RELATÓRIO DE FISCALIZAÇÃO

TC n. 009.980/2024-5 **Fiscalização n.** 96/2024

Relator: Walton Alencar Rodrigues

DA FISCALIZAÇÃO

Modalidade: Conformidade

Ato originário: Acórdão 889/2024 - Plenário

Objeto da fiscalização: Controles implementados para adequação à LGPD

Ato de designação: Portaria de designação-planejamento - Audti 268/2024, de 20/05/2024 (peça 3)
Portaria de alteração - Audti 15/2025, de 22/01/2025 (peça 947)

Período abrangido pela fiscalização: De 27/05/2024 a 14/11/2024

Composição da equipe: Regis Soares Machado - matr. 7688-0 (Coordenador)
Fernando Pereira de Faria - matr. 8118-3
Sylvio Xavier Júnior - matr. 2423-6

DO ÓRGÃO/ENTIDADE FISCALIZADO

Órgãos/entidades fiscalizados: Presidência da República, Conselho Nacional de Justiça, Conselho Nacional do Ministério Público, Câmara dos Deputados, Ministério da Gestão e da Inovação em Serviços Públicos, Controladoria-Geral da União, Supremo Tribunal Federal, Tribunal de Contas da União, Autoridade Nacional de Proteção de Dados e Senado Federal

Vinculação TCU (unidade técnica): Unidade de Auditoria Especializada em Gestão do Estado e Inovação

Responsável pelo órgão/entidade:

nome: Miriam Aparecida Belchior
cargo: Secretária-Executiva da Casa Civil da Presidência da República
período: A partir de 01/01/2023

Outros responsáveis: vide peça: “Rol de responsáveis”

PROCESSOS CONEXOS

- TC 013.140/2022-1
- TC 039.606/2020-1

Resumo

O que e por que o TCU fiscalizou?

A Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) 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. Essa lei entrou em vigor em agosto de 2020 e, aproximadamente um ano depois, o Tribunal de Contas da União (TCU) constatou que 76,7% das organizações públicas federais permaneciam nos graus inexpressivo ou inicial de adequação àquela lei[1] (TC 039.606/2020-1; Acórdão 1.384/2022-TCU-Plenário, Rel. Min. Augusto Nardes).

Passados cerca de dois anos, ao concluir-se o monitoramento do Acórdão 1.384/2022-TCU-Plenário (TC 013.140/2022-1; Acórdão 1.563/2024-TCU-Plenário, Rel. Min. Augusto Nardes), percebeu-se ter havido evolução na situação inicialmente encontrada. Dessa forma, o presente momento mostrava-se oportuno para a realização de nova ação de controle, com vistas a verificar a evolução do cumprimento da legislação pelos órgãos e entidades da Administração Pública Federal (APF), o que foi feito a partir da aplicação de um questionário de autoavaliação de controles internos (do inglês *Control Self-Assessment* – CSA) a 387 organizações públicas federais, no qual os gestores informaram a situação atual dos respectivos entes com relação à implementação de medidas para assegurar a conformidade com a LGPD, anexando as evidências correspondentes, quando solicitado.

De acordo com previsão incluída na Ação 29 do Plano Anual de Trabalho (PAT) 2024 da Rede Integrar[2], essa nova fiscalização, que está sob a relatoria do Ministro Walton Alencar, foi realizada em parceria com alguns Tribunais de Contas Estaduais (TCEs), de modo a ampliar o escopo da avaliação para incluir, além das organizações federais, também um conjunto de organizações públicas estaduais e municipais. No total, tribunais de oito estados da federação aderiram à fiscalização (TCE-AM, TCE-BA, TCE-CE, TCE-PA, TCE-PE, TCE-PR, TCE-RJ e TCE-RN).

O que o TCU encontrou?

O questionário da auditoria foi estruturado em torno de 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”. Em seguida ao preenchimento do questionário, os auditores do TCU e dos TCEs avaliaram as respostas recebidas, bem como uma amostra das evidências fornecidas.

Para permitir a comparação entre os órgãos/entidades auditados, foi criado o “indicador de adequação à LGPD” (iLGPD), o qual é calculado com base nas respostas de cada uma das organizações ao questionário aplicado, resultando em um número entre 0 e 100%. Com base nesse indicador, foram definidos quatro níveis de adequação: “Inexpressivo” (< 15%), “Iniciando” (entre 15% e 40%), “Intermediário” (entre 40% e 70%) e “Aprimorado” (> 70%). O iLGPD médio das 387 organizações auditadas foi de 44% (“Intermediário”), sendo que 173 delas (44,71%) foram classificadas nos níveis iniciais (“Inexpressivo” ou “Iniciando”). De modo geral, os resultados obtidos confirmaram ter havido evolução em relação ao cenário verificado na auditoria anterior, a qual havia constatado que mais de três quartos das organizações da APF ainda estavam nos estágios iniciais de adequação à LGPD[1].

Contudo, a avaliação média dessas 387 organizações ainda indica a necessidade premente de avanços, sobretudo em relação a pontos específicos, a exemplo das dimensões “Preparação” (subindicador iPrep = 44%), “Capacitação” (iCap = 40%), “Conformidade do Tratamento” (iConf = 37%), “Compartilhamento de Dados Pessoais” (iComp = 22%), “Violação de Dados Pessoais” (iResp = 38%) e “Medidas de Proteção” (iProt = 34%).

No total, esta auditoria identificou sete achados: i) não conclusão de medidas preparatórias com vistas a se adequar à LGPD; ii) não condução de qualquer iniciativa ligada à dimensão “Contexto organizacional”; iii) não realização de qualquer das ações ligadas à dimensão “Liderança”; iv) ausência de Política de Segurança da Informação (PSI), de nomeação do encarregado pelo tratamento de dados pessoais (DPO) e de comunicação à Autoridade Nacional de Proteção de Dados

(ANPD) e aos titulares de dados da ocorrência de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares; v) ausência de Plano de Capacitação; vi) ausência de Política de Privacidade e não atendimento a direitos dos titulares; e vii) desconhecimento dos compartilhamentos de dados pessoais com terceiros.

O que o TCU decidiu?

Em decorrência desse diagnóstico, o TCU cientificou as organizações acerca dos descumprimentos legais (ausência de PSI, de nomeação do DPO e de comunicação padronizada à ANPD) e recomendou que alguns dos chamados Órgãos Governantes Superiores – OGSs (Conselho Nacional de Justiça [CNJ], Conselho Nacional do Ministério Público [CNMP], Secretaria de Governo Digital e Secretaria de Coordenação e Governança das Empresas Estatais, ambas do Ministério da Gestão e da Inovação em Serviços Públicos [SGD/MGI e Sest/MGI, respectivamente], além da ANPD) atuem para fomentar e induzir a continuidade do aumento de maturidade dos entes sob sua supervisão administrativa, por meio da implementação de controles, em especial nas áreas mais deficientes apontadas nesta auditoria.

Para isso, esses órgãos devem editar normativos e guias, além de envolverem as unidades de controle/auditoria interno/a das 387 organizações nos respectivos processos de adequação à LGPD. Ademais, após a aprovação do acórdão, todas as organizações federais auditadas receberão relatórios de *feedback* contendo análises individualizadas e comparativas entre órgãos/entidades similares, de modo que possam prosseguir evoluindo e se adequando cada vez mais à LGPD.

Quais os benefícios esperados?

A auditoria possuía dois objetivos principais: i) elaborar diagnóstico acerca dos controles implementados por organizações públicas federais para adequação à LGPD; e ii) induzir tais órgãos e entidades a conduzirem iniciativas para providenciar o pleno cumprimento da Lei 13.709/2018. Considera-se que ambos foram cumpridos.

Em relação ao primeiro, foi construído o "Painel Nacional de Implementação da LGPD", capaz de agregar e dar transparência aos resultados das avaliações das 387 organizações federais realizadas pelo TCU e das organizações públicas estaduais e municipais conduzidas pelos oito TCEs participantes. A seu turno, quanto ao segundo objetivo, a própria metodologia utilizada (CSA) induz melhorias nos órgãos/entidades auditados. Há notícia, inclusive, acerca da implementação de controles durante o próprio curso da fiscalização, a exemplo da nomeação de encarregados de dados.

A fiscalização também serviu para conscientizar e orientar os gestores e as unidades de controle/auditoria interno/a dessas organizações na condução de iniciativas para que seus órgãos se adequem à legislação, bem como para disponibilizar, aos auditores dos TCEs participantes, sistemática e ferramentas para que possam continuar avaliando seus jurisdicionados ao longo dos próximos anos.

Quais os próximos passos?

Ao longo dos próximos anos, os OGSs acionados (CNJ, CNMP, SGD/MGI, Sest/MGI e ANPD), bem como as unidades de controle/auditoria interno/a das 387 organizações públicas federais auditadas, deverão continuar acompanhando e cobrando as respectivas evoluções em relação à implementação de controles para adequação à LGPD.

Por fim, a partir da publicação do "Painel Nacional de Implementação da LGPD", atores da sociedade civil também poderão acompanhar e cobrar gestores e organizações para que continuem se adequando à LGPD. Há perspectiva de que outros TCEs realizem a aplicação do questionário da auditoria e incluam nesse painel os dados das organizações estaduais e municipais sob suas jurisdições.

Sumário

1. Introdução

1. Tratam os autos de relatório de auditoria de conformidade, com os objetivos de elaborar diagnóstico acerca dos controles implementados por organizações públicas federais para adequação à Lei Geral de Proteção de Dados Pessoais (LGPD) e induzi-las a conduzirem iniciativas para providenciar o pleno cumprimento da Lei 13.709/2018. A auditoria foi planejada de acordo com as diretrizes constantes no **Apêndice A** – Planejamento da fiscalização. A Matriz de Planejamento pode ser encontrada no **Apêndice B**.

2. Paralelamente à avaliação realizada pelo TCU, por meio de ação coordenada no âmbito da Rede Integrar[2], Tribunais de Contas Estaduais (TCEs) de oito estados da federação (TCE-AM, TCE-BA, TCE-CE, TCE-PA, TCE-PE, TCE-PR, TCE-RJ e TCE-RN) também fiscalizaram organizações públicas estaduais e municipais sob suas respectivas jurisdições.

1.1. Decisão que originou a fiscalização e suas razões

3. A presente fiscalização foi autorizada por meio do item 9.1 do Acórdão 889/2024-TCU-Plenário e levou em consideração o fato de a avaliação anteriormente realizada pelo Tribunal acerca da implementação dos dispositivos da LGPD ter constatado que 76,7% das organizações públicas federais se encontravam nos graus inexpressivo ou inicial de adequação àquela lei (TC 039.606/2020-1; Acórdão 1.384/2022-TCU-Plenário, Rel. Min. Augusto Nardes), com riscos à privacidade e à proteção dos dados pessoais dos cidadãos.

1.2. Identificação do objeto

4. O objeto desta fiscalização é a implementação dos dispositivos da LGPD (Lei 13.709/2018) por parte das organizações públicas federais.

1.3. Objetivo e escopo da auditoria

5. O trabalho tem por objetivos principais: i) elaborar diagnóstico acerca dos controles implementados por organizações públicas federais para adequação à LGPD; e ii) induzir tais órgãos e entidades a conduzirem iniciativas para providenciar o pleno cumprimento dessa lei.

Rede Integrar - Ação 29 do Plano Anual de Trabalho (PAT) 2024

6. A Rede Integrar[2] (de Políticas Públicas Descentralizadas) é uma rede colaborativa, formada pelos Tribunais de Contas do Brasil, por meio de Acordo de Cooperação Técnica firmado entre o Instituto Rui Barbosa (IRB), a Associação dos Membros dos Tribunais de Contas do Brasil (Atricon), o TCU e os Tribunais de Contas aderentes, com o objetivo de estabelecer cooperação técnica para fiscalização e aperfeiçoamento do ciclo de implementação de políticas públicas descentralizadas.

7. Por meio dessa rede, os Tribunais de Contas do Brasil cooperam para: i) promover estudos e avaliar a oportunidade de seleção de fiscalizações de políticas públicas descentralizadas; ii) realizar trabalhos conjuntos de fiscalização de políticas descentralizadas; iii) compartilhar e desenvolver conjuntamente metodologias, processos de trabalho e tecnologias; iv) viabilizar o intercâmbio de informações; v) compartilhar bancos de dados com a finalidade de incorporá-los a um painel de indicadores; e vi) fomentar a realização de cursos, seminários, simpósios, encontros e outros eventos voltados à capacitação e ao desenvolvimento profissional.

8. No PAT 2024[3] da Rede Integrar, aprovado no III Congresso Internacional dos Tribunais de Contas (Fortaleza - CE, novembro de 2023), foi incluída a Ação 29 ("Implementação dos dispositivos da LGPD na União, Estados, DF e Municípios"). Sob a coordenação do TCU, essa ação visa a traçar um panorama da implementação da LGPD nas três esferas (União, Estados/DF e Municípios), induzindo o incremento da maturidade das organizações públicas no tratamento dos dados pessoais, fomentando a devida classificação das informações e promovendo maior transparência quanto aos tratamentos de dados e, quando pertinente e justificável, quanto aos dados em si.

9. A referida ação prevê, ainda, a construção do chamado "Painel Nacional de Implementação da LGPD", a partir da consolidação, por parte do TCU, dos dados das organizações federais com aqueles

relativos às organizações estaduais e municipais, resultantes de auditorias independentes realizadas pelos TCEs aderentes (TCE-AM, TCE-BA, TCE-CE, TCE-PA, TCE-PE, TCE-PR, TCE-RJ e TCE-RN).

1.4. Questões de auditoria

10. Esta fiscalização buscou avaliar 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 partir de duas questões de auditoria (**Apêndice B** – Matriz de Planejamento), cujas respostas resumidas são mostradas a seguir (as respostas completas podem ser encontradas no **Apêndice C** – Respostas aos questionamentos da Matriz de Planejamento).

QST-1: As organizações se estruturaram para a condução de iniciativas de adequação à LGPD?

11. A resposta à QST-1 consiste no resumo das respostas das 387 organizações federais auditadas às perguntas das primeiras quatro dimensões do questionário ("Preparação", "Contexto Organizacional", "Liderança" e "Capacitação" – Seções 2.1.1 a 2.1.4 deste relatório).

12. De modo geral, não se pode dizer que esses órgãos/entidades se estruturaram adequadamente para conduzirem iniciativas de adequação à LGPD, havendo, ainda, muito a ser feito. Entre 0 e 100%, os subindicadores médios das 387 organizações auditadas relativos a essas quatro dimensões são: "Preparação" (iPrep) = 44%, "Contexto Organizacional" (iOrg) = 59%, "Liderança" (iLid) = 68% e "Capacitação" (iCap) = 40% (Figura 13).

QST-2: As organizações implementaram medidas e controles de proteção de dados pessoais para adequação à LGPD?

13. A seu turno, a resposta à QST-2 baseia-se nas respostas das 387 organizações federais às perguntas das demais cinco dimensões ("Conformidade do Tratamento", "Direitos do Titular", "Compartilhamento de Dados Pessoais", "Violação de Dados Pessoais" e "Medidas de Proteção" – Seções 2.1.5 a 2.1.9 deste relatório).

14. De igual modo, não se pode afirmar que as organizações federais implementaram medidas e controles suficientes para se adequarem à LGPD. Os subindicadores médios (entre 0 e 100%) dos 387 entes auditados relativos a essas cinco dimensões são: "Conformidade do Tratamento" (iConf) = 37%, "Direitos do Titular" (iDir) = 62%, "Compartilhamento de Dados Pessoais" (iComp) = 22%, "Violação de Dados Pessoais" (iResp) = 38% e "Medidas de Proteção" (iProt) = 34%.

1.5. Metodologia

15. 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[4], disponibilizada no portal do TCU.

16. Com o intuito de não surpreender os gestores com a condução do trabalho e, também, com o propósito de concentrar as principais informações, orientações e documentos relacionados à auditoria, a exemplo da íntegra do questionário eletrônico aplicado, foi criada uma página no Portal do TCU[5], o que contribuiu para a obtenção de respostas de 100% dos 387 órgãos/entidades auditados (peça 922).

17. O método utilizado para avaliar as organizações foi a autoavaliação de controles internos (do inglês *Control Self-Assessment* – CSA), no qual disponibilizou-se aos gestores um questionário para que preenchessem as respostas que melhor refletiam a situação do respectivo ente com relação à implementação das medidas de adequação à LGPD, solicitando-se, adicionalmente, o envio das evidências correspondentes, em alguns casos. Por meio de ofício de comunicação da auditoria, cada organização recebeu um *link* e uma chave de acesso (*token*) única para responder o questionário *online*, o qual ficou disponível para ser respondido durante quatro semanas (de 24/6 a 19/7/2024). A Figura 1 mostra a evolução temporal das respostas das 387 organizações auditadas nesse período.

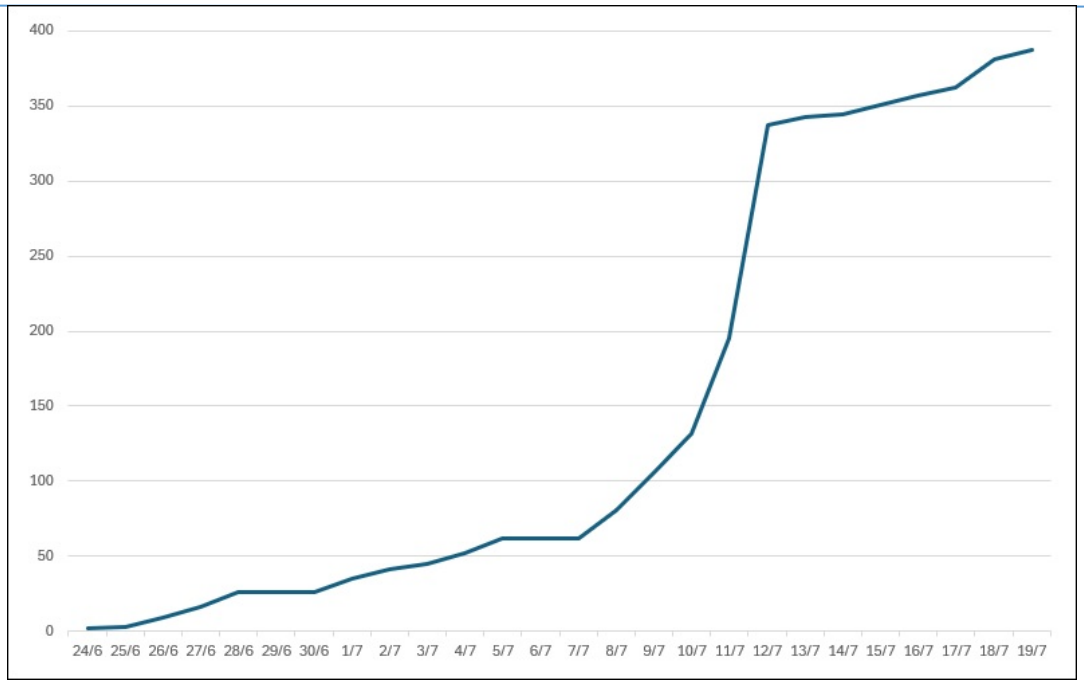


Figura 1 - Evolução temporal das respostas das 387 organizações auditadas.
(Fonte: elaboração própria, com base nas datas de submissão das respostas obtidas a partir da ferramenta LimeSurvey)

18. As perguntas do questionário tiveram como referências principais a própria LGPD (Lei 13.709/2018), a Lei 12.527/2011 (Lei de Acesso à Informação – LAI), a norma técnica ABNT NBR ISO/IEC 27701:2019 ("Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e diretrizes"), além de outros normativos (*e.g.* Instrução Normativa [IN] SGD/ME 117/2020[6] [Indicação do Encarregado pelo Tratamento dos Dados Pessoais na Administração Pública Federal – APF], IN - GSI/PR 5/2021[7] [Requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos/entidades da APF]) e de documentos elaborados pela Autoridade Nacional de Proteção de Dados – ANPD (Resolução CD/ANPD 15/2024[8] [Regulamento de Comunicação de Incidente de Segurança], "Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado"[9], "Guia Orientativo – Tratamento de dados pessoais pelo Poder Público"[10]).

19. Para aplicação do questionário (**Apêndice D** – Questionário da auditoria), que foi avaliado previamente pela ANPD, foi utilizada a plataforma LimeSurvey (*Community Edition*, versão 5.1.10+210913), frisando-se aos respondentes que este: i) não é exaustivo, ou seja, não contempla todas as medidas e controles possíveis de serem implementados para adequação das organizações à LGPD; ii) pode abranger questões e opções de resposta que tratam de medidas e controles que podem não ser aplicáveis a algumas organizações, por diversas razões (*e.g.* contexto específico, porte, objetivos institucionais, características particulares da instituição).

20. Após uma primeira seção na qual eram solicitados dados de identificação do respondente (úteis para que a equipe da fiscalização, caso necessário, pudesse entrar em contato para solicitar esclarecimentos ou tirar dúvidas) e excetuando-se as questões que demandavam anexar documentos, o questionário contemplou, no total, dezesseis questões e, assim como na auditoria anterior (TC 039.606/2020-1), foi estruturado em torno de nove dimensões, divididas em dois eixos (refletidos nas duas questões de auditoria) [Figura 2]. Algumas das questões só eram mostradas de forma condicionada às respostas do gestor em perguntas anteriores.

