais é permitida a transferência internacional de dados pessoais. Diante disso, a organização deve avaliar se as transferências internacionais que realiza estão enquadradas em uma dessas hipóteses.*

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.*

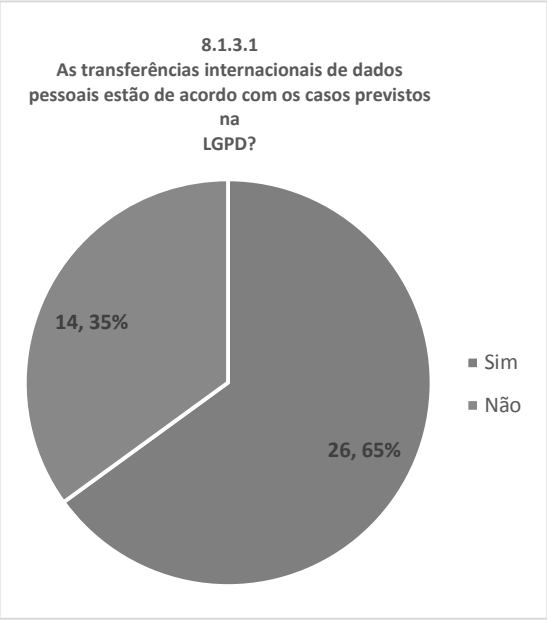
230. *Entretanto, constatou-se que 29% das organizações que responderam à questão afirmaram que ainda não verificaram se há caso de transferência internacional de dados pessoais (Figura 40).*

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.*

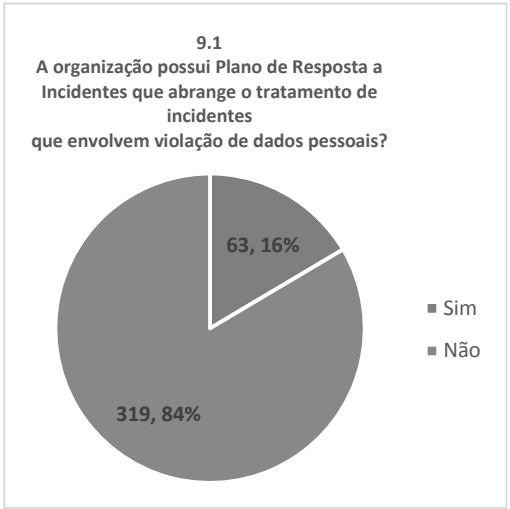
2.1.8.1 Plano de resposta a incidentes

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*

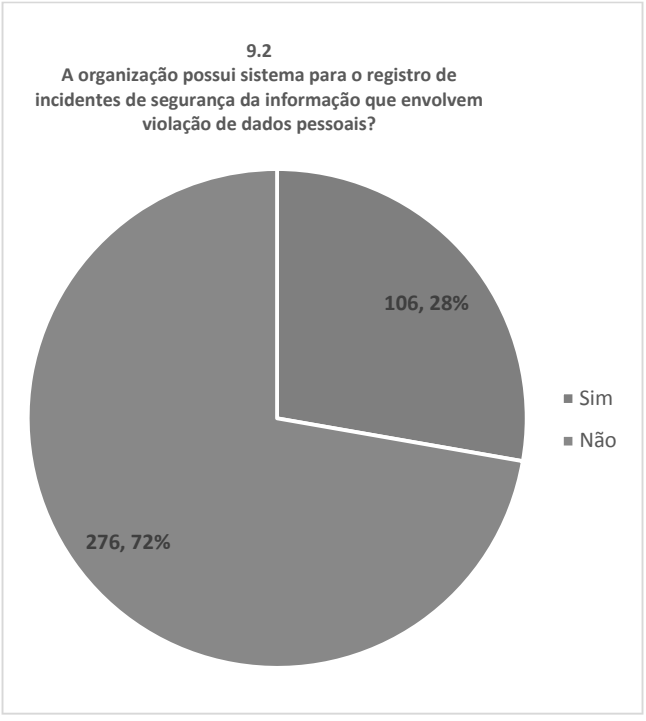
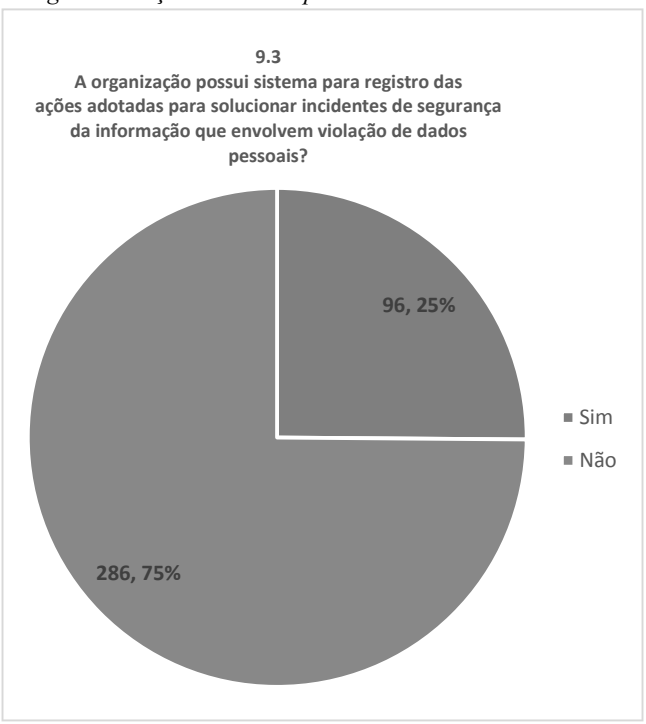


Figura 44 *- Sistema para registro de ações adotadas para solucionar incidentes de violação de dados pessoais*



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 <u>Monitoramento de eventos</u>

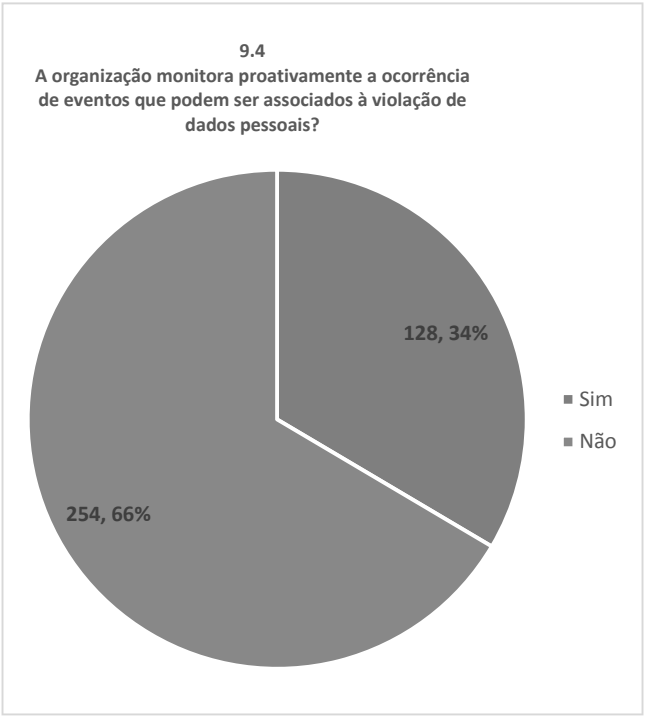
247. *A questão 9.4 buscou verificar se as organizações monitoram proativamente a ocorrência de eventos que podem ser associados à violação de dados pessoais.*

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

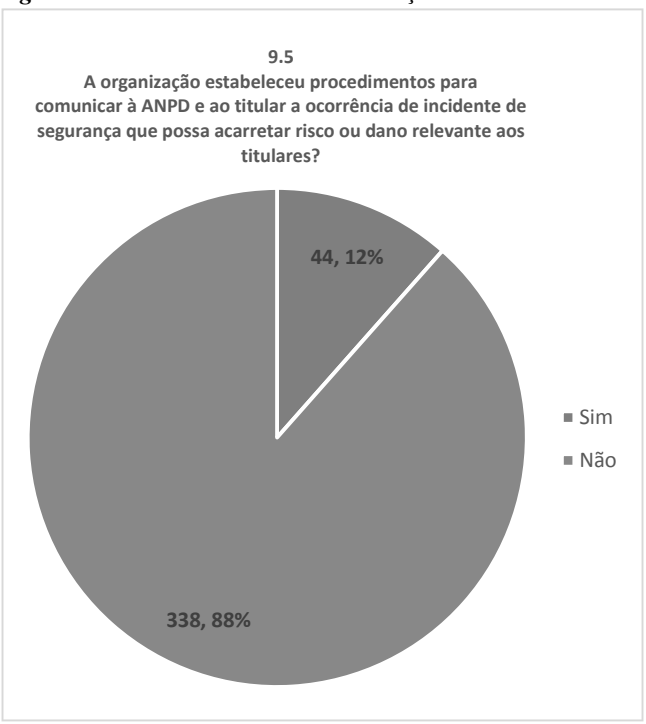
253. *A questão 9.5 buscou verificar se as organizações estabeleceram procedimentos para comunicar à ANPD e ao titular dos dados pessoais a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante ao próprio titular.*

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.*

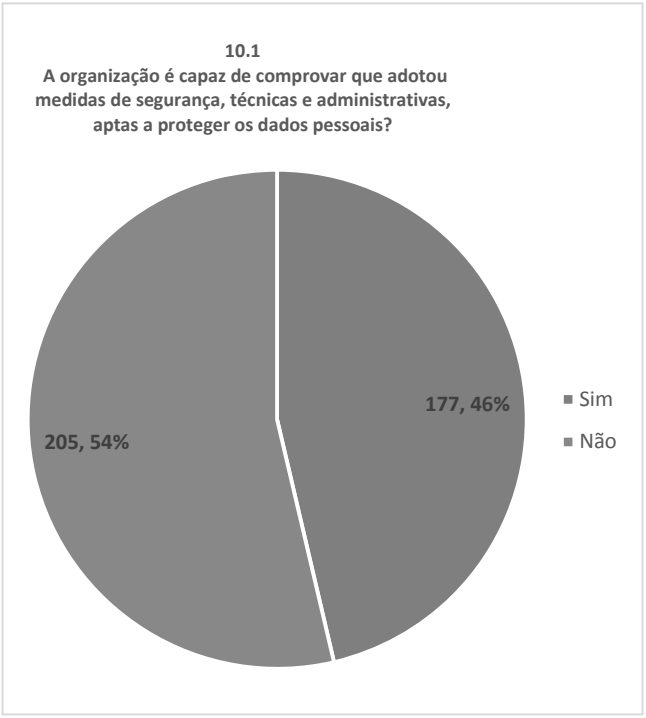
2.1.9.1 Medidas de segurança

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 <u>Controle de acesso em sistemas</u>

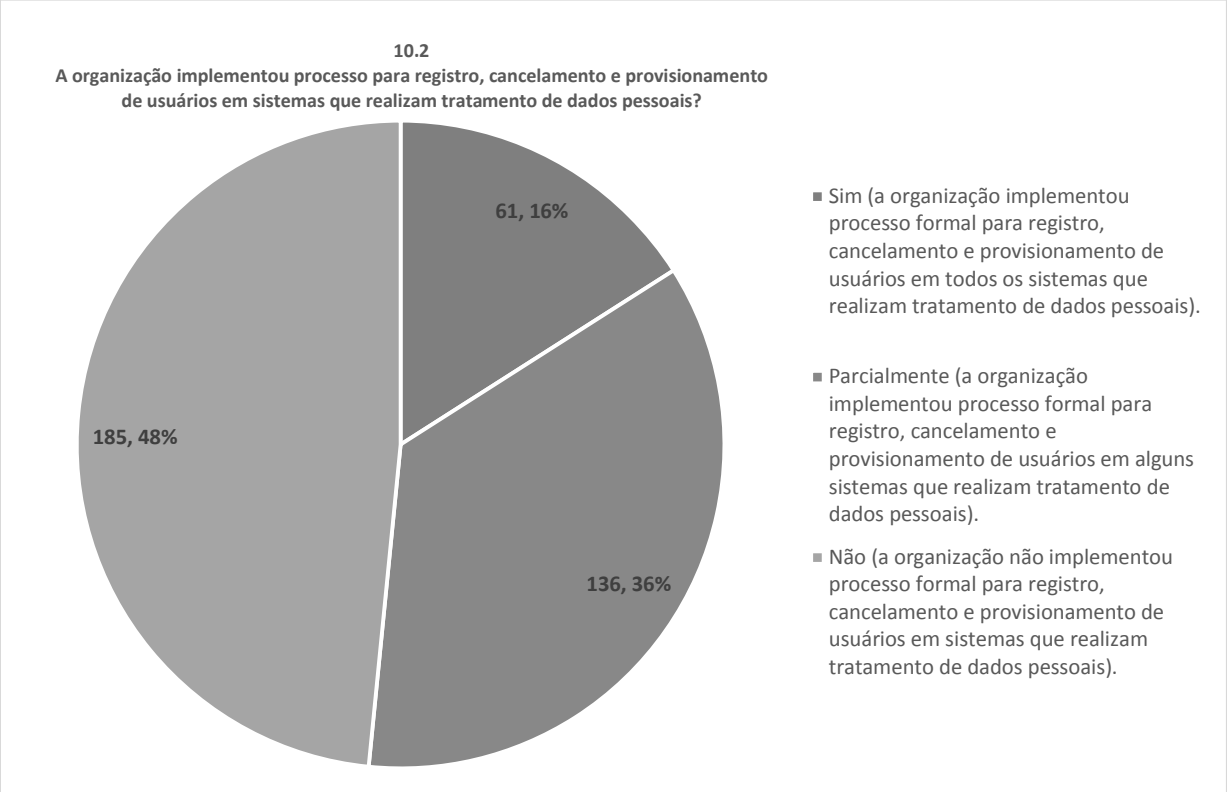
268. *A questão 10.2 buscou verificar se as organizações implementaram processo para registro, cancelamento e provisionamento de usuários em sistemas que realizam tratamento de dados pessoais.*

