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