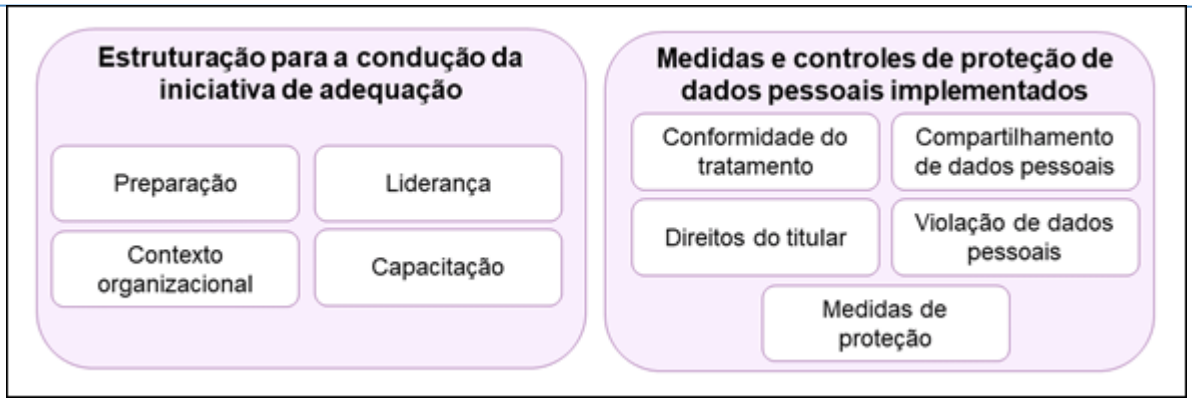


Figura 2 - Questionário da Auditoria LGPD 2024 - Dois eixos e nove dimensões.
(Fonte: TC 039.606/2020-1, relatório)

21. Foi realizado esforço no sentido de sintetizar o questionário aplicado pelo TCU na auditoria de 2021 sobre a LGPD (TC 039.606/2020-1), de modo que, apesar da significativa redução na quantidade de perguntas (naquela fiscalização, o questionário continha sessenta questões), o conteúdo avaliado abarcou praticamente os mesmos pontos, tendo sido incluídas, inclusive, novas perguntas sobre a relação LGPD x LAI (*e.g.* questões 5.2 e 11.1), a realização de tratamento de dados pessoais em solução de computação em nuvem (questão 8.1.2) e uma pergunta aberta para livre manifestação do gestor acerca dos principais desafios, deficiências e pontos de atenção relacionados à adequação da sua organização à LGPD (questão 11.2). Também foram incluídas, em algumas questões de múltipla resposta, opções de resposta que abarcavam itens de verificação inexistentes na versão do questionário aplicada em 2021[11].

22. Após a expiração do prazo de preenchimento do questionário (19/7/2024), as respostas fornecidas pelas organizações foram consolidadas e serviram de insumo para a elaboração do diagnóstico de adequação à LGPD contido neste relatório. Ademais, foi elaborada fórmula matemática para, com base nessas respostas, calcular o "indicador de adequação à LGPD" (iLGPD), de modo a permitir rápida comparabilidade entre os órgãos e entidades avaliados, bem como o seu agrupamento em níveis/faixas de adequação/maturidade. O diagnóstico é apresentado no Capítulo 2. A seu turno, o iLGPD é detalhado no **Apêndice F** – Indicador de adequação à LGPD (iLGPD).

1.6. Limitações

23. Não houve limitações. Todo o planejamento da auditoria foi cumprido.

1.7. Volume de recursos fiscalizados

24. Não se aplica.

1.8. Benefícios estimados

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

26. Por meio do questionário aplicado às 387 organizações federais auditadas, foram avaliados vários aspectos relacionados à sua adequação à LGPD e identificadas diversas fragilidades que precisam ser endereçadas (Capítulo 4), visto que impactam negativamente a proteção dos dados pessoais tratados por esses órgãos/entidades, com consequente risco de dano à privacidade dos cidadãos e, em última instância, possibilidade de prejuízos aos próprios entes (*e.g.* condenação ao pagamento de indenizações, danos à imagem, aplicação de sanções pela ANPD).

27. Para resolver esses problemas, a AudTI propõe dar ciência a alguns órgãos acerca de descumprimentos normativos expressos (ausência de PSI, de nomeação do DPO e de comunicação

padronizada à ANPD) e, no caso dos demais achados apontados, recomendar que os OGSs envolvidos, dentro do exercício do seu poder de supervisão administrativa, acionem e envolvam as unidades de controle interno das organizações em questão com vistas a sanar as fragilidades identificadas. Os resultados das avaliações dos órgãos também foram alimentados em um "Painel Nacional de Implementação da LGPD" (Capítulo 5), o qual deverá ser publicado, esperando-se que sirva para incentivar as organizações a continuarem suas ações e projetos de adequação à LGPD.

28. Com isso, espera-se que essas organizações aumentem a maturidade dos seus processos de tratamento de dados e, consequentemente, sejam capazes de proteger adequadamente os dados pessoais que tratam, diminuindo os riscos de incidentes e falhas de segurança e, consequentemente, assegurando a privacidade dos cidadãos e a materialização dos princípios previstos na LGPD.

29. Por fim, a partir do envio de relatórios individuais de *feedback* a cada um dos 387 entes auditados, espera-se que os respectivos gestores também se sintam encorajados a continuarem evoluindo suas organizações em relação à implementação dos controles e das medidas de proteção verificados.

2. Diagnóstico da adequação das organizações públicas federais à LGPD

30. Este capítulo traz o diagnóstico da implementação de uma série de dispositivos relativos à LGPD, conforme aferido por meio do questionário aplicado aos gestores das organizações auditadas (**Apêndice D** – Questionário da auditoria), o qual é composto, basicamente, por dois tipos de perguntas: i) "Tipo A": permitem a marcação de uma única opção de resposta (as diferentes opções disponíveis refletem um aumento gradativo da maturidade da organização em relação aos controles/práticas envolvidos, sendo que o respondente deve assinalar qual, dentre as opções disponíveis, melhor reflete a situação atual da sua organização, além de descrever, no respectivo campo de comentário, quando aplicável, datas, períodos, responsáveis, projetos/iniciativas e referenciar artefatos, evidências, atas e outros documentos internos); ii) "Tipo B": o respondente deve marcar múltiplas opções de resposta, isto é, deve selecionar todas as opções que descrevem itens atendidos pela sua organização.

31. Para visualização gráfica das respostas das organizações respondentes, foi construído um painel (Capítulo 5), a partir do qual foram obtidas as figuras que ilustram este capítulo. As seções a seguir, então, trazem as respostas das 387 organizações fiscalizadas a cada uma das perguntas do questionário, divididas nas 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").

2.1. Dimensões avaliadas

2.1.1. Preparação

32. Antes de iniciar o processo de adequação à LGPD, a organização deve adotar medidas e realizar ações no sentido de construir um ambiente propício para o sucesso dessa empreitada. A questão desta dimensão, então, aborda aspectos relacionados à identificação, ao planejamento e à concretização dessas medidas preparatórias.

33. Um exemplo de medida preparatória é a instituição de comitê ou grupo de trabalho para tratar do tema. Ademais, mesmo antes de formalizar qualquer normativo interno especificamente relacionado à proteção e à privacidade de dados, a organização pode produzir certos artefatos iniciais, tais como estudos, planos de ação, atas de reuniões, trocas de e-mails com propostas a respeito etc.

34. É importante que, desde o início, essas iniciativas contem com o apoio e, idealmente, até mesmo com a participação direta da alta direção da organização. Ademais, convém que sejam envolvidas pessoas da organização pertencentes a unidades que exercem atividades relevantes para o tratamento de dados pessoais (*e.g.* Segurança da Informação, Tecnologia da Informação, Jurídico, Áreas de Negócio, Auditoria/Conformidade e Ouvidoria).

35. Em um primeiro estágio de maturidade, a organização terá apenas documentado informações relacionadas aos objetivos dessas iniciativas de adequação e às ações necessárias para alcançá-los,

possivelmente especificando os recursos necessários, os responsáveis e os prazos previstos. Avançando, em um estágio intermediário, a organização já terá normatizado as principais questões relacionadas ao tema tratamento de dados (*e.g.* política de proteção de dados pessoais, plano de capacitação associado, política de privacidade), levando em consideração os princípios gerais ou todos os elementos elencados na LGPD.

36. Por fim, no nível mais maduro em relação ao tema, a organização possuirá programa de governança em privacidade de dados implementado, amplamente divulgado a todas as partes interessadas e sendo periodicamente avaliado e revisado, com vistas à melhoria contínua.

37. Como referências normativas aplicáveis à dimensão "Preparação", podem ser citadas, em especial, a Lei 13.709/2018, art. 50, § 2º, inciso I (trata da implementação de programa de governança em privacidade), bem como o item 5.4 (Planejamento) da norma ABNT NBR ISO/IEC 27701:2019.

Questionário: pergunta 2.1 (TIPO A)

Tabela 1 - Distribuição das respostas à pergunta 2.1 do questionário.
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 5])

Questão 2.1: A organização conduziu iniciativas para identificar, planejar e executar medidas preparatórias com vistas a se adequar à LGPD?	**Qtde.**	**%**
a0) Não se aplica	0	0
a1) Não (a organização não realizou medidas preparatórias com vistas a se adequar à LGPD)	11	2,84
a2) A organização iniciou, mas ainda não concluiu iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD	98	25,32
a3) A organização concluiu iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD (possui plano de ação, plano de projeto ou documento similar para direcionar os esforços nesse sentido), porém ainda não formalizou normativo interno relacionado à proteção e à privacidade de dados	54	13,95
a4) A organização concluiu iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD e já publicou uma política (ou documento similar) que considera os princípios e aspectos gerais relacionados ao tratamento de dados	84	21,71
a5) A organização já mapeou seus principais processos de tratamento de dados (natureza, escopo, finalidade, benefícios, probabilidade e gravidade dos riscos associados) e publicou normativos internos que tratam dos aspectos mais importantes relacionados à proteção e à privacidade de dados, porém ainda não possui um programa de governança em privacidade de dados implementado	87	22,48
a6) A organização já mapeou todos os processos de tratamento de dados (natureza, escopo, finalidade, benefícios, probabilidade e gravidade dos riscos associados), publicou normativos internos que tratam dos temas proteção e privacidade de dados de forma abrangente e possui programa de governança em privacidade de dados implementado, periodicamente monitorado/avaliado e atualizado continuamente	53	13,70
TOTAL	**387**	**100**

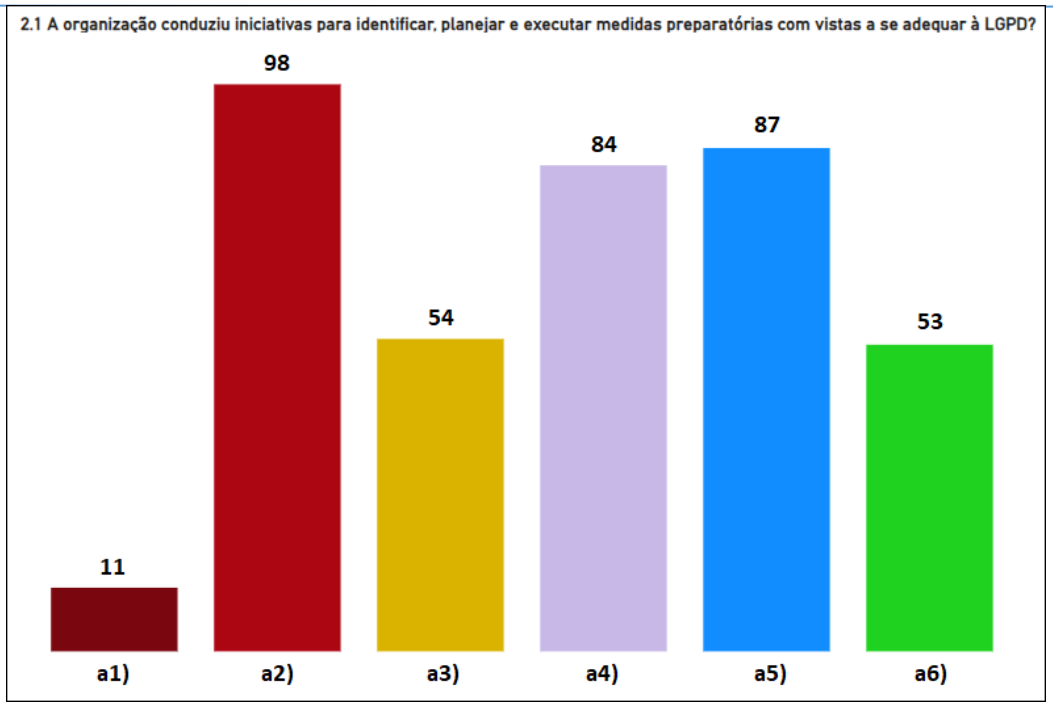


Figura 3 - Distribuição das respostas à pergunta 2.1 do questionário.
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 5])

Análise

38. A questão 2.1 mostra que 278 das 387 (71,84%) organizações federais auditadas já concluíram iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD (Tabela 1 e Figura 3, respostas a3 a a6). Dessas, 54 (13,95%) ainda não formalizaram nenhum normativo interno relacionado à proteção e à privacidade de dados (resposta a3), 171 (44,19%) já publicaram um ou mais normativos que consideram princípios e aspectos relacionados ao tema, incluindo uma política de caráter geral (respostas a4 e a5), ao passo que 53 (13,70%) avançaram, inclusive, para a implementação e a monitoração periódica de um programa de governança em privacidade de dados (resposta a6).

39. As 109 (28,16%) organizações que ainda não concluíram este tipo de iniciativa (Tabela 1, respostas "a1" e "a2"; peça 922) devem adotar, com urgência, providências para se adequarem à LGPD, que já está em vigor desde 2020, cabendo, sobretudo, ao CNJ, à SGD/MGI, à Sest/MGI e à ANPD adotarem medidas visando a orientar e induzir tais órgãos/entidades a se movimentarem nesse sentido.

2.1.2. Contexto organizacional

40. Para alcançar os resultados pretendidos pelas iniciativas de adequação à LGPD, a organização deve avaliar uma série de fatores internos e externos relevantes para atingir os objetivos associados. A questão desta dimensão, então, aborda aspectos relacionados ao mapeamento dos normativos correlatos à proteção de dados pessoais que devem ser respeitados pela organização, à identificação das partes interessadas e às análises dos diferentes tipos de dados pessoais tratados pela organização e dos processos organizacionais que realizam o tratamento desses dados.

41. Por exemplo, o Decreto-Lei 5.452/1943 (Consolidação das Leis do Trabalho – CLT) e as Leis 8.078/1990 (Código de Defesa do Consumidor – CDC), 12.414/2011 (Cadastro Positivo), 12.527/2011 (LAI) e 13.787/2018 (digitalização e utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuários de pacientes) contêm diversos dispositivos que, eventualmente, podem se aplicar à organização. Além dessas leis, podem existir normas infralegais, como regulamentos, portarias, instruções normativas, decisões judiciais/administrativas e requisitos contratuais que tragam comandos relacionados à privacidade e à proteção de dados pessoais e que, portanto, também devem ser respeitados pela organização.

42. Convém, ainda, que a organização identifique todas as partes que possuem interesses ou responsabilidades associadas ao tratamento de dados pessoais, tais como os titulares de dados pessoais, os controladores conjuntos e os operadores. O titular é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (*e.g.* cidadão, cliente, servidor público, representante de fornecedor, terceirizado). O controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (controlador conjunto é aquele que determina os propósitos e as formas do tratamento de dados pessoais junto com outro controlador). A seu turno, 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, incisos V, VI e VII).

43. Considerando que o controlador é obrigado a reparar danos causados em razão da atividade de tratamento de dados pessoais (LGPD, art. 42), a organização deve ter contrato firmado com os agentes contratados que realizam tratamento de dados em seu nome (operadores), bem como com os controladores conjuntos, contendo cláusulas para definir claramente papéis e responsabilidades e assegurar que estes adotem medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais compartilhados com eles.

44. Ademais, tanto o controlador quanto o operador devem manter registro das operações de tratamento de dados pessoais realizadas (LGPD, art. 37), sendo que a ANPD poderá determinar ao controlador que elabore Relatório de Impacto à Proteção de Dados Pessoais (RIPD) com descrição, dentre outros elementos, dos dados coletados e das metodologias de coleta e de garantia da segurança das informações (art. 38).

45. A organização deve, ainda, estabelecer políticas e salvaguardas adequadas, baseadas em avaliações sistemáticas dos impactos e dos riscos à privacidade, relativamente aos dados pessoais tratados, com vistas a mitigar possíveis probabilidades e impactos da ocorrência de situações indesejadas (art. 50, § 2º, inciso I, alínea "d"). Esses riscos devem ser avaliados sob o prisma das diversas operações realizadas com os dados (*e.g.* coleta, produção, acesso, transmissão, armazenamento, eliminação). Inclusive, tais avaliações devem nortear a organização quanto a eventual necessidade de priorizar as iniciativas de adequação à LGPD em relação a processos de negócio específicos, de mais alto risco.

46. A título de referências normativas aplicáveis à dimensão "Contexto Organizacional", podem ser citadas a Lei 13.709/2018, art. 5º, em especial incisos I, V, VI, VII e X, art. 7º, § 5º, e arts. 37, 39, 42-46 e 50, § 1º e § 2º, inciso I, alínea "d", bem como a norma ABNT NBR ISO/IEC 27701:2019, itens 5.2.1 (Entendendo a organização e seu contexto), 5.2.2 (Entendendo as necessidades e as expectativas das partes interessadas), 5.4.1.2 (Avaliação de riscos de segurança da informação), 6.5.1 (Responsabilidade pelos ativos), 6.5.2 (Classificação da informação), 7.2.6 (Contratos com operadores de dados pessoais), 7.2.7 (Controlador conjunto de dados pessoais) e 7.2.8 (Registros relativos ao tratamento de dados pessoais).

Questionário: pergunta 3.1 (TIPO B)

Tabela 2 - Distribuição das respostas à pergunta 3.1 do questionário.
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 5])

Questão 3.1: A organização conduziu iniciativa com vistas a IDENTIFICAR:	**Sim**	**Não**
OUTROS NORMATIVOS (*e.g.* leis, regulamentos, portarias, instruções normativas, decisões judiciais/administrativas, requisitos contratuais), além da LGPD, que abrangem comandos relacionados à proteção de dados pessoais, os quais a organização deve respeitar	296	91
AS DIFERENTES CATEGORIAS DE TITULARES de dados pessoais com os quais se relaciona (*e.g.* cidadão, cliente, servidor público, representante de fornecedor, terceirizado)	254	133
OS OPERADORES que realizam tratamento de dados pessoais em seu nome	226	161
Se há tratamento de dados que envolva CONTROLADOR CONJUNTO	139	248

E ADEQUAR OS INSTRUMENTOS CONTRATUAIS (*e.g.* contrato, convênio, acordo de cooperação) firmados com os operadores e os controladores conjuntos identificados, de forma a estabelecer suas respectivas responsabilidades e papéis com relação à proteção de dados pessoais	241	146
OS PROCESSOS DE NEGÓCIO que realizam tratamento de dados pessoais e os respectivos RESPONSÁVEIS (*e.g.* pessoas, departamentos, operadores, controladores conjuntos)	212	175
OS DADOS PESSOAIS TRATADOS pela organização	275	112
OS LOCAIS DE ARMAZENAMENTO dos dados pessoais tratados pela organização (*e.g.* servidor de arquivos, nuvem, dispositivo USB, *storage*, fita de *backup*, arquivos físicos [pastas, armários])	253	134
E AVALIAR OS RISCOS associados aos processos de tratamento de dados pessoais que foram identificados	159	228
A organização AINDA NÃO CONDUZIU INICIATIVA com vistas a identificar qualquer dos objetos mencionados nos itens anteriores	40	347

Análise

47. Com relação à questão 3.1 (Tabela 2), despertam preocupação as quantidades significativas de organizações que ainda não verificaram se há tratamentos de dados envolvendo controlador conjunto (248 de 387, ou 64,08%) e que não identificaram e avaliaram riscos relacionados aos seus processos de tratamento de dados pessoais (228 de 387, ou 58,92%).

48. Merecem atenção especial, inclusive quanto ao eventual planejamento de ações de controle específicas por parte deste Tribunal, os quarenta órgãos e entidades (10,34%) que sinalizaram que ainda não conduziram nenhuma das iniciativas citadas nessa questão (peça 922).

2.1.3. Liderança

49. A alta direção da organização deve demonstrar claramente liderança e comprometimento com a iniciativa de adequação à LGPD. Nesse sentido, a elaboração e a ampla divulgação de políticas relacionadas à proteção de dados pessoais, bem como a nomeação de um encarregado pelo tratamento de dados pessoais (normalmente chamado de DPO, do inglês *Data Protection Officer*), são ações fundamentais para o processo de adequação à LGPD.

50. O encarregado nomeado deve ter independência (não ser gestor responsável por sistema de informação e não fazer parte de setor/departamento que possa gerar conflito de interesses quanto à sua atuação, a exemplo das unidades de TI [IN - SGD/ME 117/2020[6], art. 1º, § 1º, inciso II]) e autonomia suficientes para reportar à alta administração, servindo como canal de comunicação efetivo entre o controlador, os titulares dos dados e a ANPD. Deve, ainda, além de ter profundo entendimento da própria LGPD, possuir conhecimentos multidisciplinares relativos a uma série de temas correlatos (*e.g.* Jurídico, Governanças Corporativa e de Dados, Gestão de Riscos, Tecnologia da Informação, Segurança da Informação, Privacidade e Proteção de Dados).

51. A questão desta dimensão, então, aborda aspectos atinentes à nomeação desse encarregado e à formalização de políticas (ou documentos similares) que busquem assegurar, no âmbito da organização, a segurança das informações e a proteção dos dados pessoais, tais como:

51.1. Política de Segurança da Informação (PSI): aprovada pela alta direção e obrigatória para os órgãos e entidades da APF (Decreto 9.637/2018, art. 15, inciso II), estabelece a abordagem da organização para gerenciar os objetivos nessa área, em linha com os requisitos do negócio e com leis e regulamentações aplicáveis;

51.2. Política de Classificação da Informação (PCI): importante para direcionar a implementação de controles adequados para a proteção de dados pessoais; fornece diretrizes para assegurar que as diferentes informações recebam níveis adequados de proteção, de acordo com a sua importância para a organização e os riscos associados;

51.3. Política de Proteção de Dados Pessoais (PPDP): alinhada à PSI e à PCI, estabelece regras e diretrizes para o tratamento e para a governança de dados pessoais dentro da organização (público interno), reforçando seu compromisso para alcançar a conformidade com os normativos de proteção de dados pessoais.

52. Em especial no que tange à classificação das informações, a LGPD demanda que sejam adotados cuidados específicos para o tratamento de dados pessoais sensíveis (que envolvem 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) e de dados pessoais de crianças e de adolescentes (Lei 13.709/2018, art. 5º, inciso II, e arts. 11-14).

53. Como referências normativas aplicáveis à dimensão "Liderança", podem ser citadas a Lei 13.709/2018, em especial art. 5º, incisos I, II e VIII, arts. 11-14, art. 23, inciso III, e arts. 41, 46 e 50, § 2º, inciso I, alíneas "a" e "d", a IN - SGD/ME 117/2020[6] (Indicação do Encarregado pelo Tratamento dos Dados Pessoais na APF), em especial art. 1º, § 1º, incisos I e II, e art. 2º, a norma ABNT NBR ISO/IEC 27701:2019, itens 5.3.2 (Política), 6.2 (Políticas de segurança da informação), 6.2.1 (Orientação da Direção para segurança da informação), 6.3.1 (Organização interna), 6.5.2 (Classificação da informação) e 6.5.2.2 (Rótulos e tratamento da informação), bem como o "Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado"[9], da ANPD.