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.*

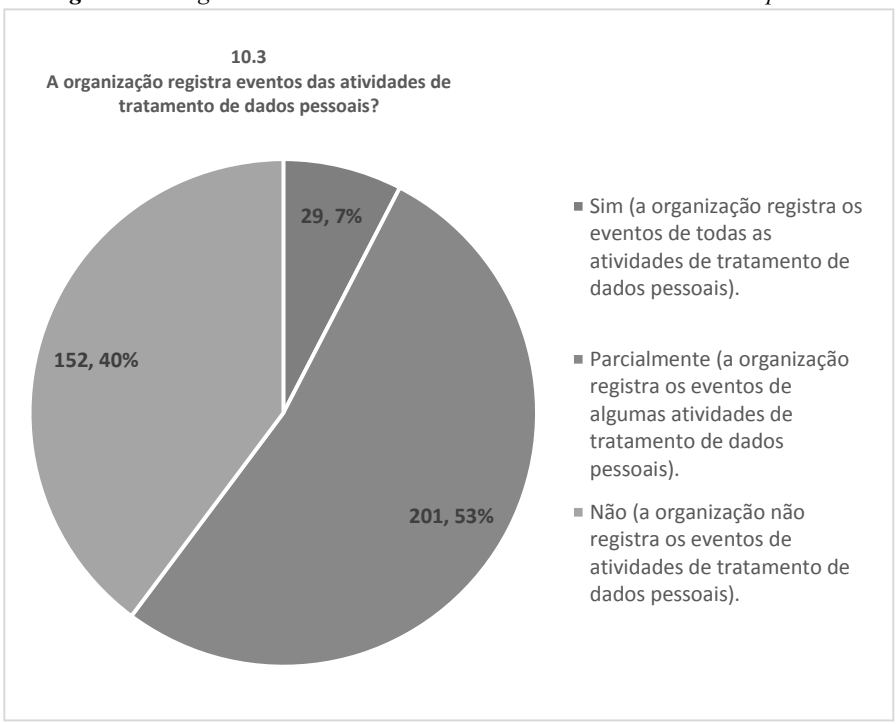
2.1.9.3 <u>Registro de eventos (logs)</u>

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

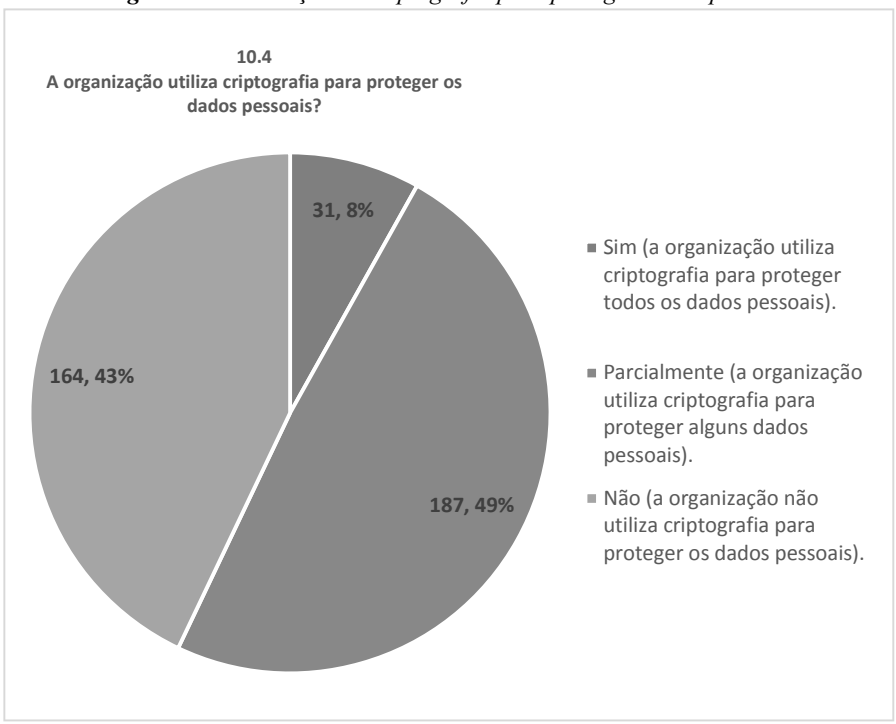
278. *A questão 10.4 buscou verificar se as organizações utilizam criptografia para proteger os dados pessoais.*

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

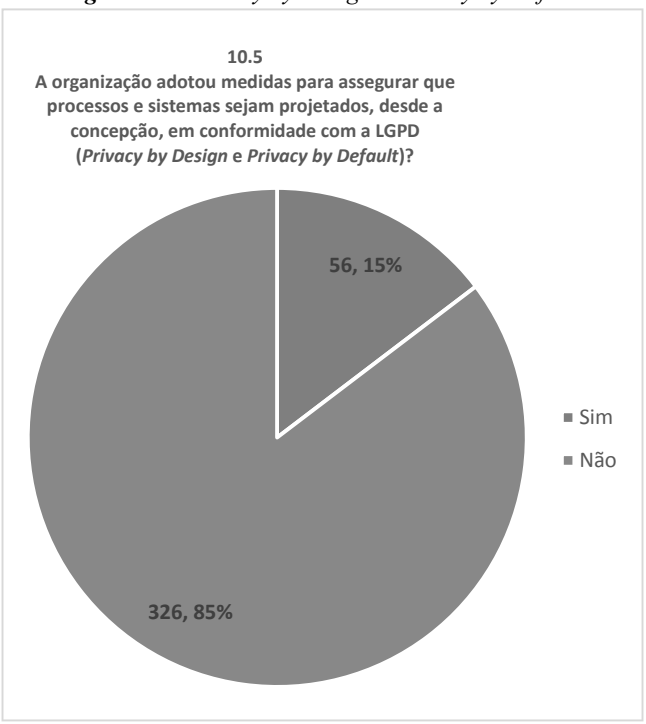
284. *A questão 10.5 buscou verificar se as organizações adotam medidas para assegurar que processos e sistemas sejam projetados, desde a concepção, em conformidade com a LGPD.*

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).*

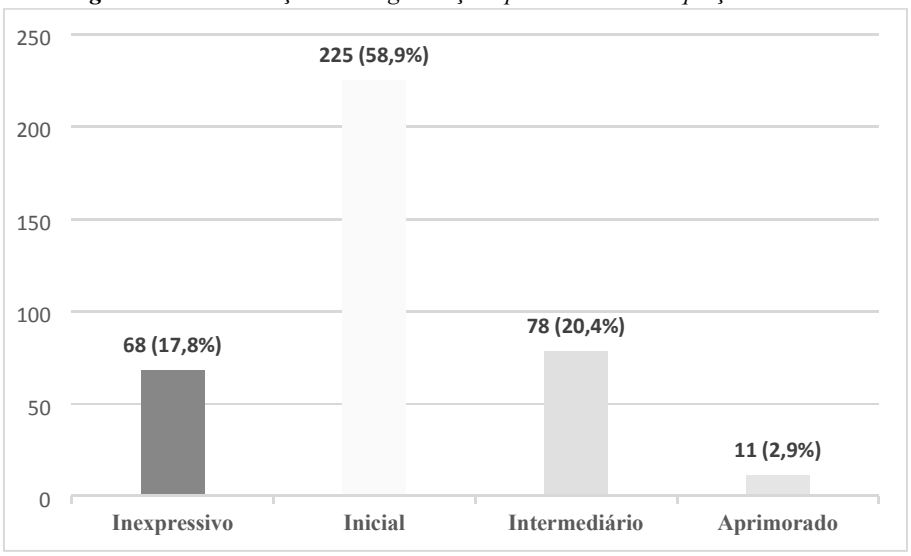
$$indicador = \frac{\sum_{i=1}^{42} notaResposta(i)}{42}$$

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*

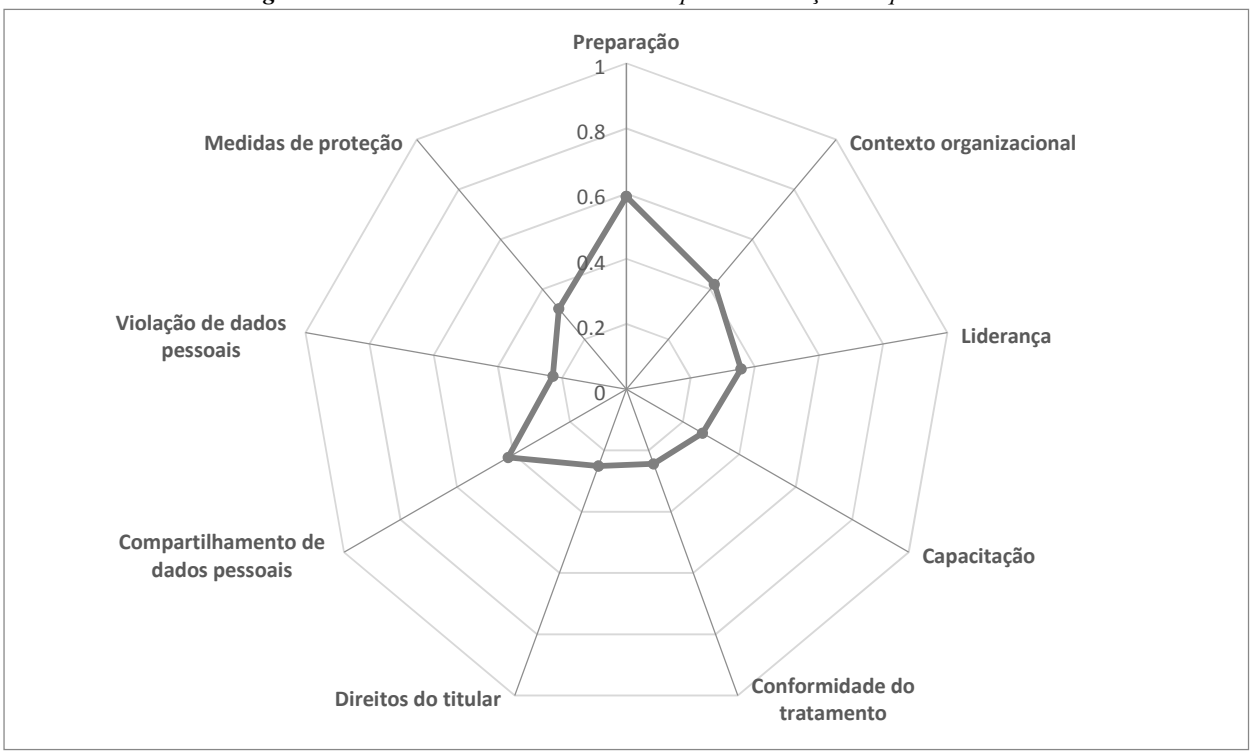


295. *O indicador também pode ser apresentado levando em consideração a nota referente a cada uma das dimensões do questionário: 'Preparação', 'Contexto Organizacional', 'Liderança', 'Capacitação', 'Conformidade do Tratamento', 'Direitos do Titular', 'Compartilhamento de Dados Pessoais', 'Violação de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

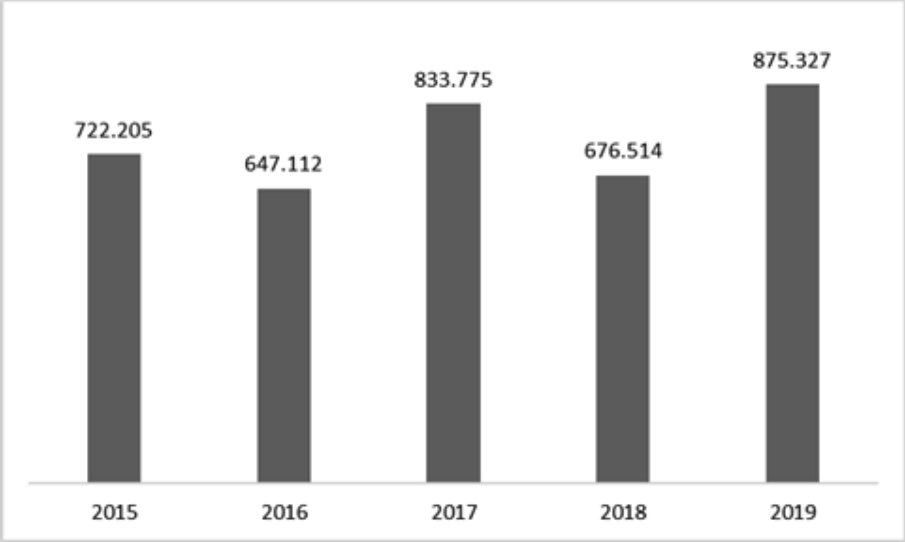
303. *Nos últimos anos, a preocupação com a privacidade dos cidadãos e com a proteção de dados pessoais ganhou destaque no debate público, fazendo com que o tema ocupasse espaço central*

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:*

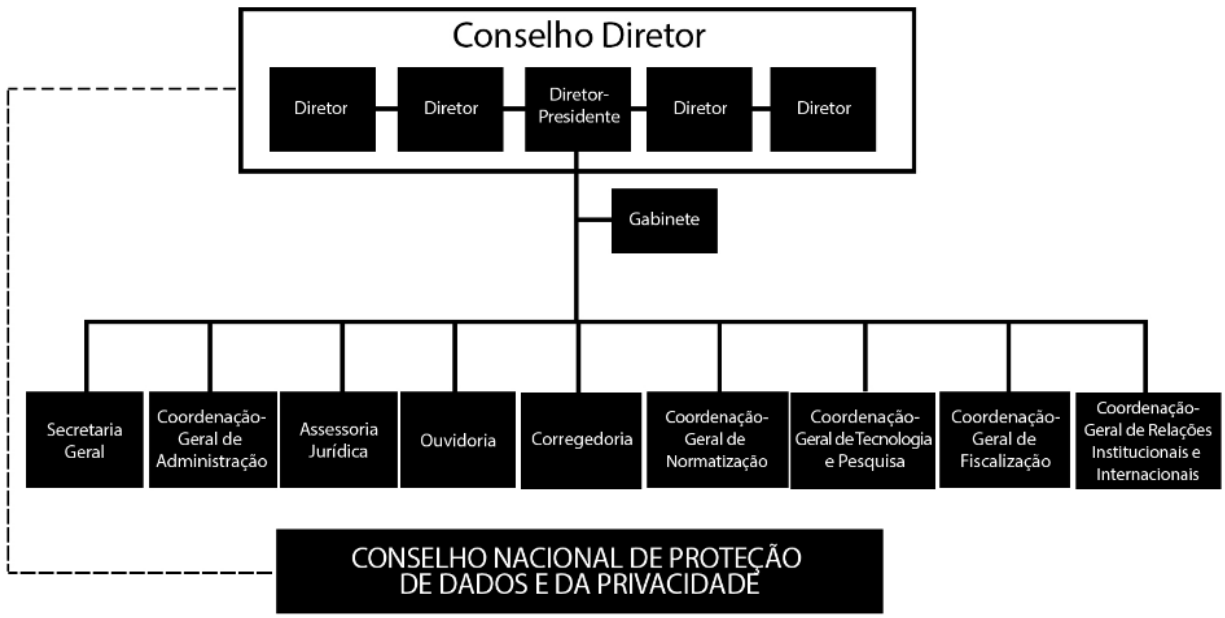
Figura 55 *- Atribuições da ANPD*

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.*

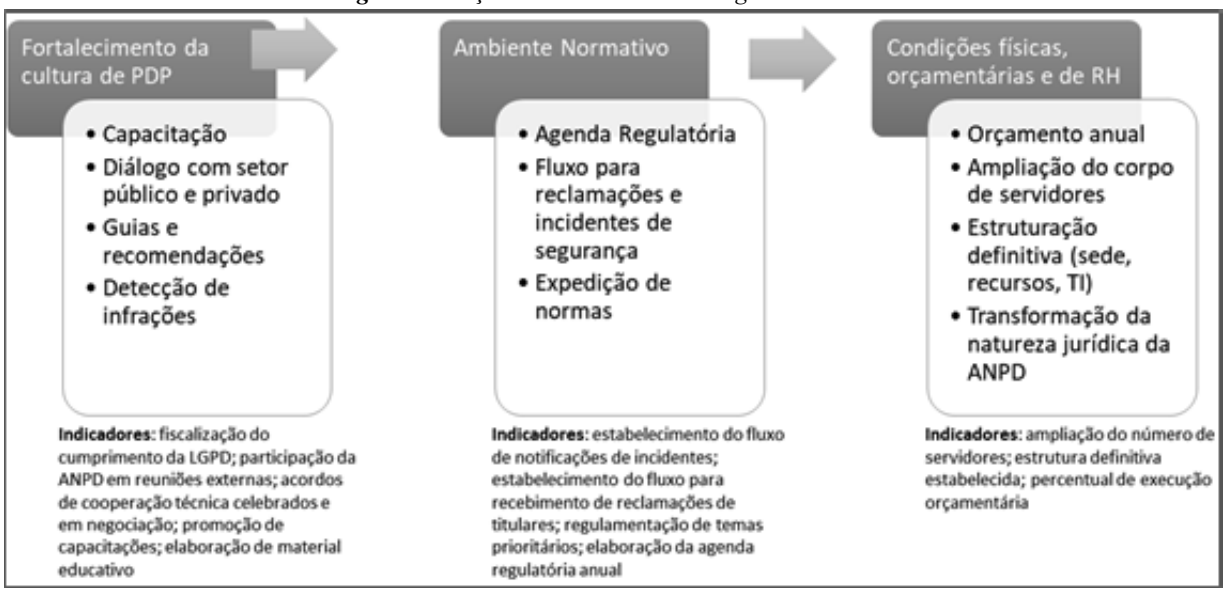
319. *As informações estão dispostas no Mapa Estratégico da ANPD, que agrupa os objetivos em dimensões, além de apresentar a sua missão e visão:*

***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

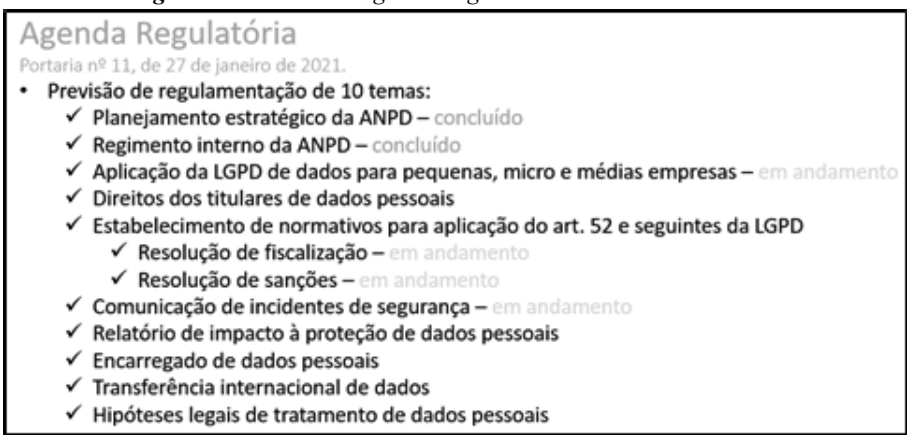
*A **autoridade nacional poderá dispor** sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência*
Art. 41, § 3º
*A **autoridade nacional poderá estabelecer** 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 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.*

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.

TRIBUNAL DE CONTAS DA UNIÃO

Auditoria para elaborar diagnóstico acerca dos controles implementados pelas organizações públicas federais para adequação à LGPD

(Acórdão 1.384/2022-TCU-Plenário, Relatoria Min. Augusto Nardes)

Relatório de *Feedback*

Organização:

Instituto Federal de Educação, Ciência e Tecnologia de Rondônia

(IFRO)

Todas as informações deste documento são consideradas públicas, conforme classificação do item 9.10 do Acórdão 1.384/2022-TCU-Plenário.

Sumário

Lista de Figuras

Lista de Tabelas

1 Introdução

Este relatório apresenta os resultados da organização **IFRO** relativos à auditoria realizada pelo TCU entre novembro de 2020 e maio de 2021 para 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 13.709/2018, denominada Lei Geral de Proteção de Dados (LGPD) (TC 039.606/2020-1; Acórdão 1.384/2022-TCU-Plenário de relatoria do Ministro Augusto Nardes).

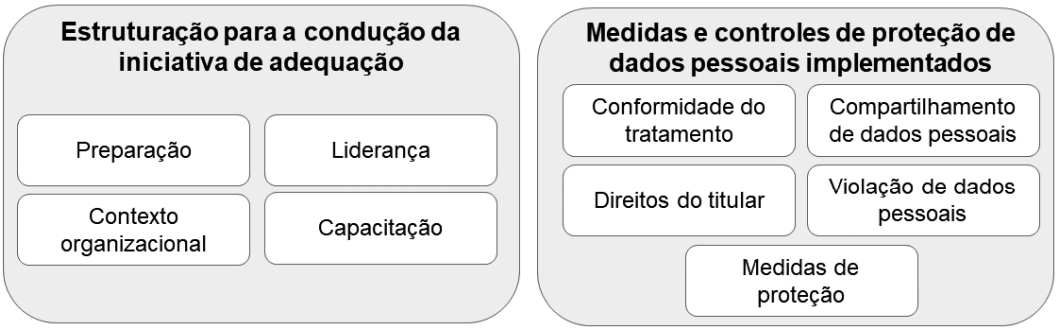
Ressalta-se que o TCU fará a divulgação dos resultados desta fiscalização conforme autorização do Plenário, mas, em atendimento ao princípio da transparência, é recomendável que a própria organização tome a iniciativa de também **publicar em seu próprio *site* as informações contidas neste relatório**.

2 Avaliação da adequação à LGPD

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 devem ser utilizadas como referência para a condução de futuras iniciativas de adequação.

O questionário contemplou 60 questões organizadas em duas perspectivas e nove dimensões (Figura 1). As questões tiveram como referência a própria LGPD e a norma técnica ABNT NBR ISO/IEC 27701:2019 (extensão das normas de segurança da informação ABNT NBR ISO/IEC 27.001 e ABNT NBR ISO/IEC 27.002 para gestão da privacidade da informação).

Figura 1 - Dimensões do questionário



De modo a consolidar os dados obtidos e a 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.

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)[1].

A partir dos valores 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

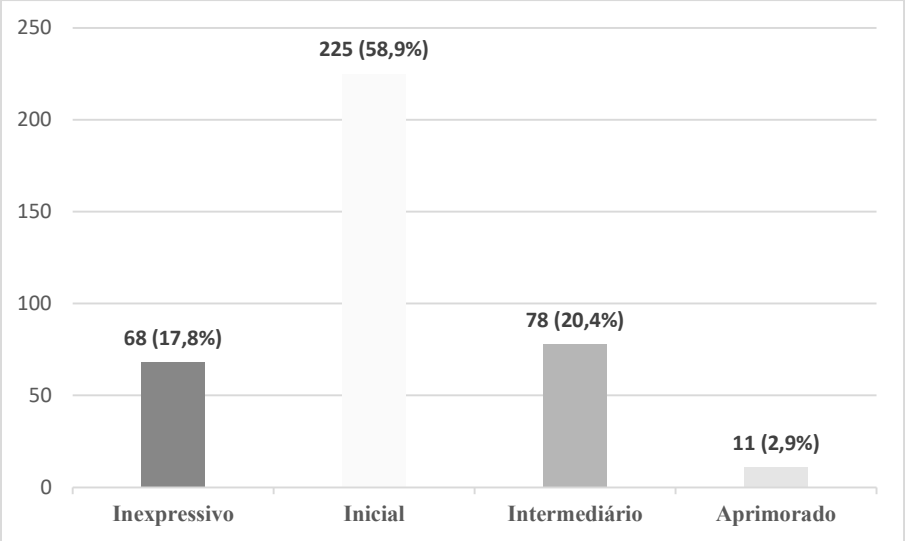
[1] O cálculo do indicador está detalhado na Seção 2.2 do relatório de auditoria.

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 classificadas em um desses níveis de maturidade.

A organização **IFRO** obteve o valor **0,60** para o indicador de adequação, o que corresponde ao nível "**Intermediário**".

O gráfico da Figura 2 apresenta a consolidação da distribuição das 382 organizações em cada nível.

Figura 2 - Distribuição das organizações por níveis de adequação à LGPD



O indicador pode ser desmembrado e também apresentado levando em consideração os valores referentes 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".

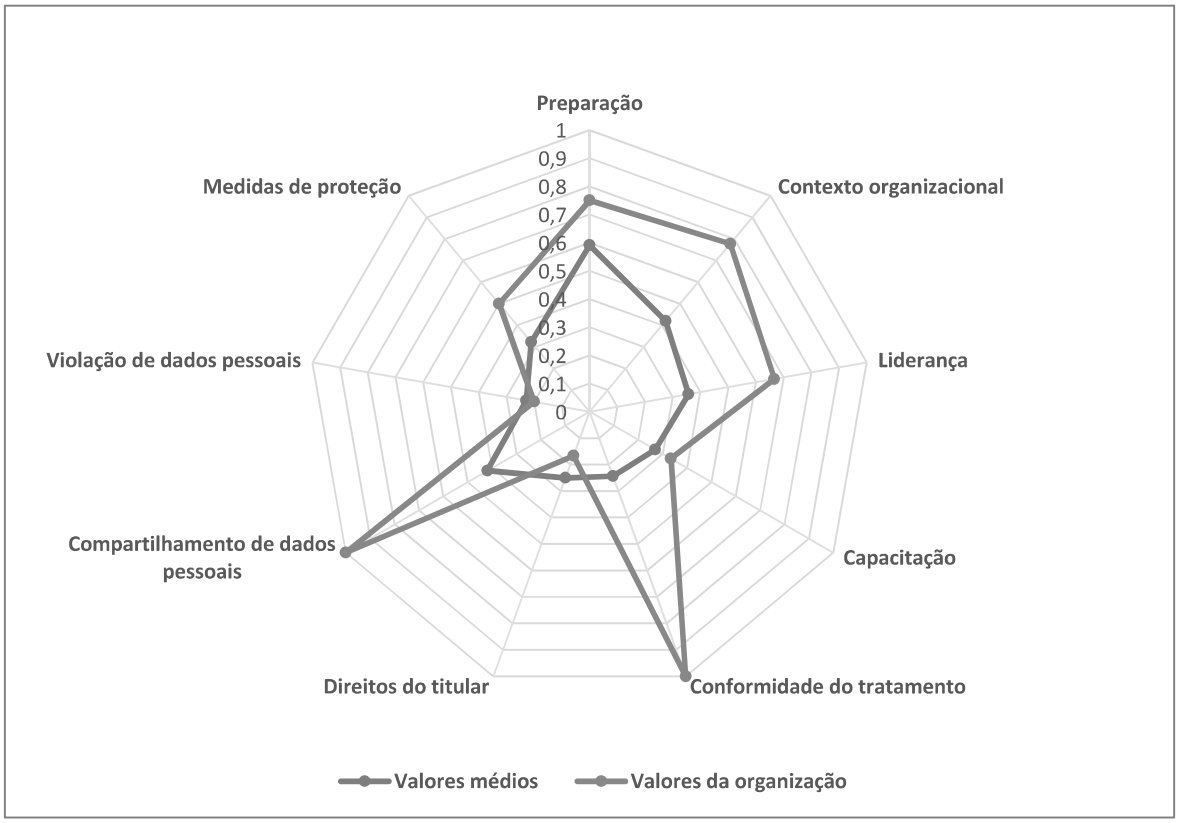
Na Tabela 1 é apresentado um resumo da avaliação da organização contendo os valores de cada dimensão do questionário e do indicador de adequação à LGPD, possibilitando comparar os valores da própria organização e os valores médios do conjunto das 382 organizações avaliadas.