Questionário: pergunta 4.1 (TIPO B)

Tabela 3 - Distribuição das respostas à pergunta 4.1 do questionário.
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 5])

Questão 4.1: A organização:	**Sim**	**Não**
Instituiu formalmente e mantém atualizada POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (ou instrumento similar)	307	80
Instituiu formalmente e mantém atualizada POLÍTICA DE CLASSIFICAÇÃO DA INFORMAÇÃO (ou instrumento similar), sendo que abordou nesse documento questões específicas relacionadas à classificação de dados pessoais, de dados pessoais sensíveis e de dados pessoais de crianças e de adolescentes	117	270
Instituiu formalmente e mantém atualizada POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS (ou instrumento similar)	221	166
Nomeou o ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS (*Data Protection Officer* – DPO) e publicou essa nomeação em veículo de comunicação oficial (*e.g.* Diário Oficial da União – DOU)	339	48
DIVULGA EM SEU SÍTIO ELETRÔNICO INSTITUCIONAL a identidade e as informações de contato (nome, e-mail, telefone) do encarregado pelo tratamento de dados pessoais, em local de fácil acesso aos titulares de dados pessoais	326	61
AINDA NÃO ATENDE NENHUM dos itens anteriores	24	363

Análise

54. Quanto à questão 4.1 (Tabela 3), merecem destaque as 270 organizações (de 387, ou 69,77%) que indicaram que ainda não formalizaram uma política que englobe a devida classificação das informações pessoais, tendo em vista que essa classificação é passo inicial para permitir que tais dados sejam efetivamente protegidos e tratados de acordo com os ditames previstos na LGPD.

55. No que se refere à PSI, tendo em vista se tratar de documento de caráter obrigatório (Decreto 9.637/2018, art. 15, inciso II, c/c a IN - GSI/PR 1/2020[12] [Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da APF], art. 9º; Resolução - CNJ 396/2021[13] [Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário – ENSEC-PJ], art. 19, inciso II; Resolução - CNMP 156/2016[14] [Institui a Política de Segurança Institucional e o Sistema Nacional de

Segurança Institucional do Ministério Público – MP], art. 22, inciso III), será feita proposta de dar ciência às oitenta organizações (20,87%) que indicaram não possuir a política que tal conduta afronta os citados normativos (peça 918).

56. Propõe-se, ainda, dar ciência aos 48 órgãos/entidades (12,4%) que manifestaram ainda não terem realizado sequer a nomeação do encarregado pelo tratamento de dados pessoais, em descumprimento ao art. 41 da Lei 13.709/2018 (peça 919).

2.1.4. Capacitação

57. É necessário que todas as pessoas da organização estejam cientes da importância dos temas privacidade e proteção de dados pessoais, bem como dos impactos e prejuízos que podem ser causados devido às violações desses dados (*e.g.* sanções aplicadas pela ANPD, indenizações, danos financeiros e à imagem da instituição). Para isso, a organização deve conduzir iniciativas tanto para conscientizar quanto para capacitar seus colaboradores nessas áreas. A conscientização é importante para que os colaboradores conheçam a legislação e as políticas e normativos institucionais relacionados à proteção de dados pessoais, bem como para que reconheçam como as suas decisões e ações, no dia a dia, podem afetar a preservação da privacidade dos titulares de dados.

58. Nesse sentido, é conveniente que a organização elabore um Plano de Capacitação que contemple ações de conscientização e que determine os conhecimentos e as competências necessárias para os recursos humanos relativamente a essa temática, sobretudo no que tange aos colaboradores diretamente envolvidos em atividades que realizam o tratamento de dados pessoais. Assim, esse Plano de Capacitação deve mapear as lacunas de conhecimentos e de habilidades associadas ao tema e, consequentemente, planejar ações de treinamento para a sua gradual redução.

59. As ações de capacitação devem considerar diferentes níveis de envolvimento dos colaboradores com essa temática, de forma que aqueles envolvidos em atividades críticas relacionadas ao tratamento de dados pessoais e que ocupam funções com responsabilidades essenciais relacionadas à proteção desses dados recebam treinamento diferenciado, além do nível básico fornecido aos demais.

60. Por fim, vale ressaltar que tanto a LGPD (Lei 13.709/2018), ao focar na proteção dos dados pessoais e na privacidade dos indivíduos, quanto a LAI (Lei 12.527/2011), ao promover a transparência e o acesso às informações públicas, buscam garantir direitos fundamentais relacionados à informação em sentido amplo. Ambas atuam para fortalecer a proteção dos direitos dos cidadãos e exigir das entidades, públicas e privadas, maior zelo quanto à gestão e ao tratamento das informações. Para isso, embora possuam finalidades distintas, essas leis (LGPD e LAI) se complementam de forma harmônica, sendo que a conformidade com ambas é fundamental para as organizações públicas.

61. As questões desta dimensão, então, abordam aspectos atinentes à avaliação, ao planejamento e à realização de ações de capacitação relacionadas à privacidade e à proteção de dados pessoais, bem como à necessidade de harmonizar a LGPD e a LAI.

62. A título de referências normativas aplicáveis à dimensão "Capacitação", podem ser citadas a Lei 13.709/2018, art. 41, § 2º, inciso III, a Lei 12.527/2011, art. 41, inciso II, bem como os itens 5.5.2 (Competência), 5.5.3 (Conscientização) e 5.5.4 (Comunicação) da norma ABNT NBR ISO/IEC 27701:2019.

Questionário: pergunta 5.1 (TIPO A)

Tabela 4 - Distribuição das respostas à pergunta 5.1 do questionário.
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 5])

Questão 5.1: Acerca da capacitação dos seus colaboradores em proteção de dados pessoais, a organização:	**Qtde.**	**%**
a0) Não se aplica	4	1,04

a1) Não possui PLANO DE CAPACITAÇÃO (ou instrumento similar) e seus colaboradores ainda não realizaram treinamento em proteção de dados pessoais	43	11,11
a2) Não possui PLANO DE CAPACITAÇÃO (ou instrumento similar), mas colaboradores específicos já realizaram treinamento em proteção de dados pessoais	118	30,49
a3) Possui PLANO DE CAPACITAÇÃO (ou instrumento similar) e, apesar de este não contemplar a temática de proteção de dados pessoais de maneira específica, já realizou treinamento abrangente (não direcionado apenas a determinados colaboradores) nessa área	79	20,41
a4) Possui PLANO DE CAPACITAÇÃO (ou instrumento similar), contemplou nesse documento a temática de proteção de dados pessoais e já realizou treinamento da maioria dos colaboradores nessa área	98	25,32
a5) Possui PLANO DE CAPACITAÇÃO (ou instrumento similar), contemplou nesse documento a temática de proteção de dados pessoais, incluindo a necessidade de treinamento diferenciado para as pessoas que exercem funções com responsabilidades essenciais quanto à proteção de dados pessoais, e já realizou treinamento de todos os colaboradores nessa área	45	11,63
TOTAL	**387**	**100**

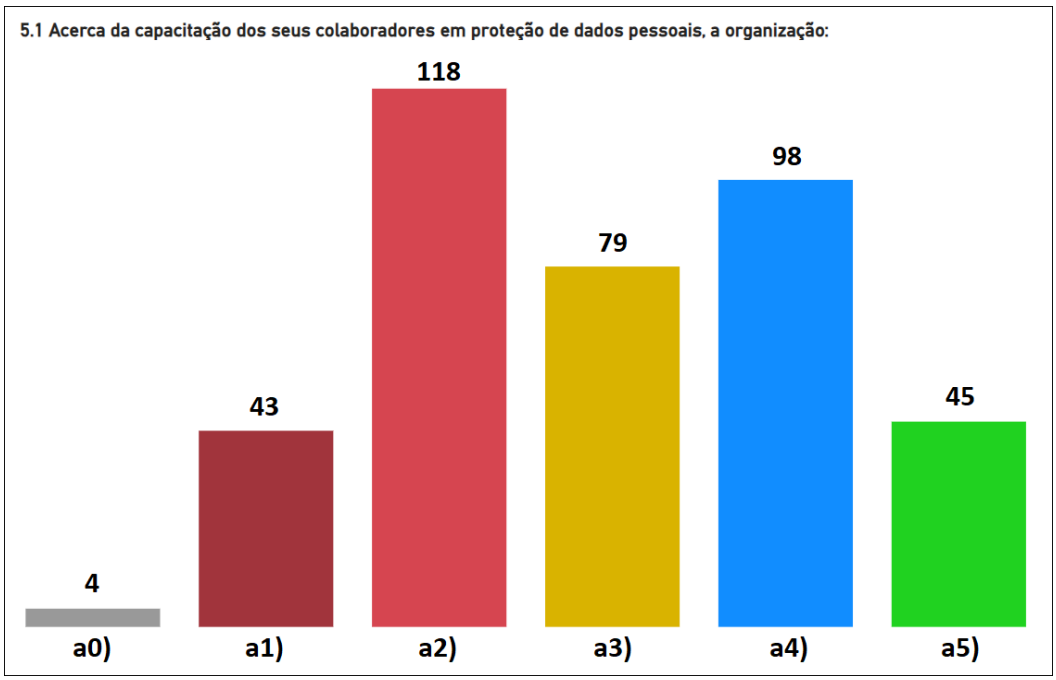


Figura 4 - Distribuição das respostas à pergunta 5.1 do questionário.
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 5])

Questionário: pergunta 5.2 (TIPO B)

Tabela 5 - Distribuição das respostas à pergunta 5.2 do questionário.
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 5])

Questão 5.2: Acerca das ações de capacitação em proteção de dados pessoais realizadas nos últimos 3 (três) anos, a organização: (responderam esta questão apenas as 340 organizações que marcaram as opções a2, a3, a4 ou a5 na questão 5.1)	**Sim**	**Não**
Levou em consideração a necessidade de COMPLEMENTAR A CAPACITAÇÃO dos participantes nesses treinamentos COM CONTEÚDO SOBRE TRANSPARÊNCIA da gestão relativa às informações de interesse coletivo ou geral (Lei 12.527/2011 – LAI)	149	191

Efetivamente CAPACITOU NO TEMA TRANSPARÊNCIA da gestão relativa às informações de interesse coletivo ou geral (LAI) MAIS DE 50% dos colaboradores que receberam treinamento em proteção de dados pessoais	46	294
OFERECEU AÇÃO DE CAPACITAÇÃO QUE TENHA ABORDADO CONJUNTAMENTE, de forma integrada, as temáticas da proteção de dados pessoais (LGPD) e da transparência da gestão (LAI)	150	190
ORIENTOU OS PARTICIPANTES nesses treinamentos, mesmo que *a posteriori*, sobre a necessidade de observarem os Enunciados da CGU divulgados por meio da PORTARIA NORMATIVA CGU 71/2023[15]	57	283
ORIENTOU OS PARTICIPANTES nesses treinamentos, mesmo que *a posteriori*, sobre a necessidade de observarem as diretrizes e orientações publicadas pela CGU por meio do "PARECER SOBRE ACESSO À INFORMAÇÃO para atender ao Despacho Presidencial de 1º de janeiro de 2023"[16]	44	296
NÃO ATENDEU NENHUM dos itens anteriores	108	232

Análise

63. Antes de tudo, convém registrar um comentário com relação aos quatro respondentes que, na questão 5.1, marcaram a opção "Não se aplica" (Tabela 4 e Figura 4, resposta a0), a qual se destinava a fornecer uma possibilidade de resposta ao gestor que, eventualmente, pudesse entender que a medida em questão ("capacitação dos colaboradores em proteção de dados pessoais"), por alguma razão, não se aplica ao respectivo órgão/entidade. Entre suas orientações, essa questão mencionava: "Caso marque a opção 'Não se aplica', o gestor deve justificar nesse campo [de comentário] o seu entendimento pela não aplicação daquela medida/controle à sua organização".

64. De antemão, a equipe de auditoria não esperava receber como resposta nenhuma marcação dessa opção, tendo em vista que, naturalmente, a LGPD se aplica a todas as organizações públicas federais e, consequentemente, faz-se necessário que os órgãos/entidades capacitem seus colaboradores nessa temática. Verificando-se as justificativas desses quatro gestores, percebe-se que, na verdade, eles não compreenderam direito o comando da questão e marcaram essa opção por não terem encontrado, entre as demais opções, alguma que se encaixasse perfeitamente com a situação da organização (*e.g.* o órgão possui plano de capacitação, mas ainda não realizou treinamento dos colaboradores nessa área).

65. Nesses casos em que a situação atual do órgão/entidade se situa entre duas das opções existentes, o mais indicado seria o gestor adotar uma postura conservadora e marcar a opção "abaixo" que mais se aproximasse da realidade do órgão. No caso do exemplo citado, o gestor deveria marcar a opção a1 ("Não possui PLANO DE CAPACITAÇÃO e seus colaboradores ainda não realizaram treinamento em proteção de dados pessoais").

66. Contudo, registre-se que tais casos não trouxeram prejuízo aos resultados da auditoria, tendo em vista que, para todos os efeitos, inclusive para fins de atribuição de nota nas questões do "Tipo A" (e, consequentemente, para o cálculo do iLGPD), as marcações da opção "Não se aplica" foram consideradas equivalentes às marcações da primeira opção de resposta disponível.

67. Portanto, a questão 5.1 mostra que quase dois terços das organizações (244 das 387, ou 63,05%) não possuem plano de capacitação, ou possuem o plano, mas ainda não incluíram nele a necessidade de realizarem treinamento específico relacionado à proteção de dados pessoais (Tabela 4 e Figura 4, respostas a0 a a3).

68. Somente 98 órgãos/entidades (25,32%) contemplaram essa temática no respectivo plano de capacitação e já treinaram a maioria dos seus colaboradores nessa área (resposta a4), enquanto apenas 45 (11,63%) preveem no plano de capacitação a necessidade de treinamento diferenciado para as pessoas

que exercem funções com responsabilidades essenciais quanto à proteção de dados pessoais e já realizaram amplo treinamento dos colaboradores nessa área (resposta a5).

69. Entende-se que as 165 organizações (42,64%) que manifestaram ainda não possuir plano de capacitação (respostas a0, a1 e a2) devem providenciar a sua elaboração, tendo em vista tratar-se de documento essencial para garantir que os colaboradores estejam conscientes acerca das principais questões e problemas afetos ao órgão e mantenham sempre as competências e habilidades necessárias ao desempenho adequado das respectivas tarefas e atividades do dia a dia da organização no que diz respeito à privacidade e à proteção de dados pessoais (peça 922).

70. A seu turno, a análise das respostas à questão 5.2 encontra-se na Seção 3.8 deste relatório, que faz parte do Capítulo 3 (LAI x LGPD).

2.1.5. Conformidade do tratamento

71. 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 do art. 6º da LGPD são seguidos e que os tratamentos são fundamentados em, ao menos, uma das bases legais descritas na legislação.

72. A questão desta dimensão, então, aborda aspectos atinentes à conformidade das atividades de tratamento de dados pessoais realizadas pela organização frente aos princípios da LGPD, a exemplo de possuírem propósitos legítimos, específicos, explícitos e informados aos titulares de dados, de modo que estes possam compreender claramente as finalidades para as quais seus dados pessoais são tratados.

73. Ademais, a coleta deve se restringir aos dados pessoais estritamente necessários para cumprir com as finalidades de tratamento informadas, a retenção (armazenamento) dos dados deve durar apenas o tempo estritamente necessário para cumprir com essas mesmas finalidades, bem como devem ser identificadas e documentadas as bases legais que fundamentam todas as atividades de tratamento de dados pessoais da organização.

74. As possíveis bases legais estão previstas na Lei 13.709/2018, art. 7º, incisos I a X (consentimento, cumprimento de obrigação legal/regulatória, execução de políticas públicas pela Administração Pública, estudos por parte de órgão de pesquisa, execução de contratos, exercício regular de direitos em processo judicial/administrativo/arbitral, proteção da vida/incolumidade física do titular ou de terceiro, tutela da saúde, interesse legítimo do controlador ou de terceiro e proteção do crédito).

75. A organização também deve manter registro detalhado (*e.g.* inventário) das operações de tratamento de dados pessoais que realiza, especialmente quando baseadas no legítimo interesse (LGPD, art. 37). Esse registro pode contemplar, por exemplo: a identificação do tratamento, sua finalidade, a base legal que o fundamenta, a descrição das categorias dos titulares de dados pessoais envolvidos, os dados pessoais coletados, o tempo de retenção dos dados, o local de armazenamento dos dados, o responsável pelo processo de tratamento e as medidas de segurança adotadas.

76. Por fim, relativamente às suas operações de maior risco (Resolução - CD/ANPD 2/2022[17] [Regulamento de aplicação da LGPD a agentes de tratamento de pequeno porte], Anexo I, art. 4º), a organização deve elaborar RIPD[18], inclusive de dados sensíveis, para avaliar os possíveis riscos associados (LGPD, art. 38). Nesse relatório, a organização descreverá os tipos de dados coletados, a metodologia utilizada na coleta e as garantias de segurança das informações, identificará a probabilidade de ocorrência de cada fator de risco e o respectivo impacto sobre as liberdades e direitos fundamentais dos titulares de dados e avaliará as medidas, as salvaguardas e os mecanismos de mitigação de risco apropriados a cada hipótese.

77. Como referências normativas aplicáveis à dimensão "Conformidade do Tratamento", podem ser citadas a Lei 13.709/2018, art. 5º, inciso XVII, art. 6º, em especial incisos I, II e III, e arts. 7º, 37, 38 e 40, bem como a norma ABNT NBR ISO/IEC 27701:2019, itens 7.2.1 (Identificação e documentação do propósito), 7.2.2 (Identificação de bases legais), 7.2.5 (Avaliação de impacto de privacidade), 7.2.8 (Registros relativos ao tratamento de dados pessoais), 7.4.1 (Limite de coleta) e 7.4.7 (Retenção).

Questionário: pergunta 6.1 (TIPO B)

Tabela 6 - Distribuição das respostas à pergunta 6.1 do questionário.
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 5])

Questão 6.1: A organização:	Sim	Não
Identificou e DOCUMENTOU AS FINALIDADES de todas as suas principais atividades de tratamento de dados pessoais	190	197
Avaliou se COLETA APENAS OS DADOS ESTRITAMENTE NECESSÁRIOS para cumprir com as finalidades de tratamento de dados pessoais que foram identificadas	158	229
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	130	257
Identificou e DOCUMENTOU AS BASES LEGAIS que fundamentam todas as suas principais atividades de tratamento de dados pessoais	196	191
POSSUI REGISTRO(S) (*e.g.* INVENTÁRIO[S] DE DADOS PESSOAIS) instituído(s) para consolidar informações relacionadas às características das atividades de tratamento de dados pessoais	172	215
CATALOGOU NO(S) REGISTRO(S)/INVENTÁRIO(S) DE DADOS PESSOAIS informações que abrangem todas as suas principais atividades de tratamento de dados pessoais	151	236
Mantém REGISTRO DAS OPERAÇÕES de tratamento de dados pessoais que realiza, em especial quando o tratamento se baseia no legítimo interesse	117	270
JÁ ELABOROU ALGUM RIPD – Relatório de Impacto à Proteção de Dados Pessoais (LGPD, art. 5º, inciso XVII)	107	280
JÁ IMPLEMENTOU CONTROLES para mitigar os riscos identificados por meio da elaboração de RIPD (Relatório de Impacto à Proteção de Dados Pessoais)	83	304
AINDA NÃO ATENDE NENHUM dos itens anteriores	125	262

Análise

78. Quanto à questão 6.1 (Tabela 6), nota-se que, à exceção da documentação das bases legais, todas as demais práticas relativas à conformidade dos tratamentos de dados pessoais com a LGPD foram atendidas apenas pela minoria dos órgãos/entidades, com destaques negativos para a falta de manutenção de registro das operações de tratamento em 270 das 387 organizações auditadas (69,77%) e a ausência de elaboração de qualquer RIPD por 280 (72,35%) desses entes.

2.1.6. Direitos do titular

79. A organização deve assegurar que os titulares tenham acesso a informações relacionadas ao tratamento de seus dados pessoais por meio da publicação, de maneira clara e concisa, de informações relativas a esses tratamentos. A organização também deve estar preparada para atender todos os direitos dos titulares que são elencados na LGPD (arts. 9º e 17-22), em especial aqueles previstos no art. 18.

80. O art. 9º da LGPD, por exemplo, prevê o direito, aos titulares de dados, de acesso facilitado a uma série de informações: finalidade do tratamento; formas e duração do tratamento; identificação e dados de contato do controlador; informações acerca do uso compartilhado de dados e sua finalidade; responsabilidades dos agentes que realizam o tratamento; e direitos do titular. Além disso, a organização deve informar as hipóteses em que, no exercício de suas competências, realiza tratamento de dados pessoais, fornecendo informações sobre a finalidade, a base legal, os procedimentos e as práticas utilizadas para a execução dessas atividades.

81. As questões desta dimensão, então, abordam aspectos atinentes à elaboração da Política de Privacidade (também chamada de "Aviso de Privacidade") e ao atendimento dos diversos direitos do

titular de dados pessoais (*e.g.* confirmação da existência de tratamento; acesso aos dados; correção de dados incompletos/inexatos/desatualizados; revogação do consentimento; anonimização, bloqueio ou eliminação de dados desnecessários/excessivos ou que dependam de consentimento do titular; portabilidade dos dados; informações sobre compartilhamento de dados).

82. A Política/Aviso de Privacidade é um documento endereçado aos usuários de um sítio, serviço ou sistema (titulares de dados – público externo) com o propósito de dar visibilidade ao tratamento de dados pessoais que ocorre no âmbito desse sítio/serviço/sistema, de modo a demonstrar que os princípios da LGPD são atendidos[19]. Além de fornecer acesso ao documento no momento da coleta dos dados pessoais, convém que a organização o divulgue de forma permanente em seu sítio institucional, em local de fácil acesso aos titulares de dados pessoais.