Tabela 1 - Resumo da avaliação da adequação à LGPD

Dimensões do questionário	Valores da organização	Valores médios
Estruturação para condução da iniciativa de adequação		
Preparação	0,75	0,59
Contexto Organizacional	0,78	0,42
Liderança	0,67	0,36
Capacitação	0,33	0,27
Medidas e controles de proteção de dados pessoais implementados		
Conformidade do Tratamento	1,00	0,24
Direitos do Titular	0,17	0,25
Compartilhamento de Dados Pessoais	1,00	0,42
Violação de Dados Pessoais	0,20	0,23
Medidas de Proteção	0,50	0,32
Indicador de adequação à LGPD	**0,60**	**0,35**

O gráfico da Figura 3 possibilita comparar visualmente os valores dos indicadores em cada dimensão que foram calculados para a organização **IFRO** relativamente aos valores médios calculados ao se considerar o conjunto das 382 organizações avaliadas.

Figura 3 - Valores da organização e valores médios por dimensões do questionário



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.

2.1 Preparação

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

As questões desta dimensão abordam aspectos relacionados à identificação e ao planejamento das medidas necessárias à adequação.

Na Tabela 2 são apresentadas as questões desta dimensão que compõem o indicador de adequação à LGPD, possibilitando comparar os valores da própria organização e os valores médios do conjunto das 382 organizações avaliadas.

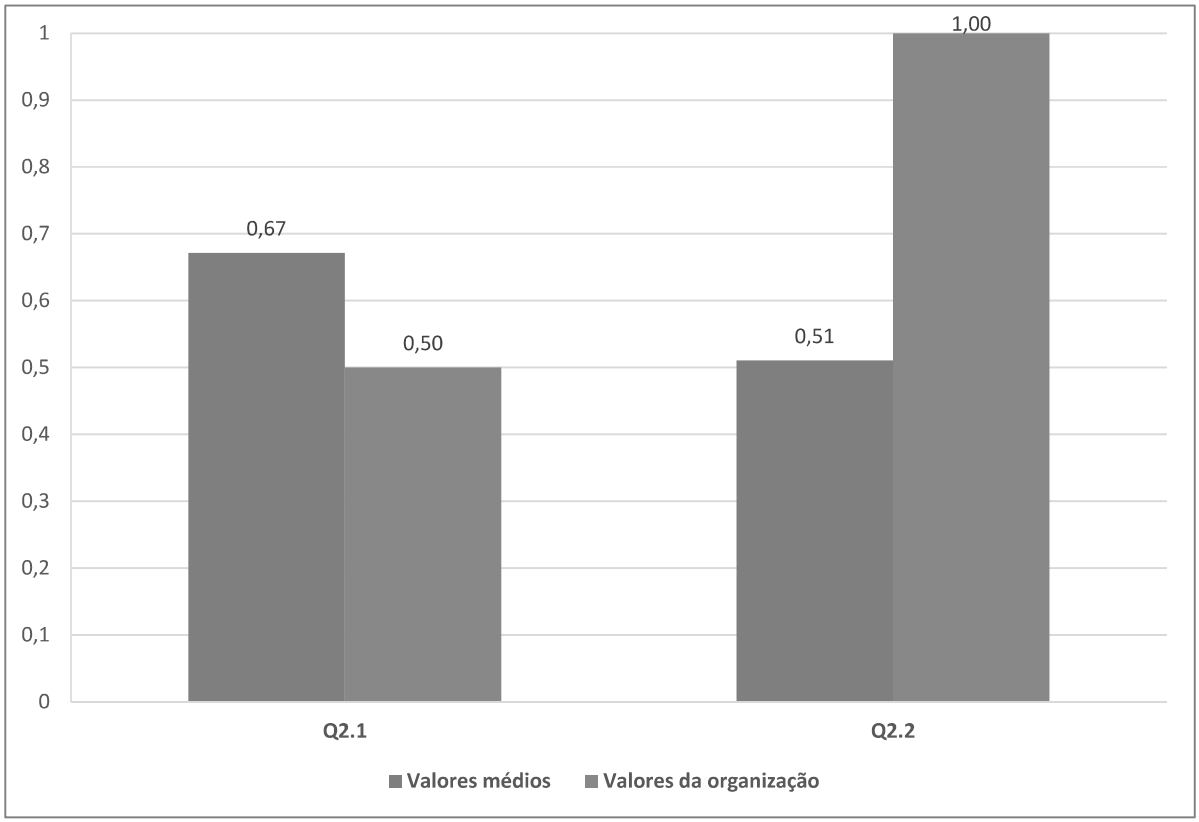
Tabela 2 - Preparação para adequação à LGPD

Questões	Valores da organização	Valores médios
2.1 A organização conduziu iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD?	0,50	0,67
2.2 A organização elaborou plano de ação, plano de projeto ou documento similar para direcionar a	1,00	0,51

iniciativa de adequação à LGPD?		

O gráfico da Figura 4 possibilita comparar visualmente os valores das questões desta dimensão que foram calculados para a organização relativamente aos valores médios calculados ao se considerar o conjunto das 382 organizações avaliadas.

Figura 4 - Valores da organização e valores médios na dimensão "Preparação"



2.2 Contexto Organizacional

Para alcançar os resultados pretendidos pela iniciativa de adequação à LGPD, a organização deve avaliar questões internas e externas que são relevantes para atingir os objetivos.

As questões desta seção abordam aspectos relacionados à identificação de normativos correlatos à proteção de dados pessoais que devem ser respeitados pela organização, à identificação das partes interessadas e à análise dos dados pessoais tratados pela organização e dos processos organizacionais que tratam esses dados.

Na Tabela 3 são apresentadas as questões desta dimensão que compõem o indicador de adequação à LGPD, possibilitando comparar os valores da própria organização e os valores médios do conjunto das 382 organizações avaliadas.

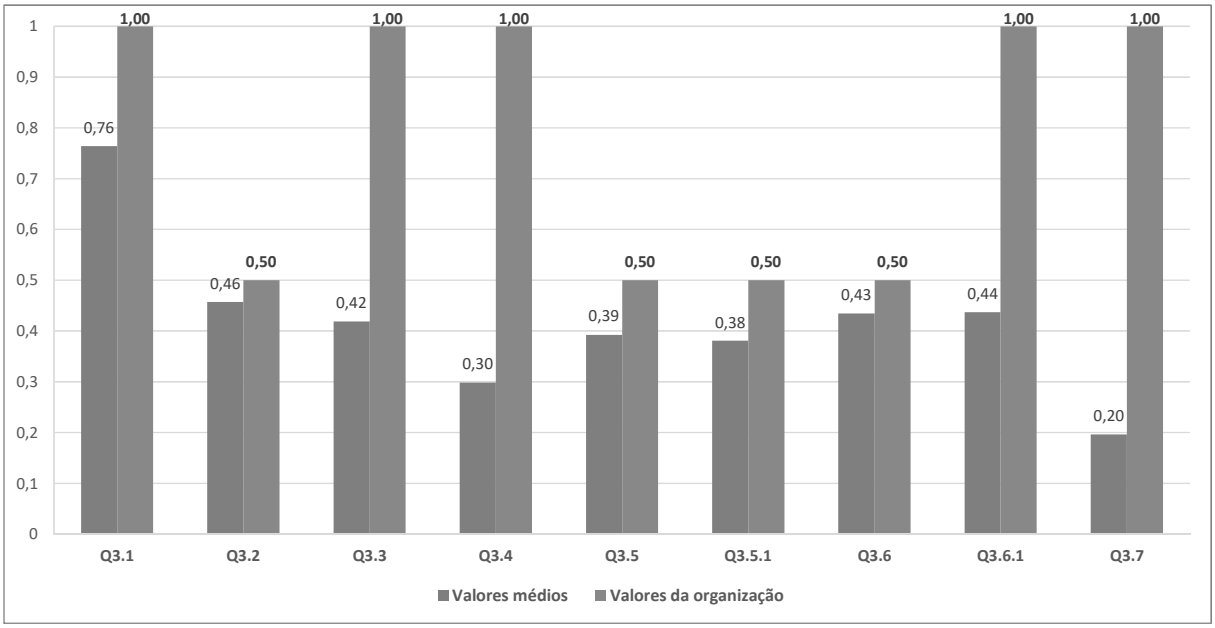
Tabela 3 - Contexto Organizacional

Questões	Valores da organização	Valores médios
3.1 A organização conduziu iniciativa para identificar outros normativos (e.g.: leis, regulamentos e instruções normativas), além da LGPD, que abrangem comandos relacionados à proteção de dados pessoais e	1,00	0,76

que também devem ser respeitados?		
3.2 A organização identificou as categorias de titulares de dados pessoais com os quais se relaciona?	0,50	0,46
3.3 A organização conduziu iniciativa para identificar os operadores que realizam tratamento de dados pessoais em seu nome?	1,00	0,42
3.4 A organização avaliou se há tratamento de dados que envolva controlador conjunto?	1,00	0,30
3.5 A organização identificou os processos de negócio que realizam tratamento de dados pessoais?	0,50	0,39
3.5.1 A organização identificou quem são os responsáveis pelos processos de negócio que realizam tratamento de dados pessoais e que já foram identificados?	0,50	0,38
3.6 A organização identificou quais são os dados pessoais tratados por ela?	0,50	0,43
3.6.1 A organização identificou os locais onde os dados pessoais identificados são armazenados?	1,00	0,44
3.7 A organização avaliou os riscos dos processos de tratamento de dados pessoais que foram identificados?	1,00	0,20

O gráfico da Figura 5 possibilita comparar visualmente os valores das questões desta dimensão que foram calculados para a organização relativamente aos valores médios calculados ao se considerar o conjunto das 382 organizações avaliadas.

Figura 5 - Valores da organização e valores médios na dimensão "Contexto Organizacional"



2.3 Liderança

A alta direção deve demonstrar liderança e comprometimento com a iniciativa de adequação à LGPD.

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 Autoridade Nacional de Proteção de Dados (ANPD) são fundamentais para o processo de adequação.

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.

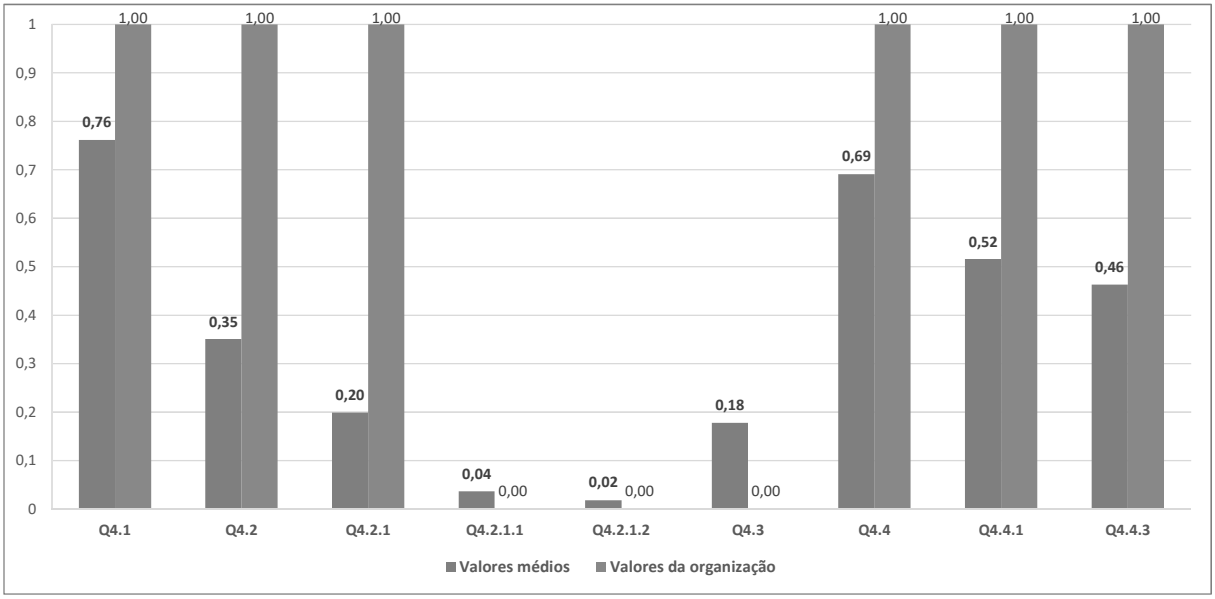
Na Tabela 4 são apresentadas as questões desta dimensão que compõem o indicador de adequação à LGPD, possibilitando comparar os valores da própria organização e os valores médios do conjunto das 382 organizações avaliadas.

Tabela 4 - Liderança

Questões	**Valores da organização**	**Valores médios**
4.1 A organização possui Política de Segurança da Informação ou instrumento similar?	1,00	0,76
4.2 A organização possui Política de Classificação da Informação ou instrumento similar?	1,00	0,35
4.2.1 A Política de Classificação da Informação (ou instrumento similar) abrange diretrizes para a classificação de dados pessoais?	1,00	0,20
4.2.1.1 A Política de Classificação da Informação (ou instrumento similar) abrange diretrizes para identificar dados pessoais sensíveis e relacionados a crianças e adolescentes?	0,00	0,04
4.2.1.2 A Política de Classificação da Informação (ou instrumento similar) abrange diretrizes para identificar dados pessoais de crianças e de adolescentes?	0,00	0,02
4.3 A organização possui Política de Proteção de Dados Pessoais (ou instrumento similar)?	0,00	0,18
4.4 A organização nomeou o encarregado pelo tratamento de dados pessoais?	1,00	0,69
4.4.1 A nomeação do encarregado foi publicada em veículo de comunicação oficial?	1,00	0,52
4.4.3 A identidade e as informações de contato do encarregado foram divulgadas na internet?	1,00	0,46

O gráfico da Figura 6 possibilita comparar visualmente os valores das questões desta dimensão que foram calculados para a organização relativamente aos valores médios calculados ao se considerar o conjunto das 382 organizações avaliadas.

Figura 6 - Valores da organização e valores médios na dimensão "Liderança"



2.4 Capacitação

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

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 importantes para a preservação da privacidade dos titulares.

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.

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

Na Tabela 5 são apresentadas as questões desta dimensão que compõem o indicador de adequação à LGPD, possibilitando comparar os valores da própria organização e os valores médios do conjunto das 382 organizações avaliadas.

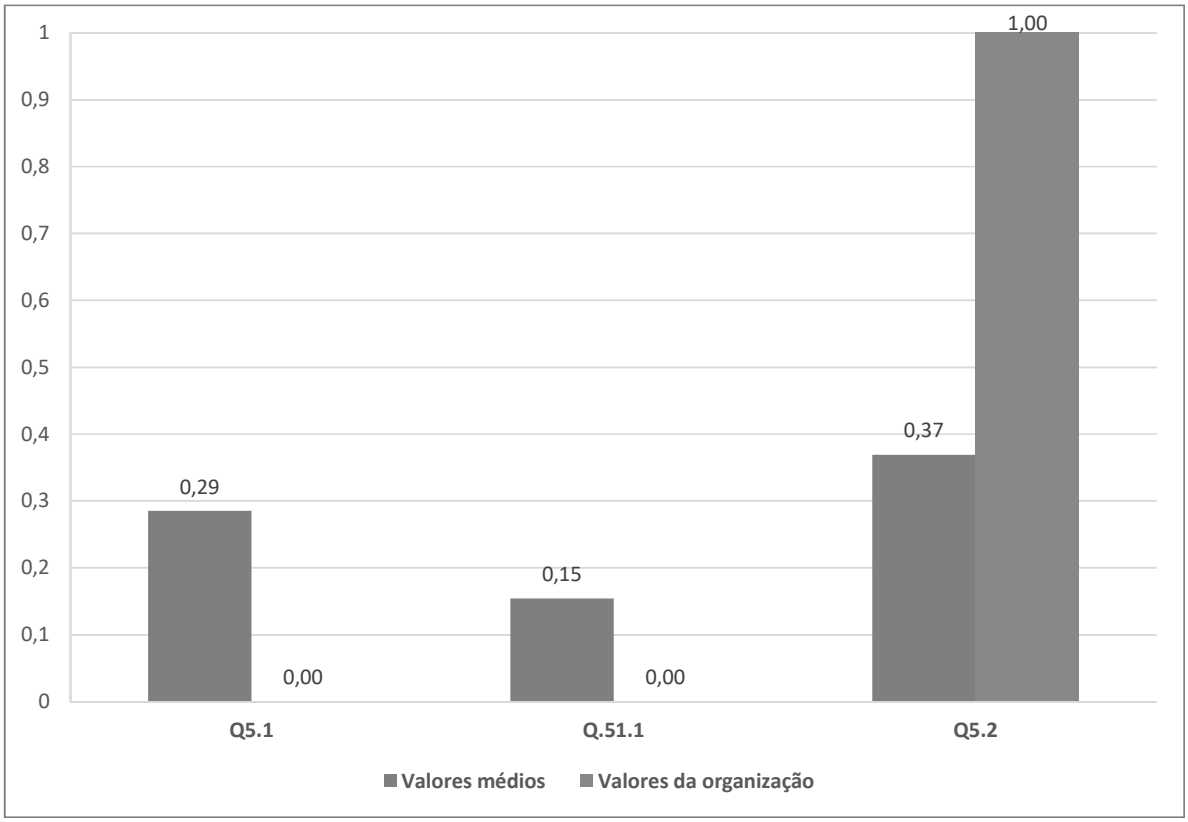
Tabela 5 - Capacitação

Questões	Valores da organização	Valores médios
5.1 A organização possui Plano de Capacitação (ou instrumento similar) que abrange treinamento e conscientização dos seus colaboradores em proteção de dados pessoais?	0,00	0,29
5.1.1 O Plano de Capacitação (ou instrumento similar) considera que pessoas que exercem funções com responsabilidades essenciais relacionadas à proteção de dados pessoais devem receber treinamento diferenciado?	0,00	0,15
5.2. Colaboradores da organização que estão diretamente envolvidos em atividades que realizam	1,00	0,37

tratamento de dados pessoais receberam treinamentos relacionados ao tema?		

O gráfico da Figura 7 possibilita comparar visualmente os valores das questões desta dimensão que foram calculados para a organização relativamente aos valores médios calculados ao se considerar o conjunto das 382 organizações avaliadas.

Figura 7 - Valores da organização e valores médios na dimensão "Capacitação"



2.5 Conformidade do Tratamento

A organização deve ser capaz de provar que os tratamentos de dados pessoais que realiza são lícitos. Para isso é fundamental 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.

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 será avaliado se a organização possui um registro para documentar detalhes das atividades de tratamento.

Na Tabela 6 são apresentadas as questões desta dimensão que compõem o indicador de adequação à LGPD, possibilitando comparar os valores da própria organização e os valores médios do conjunto das 382 organizações avaliadas.

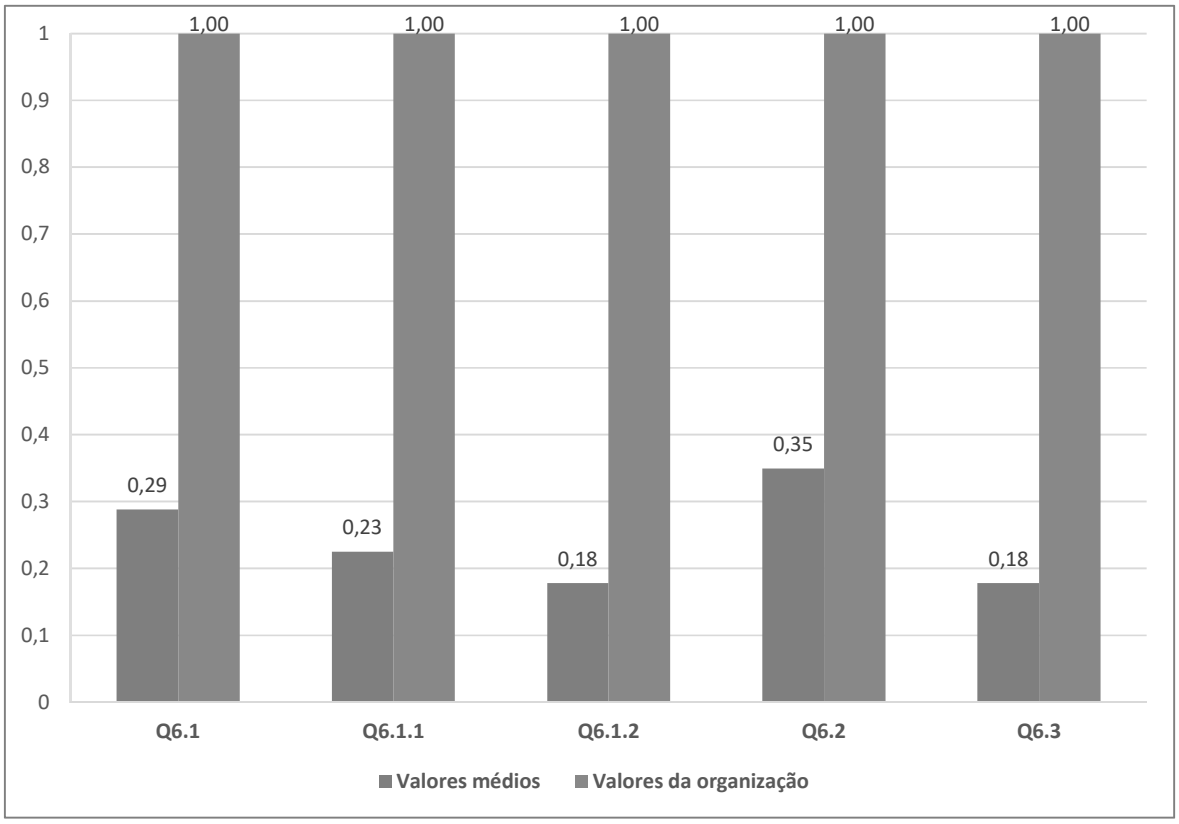
Tabela 6 - Conformidade do Tratamento

Questões	**Valores da organização**	**Valores médios**
6.1 A organização identificou e documentou as finalidades das atividades de tratamento de dados	1,00	0,29

pessoais?		
6.1.1 A organização avaliou se coleta apenas os dados estritamente necessários para cumprir com as finalidades de tratamento de dados pessoais que foram identificadas?	1,00	0,23
6.1.2 A organização avaliou 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?	1,00	0,18
6.2 A organização identificou e documentou as bases legais que fundamentam as atividades de tratamento de dados pessoais?	1,00	0,35
6.3 Há um registro (*e.g.*: inventário) instituído para consolidar informações relacionadas às características das atividades de tratamento de dados pessoais?	1,00	0,18

O gráfico da Figura 8 possibilita comparar visualmente os valores das questões desta dimensão que foram calculados para a organização relativamente aos valores médios calculados ao se considerar o conjunto das 382 organizações avaliadas.

Figura 8 - Valores da organização e valores médios na dimensão "Conformidade do Tratamento"



2.6 Direitos do Titular

A organização deve assegurar que os titulares tenham acesso a informações relacionadas ao tratamento de seus dados pessoais. Para isso, a organização deve publicar, de maneira clara e concisa, informações relativas ao tratamento de dados pessoais. A organização também deve estar preparada para atender todos os direitos dos titulares que são elencados na LGPD.

Nesta seção são abordadas questões relacionadas à elaboração da política de privacidade

e ao atendimento dos direitos dos titulares.

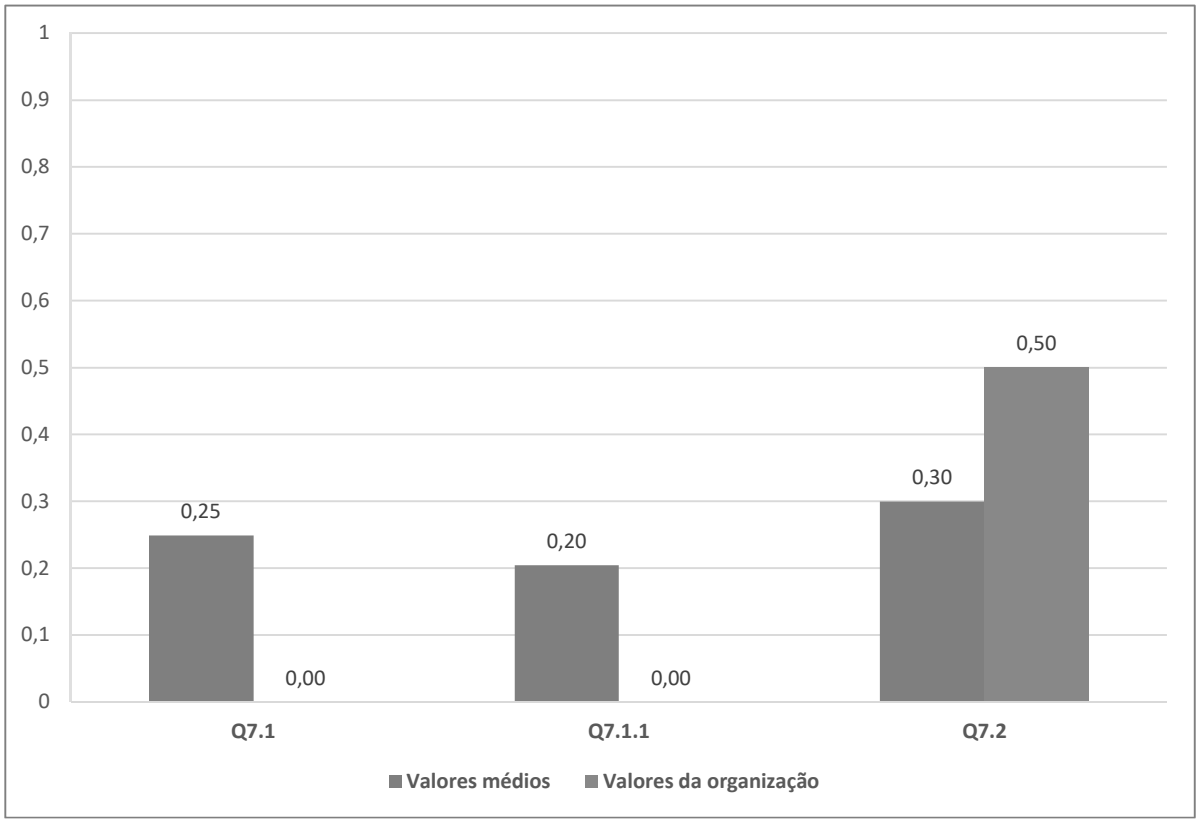
Na Tabela 7 são apresentadas as questões desta dimensão que compõem o indicador de adequação à LGPD, possibilitando comparar os valores da própria organização e os valores médios do conjunto das 382 organizações avaliadas.

Tabela 7 - Direitos do Titular

Questões	Valores da organização	Valores médios
7.1 A organização possui Política de Privacidade (ou instrumento similar)?	0,00	0,25
7.1.1 A Política de Privacidade (ou instrumento similar) está publicada na internet?	0,00	0,20
7.2 Foram implementados mecanismos para atender os direitos dos titulares elencados no art. 18 da LGPD e aplicáveis à organização?	0,50	0,30

O gráfico da Figura 9 possibilita comparar visualmente os valores das questões desta dimensão que foram calculados para a organização relativamente aos valores médios calculados ao se considerar o conjunto das 382 organizações avaliadas.

Figura 9 - Valores da organização e valores médios na dimensão "Direitos do Titular"



2.7 Compartilhamento de Dados Pessoais

A organização deve documentar detalhes relacionados ao compartilhamento de dados pessoais com terceiros.

A realização de compartilhamento demanda a adoção de controles adequados para mitigar

riscos que possam comprometer a proteção dos dados pessoais. Diante disso, a LGPD defende que as precauções a serem adotadas entre as partes envolvidas no compartilhamento sejam formalizadas em contrato e que cuidados especiais devem ser adotados no caso de transferência internacional desses dados.