83. A título de referências normativas aplicáveis à dimensão "Direitos do Titular", podem ser citadas a Lei 13.709/2018, art. 6º, em especial incisos IV e VI, arts. 9º e 17-22, art. 23, inciso I, e art. 50, inciso I, alíneas "a", "d" e "e", além da norma ABNT NBR ISO/IEC 27701:2019, itens 7.3 (Obrigações dos titulares de dados pessoais), 7.3.2 (Determinando as informações para os titulares de dados pessoais) e 7.3.3 (Fornecendo informações aos titulares de dados pessoais).

Questionário: pergunta 7.1 (TIPO A)

Tabela 7 - Distribuição das respostas à pergunta 7.1 do questionário.
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 5])

Questão 7.1: A organização elaborou e divulga em seu sítio eletrônico institucional Política de Privacidade (ou instrumento similar)?	**Qtde.**	**%**
a0) Não se aplica	6	1,55
a1) A organização NÃO ELABOROU POLÍTICA DE PRIVACIDADE (ou instrumento similar)	140	36,18
a2) A organização ELABOROU A POLÍTICA DE PRIVACIDADE (ou instrumento similar), MAS NÃO A DIVULGA em seu sítio eletrônico institucional	23	5,94
a3) A organização ELABOROU A POLÍTICA DE PRIVACIDADE (ou instrumento similar) E A DIVULGA em seu sítio eletrônico institucional	218	56,33
TOTAL	**387**	**100**

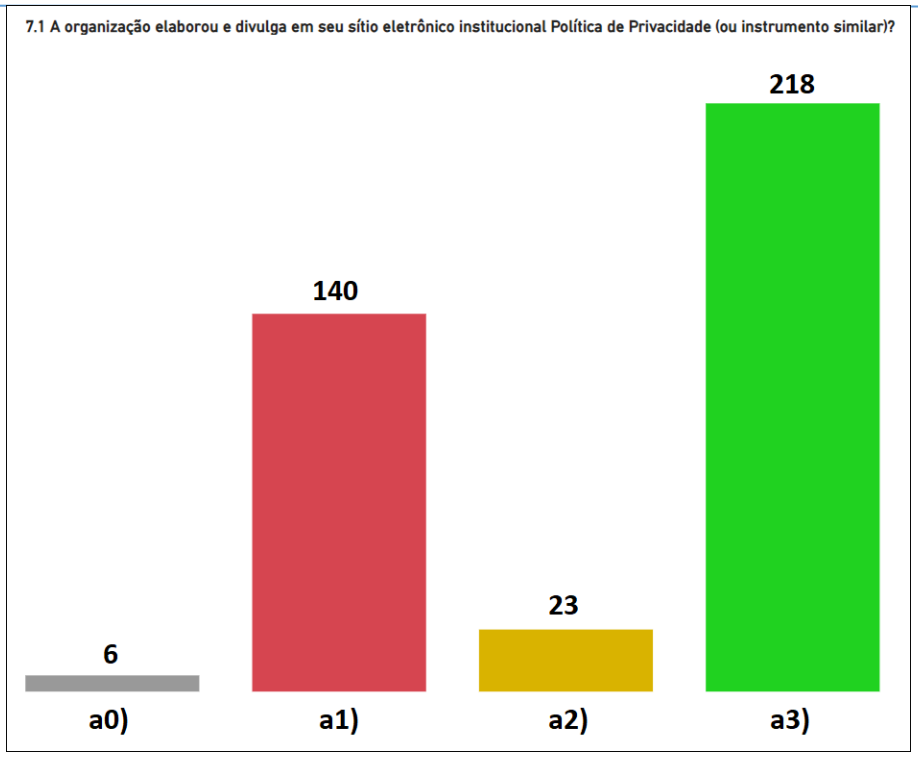


Figura 5 - Distribuição das respostas à pergunta 7.1 do questionário.
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 5])

Questionário: pergunta 7.2 (TIPO A)

Tabela 8 - Distribuição das respostas à pergunta 7.2 do questionário.
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 5])

Questão 7.2: Foram implementados mecanismos para atender os direitos dos titulares aplicáveis à organização, relacionados à obtenção de informações sobre o tratamento dos dados, de modo geral (LGPD, art. 9º), bem como sobre os seus dados específicos e o respectivo tratamento (art. 18)?	**Qtde.**	**%**
a0) Não se aplica	4	1,04
a1) Não foram implementados mecanismos para atender direitos dos titulares (LGPD, arts. 9º e 18)	86	22,22
a2) Foram implementados mecanismos para atender alguns dos direitos dos titulares (LGPD, arts. 9º e 18), mas não todos	137	35,40
a3) Foram implementados mecanismos para atender todos os direitos dos titulares (LGPD, arts. 9º e 18) aplicáveis à organização	160	41,34
TOTAL	**387**	**100**

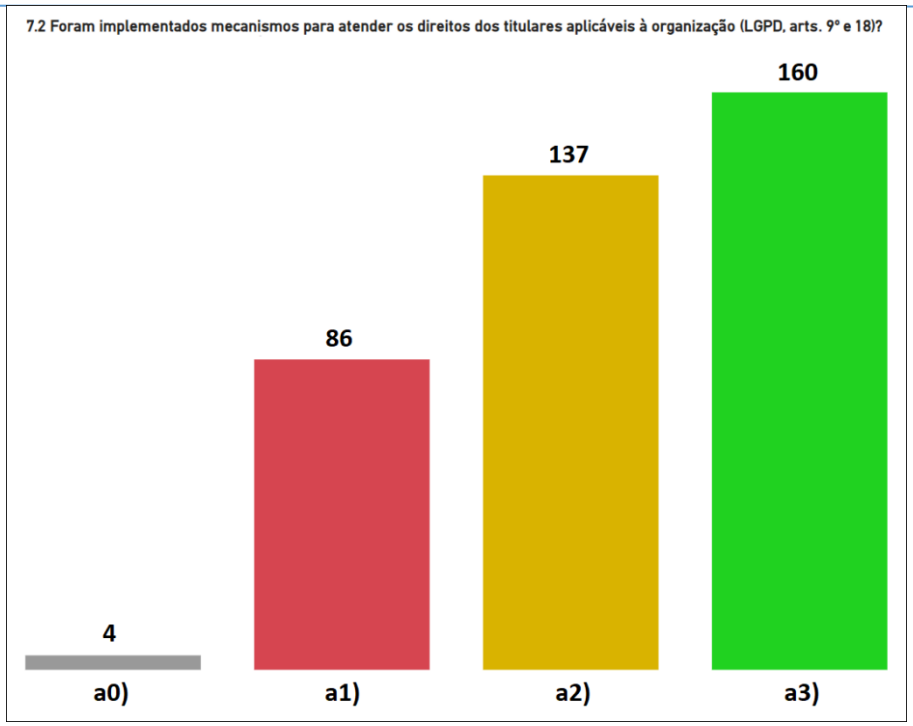


Figura 6 - Distribuição das respostas à pergunta 7.2 do questionário.
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 5])

Análise

84. Em primeiro lugar, é importante ressaltar que, para todos os efeitos, nas questões do "Tipo A", considerou-se a resposta "Não se aplica" equivalente à marcação da primeira opção de resposta disponível (parágrafos 63-66). A questão 7.1 indica que, das 387 organizações, 146 (37,73%) ainda não elaboraram Política de Privacidade (Tabela 7 e Figura 5, respostas "a0" e "a1"; peça 922), documento essencial para informar o público externo, em especial os titulares de dados, quanto aos tratamentos de dados pessoais realizados pelo órgão/entidade. Ademais, 23 organizações (5,94%), apesar de terem elaborado tal documento, não lhe dão a devida publicidade em seus sítios eletrônicos institucionais (resposta "a2").

85. No que se refere à questão 7.2, noventa das 387 organizações (23,26%) não implementaram mecanismos para atender os direitos dos titulares previstos nos arts. 9º e 18 da LGPD (Tabela 8 e Figura 6, respostas "a0" e "a1"; peça 922), ao passo que 137 órgãos/entidades (35,40%) afirmaram ter materializado instrumentos para atender apenas alguns desses direitos, mas não todos (resposta "a2").

2.1.7. Compartilhamento de dados pessoais

86. A organização deve identificar, avaliar e documentar detalhes relacionados aos compartilhamentos de dados pessoais com terceiros, tendo em vista que a realização de compartilhamento de dados pessoais demanda a adoção de controles adequados com vistas a mitigar os riscos que possam comprometer a segurança e a proteção desses dados.

87. Diante disso, a LGPD defende, por exemplo, que as partes envolvidas no compartilhamento adotem determinadas precauções, inclusive, em certos casos, exigindo a formalização de contrato, convênio ou instrumento congênere (LGPD, art. 26, § 1º, inciso IV) e a sua respectiva comunicação à ANPD (art. 26, § 2º). Nos eventuais casos de transferência internacional dos dados, a LGPD também apregoa, além da conformidade com os princípios, os direitos e o regime de proteção de dados previsto em seu escopo geral, a adoção de uma série de requisitos e cuidados especiais (arts. 33-36), os quais a organização precisa avaliar e cumprir.

88. Quanto ao uso de solução de computação em nuvem (*cloud computing*), a IN - GSI/PR 5/2021[7] prevê requisitos mínimos de segurança da informação, obrigatórios para órgãos e entidades da APF e que servem de parâmetro de boas práticas para qualquer organização que se preocupe com a segurança e a proteção dos dados que trata. Essa norma especifica medidas com vistas a proteger a confidencialidade, a integridade e a disponibilidade dos dados (*e.g.* definição de responsabilidades para os diferentes atores envolvidos na gestão da nuvem, gerenciamento de identidades e de registros/*logs*, adoção de criptografia), além de tratar da prevenção e da resposta a incidentes de segurança.

89. As questões desta dimensão, então, abordam aspectos atinentes à identificação dos dados pessoais que são compartilhados com terceiros, à devida avaliação e adequação dessas operações frente aos critérios previstos na LGPD, em especial nos arts. 26 (finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos/entidades públicos, respeitados, ainda, os princípios de proteção de dados pessoais do art. 6º) e 27 (compartilhamento de dados pessoais com pessoa de direito privado), ao registro dos eventos relacionados a esses compartilhamentos (quais dados foram compartilhados, com quem e quando), às transferências internacionais de dados pessoais e ao tratamento de dados pessoais em solução de computação em nuvem.

90. Como referências normativas aplicáveis à dimensão "Compartilhamento de Dados Pessoais", podem ser citadas a Lei 13.709/2018, em especial art. 5º, inciso XVI, arts. 26-27 e 30, arts. 33-36 e 39, arts. 44 e 50, § 2º, inciso I, alínea "d", a IN - GSI/PR 5/2021[7] (Requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos/entidades da APF), em especial arts. 17 e 18, a norma ABNT NBR ISO/IEC 27701:2019, itens 7.5.1 (Identificando as bases para a transferência de dados pessoais entre jurisdições), 7.5.2 (Países e organizações internacionais para os quais os dados pessoais podem ser transferidos), 7.5.3 (Registros de transferência de dados pessoais) e 7.5.4 (Registro de divulgação de dados pessoais para terceiros), além do "Guia Orientativo – Tratamento de dados pessoais pelo Poder Público"[10], da ANPD.

Questionário: pergunta 8.1 (TIPO A)

Tabela 9 - Distribuição das respostas à pergunta 8.1 do questionário.
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 5])

Questão 8.1: Quanto aos compartilhamentos de dados pessoais com terceiros, a organização:	**Qtde.**	**%**
a0) Não se aplica	14	3,62
a1) AINDA NÃO AVALIOU se os realiza ou AINDA NÃO IDENTIFICOU todos os dados eventualmente compartilhados	170	43,93
a2) AVALIOU se há esses compartilhamentos e, nos casos detectados, IDENTIFICOU todos os dados eventualmente compartilhados	68	17,57
a3) IDENTIFICOU todos os dados pessoais compartilhados com terceiros e INICIOU A AVALIAÇÃO desses compartilhamentos, porém ainda não pode atestar que todos estejam em conformidade com os critérios legais (LGPD, arts. 26-27)	69	17,83
a4) IDENTIFICOU todos os dados pessoais compartilhados, AVALIOU os compartilhamentos e ATESTA que todos ESTÃO EM CONFORMIDADE COM OS CRITÉRIOS LEGAIS (LGPD, arts. 26-27), apesar de ainda não manter registro dos eventos relacionados a cada compartilhamento	42	10,85
a5) IDENTIFICOU todos os dados pessoais compartilhados, AVALIOU os compartilhamentos, ATESTA que todos ESTÃO EM CONFORMIDADE COM OS CRITÉRIOS LEGAIS (LGPD, arts. 26-27), DISPONIBILIZA INFORMAÇÕES acerca do uso compartilhado de dados e sua finalidade (art. 9º, inciso V) e MANTÉM REGISTRO DETALHADO dos eventos relacionados a cada compartilhamento (quais dados foram compartilhados, com quem e quando)	24	6,20
TOTAL	**387**	**100**

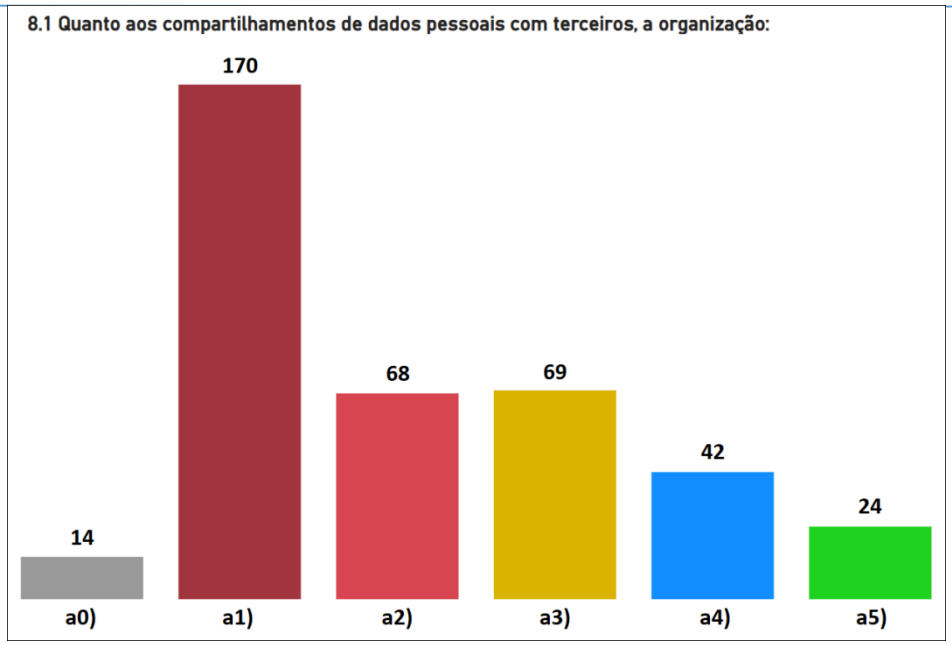


Figura 7 - Distribuição das respostas à pergunta 8.1 do questionário.
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 5])

Questionário: pergunta 8.1.1 (TIPO A)

Tabela 10 - Distribuição das respostas à pergunta 8.1.1 do questionário.
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 5])

Questão 8.1.1: A organização realiza transferência internacional de dados pessoais? (responderam esta questão apenas as 203 organizações que marcaram as opções a2, a3, a4 ou a5 na questão 8.1)	**Qtde.**	**%**
a1) Até o momento, não foi identificada transferência internacional de dados, porém a organização AINDA NÃO AVALIOU TODOS OS CASOS de compartilhamento de dados pessoais	77	37,94
a2) Todos os compartilhamentos foram avaliados e NÃO HÁ transferência internacional de dados	59	29,06
a3) Todos os compartilhamentos foram avaliados e HÁ TRANSFERÊNCIA INTERNACIONAL DE DADOS	67	33
TOTAL	**203**	**100**

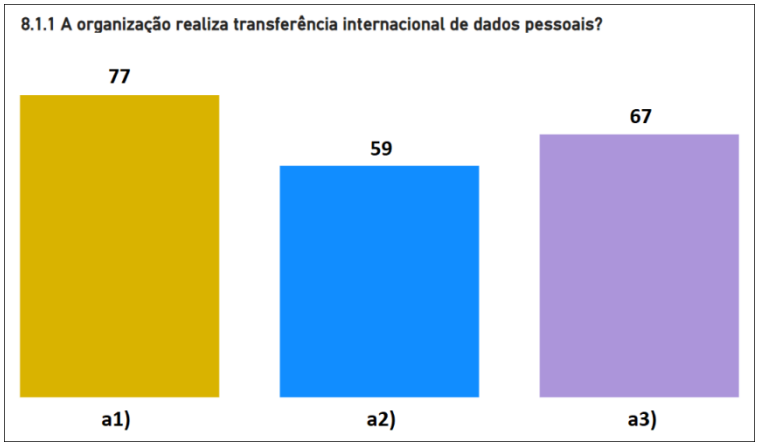


Figura 8 - Distribuição das respostas à pergunta 8.1.1 do questionário.
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 5])

Questionário: pergunta 8.1.1.1 (TIPO A)

Tabela 11 - Distribuição das respostas à pergunta 8.1.1.1 do questionário.
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 5])

Questão 8.1.1.1: As transferências internacionais de dados pessoais estão de acordo com os princípios, direitos e requisitos previstos na LGPD, em especial no art. 33? (responderam esta questão apenas as 67 organizações que marcaram a opção a3 na questão 8.1.1)	**Qtde.**	**%**
a1) A organização AINDA NÃO AVALIOU os princípios, direitos e requisitos previstos na LGPD, em especial no art. 33, em relação a todos os casos de transferência internacional de dados	20	29,85
a2) Todos os casos de transferência internacional de dados foram avaliados, porém AINDA NÃO ATENDEM integralmente os requisitos legais (LGPD, em especial art. 33)	15	22,39
a3) Todos os casos de transferência internacional de dados foram avaliados e ATENDEM INTEGRALMENTE OS REQUISITOS LEGAIS (LGPD, em especial art. 33)	32	47,76
TOTAL	**67**	**100**

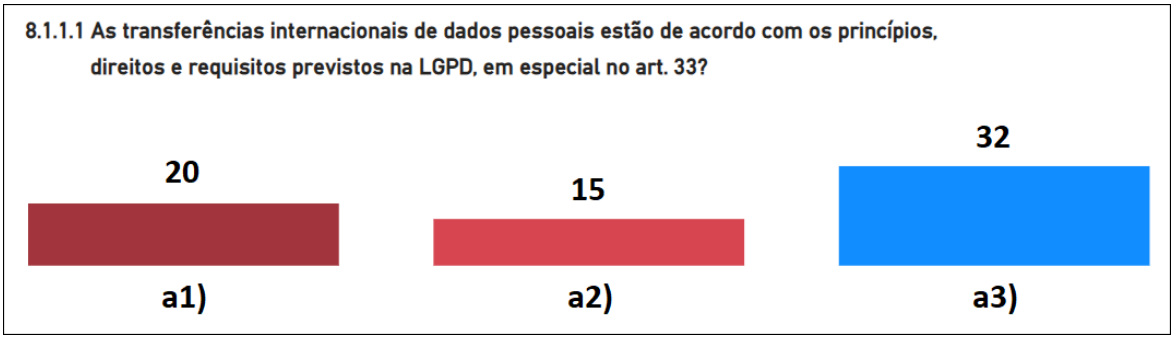


Figura 9 - Distribuição das respostas à pergunta 8.1.1.1 do questionário.
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 5])

Questionário: pergunta 8.1.2 (TIPO B)

Tabela 12 - Distribuição das respostas à pergunta 8.1.2 do questionário.
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 5])

Questão 8.1.2: Acerca de tratamento de dados pessoais em solução de computação em nuvem (*cloud computing*), a organização:	**Sim**	**Não**
REALIZA O TRATAMENTO DE DADOS PESSOAIS EM NUVEM (ainda que apenas armazenamento)	224	163
Avaliou e PODE ASSEGURAR QUE NÃO HÁ ARMAZENAMENTO DE DADOS PESSOAIS EM TERRITÓRIO ESTRANGEIRO	83	304
Realizou AVALIAÇÃO DE RISCOS relativamente a esse tratamento, amparada em análise e em relatório de impacto que foram devidamente submetidos à apreciação das instâncias competentes	36	351
INCLUIU, NOS INSTRUMENTOS CONTRATUAIS COM OS PROVEDORES DE NUVEM, CLÁUSULAS e mecanismos que garantem, ao menos, o sigilo dos dados no armazenamento e em trânsito, a não transferência dos dados a terceiros, a remoção incondicional dos dados após o término do contrato e a não utilização dos dados, para quaisquer fins, pelo provedor ou por terceiros	184	203
NÃO REALIZA NENHUM TRATAMENTO DE DADOS PESSOAIS EM NUVEM	108	279

Análise

91. A equipe de auditoria havia convencionado previamente que, nas questões do "Tipo A", a resposta "Não se aplica" seria considerada equivalente à marcação da primeira opção de resposta disponível (parágrafos 63-66). Apesar de essa interpretação ter feito bastante sentido para as questões 5.1, 7.1 e 7.2, na questão 8.1 foi identificada uma particularidade. Avaliando-se as justificativas apresentadas pelos gestores que marcaram essa opção, diferentemente desses três casos anteriores, na questão 8.1 a maioria dos gestores justificou a marcação da opção "Não se aplica" afirmando que o respectivo órgão/entidade não realiza compartilhamento de dados pessoais com terceiros.

92. No entanto, no que tange à construção do "Painel Nacional de Implementação da LGPD", de modo a manter a padronização com a solução adotada para as demais questões do "Tipo A", também na questão 8.1, para fins de cálculo do iLGPD, precisou ser atribuída a mesma nota (no caso, "0") às respostas "Não se aplica" e à primeira opção de resposta ("AINDA NÃO AVALIOU se os realiza ou AINDA NÃO IDENTIFICOU todos os dados eventualmente compartilhados").

93. Registre-se que tal atribuição penalizou injustamente essas quatorze organizações (Tabela 9 e Figura 7, resposta "a0"), visto que elas receberam avaliação "0" nesta dimensão não por deixarem de implementar controles e práticas adequadas, mas apenas por não compartilharem dados pessoais, o que, em essência, diz respeito às suas regras de negócio específicas, não ao quanto estes órgãos/entidades estejam mais ou menos adequados à LGPD. Inclusive, por essa mesma razão as questões 8.1.1 e 8.1.1.1 já haviam sido excluídas do cálculo do iLGPD (ver **Apêndice F** – Indicador de adequação à LGPD). Por questão de justiça, considera-se oportuno listar esses quatorze entes: Confe, DPU, Embratur, FUNAG, FUNASA, HFA, IFS, MME, Senai/DN, Senat/CN, Sesi/DN, Sest/CN, UFFS e UFPI.