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

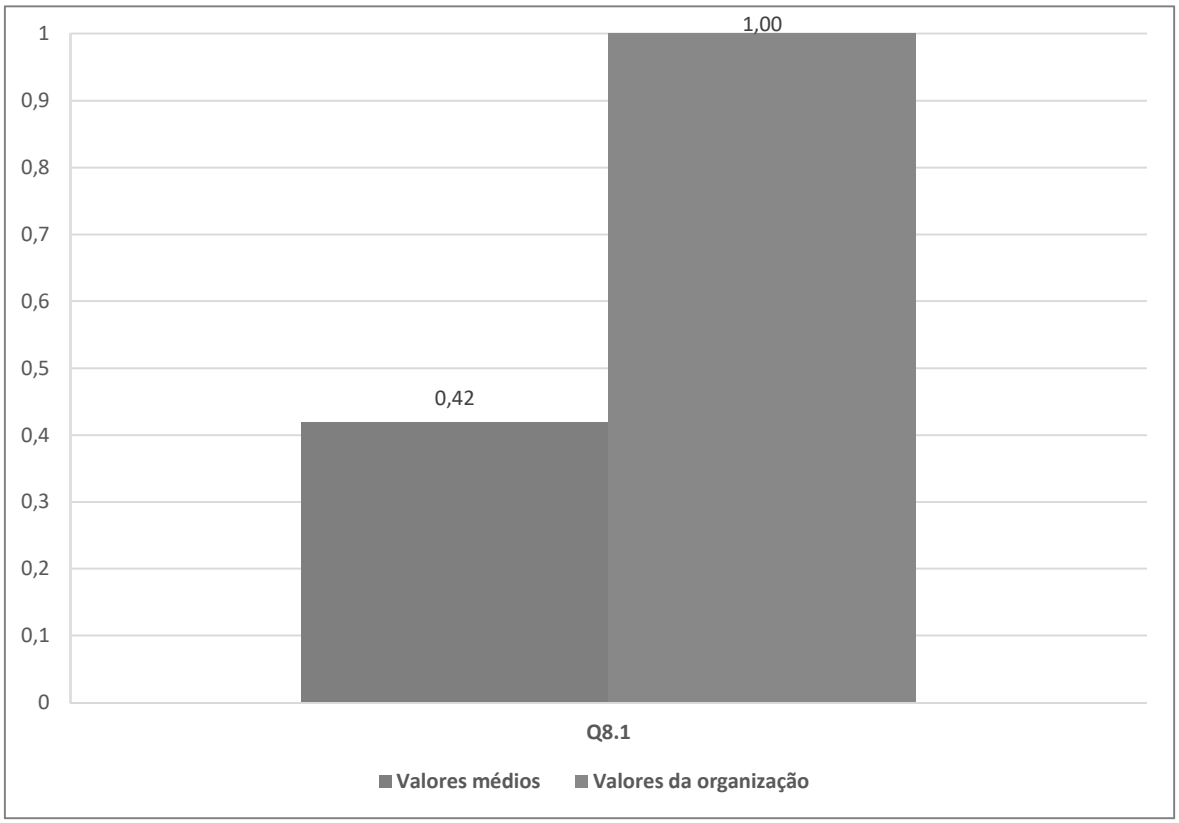
Na Tabela 8 é apresentada a questão desta dimensão que compõe o indicador de adequação à LGPD, possibilitando comparar o valor da própria organização e o valor médio do conjunto das 382 organizações avaliadas.

Tabela 8 - Compartilhamento de Dados Pessoais

Questão	Valor da organização	Valor médio
8.1 A organização identificou os dados pessoais que são compartilhados com terceiros?	1,00	0,42

O gráfico da Figura 10 possibilita comparar visualmente o valor da questão desta dimensão que foi calculado para a organização relativamente ao valor médio calculado ao se considerar o conjunto das 382 organizações avaliadas.

Figura 10 - Valor da organização e valor médio na dimensão "Compartilhamento de Dados Pessoais"



2.8 Violação de Dados Pessoais

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

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

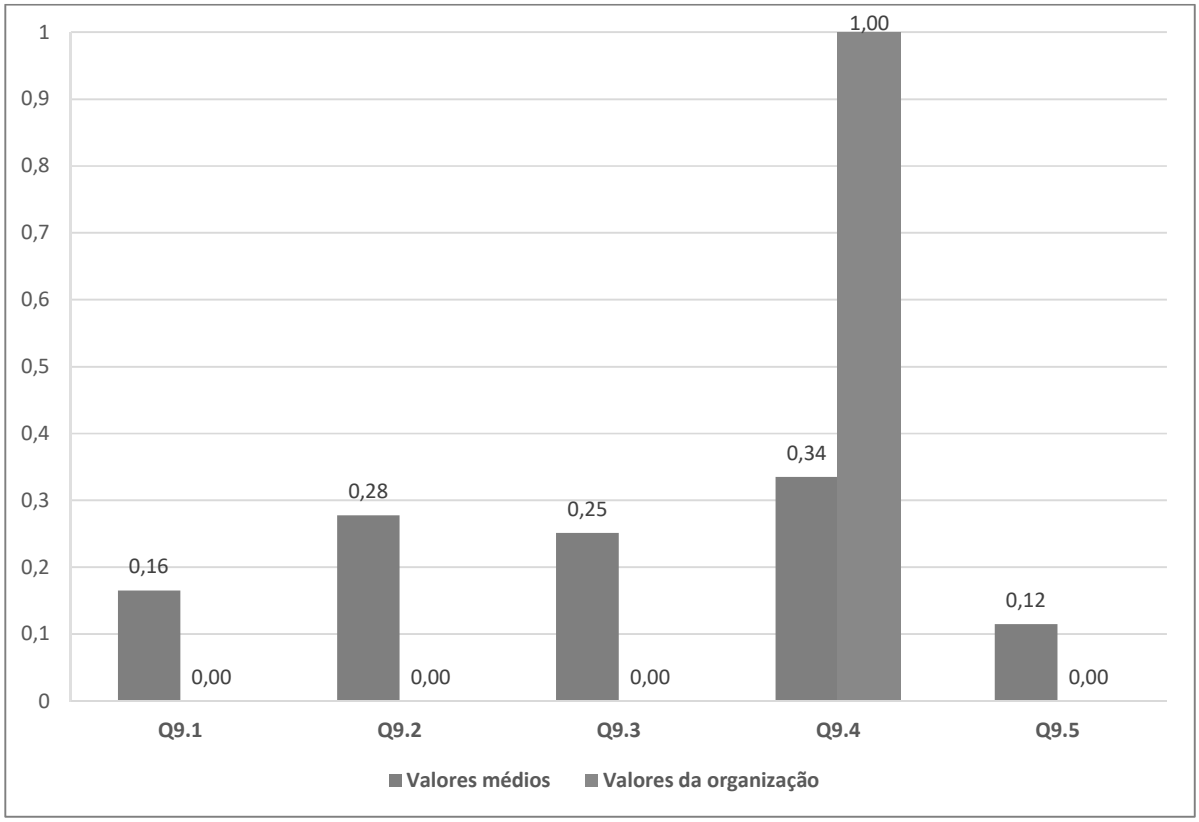
Na Tabela 9 são apresentadas as questões desta dimensão que compõem o indicador de adequação à LGPD, possibilitando comparar os valores da própria organização e os valores médios do conjunto das 382 organizações avaliadas.

Tabela 9 - Violação de Dados Pessoais

Questões	Valores da organização	Valores médios
9.1 A organização possui Plano de Resposta a Incidentes (ou documento similar) que abrange o tratamento de incidentes que envolvem violação de dados pessoais?	0,00	0,16
9.2 A organização possui sistema para o registro de incidentes de segurança da informação que envolvem violação de dados pessoais?	0,00	0,28
9.3 A organização possui sistema para registro das ações adotadas para solucionar incidentes de segurança da informação que envolvem violação de dados pessoais?	0,00	0,25
9.4 A organização monitora proativamente a ocorrência de eventos que podem ser associados à violação de dados pessoais?	1,00	0,34
9.5 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?	0,00	0,12

O gráfico da Figura 11 possibilita comparar visualmente os valores das questões desta dimensão que foram calculados para a organização relativamente aos valores médios calculados ao se considerar o conjunto das 382 organizações avaliadas.

Figura 11 - Valores da organização e valores médios na dimensão "Violação de Dados Pessoais"



2.9 Medidas de Proteção

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.

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.

Na Tabela 10 são apresentadas as questões desta dimensão que compõem o indicador de adequação à LGPD, possibilitando comparar os valores da própria organização e os valores médios do conjunto das 382 organizações avaliadas.

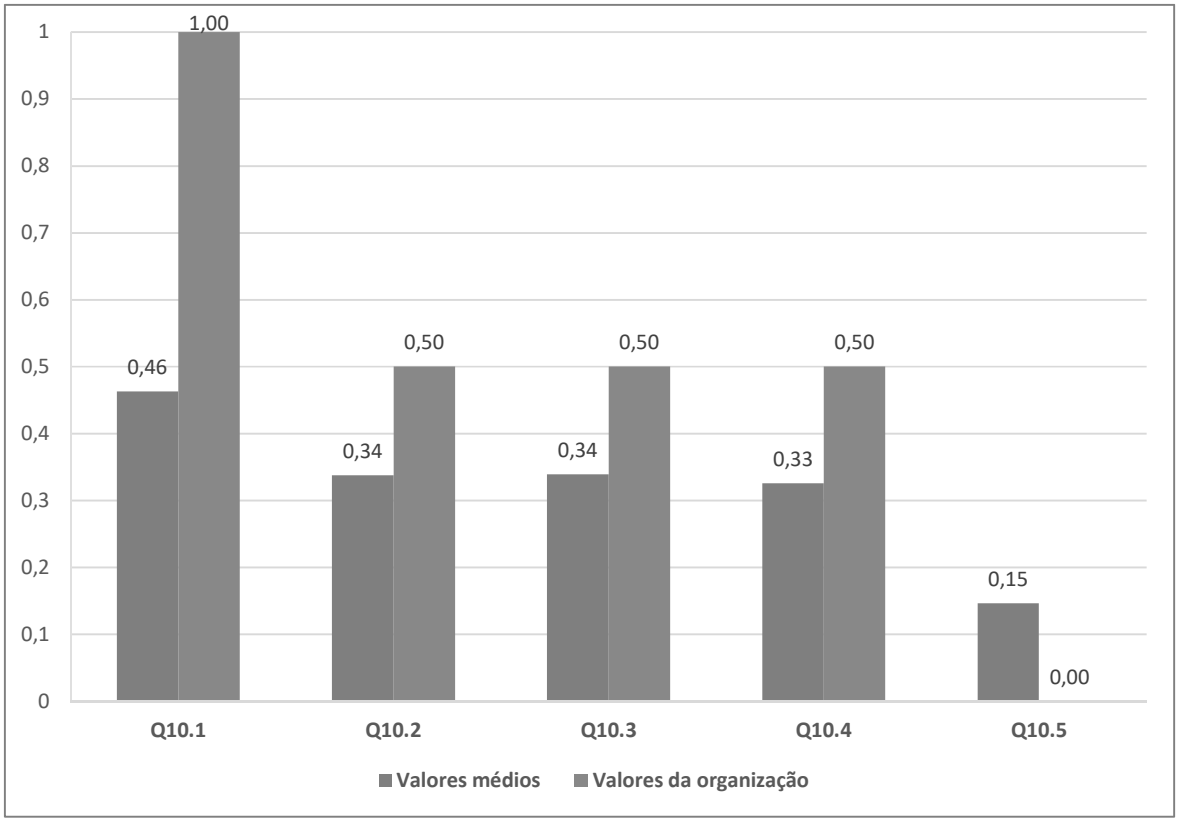
Tabela 10 - Medidas de Proteção

Questões	Valores da organização	Valores médios
10.1 A organização é capaz de comprovar que adotou medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais?	1,00	0,46
10.2 A organização implementou processo para registro, cancelamento e provisionamento de usuários em sistemas que realizam tratamento de dados pessoais?	0,50	0,34
10.3 A organização registra eventos das atividades de tratamento de dados pessoais?	0,50	0,34
10.4 A organização utiliza criptografia para proteger os dados pessoais?	0,50	0,33

10.5 A organização adotou medidas para assegurar que processos e sistemas sejam projetados, desde a concepção, em conformidade com a LGPD (*Privacy by Design e Privacy by Default*)?	0,00	0,15

O gráfico da Figura 12 possibilita comparar visualmente os valores das questões desta dimensão que foram calculados para a organização relativamente aos valores médios calculados ao se considerar o conjunto das 382 organizações avaliadas.

Figura 12 - Valores da organização e valores médios na dimensão "Medidas de Proteção"



3 Respostas ao questionário

1. Identificação do respondente

2. Preparação

2.1 A organização conduziu iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD?

Parcialmente (a organização iniciou, mas ainda não concluiu iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD).

Referência(s): Lei 13.709/2018, art. 50, § 2º, inciso I. ABNT NBR ISO/IEC 27.701/2019, item 5.4.

A organização deve conduzir iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD.
Um exemplo de iniciativa pode ser a instituição de comitê ou grupo de trabalho.

É importante que a iniciativa conte com o apoio ou, até mesmo, com a participação direta da alta direção da organização. Ademais, convém que sejam envolvidas pessoas pertencentes a unidades que exercem atividades relevantes para o tratamento de dados pessoais (*e.g.*: Segurança da Informação, Tecnologia da Informação, Direito, Auditoria/Conformidade e Ouvidoria).
Um exemplo de artefato que pode ser produzido pela iniciativa é o plano de ação.

2.2 A organização elaborou plano de ação, plano de projeto ou documento similar para direcionar a iniciativa de adequação à LGPD?

Sim

Referência(s): Lei 13.709/2018, art. 50, § 2º, inciso I. ABNT NBR ISO/IEC 27.701/2019, item 5.4.