94. Devido a essa particularidade, sugere-se que, em eventual próxima aplicação do questionário desta auditoria, o cálculo do iLGPD passe a desconsiderar a dimensão "Compartilhamento de dados pessoais" para as organizações que marcarem a opção de resposta "Não se aplica" na questão 8.1.

95. Feitas essas considerações, tem-se que, no que tange à questão 8.1, das 387 organizações, 170 (43,93%) ainda não avaliaram se compartilham dados pessoais com terceiros ou ainda não realizaram a devida identificação dos dados eventualmente compartilhados (Tabela 9 e Figura 7, resposta "a1"; peça 922), o que representa número expressivo. Entende-se que esses 170 órgãos/entidades devem avaliar a possibilidade de priorizar e de identificar esses compartilhamentos, tendo em vista o alto risco de vazamento de dados que representam, uma vez que, nesses casos, não se pode garantir que estejam de acordo com os critérios legais (LGPD, arts. 26-27).

96. Ademais, das 387 organizações auditadas, menos de um quinto (66, ou 17,05%) afirmaram que seus compartilhamentos de dados pessoais estão em conformidade com a Lei 13.709/2018 (respostas a4 e a5), sendo que apenas 24 (6,20%) sinalizaram que disponibilizam informações acerca desses compartilhamentos e sua finalidade (LGPD, art. 9º, inciso V) e mantêm registro detalhado dos eventos relacionados a cada compartilhamento (resposta "a5").

97. Das 203 organizações que já avaliaram seus compartilhamentos (questão 8.1.1), apenas 67 (33%) indicaram realizar transferência internacional de dados pessoais, isto é, afirmaram compartilhar esses dados com ente de outro país (Tabela 10 e Figura 8, resposta a3). E, desses 67 órgãos/entidades (questão 8.1.1.1), menos da metade (32, ou 47,76%) atestaram que esses compartilhamentos estão de acordo com as previsões da LGPD, em especial aquelas do art. 33 (Tabela 11 e Figura 9, resposta "a3").

98. Sobre o uso de soluções de computação em nuvem (*cloud computing*) para realizar tratamentos de dados pessoais (questão 8.1.2), a minoria das organizações avaliou adequadamente aspectos relevantes acerca desses tratamentos, com destaque negativo para o fato de que, das 387 organizações, pouco mais de um quinto (83, ou 21,45%) disseram ser capazes de assegurar que não há armazenamento de dados pessoais em território estrangeiro e menos de um décimo (36, ou 9,3%) afirmaram ter avaliado riscos em relação a tais tratamentos (Tabela 12).

2.1.8. Violação de dados pessoais

99. Como parte do seu processo de gestão de incidentes de segurança da informação, convém que a organização estabeleça papéis, responsabilidades e procedimentos específicos para assegurar respostas rápidas, efetivas e ordenadas a incidentes de segurança que envolvam violação de dados pessoais. Convém, ainda, que a organização possua um sistema de informação de gestão de incidentes próprio/adequado para registrar tanto os incidentes em si quanto o histórico das ações adotadas para solucioná-los/tratá-los, desde a eventual adoção inicial de uma solução de contorno, previamente à atuação para efetivamente analisar e erradicar as causas-raízes do incidente.

100. Ademais, tendo em vista que a identificação/detecção precoce pode diminuir significativamente os impactos causados por esses incidentes, a organização deve adotar mecanismos para monitorar proativa e continuamente os eventos que podem sinalizar (sinais precursores e indicadores) a ocorrência de incidentes de segurança associados à violação de dados pessoais, de modo que seja capaz de agir rapidamente nesses casos.

101. Por fim, a organização deve comunicar, em até três dias úteis, tanto à ANPD quanto aos próprios titulares de dados a ocorrência de incidente de segurança da informação que possa lhes acarretar risco ou dano relevante. Essa notificação deve mencionar, entre outras coisas: a natureza e a categoria dos dados pessoais afetados; informações sobre os titulares afetados, incluindo seu número e a discriminação de crianças, adolescentes e idosos, se houver; medidas técnicas e de segurança adotadas para a proteção dos dados, antes e após o incidente; riscos relacionados ao incidente; medidas que foram ou serão adotadas para reverter ou mitigar os efeitos do incidente sobre os titulares; datas da ocorrência do incidente e de seu conhecimento pelo controlador; dados do encarregado; descrição do incidente, incluindo a sua causa. Caso a organização não encaminhe tempestivamente essa comunicação, deverá expor, também, os motivos que levaram à demora (Resolução - CD/ANPD 15/2024[8], art. 6º).

102. A questão desta dimensão, então, aborda aspectos atinentes à identificação, ao registro e ao tratamento/resposta a incidentes de segurança da informação que envolvam violação de dados pessoais, bem como à existência de mecanismos e de procedimentos padronizados para notificação da ANPD e dos titulares de dados envolvidos nos casos de incidente.

103. A título de referências normativas aplicáveis à dimensão "Violação de Dados Pessoais", podem ser citadas a Lei 13.709/2018, em especial arts. 48 e 50, § 2º, inciso I, alínea "g", a Resolução - CD/ANPD 15/2024[8] (Regulamento de Comunicação de Incidente de Segurança), em especial arts. 6º-10, bem como a norma ABNT NBR ISO/IEC 27701:2019, itens 6.13.1.1 (Responsabilidades e procedimentos), 6.13.1.4 (Avaliação e decisão dos eventos de segurança da informação) e 6.13.1.5 (Resposta aos incidentes de segurança da informação).

Questionário: pergunta 9.1 (TIPO B)

Tabela 13 - Distribuição das respostas à pergunta 9.1 do questionário.
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 5])

Questão 9.1: A organização:	Sim	Não
Elaborou e mantém atualizado PLANO DE RESPOSTA A INCIDENTES (ou documento similar), sendo que abordou nesse documento questões específicas relacionadas ao tratamento/resposta a incidentes de segurança da informação que envolvem violação de dados pessoais	127	260
REGISTRA TODOS OS INCIDENTES de segurança da informação que envolvem violação de dados pessoais em sistema próprio/adequado a esse propósito	163	224
Sempre registra no sistema próprio/adequado a esse propósito TODAS AS AÇÕES QUE FORAM ADOTADAS PARA TRATAR/RESPONDER AO INCIDENTE de segurança da informação que envolve violação de dados pessoais, incluindo a eventual adoção de solução de contorno em um primeiro momento	132	255
MONITORA PROATIVA E CONTINUAMENTE a ocorrência de eventos (sinais precursores e indicadores) que podem ser associados a incidentes de segurança da informação que envolvem violação de dados pessoais	179	208

Estabeleceu e executa PROCEDIMENTOS PADRONIZADOS PARA COMUNICAR À ANPD E AO TITULAR DE DADOS a ocorrência de incidente de segurança da informação que possa acarretar risco ou dano relevante ao(s) titular(es)	137	250
AINDA NÃO ATENDE NENHUM dos itens anteriores	127	260

Análise

104. Quanto à gestão dos incidentes de segurança da informação envolvendo violação de dados pessoais, a minoria das 387 organizações assinalou atender aos itens relacionados (questão 9.1), sobretudo no que se refere à ausência de plano de resposta a esses incidentes (apenas 127, ou 32,82%, afirmaram ter elaborado tal documento), à falta de um sistema adequado para registro das ações adotadas nesses casos (somente 132, ou 34,11%, disseram registrar essas ações em sistema próprio) e à inexistência de processo padronizado para reportar esses incidentes à ANPD e ao titular de dados (apenas 137, ou 35,4%, marcaram que realizam essa comunicação de forma padronizada) [Tabela 13].

105. Acerca desse último ponto, inclusive, sugere-se dar ciência aos 250 órgãos/entidades que não executam procedimentos padronizados para comunicar incidentes à ANPD e aos titulares de dados, tendo em vista o possível descumprimento ao art. 48 da Lei 13.709/2018 (peça 920).

2.1.9. Medidas de proteção

106. A organização deve adotar amplas medidas de segurança, técnicas e administrativas, que tratam de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (LGPD, art. 46), com vistas a proteger os dados pessoais. Em especial, se houver, devem ser protegidos os dados pessoais sensíveis (relacionados a raça/etnia, saúde, vida sexual, convicção religiosa, opinião política, filiação a sindicato/organização de caráter religioso, filosófico ou político, dado genético ou biométrico) e os dados de crianças e de adolescentes.

107. Para isso, convém que o órgão/entidade defina papéis, responsabilidades e procedimentos claros voltados à proteção desses dados e implemente controles específicos que sejam capazes de mitigar riscos que possam resultar em violações de privacidade. Entre tais controles, pode-se citar a definição de processo formal para registro e cancelamento de usuários nos sistemas que realizam tratamento de dados pessoais, de modo a viabilizar a atribuição de direitos de acesso adequados a esses usuários.

108. O mesmo deve ser feito com o processo de provisionamento para conceder ou revogar os direitos de acesso, os quais devem observar os princípios da "necessidade de conhecer" (o colaborador só deve ter permissão para acessar informações que necessita para realizar seu trabalho) e da "necessidade de uso" (o colaborador só deve ter permissão para acessar recursos de TI [*e.g.* equipamentos, aplicações, procedimentos, salas] que necessita para desempenhar suas tarefas).

109. Adicionalmente, convém que a organização registre e monitore os eventos (*logs*) relacionados às 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 ocorrerem mudanças nesses dados, também deve ser registrada a ação realizada (*e.g.* inclusão, alteração ou exclusão). Convém, ainda, que a organização faça uso de soluções criptográficas para proteger de acessos indevidos os dados pessoais armazenados (em repouso) e trafegados (em trânsito), seja na rede interna da organização ou mesmo na Internet (durante o envio para um servidor na nuvem, por exemplo).

110. A organização também deve fornecer a seus colaboradores diretrizes e orientações a respeito do uso de técnicas e ferramentas tecnológicas capazes de anonimizar, pseudonimizar, ocultar, mascarar e/ou tarjar dados pessoais, em especial no que se refere a temas transversais das organizações públicas (*e.g.* licitações, contratos, gestão de recursos humanos), o que contribui para evitar negativas indevidas, com base na LGPD, de pedidos de acesso solicitados via LAI (Lei 12.527/2011), com prejuízo à transparência das informações e ao controle social da Administração Pública (ver Capítulo 3).

111. Por fim, a organização deve assegurar que seus processos e sistemas sejam projetados, desde a concepção, de forma que os tratamentos de dados pessoais associados estejam limitados ao que é estritamente necessário ao alcance das finalidades pretendidas (*Privacy by Design* e *Privacy by Default*).

112. A questão desta dimensão, então, aborda aspectos atinentes à implementação de controles adequados para proteger os dados pessoais e mitigar os riscos de violação, a exemplo da restrição e do rastreamento das atividades e dos acessos aos sistemas que realizam o tratamento desses dados, da utilização de criptografia para evitar acessos indevidos (a dados armazenados ou mesmo em trânsito), do uso de técnicas e de ferramentas para mascaramento/ocultação/tarjamento de dados pessoais e da concepção de processos e de sistemas que estejam conformes com os ditames da LGPD.

113. Como referências normativas úteis à dimensão "Medidas de Proteção", podem ser citadas a Lei 12.527/2011, arts. 3º e 7º, § 2º, arts. 10-14, e arts. 31 e 40, a Lei 13.709/2018, art. 13, § 4º, arts. 44 e 46, em especial § 2º, e arts. 49 e 50, § 2º, inciso I, alíneas "c" e "d", o Decreto 7.724/2012 (Regulamenta a LAI), arts. 11-20, 55, 57, 58, inciso III, e arts. 67 e 68, a Portaria Normativa - CGU 71/2023[15] (Aprova enunciados referentes à aplicação da Lei 12.527/2011), sobretudo o Enunciado 12, bem como as normas ABNT NBR ISO/IEC 27002:2013, item 6.1 (Organização interna), em especial item 6.1.1 (Responsabilidades e papéis pela segurança da informação), e ABNT NBR ISO/IEC 27701:2019, itens 6.6.2.1 (Registro e cancelamento de usuário), 6.6.2.2 (Provisionamento para acesso de usuário), 6.7 (Criptografia), 6.9.4.1 (Registros de eventos [*logs*]) e 7.4 (*Privacy by Design* e *Privacy by Default*).

Questionário: pergunta 10.1 (TIPO B)

Tabela 14 - Distribuição das respostas à pergunta 10.1 do questionário.
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 5])

Questão 10.1: A organização:	**Sim**	**Não**
É capaz de comprovar que ADOTA AMPLAS MEDIDAS DE SEGURANÇA, TÉCNICAS E ADMINISTRATIVAS aptas a proteger os dados pessoais que trata, tendo, inclusive, definido e atribuído papéis, responsabilidades e procedimentos específicos com esse propósito	132	255
Implementou PROCESSO FORMAL PARA REGISTRO, CANCELAMENTO E PROVISIONAMENTO DE USUÁRIOS nos sistemas que realizam tratamento de dados pessoais	160	227
REGISTRA E MONITORA EVENTOS (*LOGS*) relacionados às atividades de tratamento de dados pessoais	147	240
Utiliza criptografia para proteger os dados pessoais quando estes estão em repouso, ou seja, a chamada CRIPTOGRAFIA DE ARMAZENAMENTO	100	287
Utiliza criptografia para proteger os dados pessoais quando estes estão em trânsito na rede interna da organização ou na Internet, ou seja, a chamada CRIPTOGRAFIA DE PONTA-A-PONTA	188	199
Possui NORMA(S) INTERNA(S) que orientam os colaboradores quanto à obrigatoriedade do uso de MASCARAMENTO/OCULTAÇÃO/TARJAMENTO em documentos de interesse coletivo ou geral que contenham dados pessoais, de modo a possibilitar dar acesso a tais documentos sem comprometer esses dados	81	306
Disponibiliza aos colaboradores FERRAMENTA/SOLUÇÃO TECNOLÓGICA PARA REALIZAÇÃO DO MASCARAMENTO/OCULTAÇÃO/TARJAMENTO em documentos de interesse coletivo ou geral que contenham dados pessoais	125	262
Adota medidas para assegurar que seus processos e sistemas sejam projetados, desde a concepção, em conformidade com a LGPD (*PRIVACY BY DESIGN* E *PRIVACY BY DEFAULT*)	118	269
AINDA NÃO ATENDE NENHUM dos itens anteriores	77	310

Análise

114. A minoria das 387 organizações, também, indicou implementar medidas para proteger adequadamente os dados pessoais que trata (questão 10.1), com destaques negativos para a baixa

realização de criptografia sobre os dados armazenados (apenas 100, ou 25,84%, afirmaram criptografar esses dados) e a falta de normatização a respeito (somente 81, ou 20,93%) e de utilização de soluções para mascarar os dados pessoais em documentos de interesse coletivo ou geral (apenas 125, ou 32,3%), os quais, eventualmente, podem precisar ser divulgados (Tabela 14).

115. Frise-se que ambas (criptografia e mascaramento/tarjamento de dados) são medidas capazes de evitar a materialização da maioria dos riscos de violação de dados pessoais aqui tratados.

2.2. Questões finais

116. Espera-se que os gestores compreendam bem cada uma das nove dimensões avaliadas nesta auditoria (Seções 2.1.1 a 2.1.9 deste relatório), bem como as subpráticas específicas questionadas no bojo de cada uma dessas dimensões, de modo que possam se programar para, ao longo dos próximos meses/anos, implementarem, nas respectivas organizações, os controles faltantes/pendentes, de forma obrigatória (no caso de estarem prescritos em lei ou regulamento aplicável às organizações públicas federais) ou de maneira opcional (no caso de boas práticas que forem aplicáveis às suas realidades organizacionais, segundo suas próprias avaliações), frisando-se, novamente, que o questionário não pretendeu ser exaustivo em relação às medidas e aos controles possíveis de serem implementados para adequação das organizações à LGPD.

117. Nesse sentido, torna-se fundamental, também, a atuação das unidades de controle/auditoria interno/a para assegurar que as leis, as normas gerais e as normas internas sejam efetivamente observadas, bem como para avaliar riscos em relação aos processos de trabalho da organização. No âmbito do Poder Executivo federal, as instâncias do sistema de controle interno são as Assessorias Especiais de Controle Interno (AECI) e as auditorias internas, de acordo com o Decreto 3.591/2000 (Sistema de Controle Interno do Poder Executivo Federal) e as INs CGU 3/2017[20] e 13/2020[21].

Questionário: pergunta 11.1 (TIPO B)

118. A questão 11.1 aferiu se a instância de controle interno da organização, ao longo dos últimos três anos, atuou nas áreas de proteção de dados pessoais (LGPD) e de transparência da gestão (LAI).

Tabela 15 - Distribuição das respostas à pergunta 11.1 do questionário.
(Fonte: respostas das organizações à pergunta 11.1 do questionário)

Questão 11.1: Nos últimos 3 (três) anos, a instância do "sistema de controle interno governamental" da organização realizou avaliação relacionada com o tema:	**Sim**	**Não**
PROTEÇÃO DE DADOS PESSOAIS (Lei Geral de Proteção de Dados Pessoais – LGPD)	137	250
TRANSPARÊNCIA DA GESTÃO relativa às informações de interesse coletivo ou geral (Lei de Acesso à Informação – LAI)	193	194
AINDA NÃO FOI REALIZADA AVALIAÇÃO DE NENHUM DESSES TEMAS (LGPD ou LAI)	159	228

Análise

119. A análise das respostas à questão 11.1 encontra-se na Seção 3.8 deste relatório.

Questionário: pergunta 11.2 (texto aberto)

120. Por fim, por meio de uma pergunta com opção de resposta em texto aberto (questão 11.2), oportunizou-se que os gestores registrassem os principais desafios, deficiências e pontos de atenção relacionados à adequação das suas respectivas organizações à LGPD, bem como quaisquer outras considerações, comentários ou críticas que considerassem pertinentes.

Análise

121. A Figura 10 apresenta uma nuvem na qual o tamanho das palavras ou expressões é proporcional ao número de vezes em que essas foram citadas nas respostas à referida questão.

Figura 10 - Desafios, deficiências e pontos de atenção mais citados pelos gestores das organizações auditadas.
(Fonte: elaboração própria, com base nas respostas das organizações à pergunta 11.2 do questionário)

122. Desconsiderando-se "LGPD", "dado" e "dados pessoais", naturalmente bastante citadas, vê-se que foram muito referenciadas nas respostas, entre outras, as palavras "proteção", "privacidade", "segurança", "adequação" e "processo". Não é difícil perceber que tais palavras estão diretamente relacionadas ao conjunto de controles avaliados nesta auditoria, ao longo das nove dimensões definidas, por meio do questionário aplicado às organizações (**Apêndice D** – Questionário da auditoria).

2.3. Análise de evidências

123. Em uma auditoria com o uso da metodologia CSA (parágrafo 17), a solicitação da anexação de evidências contribui para gerar expectativa de controle e, consequentemente, para aumentar a confiabilidade das respostas fornecidas pelos gestores.

124. A partir das evidências recebidas, os auditores passam a ser capazes de realizar, além das avaliações apenas formais (testes de *design*), também avaliações materiais (testes de operação). Ou seja, os auditores podem aprofundar a análise sobre os controles envolvidos, uma vez que podem avançar de uma avaliação sobre a mera existência ou não de determinada medida ou documento (*e.g.* "O órgão possui política de proteção de dados?") para uma avaliação acerca da qualidade da medida/documento em questão (*e.g.* "A política de proteção de dados do órgão é boa/suficiente/adequada?").

125. Com esse raciocínio em mente, durante a fase de planejamento da auditoria foram definidos vários documentos passíveis de serem solicitados para possível análise qualitativa pela equipe. Em efeito, o questionário aplicado (**Apêndice D** – Questionário da auditoria) demandou a anexação de cinco documentos, a saber: Q4.1.1: Política de Proteção de Dados Pessoais (ou instrumento similar); Q5.1.1: Plano de Capacitação (ou instrumento similar); Q6.1.1: Relatório de Impacto à Proteção de Dados Pessoais (RIPD); Q7.1.1: Política de Privacidade (ou instrumento similar); e Q9.1.1: Plano de Resposta a Incidentes (ou documento similar). Essa solicitação era condicional, isto é, tais pedidos só apareciam caso o respondente, na pergunta anterior, indicasse que o órgão possuía esse documento.

126. Ademais, para nortear essas análises qualitativas, para dois desses documentos foram elaborados, previamente, *checklists* de verificação (**Apêndice G** – *Checklist* para verificação de Política de Proteção de Dados Pessoais; e **Apêndice H** – *Checklist* para verificação de Política de Privacidade).

127. Durante a execução da auditoria, surgiu a ideia de utilizar uma solução programada com o uso de inteligência artificial (IA) para automatizar a avaliação, com base nos citados *checklists*, dos documentos anexados pelos gestores. Nesse ponto, cabe um agradecimento especial ao auditor Fernando Lima Gama Júnior, que desenvolveu a ferramenta capaz de analisar as evidências de forma automatizada

e com resultados confiáveis, aferidos por meio de análises individuais de alguns resultados feitas pela equipe de auditores (ver **Apêndice I** – Análise de evidências com uso de IA [GabiChecks]).

128. No total, em resposta às questões Q4.1.1 e Q7.1.1, foram recebidos 461 documentos, sendo 220 políticas de proteção de dados pessoais e 241 políticas de privacidade. A ideia inicial era avaliar todos, porém, em virtude dos custos operacionais associados, bem como do caráter ainda experimental da solução desenvolvida (GabiChecks), considerou-se suficiente analisar uma amostra representativa e aleatória de cerca de um terço desses documentos, ou seja, 145, sendo 71 políticas de proteção de dados pessoais e 74 políticas de privacidade. As Tabelas 16 e 17 sintetizam os resultados obtidos.