A organização deve documentar informações relacionadas aos objetivos da iniciativa de adequação e às ações necessárias para alcançá-los.

3. Contexto organizacional

3.1 A organização conduziu iniciativa para identificar outros normativos (e.g.: leis, regulamentos e instruções normativas), além da LGPD, que abrangem comandos relacionados à proteção de dados pessoais e que também devem ser respeitados?

Sim

Referência(s): ABNT NBR ISO/IEC 27.701/2019, item 5.2.1.

Além da LGPD, há outros normativos que abordam o tratamento de dados pessoais e que também devem ser respeitados por determinadas organizações.
O Código de Defesa do Consumidor, a Lei do Cadastro Positivo, a Consolidação das Leis Trabalhistas (CLT), a Lei de Acesso à Informação e a Lei 13.787/2018 (que dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente) são alguns exemplos desses normativos.

3.2 A organização identificou as categorias de titulares de dados pessoais com os quais se relaciona?

Parcialmente (algumas categorias de titulares de dados pessoais foram identificadas).

Referência(s): Lei 13.709/2018, art. 5º, inciso V. ABNT NBR ISO/IEC 27.701/2019, itens 6.5.2 e 7.2.8.

Convém que a organização identifique as partes interessadas que possuem interesses ou responsabilidades associados ao tratamento de dados pessoais, o que pode abranger, por exemplo: titulares de dados pessoais, operadores e controladores conjuntos.

O titular é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. Os titulares podem ser enquadrados em diferentes categorias como: cidadão, cliente, servidor público, representante de fornecedor e terceirizado.

3.3 A organização conduziu iniciativa para identificar os operadores que realizam tratamento de dados pessoais em seu nome?

Sim (a iniciativa foi concluída e todos os operadores foram identificados).

Referência(s): Lei 13.703/2018, art. 5º, incisos VI e VII. ABNT NBR ISO/IEC 27.701/2019, item 5.2.2.

Convém que a organização identifique as partes interessadas que possuem interesses ou responsabilidades associados ao tratamento de dados pessoais, o que pode abranger, por exemplo: titulares de dados pessoais, operadores e controladores conjuntos.
O operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, 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.

3.3.1 A organização adequou os contratos firmados com os operadores identificados de forma a estabelecer suas responsabilidades e papéis com relação à proteção de dados pessoais?

Parcialmente (A organização adequou os contratos firmados com alguns operadores que foram identificados).

Referência(s): Lei 13.709/2018, art. 39; arts. 42-46. ABNT NBR ISO/IEC 27.701/2019, item 7.2.6.

O controlador deve ter contrato firmado com os operadores de dados pessoais para assegurar que estes adotem medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais que são compartilhados com eles.

3.4 A organização avaliou se há tratamento de dados que envolva controlador conjunto?

Sim

Referência(s): Lei 13.709/2018, art. 5º, inciso VI; art. 7º, § 5º. ABNT NBR ISO/IEC 27.701/2019, itens 5.2.2 e 7.2.7.

Convém que a organização identifique as partes interessadas que possuem interesses ou responsabilidades associados ao tratamento de dados pessoais, o que pode abranger, por exemplo: titulares de dados pessoais, operadores e controladores conjuntos.
O controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Por sua vez, controlador conjunto é o controlador de dados pessoais que determina os propósitos e as formas do tratamento de dados pessoais junto com outro(s) controlador(es).

3.4.1 Caso exista controlador conjunto, os papéis e responsabilidades de cada um dos controladores estão definidos em contrato, acordo de cooperação ou instrumento similar?

Não se aplica (não há relação da organização com controlador conjunto).

Referência(s): Lei 13.709/2018, arts. 42-45. ABNT NBR ISO/IEC 27.701/2019, item 7.2.7.

É conveniente que a organização estabeleça formalmente os papéis e as responsabilidades de cada controlador caso haja controlador conjunto.
Caso não haja tratamento de dados que envolva controlador conjunto, assinale a alternativa "não se aplica".

3.5 A organização identificou os processos de negócio que realizam tratamento de dados pessoais?

Parcialmente (alguns processos de negócio que realizam tratamento de dados pessoais foram identificados).

Referência(s): Lei 13.709/2018, art. 37. ABNT NBR ISO/IEC 27.701/2019, item 7.2.8.

O tratamento de dados pessoais envolve toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento,

arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

3.5.1 A organização identificou quem são os responsáveis pelos processos de negócio que realizam tratamento de dados pessoais e que já foram identificados?

Parcialmente (a organização identificou os responsáveis por alguns dos processos de negócio que realizam tratamento de dados pessoais e que já foram identificados).

Referência(s): Lei 13.709/2018, art. 37. ABNT NBR ISO/IEC 27.701/2019, item 7.2.8.

Os responsáveis pelo tratamento de dados pessoais podem abranger, por exemplo, pessoas, departamentos, operadores e controlador(es) conjunto(s).

3.6 A organização identificou quais são os dados pessoais tratados por ela?

Parcialmente (alguns dados pessoais tratados pela organização foram identificados).

Referência(s): Lei 13.709/2018, art. 5º, inciso I; art. 37. ABNT NBR ISO/IEC 27.701/2019, itens 6.5.2 e 7.2.8.

O dado pessoal é uma informação relacionada à pessoa natural identificada ou identificável, como nome, RG e CPF.

3.6.1 A organização identificou os locais onde os dados pessoais identificados são armazenados?

Sim (a organização identificou os locais onde são armazenados todos os dados pessoais que já foram identificados).

Referência(s): Lei 13.709/2018, art. 5º, inciso I; art. 37. ABNT NBR ISO/IEC 27.701/2019, itens 6.5.1 e 7.2.8.

Os dados pessoais podem ser armazenados em ativos de TI (e.g.: servidor de arquivos, nuvem, dispositivo USB, storage, fita de backup) ou em arquivos físicos (e.g.: pastas e armários). As organizações também devem identificar o local (endereço) onde se encontram os dados.

3.7 A organização avaliou os riscos dos processos de tratamento de dados pessoais que foram identificados?

Sim

Critério(s): Lei 13.709/2018, art. 50, § 1º e § 2º, inciso I, alínea "d". ABNT NBR ISO/IEC 27.701/2019, item 5.4.1.2.

A organização deve avaliar os riscos associados aos processos que realizam tratamento de dados pessoais.
Essa avaliação auxilia a organização a compreender as consequências e as probabilidades dos riscos para direcionar a definição de quais processos devem ser priorizados na iniciativa de adequação à LGPD.

4. Liderança

4.1 A organização possui Política de Segurança da Informação ou instrumento similar?

Sim

Referência(s): Lei 13.709/2018, art. 46; art. 50, § 2º, inciso I, alíneas "a" e "d". ABNT NBR ISO/IEC 27.701/2019, itens 5.3.2 e 6.2.

Uma Política de Segurança da Informação estabelece a abordagem da organização para gerenciar os objetivos de segurança da informação. A referida política deve ser aprovada pela alta direção e estar de acordo com os requisitos de negócio e com leis e regulamentações aplicáveis.

4.2 A organização possui Política de Classificação da Informação ou instrumento similar?

Sim

Referência(s): Lei 13.709/2018, art. 46; art. 50, § 2º, inciso I, alíneas "a" e "d". ABNT NBR ISO/IEC 27.701/2019, item 6.5.2.
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 para a organização.

4.2.1 A Política de Classificação da Informação (ou instrumento similar) abrange diretrizes para a classificação de dados pessoais?

Sim

Referência(s): Lei 13.709/2018, art. 46; art. 50, § 2º, inciso I, alíneas "a" e "d". ABNT NBR ISO/IEC 27.701/2019, item 6.5.2.

A Política de Classificação da Informação deve considerar a classificação de dados pessoais para viabilizar a identificação de quais desses dados são tratados pela organização, o que é importante para direcionar a implementação de controles adequados para a proteção de dados pessoais.

4.2.1.1 A Política de Classificação da Informação (ou instrumento similar) abrange diretrizes para identificar dados pessoais sensíveis e relacionados a crianças e adolescentes?

Não

Referência(s): Lei 13.709/2018, art. 5º, inciso II; art. 46; art. 50, § 2º, inciso I, alíneas "a" e "d". ABNT NBR ISO/IEC 27.701/2019, item 6.5.2.2.

O dado pessoal sensível é o 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.
A LGPD demanda que sejam adotados cuidados específicos para o tratamento de dados pessoais sensíveis.

4.2.1.2 A Política de Classificação da Informação (ou instrumento similar) abrange diretrizes para identificar dados pessoais de crianças e de adolescentes?

Não

Referência(s): Lei 13.709/2018, art. 14; art. 46; art. 50, § 2º, inciso I, alíneas "a" e "d". ABNT NBR ISO/IEC 27.701/2019, item 6.5.2.2.

A LGPD demanda que sejam adotados cuidados específicos para o tratamento de dados pessoais de crianças e de adolescentes.

4.3 A organização possui Política de Proteção de Dados Pessoais (ou instrumento similar)?

Não

Referência(s): Lei 13.709/2018, art. 46; art. 50, § 2º, inciso I, alíneas "a" e "d". ABNT NBR ISO/IEC 27.701/2019, itens 6.2.1.

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 provê apoio e comprometimento da organização para alcançar a conformidade com os normativos de proteção de dados pessoais.
A Política de Proteção de Dados Pessoais pode ser definida e publicada em documento específico ou incluída no texto da Política de Segurança da Informação já existente.
Vale ressaltar que a Política de Proteção de Dados Pessoais não se confunde com a Política de Privacidade. Enquanto a primeira é voltada para o público interno da organização, a segunda é direcionada para o público externo (e.g.: titulares de dados pessoais).

4.4 A organização nomeou o encarregado pelo tratamento de dados pessoais?

Sim

Referência(s): Lei 13.709/2018, art. 5º, inciso VIII; art. 41. IN SGD/ME 117/2020. ABNT NBR ISO/IEC 27.701/2019, item 6.3.1.

O encarregado é a pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).
O termo DPO (*Data Protection Officer*) é comumente utilizado para se referir ao encarregado.
Convém que o encarregado possua, além de profundo conhecimento da Lei 13.709/2018, conhecimentos relativos a temas como: Direito, Governança Corporativa, Gestão de Riscos, Tecnologia da Informação e Segurança da Informação.

4.4.1 A nomeação do encarregado foi publicada em veículo de comunicação oficial?

Sim

Referência(s): Lei 13.709/2018, art. 5º, inciso VIII; art. 41. IN SGD/ME 117/2020, art 2º. ABNT NBR ISO/IEC 27.701/2019, item 6.3.1.

A organização deve designar oficialmente o encarregado. Diante disso, é conveniente que a nomeação do encarregado seja publicada em veículo de comunicação oficial como o Diário Oficial da União (DOU).

4.4.2 Em qual setor da organização está lotado o encarregado?

Outros

Referência(s): Lei 13.709/2018, art. 5º, inciso VIII; art. 41. IN SGD/ME 117/2020, art 1º, § 1º, inciso II. ABNT NBR ISO/IEC 27.701/2019, item 6.3.1.

O encarregado deve ser independente e ter liberdade para reportar à alta administração. É recomendável que o encarregado não faça parte de um setor no qual possa haver conflito de interesses.

4.4.3 A identidade e as informações de contato do encarregado foram divulgadas na internet?

Sim

Referência(s): Lei 13.709/2018, art. 5º, inciso VIII; art. 41, § 1º. IN SGD/ME 117/2020, art 2º. ABNT NBR ISO/IEC 27.701/2019, item 6.3.1.

A identidade e as informações de contato (*e.g.*: e-mail, telefone) do encarregado devem ser divulgadas publicamente, preferencialmente no sítio eletrônico da organização.

5. Capacitação

5.1 A organização possui Plano de Capacitação (ou instrumento similar) que abrange treinamento e conscientização dos seus colaboradores em proteção de dados pessoais?

Não

Referência(s): ABNT NBR ISO/IEC 27.701/2019, itens 5.5.2, 5.5.3 e 5.5.4.

É conveniente que a organização elabore um Plano de Capacitação que determine as competências necessárias para os recursos humanos envolvidos em atividades que realizam o tratamento de dados pessoais. O Plano de Capacitação deve mapear as lacunas de conhecimento associadas ao tema, bem como planejar ações de treinamento para redução dessas lacunas.
Ademais, é necessário que todas as pessoas da organização estejam cientes da importância do tema proteção de dados pessoais e dos impactos que podem ser causados devido à violação desses dados.
Diante disso, é importante que o plano de capacitação também contemple ações de conscientização.
Nada impede que a organização elabore um plano de conscientização apartado de um plano de treinamento.

5.1.1 O Plano de Capacitação (ou instrumento similar) considera que pessoas que exercem funções com responsabilidades essenciais relacionadas à proteção de dados pessoais devem receber treinamento diferenciado?

Não aplicável

Referência(s): ABNT NBR ISO/IEC 27.701/2019, itens 5.5.2, 5.5.3 e 5.5.4.

Por exemplo, recursos humanos envolvidos em atividades críticas relacionadas ao tratamento de dados pessoais devem receber treinamento além do nível básico fornecido aos demais colaboradores.

5.2. Colaboradores da organização que estão diretamente envolvidos em atividades que realizam tratamento de dados pessoais receberam treinamentos relacionados ao tema?

Sim (todos os colaboradores da organização que estão diretamente envolvidos em atividades que realizam tratamento de dados pessoais receberam treinamentos relacionados ao tema).

Referência(s): ABNT NBR ISO/IEC 27.701/2019, itens 5.5.2, 5.5.3 e 5.5.4.

Diante da vigência da LGPD, é conveniente que os colaboradores envolvidos diretamente em atividades que realizam o tratamento de dados pessoais já tenham participado de treinamentos correlatos ao tema.

6. Conformidade do tratamento

6.1 A organização identificou e documentou as finalidades das atividades de tratamento de dados pessoais?

Sim (todas as finalidades das atividades de tratamento de dados pessoais foram identificadas e documentadas).

Referência(s): Lei 13.709/2018, art. 6º, inciso I. ABNT NBR ISO/IEC 27.701/2019, item 7.2.1.

As atividades de tratamento de dados pessoais devem ter propósitos legítimos, específicos, explícitos e informados ao titular.
A organização deve assegurar que os titulares de dados pessoais entendam a(s) finalidade(s) pelas quais os seus dados pessoais são tratados.

6.1.1 A organização avaliou se coleta apenas os dados estritamente necessários para cumprir com as finalidades de tratamento de dados pessoais que foram identificadas?

Sim

Referência(s): Lei 13.709/2018, art. 6º, incisos II e III. ABNT NBR ISO/IEC 27.701/2019, item 7.4.1.

Os dados pessoais coletados devem se limitar ao que é estritamente necessário para cumprir com as finalidades de tratamento.

6.1.2 A organização avaliou 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?

Sim

Referência(s): Lei 13.709/2018, art. 40. ABNT NBR ISO/IEC 27.701/2019, item 7.4.7.

A organização não deve reter dados pessoais por tempo maior do que o estritamente necessário.

6.2 A organização identificou e documentou as bases legais que fundamentam as atividades de tratamento de dados pessoais?

Sim (as bases legais que fundamentam todas as atividades de tratamento de dados pessoais da organização foram definidas e documentadas).

Referência(s): Lei 13.709/2018 art. 7º. ABNT NBR ISO/IEC 27.701/2019, item 7.2.2.

A organização deve determinar e documentar as bases legais que fundamentam as atividades de tratamento de dados pessoais.

As bases legais são relacionadas no art. 7º da Lei 13.709/2018: consentimento; cumprimento de obrigação legal ou regulatória; execução de políticas públicas pela Administração Pública; estudos por órgão de pesquisa; execução de contrato; exercício regular de direitos em processo judicial, administrativo ou arbitral; proteção da vida ou da incolumidade física; tutela da saúde; interesse legítimo; e proteção do crédito.

6.3 Há um registro (*e.g.*: inventário) instituído para consolidar informações relacionadas às características das atividades de tratamento de dados pessoais?

Sim

Referência(s): Lei 13.709/2018, art. 37. ABNT NBR ISO/IEC 27.701/2019, item 7.2.8.

Uma maneira de reter os registros das características das atividades de tratamento de dados pessoais é por meio de um inventário, o qual pode contemplar, por exemplo: finalidade do tratamento; base legal que fundamenta o tratamento; descrição das categorias dos titulares de dados pessoais envolvidos no tratamento; dados pessoais coletados; tempo de retenção dos dados; local de armazenamento dos dados; responsável pelo processo de tratamento; e medidas de segurança adotadas.

6.4 A organização elaborou Relatório de Impacto à Proteção de Dados Pessoais?

Não.

Referência(s): Lei 13.709/2018, art. 5º, inciso XVII; art. 38. ABNT NBR ISO/IEC 27.701/2019, item 7.2.5.

O Relatório de Impacto à Proteção de Dados Pessoais é uma documentação do controlador que contempla a descrição dos processos de tratamento de dados pessoais que podem gerar riscos aos titulares e das medidas adotadas para tratamento desses riscos.
O relatório deve conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise da organização quanto às medidas, salvaguardas e mecanismos de mitigação de riscos.

6.4.1 A organização implementou controles para mitigar os riscos identificados por meio da elaboração do Relatório de Impacto de Proteção de Dados Pessoais?

Não aplicável

Referência(s): Lei 13.709/2018, art. 5º, inciso XVII; art. 38. ABNT NBR ISO/IEC 27.701/2019, item 7.2.5.

A organização deve adotar medidas para tratar os riscos identificados por meio da avaliação de impacto sobre a proteção de dados pessoais.

7. Direitos do titular

7.1 A organização possui Política de Privacidade (ou instrumento similar)?

Não

Referência(s): Lei 13.709/2018, art. 6º, inciso VI; art. 9º; art. 23, inciso I; art. 50, inciso I, alíneas "a", "d" e "e". ABNT NBR ISO/IEC 27.701/2019, itens 7.3.2 e 7.3.3.

A Política de Privacidade deve documentar e comunicar aos titulares de dados pessoais, de maneira clarae concisa, informações relativas ao tratamento de seus dados pessoais.
A LGPD exemplifica informações que devem constar no referido artefato: as finalidades dos tratamentos; as formas e as durações dos tratamentos; a identificação e os dados de contato do controlador; as informações acerca do uso compartilhado de dados; as responsabilidades dos agentes que realizam os tratamentos; e os direitos do titular.
Além disso, o Poder Público deve informar as hipóteses em que, no exercício de suas competências, realiza tratamento de dados pessoais, fornecendo informações sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades.
O termo "Aviso de Privacidade" é comumente utilizado para se referir à Política de Privacidade.

7.1.1 A Política de Privacidade (ou instrumento similar) está publicada na internet?

Não aplicável

Referência(s): Lei 13.709/2018, art. 6º, inciso VI; art. 9º; art. 50, inciso I, alínea "e". ABNT NBR ISO/IEC 27.701/2019, item 7.3.3.

A Política de Privacidade deve ser publicada em local facilmente acessível pelos titulares de dados pessoais. Além de fornecer acesso à política no momento da coleta dos dados pessoais, convém que a organização forneça acesso ao artefato de forma permanente no sítio institucional.

7.1.1.1 Favor informar o endereço da internet (URL) onde a política está publicada:

Não aplicável

7.2 Foram implementados mecanismos para atender os direitos dos titulares elencados no art. 18 da LGPD e aplicáveis à organização?

Parcialmente (foram implementados mecanismos para atender alguns direitos dos titulares elencados no art. 18 da LGPD e aplicáveis à organização).

Referência(s): Lei 13.709/2018, art. 17-22. ABNT NBR ISO/IEC 27.701/2019, item 7.3.

Quando aplicável, a organização deve atender aos direitos dos titulares estabelecidos no art.18 da LGPD como, por exemplo: confirmação da existência de tratamento; acesso aos dados; e correção de dados.

8. Compartilhamento de dados pessoais

8.1 A organização identificou os dados pessoais são compartilhados com terceiros?

Sim (os dados pessoais que são compartilhados com terceiros foram identificados).

Referência(s): Lei 13.709/2018, art. 5º, inciso XVI; arts. 26-27; art. 39. ABNT NBR ISO/IEC 27.701/2019, item 7.5.3 e 7.5.4.

É conveniente que a organização tenha documentado quais os dados pessoais que são compartilhados com terceiros.

8.1.1 Os compartilhamentos de dados pessoais identificados estão em conformidade com os critérios estabelecidos na LGPD?

Parcialmente (alguns compartilhamentos de dados pessoais estão em conformidade com os critérios estabelecidos na LGPD).

Referência(s): Lei 13.709/2018, art. 5º, inciso XVI; arts. 26-27; art. 39. ABNT NBR ISO/IEC 27.701/2019, item 7.5.3 e 7.5.4.

Os compartilhamentos de dados pessoais devem respeitar os critérios estabelecidos na LGPD. Diante disso, os casos de compartilhamento devem ser avaliados para que sejam efetuados os devidos ajustes.
O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal e respeitar os princípios elencados no art. 6º da LGPD.
Ademais, há a necessidade de que os contratos e convênios que impliquem uso compartilhado, transferência ou comunicação de dados pessoais com entidades privadas sejam objeto de comunicação à ANPD.

8.1.2 A organização registra eventos relacionados à transferência dos dados pessoais que são compartilhados com terceiros e que foram identificados?

Parcialmente (a organização registra eventos relacionados à transferência de alguns dados pessoais que são compartilhados com terceiros e que foram identificados).

Referência(s): Lei 13.709/2018, art. 5º, inciso XVI; arts. 26-27; art. 39. ABNT NBR ISO/IEC 27.701/2019, item 7.5.4.

É conveniente que a organização tenha registros de quais dados foram compartilhados, com quem foram compartilhados e quando foram compartilhados.

8.1.3 Algum caso de compartilhamento envolve transferência internacional de dados pessoais?

A organização ainda não verificou se há caso de compartilhamento que envolva transferência internacional de dados pessoais.

Referência(s): Lei 13.709/2018, arts 33-36. ABNT NBR ISO/IEC 27.701/2019, item 7.5.1 e 7.5.2.

A LGPD relaciona os casos nos quais é permitida a transferência internacional de dados pessoais. Diante disso, é conveniente que a organização identifique os casos em que isso ocorre para avaliar se estão em conformidade com as hipóteses estabelecidos na lei.

8.1.3.1 As transferências internacionais de dados pessoais estão de acordo com os casos previstos na LGPD?

Não aplicável

Referência(s): Lei 13.709/2018, arts. 33-36. ABNT NBR ISO/IEC 27.701/2019, item 7.5.2.

A organização deve avaliar se a transferência internacional de dados pessoais se enquadra em um dos casos previstos no art. 33 da LGPD.

9. Violação de dados pessoais

9.1 A organização possui Plano de Resposta a Incidentes (ou documento similar) que abrange o tratamento de incidentes que envolvem violação de dados pessoais?

Não

Referência(s): Lei 13.709/2018, art. 50, § 2º, inciso I, alínea "g". ABNT NBR ISO/IEC 27.701/2019, item 6.13.1.1.

Como parte do processo de gestão de incidentes de segurança da informação global, é conveniente que a organização estabeleça responsabilidades e procedimentos para assegurar respostas rápidas, efetivas e ordenadas a incidentes que envolvem violação de dados pessoais.

9.2 A organização possui sistema para o registro de incidentes de segurança da informação que envolvem violação de dados pessoais?

Não

Referência(s): Lei 13.709/2018, art. 50, § 2º, inciso I, alínea "g". ABNT NBR ISO/IEC 27.701/2019, item 6.13.1.1.

Convém que a organização possua um sistema de informação de gestão de incidentes que viabiliza o tratamento de casos que envolvem violação de dados pessoais. Essa gestão inclui o registro dos incidentes.

9.3 A organização possui sistema para registro das ações adotadas para solucionar incidentes de segurança da informação que envolvem violação de dados pessoais?

Não

Referência(s): Lei 13.709/2018, art. 50, § 2º, inciso I, alínea "g". ABNT NBR ISO/IEC 27.701/2019, item 6.13.1.5.

Convém que a organização possua sistema para o registro das ações adotadas para solucionar os incidentes que envolvem violação de dados pessoais. O tratamento de incidentes pode envolver, primeiramente, a adoção de solução de contorno para, posteriormente, haver análise e erradicação da causa.

9.4 A organização monitora proativamente a ocorrência de eventos que podem ser associados à violação de dados pessoais?

Sim

Referência(s): Lei 13.709/2018, art. 50, § 2º, inciso I, alínea "g". ABNT NBR ISO/IEC 27.701/2019, itens 6.13.1.4 e 6.13.1.5.

Convém que a organização adote mecanismo para monitorar proativamente os eventos de segurança da informação que são associados à violação de dados pessoais para adotar medidas necessárias caso ocorram.
A identificação precoce de incidentes pode diminuir significativamente os impactos causados por eles.

9.5 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?

Não

Referência(s): Lei 13.709/2018, art. 48. ABNT NBR ISO/IEC 27.701/2019, item 6.13.1.5.

A organização deve comunicar à ANPD e ao titular a ocorrência de incidente de segurança da informação que possa acarretar risco ou dano relevante aos titulares. A notificação 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. Caso a organização não encaminhe a comunicação tempestivamente, deverá ser exposto, também, os motivos que levaram à demora.

10. Medidas de proteção

10.1 A organização é capaz de comprovar que adotou medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais?

Sim

Referência(s): Lei 13.709/2018, art. 46. ABNT NBR ISO/IEC 27.002/2013, item 6.1.

A organização deve 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.

10.2 A organização implementou processo para registro, cancelamento e provisionamento de usuários em sistemas que realizam tratamento de dados pessoais?

Parcialmente (a organização implementou processo formal para registro, cancelamento e provisionamento de usuários em alguns sistemas que realizam tratamento de dados pessoais).

Referência(s): Lei 13.709/2018, art. 46. ABNT NBR ISO/IEC 27.701/2019, itens 6.6.2.1 e 6.6.2.2.

Convém que a organização defina processo formal para registro e cancelamento de usuários para viabilizar a atribuição dos direitos de acesso aos sistemas que realizam tratamento de dados pessoais.
O mesmo deve ser feito com o processo de provisionamento para conceder ou revogar os direitos de acesso dos usuários nesses sistemas.
Convém que a concessão de direitos de acesso observe os princípios de "necessidade de conhecer" e "necessidade de uso".

10.3 A organização registra eventos das atividades de tratamento de dados pessoais?

Parcialmente (a organização registra os eventos de algumas atividades de tratamento de dados pessoais).

Referência(s): Lei 13.709/2018, art. 46. ABNT NBR ISO/IEC 27.701/2019, item 6.9.4.1.

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).

10.4 A organização utiliza criptografia para proteger os dados pessoais?

Parcialmente (a organização utiliza criptografia para proteger alguns dados pessoais).

Referência(s): Lei 13.709/2018, art. 46; art. 50, § 2º, inciso I, alínea "c". ABNT NBR ISO/IEC 27.701/2019, item 6.7.

A utilização de criptografia pode proteger a confidencialidade, a autenticidade e/ou a integridade da informação. Por exemplo, devido à criticidade dos dados sensíveis, a adoção de mecanismos para criptografá-los em trânsito e no armazenamento pode mitigar riscos associados à violação de dados pessoais.

10.5 A organização adotou medidas para assegurar que processos e sistemas sejam projetados, desde a concepção, em conformidade com a LGPD (*Privacy by Design e Privacy by Default*)?

Não

Referência(s): Lei 13.709/2018, art. 46, § 2º. ABNT NBR ISO/IEC 27.701/2019, item 7.4.

A organização deve assegurar que os processos e sistemas sejam projetados de forma que os tratamentos de dados pessoais estejam limitados ao que é estritamente necessário para alcance da finalidade pretendida.