Tabela 16 - Avaliação automatizada, com uso de IA, de 71 políticas de proteção de dados pessoais.
(Fonte: elaboração própria, a partir da base de dados gerada pela execução do GabiChecks [íntegra na peça 915, p. 1-2])

#	Sigla	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Total
1	UFES	1	0	0	0	0	0	0	0	1	1	**3**
2	CFO	1	0	0	0	0	0	0	1	1	1	**4**
3	EMGEA	1	0	1	0	0	0	0	0	1	1	**4**
...												
69	TRT6	1	1	1	1	1	1	1	1	1	1	**10**
70	TRT9	1	1	1	1	1	1	1	1	1	1	**10**
71	UNIFAL-MG	1	1	1	1	1	1	1	1	1	1	**10**
Totais:		**71**	**39**	**53**	**60**	**61**	**64**	**60**	**66**	**71**	**50**	

Tabela 17 - Avaliação automatizada, com uso de IA, de 74 políticas de privacidade.
(Fonte: elaboração própria, a partir da base de dados gerada pela execução do GabiChecks [íntegra na peça 915, p.3-4])

#	Sigla	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Total
1	FUB	1	0	0	0	0	0	0	0	0	0	0	**1**
2	MME	1	0	0	0	0	0	0	0	0	0	0	**1**
3	UFTM	1	0	0	0	0	0	0	0	0	0	0	**1**
...													
72	TRT23	1	1	1	1	1	1	1	1	1	1	1	**11**
73	UFPI	1	1	1	1	1	1	1	1	1	1	1	**11**
74	UNIFEI	1	1	1	1	1	1	1	1	1	1	1	**11**
Totais:		**74**	**39**	**58**	**55**	**60**	**46**	**59**	**56**	**60**	**65**	**30**	

129. Como era de se esperar, a avaliação do primeiro quesito (“Existe o documento?”) retornou “1” (“Sim”) para todos os casos, tendo em vista que se passou um documento PDF para a ferramenta analisar e já se afirmou, de antemão, tratar-se de uma política de proteção de dados pessoais (Tabela 16) ou de uma política de privacidade (Tabela 17).

130. No caso das políticas de proteção de dados pessoais (Tabela 16), é interessante notar que todos os 71 documentos analisados também atenderam o quesito 9 (“A política de PD prevê a necessidade de comunicação/conscientização aos interessados?”). Os quesitos menos atendidos foram o segundo (“A política de PD foi publicada para as partes interessadas?”; apenas 39 de 71, ou 54,93%) e o décimo (“A política de PD prevê a sua revisão periódica ou quando ocorrerem mudanças significativas?”; 50 de 71, ou 70,42%).

131. A seu turno, quanto às políticas de privacidade (Tabela 17), os quesitos menos atendidos foram o segundo ("A política foi publicada para as partes interessadas?"; somente 39 de 74, ou 52,7%), o sexto ("A política informa sobre como o titular de dados pode obter as informações previstas no art. 18 da LGPD?"; 46 de 74, ou 62,16%) e o décimo primeiro ("A política informa a data de sua última atualização?"; 30 de 74, ou 40,54%).

132. Tais análises, em função de serem automatizadas, permitem identificar rapidamente órgãos e entidades com uma política (ou outro tipo de documento) supostamente de menor qualidade (a partir do atendimento de menos quesitos do *checklist* fornecido), de modo que se possa planejar ações de controle voltadas para suprir essas carências com foco nessas organizações específicas (primeiras linhas das Tabelas 16 e 17).

133. É preciso, no entanto, reforçar a importância de revisões posteriores, por parte dos auditores da equipe, dos resultados derivados do uso desse tipo de automação, sobretudo caso eles venham a subsidiar propostas sancionatórias às organizações envolvidas. No caso concreto, foram identificadas inconsistências pontuais nas análises de alguns quesitos realizadas pelo GabiChecks, tendo sido erroneamente atribuída a nota "0" ("Não") e associadas mensagens tais como "Não foi possível encontrar um documento anexado a esta conversa", "Não encontrei um documento para analisar" ou "Não foi fornecido nenhum arquivo para análise", sendo que havia um documento PDF para ser analisado.

2.4. Comparação entre o iLGPD 2021 e o iLGPD 2024

134. De modo a possibilitar uma rápida comparação dos resultados desta auditoria com aqueles obtidos na auditoria de 2021[1], foi feito o exercício teórico de enquadrar os dados atuais, também, nas mesmas faixas/níveis de adequação que haviam sido definidas naquela fiscalização ("Inexpressivo": indicador ≤ 15%; "Inicial": indicador entre 15% e 50%; "Intermediário": indicador entre 50% e 80%; e "Aprimorado": indicador > 80%). Os resultados são apresentados na Tabela 18.

Tabela 18 - Rápida comparação entre o iLGPD 2021 e o iLGPD 2024.
(Fonte: elaboração própria, com base nos dados do TC 039.606/2020-1 e desta auditoria)

Nível de adequação à LGPD	Auditoria 2021	Auditoria 2024
Inexpressivo	68 (17,8%)	52 (13,44%)
Inicial	225 (58,9%)	174 (44,96%)
Intermediário	78 (20,4%)	128 (33,07%)
Aprimorado	11 (2,9%)	33 (8,53%)
Totais	**382 (100%)**	**387 (100%)**

135. Dessa análise, percebe-se que, provavelmente, houve evolução na adequação das organizações públicas federais à LGPD entre essas duas avaliações (2021 e 2024), com a diminuição das quantidades de órgãos/entidades que figuram nos primeiros níveis ("Inexpressivo" e "Inicial") e o aumento dos números de entes que se enquadram nos níveis "Intermediário" e "Aprimorado".

136. Essa comparação, contudo, é feita apenas para fins didáticos, tendo em vista que os questionários aplicados nessas duas fiscalizações são diferentes, apesar de versarem, em essência, sobre os mesmos conteúdos e terem sido estruturados em torno dos mesmos dois eixos e nove dimensões (Figura 2). Ademais, na auditoria atual, houve mudança nas faixas de valores que determinam a classificação das organizações nos diferentes níveis de adequação à LGPD (Figura 15; ver **Apêndice F** – Indicador de adequação à LGPD).

3. LAI x LGPD

137. As Leis 12.527/2011 (LAI) e 13.709/2018 (LGPD) representam dois marcos regulatórios fundamentais no Brasil, cada uma abordando aspectos cruciais da relação entre o Estado, os cidadãos e os seus respectivos dados pessoais.

138. Enquanto a LAI visa a garantir o acesso público às informações detidas pelo Estado, fomentando a transparência e o controle social, a LGPD busca proteger os dados pessoais dos indivíduos, estabelecendo regras sobre a coleta, o tratamento e a transferência desses dados.

139. Embora possuam objetivos complementares (promoção da transparência e proteção da privacidade), essas duas legislações são baseadas em princípios que podem, à primeira vista, em determinadas situações, parecer conflitantes. Pior ainda são os casos, não raros, em que gestores utilizam a LGPD como pano de fundo para justificar retrocessos e falta de transparência quanto à divulgação de informações de interesse público[22].

140. A seguir, então, são detalhados os princípios que norteiam essas legislações (LAI e LGPD), bem como os falsos conflitos entre eles.

3.1. Princípios que norteiam a Lei de Acesso à Informação (LAI)

141. Publicidade como preceito geral: estabelece que a informação detida pelo Estado é pública por natureza e deve ser acessível a todos os cidadãos, salvo em casos específicos previstos em lei;

142. Sigilo como exceção: o sigilo é aplicado apenas em situações estritamente necessárias para a segurança do Estado e da sociedade, o que garante que o acesso às informações não seja indevidamente restringido;

143. Transparência: a LAI exige que as informações sejam disponibilizadas de forma clara, precisa e em linguagem acessível, promovendo, assim, a transparência na gestão pública;

144. Controle social: permite que os cidadãos monitorem e avaliem as ações do governo, contribuindo para a fiscalização e o controle da gestão pública.

3.2. Princípios que norteiam a Lei Geral de Proteção de Dados Pessoais (LGPD)

145. Proteção da privacidade: a LGPD coloca a privacidade como um direito fundamental, protegendo os dados pessoais dos indivíduos contra uso indevido;

146. Consentimento do titular: exige, para viabilizar o tratamento de dados pessoais, a obtenção do consentimento do titular dos dados, de forma clara e específica, salvo nas exceções previstas em lei;

147. Finalidade: o tratamento dos dados deve ter uma finalidade legítima, específica e informada ao titular dos dados, não podendo ocorrer de forma incompatível com esses propósitos;

148. Necessidade: os dados coletados e os respectivos períodos de guarda devem se limitar ao mínimo necessário para a realização dos fins pretendidos, evitando-se a coleta de dados em excesso ou o seu armazenamento por tempo além do necessário;

149. Segurança da informação: a LGPD exige a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas.

3.3. Dados pessoais sensíveis

150. A LGPD define dados pessoais sensíveis como aqueles relacionados à origem racial ou étnica, convicções religiosas, opiniões políticas, filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, estabelecendo restrições específicas ao tratamento de tais dados e exigindo, em muitos casos, consentimento explícito do titular para o seu uso.

151. Por outro lado, a LAI promove o acesso amplo e irrestrito às informações detidas pelo Estado, fundamentando-se na premissa de que a transparência é valor essencial para promover o controle social e sustentar a própria democracia. A LAI permite que cidadãos solicitem e recebam informações do governo, incluindo dados que, sob a ótica da LGPD, podem ser considerados sensíveis.

3.4. Potenciais pontos de conflito

152. Acesso x Proteção: o conflito mais evidente entre a LAI e a LGPD surge na tensão entre o direito de acesso à informação pública e a necessidade de proteger a privacidade e os dados pessoais,

especialmente aqueles considerados sensíveis. Enquanto a LAI visa a garantir a máxima divulgação das informações, a LGPD busca limitar o tratamento de dados pessoais para proteger a privacidade dos indivíduos.

153. Consentimento do titular: a LGPD enfatiza a importância do consentimento do titular dos dados para o tratamento dos seus dados pessoais, incluindo aqueles considerados sensíveis. No entanto, a aplicação desse princípio pode ser desafiadora no contexto da LAI, no qual o acesso às informações detidas pelo Estado pode envolver a eventual divulgação de dados pessoais sem o consentimento direto do titular.

154. Finalidade e necessidade: a LGPD estabelece que o tratamento de dados pessoais deve ser realizado para finalidades legítimas, explícitas e informadas ao titular de dados, além de se limitar ao mínimo necessário para alcançar essas finalidades. Ao promover o acesso amplo às informações, a LAI pode entrar em conflito com esses princípios caso a divulgação de informações inclua dados pessoais sensíveis sem uma finalidade específica que justifique o seu tratamento.

3.5. Resolução dos conflitos LAI x LGPD

155. A resolução dos conflitos entre a LAI e a LGPD exige uma abordagem equilibrada, a qual considere tanto o interesse público no acesso às informações quanto a importância de se proteger a privacidade e os dados pessoais dos indivíduos, em especial aqueles considerados sensíveis. Tal abordagem pode envolver:

155.1. Ponderação de interesses: avaliar, caso a caso, a necessidade de divulgação das informações em relação à necessidade de proteção dos dados pessoais sensíveis, aplicando-se, também, o princípio da proporcionalidade;

155.2. Anonimização/pseudonimização/ocultação/mascaramento: sempre que possível, anonimizar, pseudonimizar, ocultar ou mascarar os dados pessoais sensíveis contidos nos documentos e informações a serem divulgados, de modo a garantir a proteção da privacidade dos indivíduos, sem prejuízo do fomento à transparência.

155.3. Exceções: definir claramente as situações em que se pode restringir o acesso à informação para proteger dados pessoais sensíveis, garantindo a justa e transparente aplicação dessas exceções.

3.6. Preponderância de uma lei sobre a outra em pontos específicos

156. A preponderância de uma legislação sobre a outra não é um conceito absoluto, mas, sim, relativo e dependente do contexto específico de cada caso. Em determinadas situações, os princípios da LAI podem ter precedência, especialmente quando o interesse público na transparência e no acesso às informações é considerado primordial para a fiscalização da gestão pública e o exercício da cidadania. Por outro lado, em situações em que a proteção dos dados pessoais é essencial para a salvaguarda da privacidade e da dignidade humana, os princípios da LGPD devem prevalecer.

157. Uma situação específica de possível preponderância pode ocorrer em casos em que a divulgação de informações públicas envolve dados pessoais sensíveis, pois a LGPD pode ter uma posição de maior relevância, ao exigir que sejam adotadas medidas de proteção adequadas para evitar danos aos titulares dos dados. A seu turno, a LAI pode prevalecer em situações em que a divulgação de informações é essencial para o controle social e a fiscalização de atos governamentais, desde que sejam respeitadas as devidas cautelas para a proteção de dados pessoais, em especial aqueles sensíveis.

3.7. Hermenêutica adequada para avaliar casos concretos

158. A hermenêutica jurídica (arte/ciência de interpretar as leis) desempenha papel crucial na resolução dos eventuais conflitos entre a LAI e a LGPD. Para avaliar casos concretos, recomenda-se adotar uma abordagem hermenêutica que privilegie a ponderação de interesses e a proporcionalidade. Isso significa avaliar cuidadosamente os principais aspectos em jogo em cada caso, buscando-se o melhor equilíbrio entre o direito ao acesso à informação, por um lado (LAI), e a proteção da privacidade dos indivíduos e a segurança dos dados pessoais, por outro (LGPD).

159. Uma interpretação legislativa baseada na ponderação de interesses envolve a análise das finalidades específicas da divulgação das informações e do tratamento daquele conjunto de dados pessoais, levando-se em consideração e sopesando-se os princípios norteadores de ambas as leis. Essa abordagem permite identificar soluções que harmonizem os direitos e os deveres estabelecidos em cada uma delas (LAI e LGPD), garantindo-se, assim, que estes sejam respeitados, na medida do possível.

160. Além disso, a interpretação conforme a Constituição é outra ferramenta hermenêutica relevante, capaz de assegurar que a aplicação das leis esteja alinhada com os direitos fundamentais e os valores constitucionais. Isso inclui a proteção da privacidade, a liberdade de expressão e o direito à informação, que devem ser sempre considerados na análise de casos concretos envolvendo LAI e LGPD.

161. Constata-se, portanto, que inexiste preponderância absoluta de uma legislação sobre a outra, sendo necessário, quando da análise de conflitos aparentes entre a LAI e a LGPD, avaliar questões específicas e sopesar os princípios envolvidos em cada situação concreta.

162. Logo, a escolha da hermenêutica mais adequada para a avaliação de casos concretos se torna essencial para a resolução de conflitos potenciais entre essas duas leis. A adoção de uma abordagem hermenêutica que privilegie a ponderação de interesses e a proporcionalidade, bem como a interpretação conforme a Constituição, são fundamentais para garantir uma coexistência harmoniosa entre a promoção da transparência, trazida pela LAI, e a proteção da privacidade, buscada pela LGPD, assegurando-se e respeitando-se, assim, os direitos fundamentais dos cidadãos.

3.8. Análise das respostas às questões 5.2 e 11.1

163. Das 387 organizações auditadas, 47 (12,15%) manifestaram não ter realizado treinamento dos colaboradores em proteção de dados pessoais (Tabela 4 [repetida a seguir], respostas a0 e a1). As 340 organizações restantes, então, foram instadas a responder acerca da realização de ações complementares relacionadas à necessidade de transparência da gestão quanto às informações de interesse coletivo ou geral (Lei 12.527/2011), ou seja, quanto à capacitação desse mesmo público-alvo, também, em relação à LAI (Tabela 5 [repetida a seguir]), de modo a se evitar/amenizar os potenciais conflitos de interpretação LGPD x LAI.

Tabela 4 (repetição) - Distribuição das respostas à pergunta 5.1 do questionário.
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 5])

Questão 5.1: Acerca da capacitação dos seus colaboradores em proteção de dados pessoais, a organização:	**Qtde.**	**%**
a0) Não se aplica	4	1,04
a1) Não possui PLANO DE CAPACITAÇÃO (ou instrumento similar) e seus colaboradores ainda não realizaram treinamento em proteção de dados pessoais	43	11,11
a2) Não possui PLANO DE CAPACITAÇÃO (ou instrumento similar), mas colaboradores específicos já realizaram treinamento em proteção de dados pessoais	118	30,49
a3) Possui PLANO DE CAPACITAÇÃO (ou instrumento similar) e, apesar de este não contemplar a temática de proteção de dados pessoais de maneira específica, já realizou treinamento abrangente (não direcionado apenas a determinados colaboradores) nessa área	79	20,41
a4) Possui PLANO DE CAPACITAÇÃO (ou instrumento similar), contemplou nele a temática de proteção de dados pessoais e já realizou treinamento da maioria dos colaboradores nessa área	98	25,32
a5) Possui PLANO DE CAPACITAÇÃO (ou instrumento similar), contemplou nesse documento a temática de proteção de dados pessoais, incluindo a necessidade de treinamento diferenciado para as pessoas que exercem funções com responsabilidades essenciais quanto à proteção de dados pessoais, e já realizou treinamento de todos os colaboradores nessa área	45	11,63
TOTAL	**387**	**100**

Tabela 5 (repetição) - Distribuição das respostas à pergunta 5.2 do questionário.
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 5])

Questão 5.2: Acerca das ações de capacitação em proteção de dados pessoais realizadas nos últimos 3 (três) anos, a organização: (responderam esta questão apenas as 340 organizações que marcaram as opções a2, a3, a4 ou a5 na questão 5.1)	**Sim**	**Não**
Levou em consideração a necessidade de COMPLEMENTAR A CAPACITAÇÃO dos participantes nesses treinamentos COM CONTEÚDO SOBRE TRANSPARÊNCIA da gestão relativa às informações de interesse coletivo ou geral (Lei 12.527/2011 – LAI)	149	191
Efetivamente CAPACITOU NO TEMA TRANSPARÊNCIA da gestão relativa às informações de interesse coletivo ou geral (LAI) MAIS DE 50% dos colaboradores que receberam treinamento em proteção de dados pessoais	46	294
OFERECEU AÇÃO DE CAPACITAÇÃO QUE TENHA ABORDADO CONJUNTAMENTE, de forma integrada, as temáticas da proteção de dados pessoais (LGPD) e da transparência da gestão (LAI)	150	190
ORIENTOU OS PARTICIPANTES nesses treinamentos, mesmo que *a posteriori*, sobre a necessidade de observarem os Enunciados da CGU divulgados por meio da PORTARIA NORMATIVA CGU 71/2023[15]	57	283
ORIENTOU OS PARTICIPANTES nesses treinamentos, mesmo que *a posteriori*, sobre a necessidade de observarem as diretrizes e orientações publicadas pela CGU por meio do "PARECER SOBRE ACESSO À INFORMAÇÃO para atender ao Despacho Presidencial de 1º de janeiro de 2023"[16]	44	296
NÃO ATENDEU NENHUM dos itens anteriores	108	232

164. As respostas à questão 5.2 indicaram a necessidade de que os órgãos/entidades realizem treinamentos com vistas a conscientizar seus colaboradores e torná-los capazes de harmonizar, nas suas atividades do dia a dia, sem maiores problemas, esses dois diplomas legais (LAI e LGPD). Das 340 organizações, apenas 46 (13,53%) afirmaram ter capacitado em LAI mais da metade dos colaboradores que receberam treinamento em proteção de dados pessoais, enquanto somente 57 (16,77%) e 44 (12,94%) orientaram seus colaboradores em relação à existência de normativos relacionados emitidos pela CGU (Portaria Normativa - CGU 71/2023[15] e "Parecer sobre acesso à informação para atender ao Despacho Presidencial de 1º de janeiro de 2023"[16], respectivamente).

165. A seu turno, as respostas à questão 11.1 mostraram que, nos últimos três anos, as instâncias de controle/auditoria interno/a de várias das organizações (159 de 387, ou 41,09%) não realizaram avaliação relacionada a qualquer desses temas, LGPD ou LAI (Tabela 15 [repetida a seguir]).

Tabela 15 (repetição) - Distribuição das respostas à pergunta 11.1 do questionário.
(Fonte: respostas das organizações à pergunta 11.1 do questionário)

Questão 11.1: Nos últimos 3 (três) anos, a instância do "sistema de controle interno governamental" da organização realizou avaliação relacionada com o tema:	**Sim**	**Não**
PROTEÇÃO DE DADOS PESSOAIS (Lei Geral de Proteção de Dados Pessoais – LGPD)	137	250
TRANSPARÊNCIA DA GESTÃO relativa às informações de interesse coletivo ou geral (Lei de Acesso à Informação – LAI)	193	194
AINDA NÃO FOI REALIZADA AVALIAÇÃO DE NENHUM DESSES TEMAS (LGPD ou LAI)	159	228

4. Achados de Auditoria

166. Este capítulo detalha os achados de auditoria e as evidências que os suportam.

4.1. Não conclusão de medidas preparatórias com vistas a se adequar à LGPD

Situação encontrada

167. Apesar de a LGPD ter entrado em vigor em agosto de 2020, dos 387 órgãos/entidades auditados, 109 (28,16%) manifestaram que ainda não concluíram qualquer iniciativa voltada à identificação, ao planejamento e à execução de medidas preparatórias para se adequarem à lei (Tabela 1, respostas "a1" e "a2"; logo após o parágrafo 37).

Critérios de auditoria

168. Lei 13.709/2018, art. 3º, *caput*;

169. Decreto-Lei 200/1967, art. 6º, inciso I;

170. Norma ABNT NBR ISO/IEC 27701:2019, item 5.4 (Planejamento).

Evidências

171. Respostas das 387 organizações ao questionário da auditoria, sintetizadas na peça 922 (Coluna "Q2.1": respostas "a1" listam onze entes que não realizaram nenhuma medida preparatória; respostas "a2" mostram 98 entes que iniciaram, mas ainda não concluíram qualquer iniciativa).

Causas (alegadas pelos gestores)

172. No campo de comentário associado à questão 2.1, os onze gestores que responderam que o órgão/entidade não realizou nenhuma medida preparatória, de modo geral, assim justificaram:

172.1. A alta gestão da organização não priorizou o tema;

172.2. O órgão/entidade foi criado recentemente;

172.3. O encarregado pelo tratamento de dados pessoais ainda não foi nomeado ou foi nomeado há pouco tempo;

172.4. A organização tem carência de pessoal.

Efeitos reais e potenciais

173. A não aderência à LGPD impacta negativamente a proteção dos dados pessoais tratados por essas 109 organizações, com consequente risco de dano à privacidade dos titulares de dados envolvidos e possibilidade de prejuízos aos próprios órgãos/entidades (*e.g.* condenação ao pagamento de indenizações, danos à imagem, sanções aplicadas pela ANPD).

Conclusão

174. Desde a entrada em vigor da LGPD (mais de quatro anos atrás), os órgãos/entidades tiveram tempo mais que suficiente para se planejarem e se prepararem para cumprir a lei.

175. Nesse sentido, conclui-se que essas 109 organizações estão bem atrasadas e, portanto, devem adotar urgentemente providências para se adequarem à legislação. Medidas iniciais podem ser a criação de um comitê/grupo de trabalho para tratar do tema ou, então, a elaboração de um plano de ação para adequação à LGPD, identificando responsáveis e prevendo prazos para as diferentes ações/atividades.

176. É importante que a alta direção priorize essa iniciativa e que haja o envolvimento de setores-chave da organização, que lidam com o tratamento de dados pessoais no seu dia a dia.

Proposta de encaminhamento e benefício esperado

177. Propõe-se recomendar que essas 109 organizações federais realizem iniciativas voltadas à identificação, ao planejamento e à execução de medidas preparatórias para se adequarem à LGPD, bem como que as respectivas unidades de controle/auditoria interno/a e os OGSs envolvidos (CNJ, SGD/MGI, Sest/MGI e ANPD – ver peça 922), dentro do exercício do seu poder de supervisão

administrativa, acompanhem a evolução desses órgãos/entidades ao longo dos próximos anos e induzam o endereçamento dessa fragilidade.

178. Com isso, espera-se que tais órgãos aumentem a maturidade de seus processos de tratamento de dados pessoais e, com isso, minimizem os riscos envolvidos (ver tópico "Efeitos reais e potenciais").

4.2. Não condução de qualquer iniciativa ligada à dimensão "Contexto organizacional"

Situação encontrada

179. Das 387 organizações fiscalizadas, as respostas ao questionário da auditoria identificaram quarenta (10,34%) que ainda não conduziram nenhuma das iniciativas avaliadas na dimensão "Contexto organizacional" (Tabela 2, último item; logo após o parágrafo 46).

Critérios de auditoria

180. Lei 13.709/2018, art. 5º, em especial incisos I, V, VI, VII e X, art. 7º, § 5º, e arts. 37, 39, 42-46 e 50, § 1º e § 2º, inciso I, alínea "d";

181. Norma ABNT NBR ISO/IEC 27701:2019, itens 5.2.1 (Entendendo a organização e seu contexto), 5.2.2 (Entendendo as necessidades e as expectativas das partes interessadas), 5.4.1.2 (Avaliação de riscos de segurança da informação), 6.5.1 (Responsabilidade pelos ativos), 6.5.2 (Classificação da informação), 7.2.6 (Contratos com operadores de dados pessoais), 7.2.7 (Controlador conjunto de dados pessoais) e 7.2.8 (Registros relativos ao tratamento de dados pessoais).

Evidências

182. Respostas das 387 organizações federais ao questionário aplicado (peça 922, coluna "Q3.1").

Causas (alegadas pelos gestores)

183. A questão 3.1 não possuía um campo de comentário associado. Contudo, tendo em vista que, das quarenta organizações em questão, trinta (75%) também estão incluídas no achado anterior, pode-se supor que as causas são as mesmas ou similares (parágrafo 172 e subparágrafos).

Efeitos reais e potenciais

184. A ausência de condução de qualquer iniciativa relativa ao "Contexto organizacional" coloca essas quarenta organizações em uma posição muito frágil quanto à adequação à LGPD, considerando que tal dimensão abarca, em essência, atividades de identificação de diversos objetos básicos relacionados aos tratamentos de dados pessoais.

185. Com isso, pode-se dizer que esta fragilidade, inclusive, tem potencial para se alastrar pelas demais dimensões, pois a ausência da identificação desses elementos iniciais faz com que o órgão/entidade seja praticamente incapaz de proteger adequadamente os dados pessoais que trata, visto que não se pode assegurar a proteção daquilo que não se conhece direito. A peça 922 ilustra esse "efeito cascata", à medida que a maioria dessas quarenta organizações (coluna "Q3.1" marcada com um "X") incorreram, também, nos achados seguintes, correspondentes às demais dimensões avaliadas.

186. Em última instância, essa não aderência à LGPD diminui a proteção dos dados pessoais tratados por esses quarenta órgãos/entidades e representa risco de dano à privacidade dos cidadãos e possibilidade de prejuízos às próprias organizações (*e.g.* danos à imagem, recebimento de sanções da ANPD, condenações judiciais ao pagamento de indenizações).

Conclusão

187. As quarenta organizações que não conduziram qualquer iniciativa associada ao "Contexto organizacional" apresentam risco elevado em relação à proteção dos dados pessoais que tratam, pois essa dimensão, de certa forma, cuida de atividades iniciais relacionadas ao processo de adequação à LGPD (identificação de elementos básicos dos tratamentos de dados realizados), as quais acabam servindo de suporte para as demais dimensões.

188. Portanto, tais organizações devem adotar medidas para identificarem os objetos referidos na dimensão "Contexto organizacional" (subitens da questão 3.1), relacionados aos tratamentos de dados pessoais realizados no âmbito do órgão/entidade (*e.g.* normativos subjacentes; dados tratados; categorias de titulares; locais de armazenamento; riscos envolvidos; operadores, controladores conjuntos e contratos associados; processos de negócio e seus responsáveis).

Proposta de encaminhamento e benefício esperado

189. Propõe-se recomendar que esses quarenta órgãos/entidades conduzam iniciativas ligadas à dimensão "Contexto organizacional" (*e.g.* mapear normativos afetos à proteção de dados pessoais aplicáveis ao ente; identificar elementos relacionados aos tratamentos de dados pessoais; adequar instrumentos contratuais; avaliar riscos associados aos processos de tratamento de dados), bem como que as respectivas unidades de controle/auditoria interno/a e os OGSs envolvidos (CNJ, SGD/MGI e ANPD – ver peça 922), dentro do exercício do seu poder de supervisão administrativa, acompanhem a evolução dessas organizações ao longo dos próximos anos e induzam o endereçamento dessa fragilidade.

190. Com isso, espera-se que essas organizações aumentem a maturidade de seus processos de tratamento de dados pessoais como um todo, inclusive com reflexo nas demais dimensões avaliadas no bojo desta auditoria.

4.3. Não realização de qualquer das ações ligadas à dimensão "Liderança"

Situação encontrada

191. Das 387 organizações avaliadas, 24 (6,2%) disseram que ainda não realizaram nenhuma das ações avaliadas relacionadas à dimensão "Liderança" (Tabela 3, último item; logo após o parágrafo 53).

Critérios de auditoria

192. Lei 13.709/2018, em especial art. 5º, incisos I, II e VIII, arts. 11-14, art. 23, inciso III, e arts. 41, 46 e 50, § 2º, inciso I, alíneas "a" e "d";

193. IN - SGD/ME 117/2020[6] (Indicação do Encarregado pelo Tratamento dos Dados Pessoais na APF), em especial art. 1º, § 1º, incisos I e II, e art. 2º;

194. Norma ABNT NBR ISO/IEC 27701:2019, itens 5.3.2 (Política), 6.2 (Políticas de segurança da informação), 6.2.1 (Orientação da Direção para segurança da informação), 6.3.1 (Organização interna), 6.5.2 (Classificação da informação) e 6.5.2.2 (Rótulos e tratamento da informação);

195. "Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado"[9], da ANPD.

Evidências

196. Respostas das 387 organizações federais ao questionário aplicado (peça 922, coluna "Q4.1").

Causas (alegadas pelos gestores)

197. No campo de comentário correspondente ao item em que a organização sinalizava não ter realizado nenhuma das ações avaliadas na dimensão "Liderança", as manifestações dos gestores respondentes, em geral, foram no sentido de que tais ações estão em curso, porém ainda não foram finalizadas ("As medidas arroladas encontram-se em processo de desenvolvimento", "O [órgão X] encontra-se em processo de discussão para implantação da LGPD", "Processo ainda não finalizado", "o processo de formalização da nomeação do encarregado de dados está em andamento", "Quanto a designação de encarregado de dados, consta processo em tramitação", "Os nomes foram escolhidos, mas ainda não saiu a portaria", "Estamos trabalhando no desenvolvimento das políticas").

198. Ou seja, pode-se supor que a causa subjacente é a não priorização do processo de adequação à LGPD por parte da alta administração dessas 24 organizações, o que acarreta a não priorização dessa demanda, também, pelos gestores das áreas que seriam responsáveis, na ponta, pela sua materialização.

Efeitos reais e potenciais

199. A formalização de políticas (ou documentos similares) que busquem assegurar a segurança das informações e a proteção dos dados pessoais, bem como a nomeação do encarregado pelo tratamento de dados pessoais, são medidas essenciais que demonstram o comprometimento da alta administração do órgão/entidade com a iniciativa de adequação à LGPD.

200. Se não houver essa liderança e esse comprometimento por parte da alta direção, dificilmente serão implementadas as medidas necessárias para que o órgão/entidade se adeque à lei. Prova disso é o fato de que essas mesmas 24 organizações (peça 922, coluna "Q4.1" marcada com um "X") acabaram incorrendo na maioria dos demais achados relatados.

201. Com isso, tal fragilidade resulta na proteção inadequada dos dados pessoais tratados por esses 24 entes e, consequentemente, traz riscos à privacidade dos cidadãos envolvidos nas respectivas políticas públicas, os quais podem impactar negativamente a própria organização (*e.g.* danos reputacionais e prejuízos derivados de condenações judiciais ou de aplicação de sanção pela ANPD).

Conclusão

202. A não realização de qualquer ação associada à dimensão "Liderança" indica que a alta administração dessas 24 organizações não está priorizando as iniciativas de adequação à LGPD, o que, consequentemente, acarreta risco elevado de que os dados pessoais tratados no âmbito desses órgãos/entidades estejam desprotegidos.

203. Sem a formalização de documentos norteadores ou a designação do responsável pela sua condução, vê-se que o processo de adequação dessas organizações à LGPD dificilmente se materializará.

204. Assim, essas 24 organizações precisam adotar medidas para elaborarem e instituírem as políticas em questão (PSI, PCI e PPDP), bem como para providenciarem, o quanto antes, a nomeação dos encarregados pelo tratamento de dados pessoais e a divulgação das respectivas informações.

Proposta de encaminhamento e benefício esperado

205. Propõe-se recomendar que essas 24 organizações realizem iniciativas ligadas à dimensão "Liderança" (*e.g.* formalização das políticas em questão [PSI, PCI e PPDP], nomeação do encarregado de dados e publicação das suas informações de contato), bem como que as respectivas unidades de controle/auditoria interno/a e os OGSs envolvidos (SGD/MGI, Sest/MGI e ANPD – ver peça 922), dentro do exercício do seu poder de supervisão administrativa, acompanhem a evolução desses órgãos/entidades ao longo dos próximos anos e induzam o endereçamento da fragilidade em questão, de modo que tais entes aumentem sua maturidade quanto ao tratamento de dados pessoais, inclusive com reflexo nas demais dimensões avaliadas nesta auditoria.

4.4. Ausência de PSI, de nomeação do DPO e de comunicação padronizada à ANPD

Situação encontrada

206. Das 387 organizações avaliadas:

206.1. 80 (20,67%) não possuem Política de Segurança da Informação (Tabela 3, primeiro item; logo após o parágrafo 53);

206.2. 48 (12,4%) não nomearam o encarregado de dados (Tabela 3, quarto item);

206.3. 250 (64,6%) não padronizaram a comunicação à ANPD e aos titulares de dados de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares (Tabela 13, penúltimo item; logo após o parágrafo 103).

Critérios de auditoria

207. PSI: Decreto 9.637/2018, art. 15, inciso II, c/c a IN - GSI/PR 1/2020[12] (Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da APF), art. 9º; Resolução - CNJ 396/2021[13]

(Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário – ENSEC-PJ), art. 19, inciso II; Resolução - CNMP 156/2016[14] (Institui a Política de Segurança Institucional e o Sistema Nacional de Segurança Institucional do Ministério Público), art. 22, inciso III;

208. Nomeação do encarregado de dados: Lei 13.709/2018, art. 41;

209. Comunicação de incidentes à ANPD: Lei 13.709/2018, art. 48.

Evidências

210. Respostas das 387 organizações federais ao questionário aplicado (peças 918, 919 e 920).

Causas

211. O questionário solicitou que os respondentes fornecessem, no respectivo campo de comentário, mais detalhes sobre alguns dos itens que marcassem (no caso do item relativo à PSI, por exemplo, deveria ser fornecido o número do documento interno, no órgão, correspondente à política).

212. Tendo em vista que este achado se refere a itens das questões 4.1 (formalização da PSI e nomeação do DPO) e 9.1 (comunicação à ANPD) que não foram marcados pelos gestores, consequentemente eles não possuem justificativas associadas por parte dos respondentes.

213. No que se refere à questão 4.1, considera-se que a causa raiz consta no achado anterior (não priorização do processo de adequação à LGPD pela alta direção da organização, o que acarreta a não priorização das demandas relacionadas por parte dos gestores).

214. A seu turno, o não estabelecimento de comunicação padronizada à ANPD e aos titulares de dados acerca dos incidentes de segurança, por se tratar de prática mais avançada, além da falta de apoio da alta administração, pode ser associado à baixa maturidade das organizações, de modo geral. Tanto que essa fragilidade afeta quase dois terços (64,6%) dos órgãos/entidades.

Efeitos reais e potenciais

215. A PSI é a política que norteia a abordagem de alto nível da organização para gerenciar os objetivos relacionados à segurança da informação. Com isso, por se tratar de documento basilar nessa área, a sua ausência prejudica sobremaneira o atingimento desse propósito.

216. Por sua vez, a falta de nomeação do encarregado pelo tratamento de dados pessoais, além de privar o órgão/entidade de alguém cuja missão está diretamente relacionada à implementação da LGPD, o que contribui para alavancar as iniciativas nesse sentido, também faz com que a organização não mantenha um canal de comunicação efetivo com a ANPD e mesmo com os titulares dos dados.

217. Por fim, a ausência de processo padronizado de comunicação dos incidentes que possam acarretar risco ou dano relevante aos titulares de dados afeta negativamente alguns dos pilares nos quais se baseia a própria LGPD, a exemplo dos princípios da transparência (fornecimento de informações claras e precisas acerca dos tratamentos de dados) e da prevenção (adoção de medidas para prevenir a ocorrência de danos em virtude desses tratamentos) [Lei 13.709/2018, art. 6º, incisos VI e VIII].

Conclusão

218. A ausência de PSI, de nomeação do encarregado de dados e de comunicação padronizada dos incidentes de segurança à ANPD e aos titulares são fatores que prejudicam bastante o processo de implementação da LGPD. Os dois primeiros, principalmente, por se tratar de elementos-chave na estruturação do órgão/entidade para se adequar à lei: a PSI é a política que definirá os objetivos da organização relativos à segurança da informação e o DPO é o principal ator na condução desse processo.

219. A necessidade de nomeação do DPO e de comunicação dos incidentes à ANPD e aos titulares de dados constam na LGPD (Lei 13.709/2018, arts. 41 e 48, respectivamente), ao passo que a obrigatoriedade de formalização da PSI, por sua importância, é prevista, inclusive, em normas

especificamente direcionadas ao Ministério Público e aos Poderes Executivo e Judiciário (ver tópico "Critérios de auditoria").

220. Consequentemente, a fragilidade representada pela ausência desses elementos, além de representar descumprimento normativo expresso, implica em grave risco de não atingimento dos objetivos pretendidos pela LGPD, devendo, portanto, ser cientificada aos órgãos/entidades em tela.

Proposta de encaminhamento e benefício esperado

221. Propõe-se dar ciência às organizações relacionadas:

221.1. na peça 918 de que a ausência de estabelecimento formal de uma PSI afronta o disposto no Decreto 9.637/2018, art. 15, inciso II, c/c a Instrução Normativa - GSI/PR 1/2020, art. 9º, bem como na Resolução - CNJ 396/2021, art. 19, inciso II, e na Resolução - CNMP 156/2016, art. 22, inciso III;

221.2. na peça 919 de que a ausência de nomeação do encarregado pelo tratamento de dados pessoais afronta o disposto na Lei 13.709/2018, art. 41, *caput*;

221.3. na peça 920 de que a falta de comunicação à ANPD e aos titulares de dados da ocorrência de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares afronta o disposto na Lei 13.709/2018, art. 48, *caput*.

222. Com isso, espera-se que esses órgãos/entidades empreendam esforços para atenderem os itens em questão, providenciando, o quanto antes, a formalização de uma PSI, a nomeação do encarregado de dados e a definição de um processo padronizado de comunicação de incidentes de segurança à ANPD e aos titulares de dados.

4.5. Ausência de Plano de Capacitação

Situação encontrada

223. Das 387 organizações fiscalizadas, 161 (41,6%) manifestaram que ainda não possuem Plano de Capacitação (Tabela 4, respostas "a1" e "a2"; logo após o parágrafo 62).

Critérios de auditoria

224. Lei 13.709/2018, art. 41, § 2º, inciso III;

225. Lei 12.527/2011, art. 41, inciso II;

226. Norma ABNT NBR ISO/IEC 27701:2019, itens 5.5.2 (Competência), 5.5.3 (Conscientização) e 5.5.4 (Comunicação).

Evidências

227. Respostas das 387 organizações ao questionário da auditoria, sintetizadas na peça 922 (Coluna "Q5.1": respostas "a1" listam 43 órgãos/entidades que disseram que não possuem plano de capacitação e que seus colaboradores não realizaram treinamento em proteção de dados pessoais; respostas "a2" designam 118 entes que afirmaram que, apesar de colaboradores específicos já terem realizado treinamento na área, ainda não possuem plano de capacitação).

Causas (alegadas pelos gestores)

228. No campo de comentário associado, esses 161 gestores (questão 5.1, respostas "a1" e "a2") afirmaram que os planos de capacitação contemplando a temática de proteção de dados pessoais efetivamente ainda não foram formalizados, porém registraram que, de modo geral, já foram realizadas algumas ações de conscientização e de treinamento, sobretudo no que tange à capacitação dos respectivos encarregados de dados. Em alguns casos, foi acrescido que esse processo de formalização do plano de capacitação está em trâmite ou em vias de ser aprovado.

229. Algumas organizações mencionaram a carência de pessoal ou a troca recente de gestão como justificativas para o fato de ainda não possuírem plano de capacitação.

Efeitos reais e potenciais

230. A ausência de plano de capacitação e, mais especificamente, da previsão da realização de ações internas voltadas à conscientização, à sensibilização e ao treinamento quanto às temáticas de privacidade e proteção de dados pessoais, bem como à sua harmonização com a LAI, resulta em colaboradores que não estão preparados para lidar com a importância desses temas e nem com os diversos impactos e prejuízos que as violações relacionadas podem causar ao órgão/entidade (*e.g.* aplicação de sanções pela ANPD, condenação ao pagamento de indenizações, danos financeiros e à imagem da instituição).

231. Os riscos associados à capacitação insuficiente nesses temas são significativos, em especial quando se referem a colaboradores que, no seu dia a dia, exercem funções com responsabilidades essenciais relacionadas aos tratamentos de dados realizados no âmbito da organização.

Conclusão

232. Para atingir seus objetivos, as organizações modernas baseiam-se no conceito do "tripé da gestão" (também chamado de "triângulo dourado"), formado por pessoas, processos e tecnologia (PPT). Desses três, as pessoas (colaboradores que trabalham na organização) são o elemento mais importante do triângulo. Portanto, não se pode esperar que um órgão/entidade funcione a contento e consiga entregar bons resultados sem primeiro treinar e capacitar suficientemente seus colaboradores.

233. Esse aspecto, então, foi avaliado na dimensão "Capacitação", especificamente no que se refere à conscientização e ao treinamento dos colaboradores da organização em relação aos temas privacidade e proteção de dados pessoais, passos essenciais para assegurar que o órgão/entidade esteja adequado à LGPD e, com isso, seja capaz de proteger adequadamente os dados que trata.

234. Nesse sentido, conclui-se que essas 161 organizações que não possuem Plano de Capacitação sequer mapearam, ainda, o conjunto de conhecimentos, competências e habilidades necessárias para que os seus colaboradores desempenhem melhor, no dia a dia, as tarefas e as atividades que levarão o órgão/entidade a gerar os resultados pretendidos pela organização com a implementação da LGPD e, consequentemente, atingir seus objetivos.

235. Diante disso, é importante que tais organizações adotem providências para garantir que seus colaboradores, em especial aqueles que lidam com processos de tratamento de dados pessoais, inteirem-se da legislação e dos demais normativos aplicáveis ao tema e de como as suas decisões e ações diárias afetam a privacidade e a proteção dos dados dos titulares, sendo que uma das primeiras medidas nessa direção é a elaboração de um Plano de Capacitação.

Proposta de encaminhamento e benefício esperado

236. Propõe-se recomendar que essas 161 organizações elaborem Plano de Capacitação e contemplem nele a temática de proteção de dados pessoais, incluindo a necessidade de treinamento diferenciado para as pessoas que exercem funções com responsabilidades essenciais quanto à proteção de dados pessoais, bem como que as respectivas unidades de controle/auditoria interno/a e os OGSs envolvidos (CNJ, CNMP, SGD/MGI, Sest/MGI e ANPD – ver peça 922), dentro do exercício do seu poder de supervisão administrativa, acompanhem a evolução desses órgãos/entidades ao longo dos próximos anos e induzam o endereçamento dessa fragilidade.

237. Com isso, espera-se que tais órgãos sejam dotados de colaboradores não apenas cientes da importância da LGPD e dos princípios representados por essa legislação, mas que sejam capazes de, no seu dia a dia, assegurar a proteção dos dados tratados pela organização, em benefício dos cidadãos.

4.6. Ausência de Política de Privacidade e não atendimento a direitos dos titulares

Situação encontrada

238. Das 387 organizações avaliadas:

238.1. 146 (37,73%) não elaboraram Política de Privacidade (Tabela 7, respostas "a0" e "a1"; logo após o parágrafo 83);

238.2. 90 (23,26%) não implementaram mecanismos para atender direitos dos titulares (Tabela 8, respostas "a0" e "a1"; logo após a Tabela 7).

Critérios de auditoria

239. Lei 13.709/2018, art. 6º, em especial incisos IV e VI, arts. 9º e 17-22, art. 23, inciso I, e art. 50, inciso I, alíneas "a", "d" e "e";

240. Norma ABNT NBR ISO/IEC 27701:2019, itens 7.3 (Obrigações dos titulares de dados pessoais), 7.3.2 (Determinando as informações para os titulares de dados pessoais) e 7.3.3 (Fornecendo informações aos titulares de dados pessoais).

Evidências

241. Respostas das 387 organizações ao questionário, sintetizadas na peça 922 (Coluna "Q7.1": respostas "a0" registram seis órgãos/entidades que marcaram a opção "Não se aplica"; respostas "a1" listam 140 entes que afirmaram que não elaboraram Política de Privacidade; Coluna "Q7.2": respostas "a0" designam quatro organizações que selecionaram a opção "Não se aplica"; respostas "a1" se referem a 86 órgãos/entidades que disseram não ter implementado mecanismos para atender direitos dos titulares).

Causas (alegadas pelos gestores)

242. Nas duas questões (7.1 e 7.2), o questionário fornecia um campo de comentário para que os gestores pudessem complementar as suas respostas, fornecendo mais detalhes, se entendessem cabíveis.

243. Quanto à ausência de Política de Privacidade (questão 7.1), houve algumas alegações de carência de pessoal e de que a alta gestão ainda não se convenceu da importância do tema "adequação à LGPD". A grande maioria das organizações, no entanto, registrou que está planejando a elaboração dessa política (por conta própria ou por meio da contratação de consultoria) ou, então, que o documento já está em fase de elaboração ou mesmo com minuta pronta e aguardando aprovação para poder ser publicado.

244. A seu turno, sobre a não implementação de mecanismos para atender os direitos dos titulares de dados (questão 7.2), também houve alegações de falta de pessoal e, no caso de universidades federais, de ocorrência de greves. Muitos órgãos/entidades disseram que, apesar de não disponibilizarem meios específicos para os titulares poderem exercer seus direitos, recebem solicitações nesse sentido por e-mail e as atendem. Alguns responderam que já há cronograma para a implementação desses mecanismos.

245. Entende-se que, de modo geral, as causas estão relacionadas à carência de pessoal, à baixa maturidade dos órgãos e à não priorização do tema por parte das respectivas altas administrações.

Efeitos reais e potenciais

246. É por meio da Política de Privacidade que a organização informa os usuários e lhes fornece detalhes acerca dos tratamentos de dados pessoais que ocorrem no âmbito de um sítio/serviço/sistema qualquer. Ao não elaborar tal política e, consequentemente, ao não a disponibilizar ao usuário, o órgão/entidade peca em seu dever de transparência para com os titulares de dados (público externo), descumprindo um dos princípios basilares da LGPD.

247. Com isso, sequer se poderia dizer que esteja sendo regularmente obtido o eventual consentimento do titular, nos casos em que este se faz necessário para o tratamento de dados em questão, tendo em vista o desconhecimento do usuário acerca dessas informações básicas.

248. Por sua vez, ao não disponibilizar os meios adequados para que os titulares possam exercer os direitos que a LGPD lhes assegura (*e.g.* confirmar a existência de tratamento, acessar/corrigir/exportar

os dados a seu respeito, revogar o consentimento), na prática, pode-se dizer que a organização está sonegando tais direitos aos cidadãos e esvaziando a efetividade dessa lei.

Conclusão

249. A dimensão "Direitos do Titular" avalia aspectos relativos à devida prestação de informações aos titulares de dados e à viabilização que estes exerçam direitos previstos na LGPD.

250. As 146 organizações que não elaboraram Política de Privacidade e as noventa que não implementaram mecanismos para atender os direitos dos titulares previstos nos arts. 9º e 17-22 da LGPD estão se afastando dos propósitos pretendidos por essa legislação e, consequentemente, prejudicando a privacidade dos cidadãos e a proteção dos respectivos dados.

Proposta de encaminhamento e benefício esperado

251. Propõe-se recomendar que esses 146 órgãos/entidades elaborem Política de Privacidade e a divulguem em seu sítio eletrônico institucional e que essas noventa organizações implementem mecanismos para atender os direitos dos titulares previstos nos arts. 9º e 18 da LGPD, bem como que as respectivas unidades de controle/auditoria interno/a e os OGSs envolvidos (CNJ, SGD/MGI, Sest/MGI e ANPD – ver peça 922), dentro do exercício do seu poder de supervisão administrativa, acompanhem a evolução dessas organizações pelos próximos anos e induzam o endereçamento dessa fragilidade.

252. Com isso, espera-se que tais órgãos/entidades deixem os titulares melhor informados acerca dos tratamentos de dados pessoais realizados e com plena capacidade de exercerem seus direitos, contribuindo, assim, para o atingimento dos objetivos da LGPD.

4.7. Desconhecimento dos compartilhamentos de dados pessoais com terceiros

Situação encontrada

253. Das 387 organizações auditadas, 170 (43,93%) assinalaram que ainda não avaliaram se realizam compartilhamentos de dados pessoais com terceiros ou que ainda não identificaram todos os dados eventualmente compartilhados (Tabela 9, respostas "a1"; logo após o parágrafo 90).

Critérios de auditoria

254. Lei 13.709/2018, em especial art. 5º, inciso XVI, arts. 26-27 e 30;

255. Norma ABNT NBR ISO/IEC 27701:2019, itens 7.5.1 (Identificando as bases para a transferência de dados pessoais entre jurisdições), 7.5.2 (Países e organizações internacionais para os quais os dados pessoais podem ser transferidos), 7.5.3 (Registros de transferência de dados pessoais) e 7.5.4 (Registro de divulgação de dados pessoais para terceiros);

256. "Guia Orientativo – Tratamento de dados pessoais pelo Poder Público"[10], da ANPD.

Evidências

257. Respostas das 387 organizações ao questionário da auditoria, contidas na peça 922 (Coluna "Q8.1": respostas "a1" listam 170 órgãos/entidades que afirmaram que não avaliaram se compartilham dados pessoais ou que ainda não identificaram todos os dados eventualmente compartilhados).

Causas (alegadas pelos gestores)

258. No campo de comentário da questão 8.1, algumas dessas 170 organizações afirmaram que a verificação da ocorrência ou não de compartilhamentos de dados pessoais com terceiros já foi realizada em algumas áreas do órgão/entidade, porém ainda não em todas. Muitos gestores disseram que o inventário de dados pessoais do ente está sendo elaborado ou está em processo de revisão/atualização e que, no escopo dessa ação, todos os compartilhamentos de dados serão identificados.

259. Ademais, houve outras justificativas, tais como a falta, no órgão/entidade, de uma área específica que cuide da LGPD, a posse da gestão atual da organização há pouco tempo e a nomeação recente do encarregado pelo tratamento de dados pessoais.

Efeitos reais e potenciais

260. O desconhecimento sobre os compartilhamentos de dados pessoais com terceiros leva a uma situação em que a organização é incapaz de assegurar a segurança e a proteção desses dados, tendo em vista que sequer identificou e avaliou os dados compartilhados.

261. Ao não identificar os compartilhamentos e ao não manter o devido registro de quais dados são compartilhados, com quem e quando, o órgão/entidade não tem como adotar controles adequados para mitigar os riscos associados a esses compartilhamentos (*e.g.* vazamento de dados pessoais).

Conclusão

262. A organização deve identificar, avaliar e documentar detalhes dos compartilhamentos de dados pessoais realizados com terceiros, de modo que possa implementar controles para proteger tais dados de acordo com os ditames da LGPD, tendo em vista que a responsabilidade por essa proteção continua recaindo sobre ela (Lei 13.709/2018, art. 44, parágrafo único).

263. Portanto, tem-se que os 170 órgãos/entidades que não avaliaram seus compartilhamentos ou não identificaram todos os dados pessoais que, eventualmente, compartilham com terceiros podem estar comprometendo a segurança desses dados e, em última instância, a privacidade dos cidadãos envolvidos.

264. Dessa forma, tais organizações devem se mobilizar para realizarem a identificação dos compartilhamentos de dados pessoais, avaliarem a adequação dessas operações frente aos critérios previstos na LGPD e manterem o devido registro dos eventos relacionados a esses compartilhamentos.

Proposta de encaminhamento e benefício esperado

265. Propõe-se recomendar que esses 170 órgãos/entidades avaliem se compartilham dados pessoais com terceiros e identifiquem os dados eventualmente compartilhados, bem como que as respectivas unidades de controle/auditoria interno/a e os OGSs envolvidos (CNJ, CNMP, SGD/MGI, Sest/MGI e ANPD – ver peça 922), dentro do exercício do seu poder de supervisão administrativa, acompanhem a evolução dessas organizações e induzam o endereçamento dessa fragilidade.

266. Com isso, espera-se que tais órgãos sejam capazes de assegurar níveis mínimos de segurança e de proteção aos dados pessoais que compartilham com terceiros.

5. Painel Nacional de Implementação da LGPD

267. Esta auditoria incluiu a construção de um painel (*dashboard*) – utilizando a ferramenta Microsoft Power BI – para permitir a visualização gráfica e interativa das informações fornecidas pelas organizações em resposta ao questionário. Frise-se que, até a publicação do acórdão resultante da auditoria, o acesso ao painel se restringiu aos auditores do TCU e dos TCEs participantes da fiscalização.

268. Além de mostrar a situação observada a partir da realização desta auditoria, esse mesmo painel poderá continuar a ser alimentado, tanto pelo TCU quanto pelos TCEs (mesmo por aqueles que não participaram desta fiscalização), com os dados relativos às respostas das organizações em novos ciclos de aplicação do questionário, permitindo, assim, um acompanhamento mais efetivo da evolução da implementação dos dispositivos da LGPD por parte das organizações públicas.

269. O painel contém uma primeira aba ("Introdução"), a qual traz informações gerais acerca da fiscalização, bem como as descrições de cada uma das nove dimensões avaliadas. A seguir, a aba "Lista das Organizações" apresenta todas as 387 organizações públicas federais que foram auditadas pelo TCU (peça 922), além das organizações estaduais e municipais que foram fiscalizadas pelos TCEs.

270. Adicionalmente, há onze abas de visualização de dados, correspondentes às nove 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"), ao "iLGPD" (indicador de adequação à LGPD)

e uma última aba denominada "Radar", a qual possibilita comparar os resultados de organizações individuais com os resultados (médios) de um grupo de organizações.

271. Os gráficos de todas as abas de visualização de dados são dinâmicos, o que significa que o universo dos dados apresentados pode ser alterado com base na aplicação dos filtros disponíveis (Figura 11), restringindo-se interativamente a visualização das respostas das organizações de modo a mostrar apenas aquelas que atendem o(s) critério(s) selecionado(s). É possível, inclusive, combinar essas filtragens, ou seja, aplicar múltiplos filtros simultaneamente.

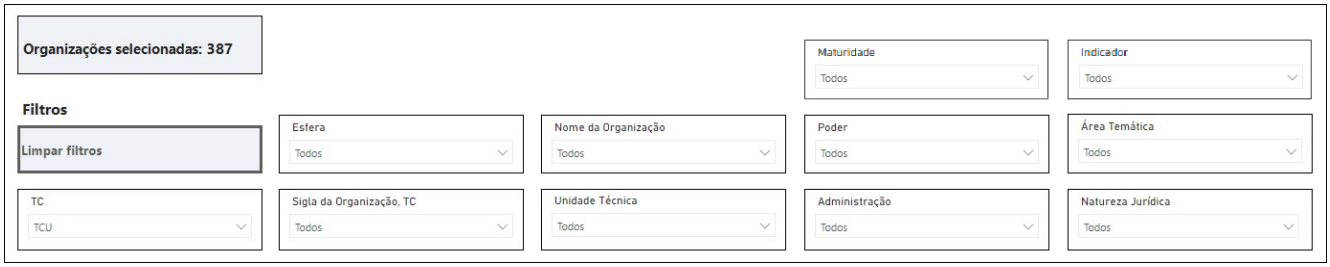


Figura 11 - Painel Nacional de Implementação da LGPD - Filtros disponíveis.
(Fonte: painel construído para visualizar as respostas das organizações)

272. A partir da aplicação desses filtros, as respostas das organizações participantes podem ser visualizadas e comparadas com base em diversos critérios distintos, permitindo, assim, ampla segmentação das análises. Esses filtros, inclusive, foram usados para gerar os gráficos que ilustram os relatórios individuais de *feedback* a serem enviados às organizações.

273. A seguir, descrevem-se as onze abas de visualização de dados (nove relativas às dimensões avaliadas, mais as abas "iLGPD" e "Radar"), sendo que os gráficos mostram os dados completos relativos às 387 organizações federais auditadas pelo TCU, sem a aplicação dos filtros.

Abas das "Dimensões"

274. Cada uma das abas das nove dimensões apresenta os gráficos contendo as distribuições das respostas das organizações auditadas a cada uma das perguntas individuais do questionário. No caso das questões do "Tipo A" (resposta única), foram utilizados gráficos de barras, sendo que alguns, inclusive, ilustraram este relatório, a exemplo da Figura 3 (gráfico relativo à questão 2.1), repetida a seguir.

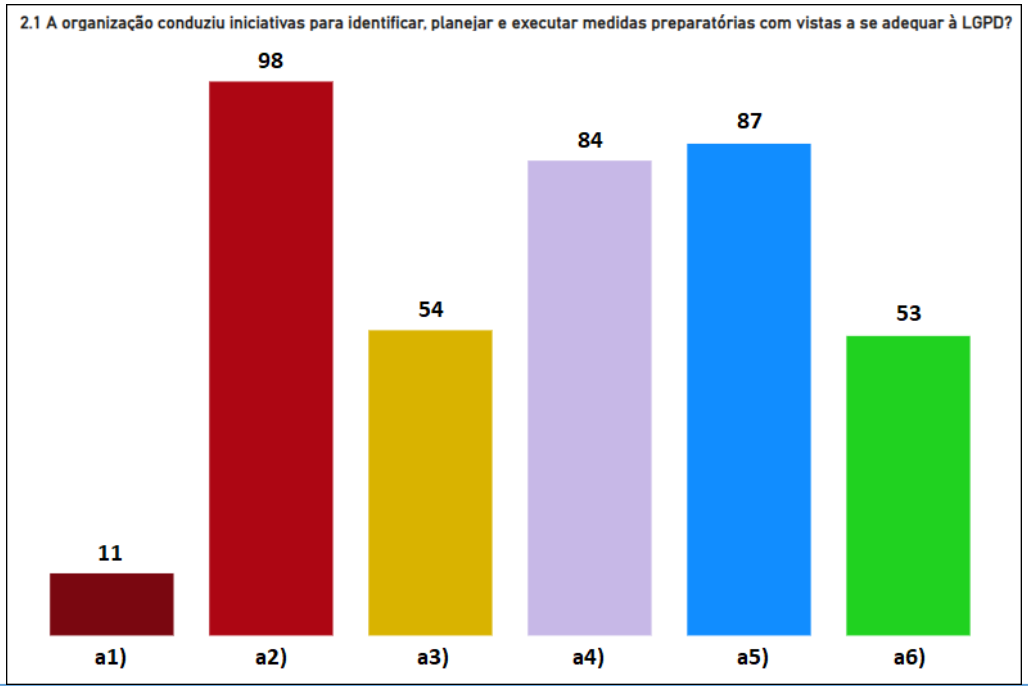


Figura 3 (repetição) - Distribuição das respostas à pergunta 2.1 do questionário.
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 5])

275. No caso das questões do "Tipo B" (múltiplas respostas), para melhor visualização, os gráficos correspondentes foram apresentados neste relatório na forma de tabelas. Por exemplo, a Figura 12 ilustra as respostas da questão 4.1 conforme elas são mostradas no painel. Neste relatório, porém, essas respostas encontram-se na Tabela 3, repetida a seguir, por conveniência.

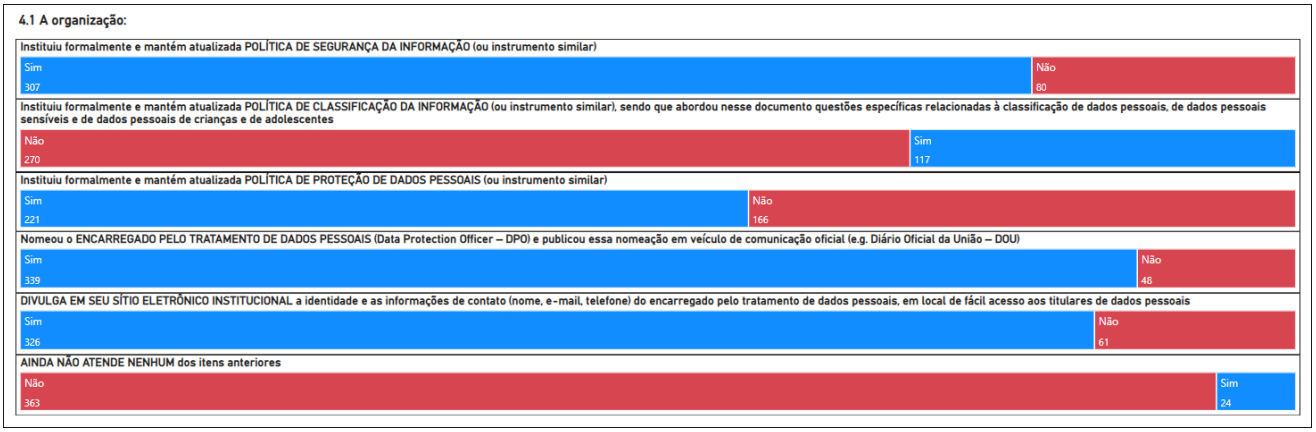


Figura 12 - Painel Nacional - Distribuição das respostas à pergunta 4.1 do questionário.
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 5])

Tabela 3 (repetição) - Distribuição das respostas à pergunta 4.1 do questionário.
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 5])

Questão 4.1: A organização:	**Sim**	**Não**
Instituiu formalmente e mantém atualizada POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (ou instrumento similar)	307	80
Instituiu formalmente e mantém atualizada POLÍTICA DE CLASSIFICAÇÃO DA INFORMAÇÃO (ou instrumento similar), sendo que abordou nesse documento questões específicas relacionadas à classificação de dados pessoais, de dados pessoais sensíveis e de dados pessoais de crianças e de adolescentes	117	270
Instituiu formalmente e mantém atualizada POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS (ou instrumento similar)	221	166
Nomeou o ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS (*Data Protection Officer* – DPO) e publicou essa nomeação em veículo de comunicação oficial (*e.g.* DOU)	339	48
DIVULGA EM SEU SÍTIO ELETRÔNICO INSTITUCIONAL a identidade e as informações de contato (nome, e-mail, telefone) do encarregado pelo tratamento de dados pessoais, em local de fácil acesso aos titulares de dados pessoais	326	61
AINDA NÃO ATENDE NENHUM dos itens anteriores	24	363

Aba "iLGPD"

276. Esta aba apresenta, na forma de ponteiros que variam de 0 a 100%, o "indicador de adequação à LGPD" (iLGPD) e os subindicadores relativos a cada uma das nove dimensões avaliadas nesta auditoria (Figura 13).

277. Cada um desses ponteiros mostra os valores médio (abaixo, em tamanho maior) e mediano (acima, em tamanho menor) das avaliações das organizações naquele (sub)indicador. Enquanto a média é encontrada somando-se as notas correspondentes a todos os órgãos/entidades selecionados e, então,

dividindo-se esse resultado pela quantidade de organizações, a mediana nada mais é do que o valor do meio (central) quando se ordena as notas das organizações selecionadas da menor para a maior.

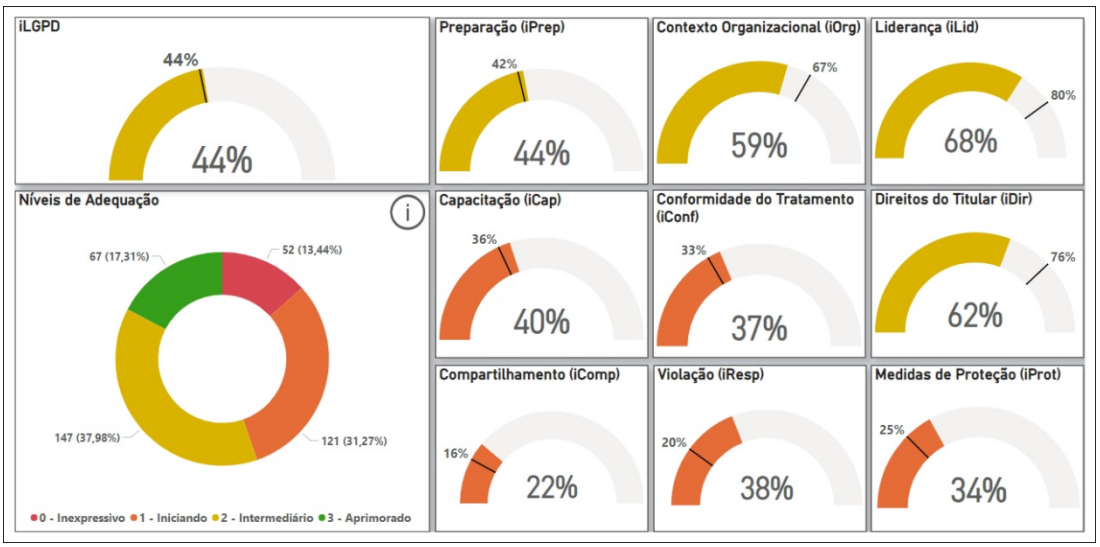


Figura 13 - Painel Nacional - Aba "iLGPD" (iLGPD, subindicadores das nove dimensões e níveis de adequação).
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 5])

278. Ademais, essa aba também mostra um gráfico com a estratificação do conjunto de organizações selecionadas de acordo com os quatro níveis/faixas de adequação à LGPD que foram definidos: "Inexpressivo" ($0 \leq$ iLGPD $< 15\%$), "Iniciando" ($15\% \leq$ iLGPD $< 40\%$), "Intermediário" ($40\% \leq$ iLGPD $\leq 70\%$) e "Aprimorado" ($70\% <$ iLGPD $\leq 100\%$). Mais detalhes sobre o iLGPD e esses níveis/faixas podem ser consultados no **Apêndice F** – Indicador de adequação à LGPD (iLGPD).

Aba "Radar"

279. Por fim, esta última aba possibilita comparar os resultados de organizações individuais (gráfico à direita) com os resultados médios de grupos de organizações (gráfico à esquerda), de acordo com os filtros selecionados (Figura 14), funcionalidade útil para a realização de análises comparativas. Nesses gráficos, é possível filtrar para que sejam mostrados apenas os resultados das organizações que se enquadram em determinado nível de adequação ("Inexpressivo", "Iniciando", "Intermediário", "Aprimorado") ou somente os resultados das avaliações relativas ao indicador geral (iLGPD) ou a um ou mais dos nove subindicadores (iPrep, iOrg, iLid, iCap, iConf, iDir, iComp, iResp e iProt).

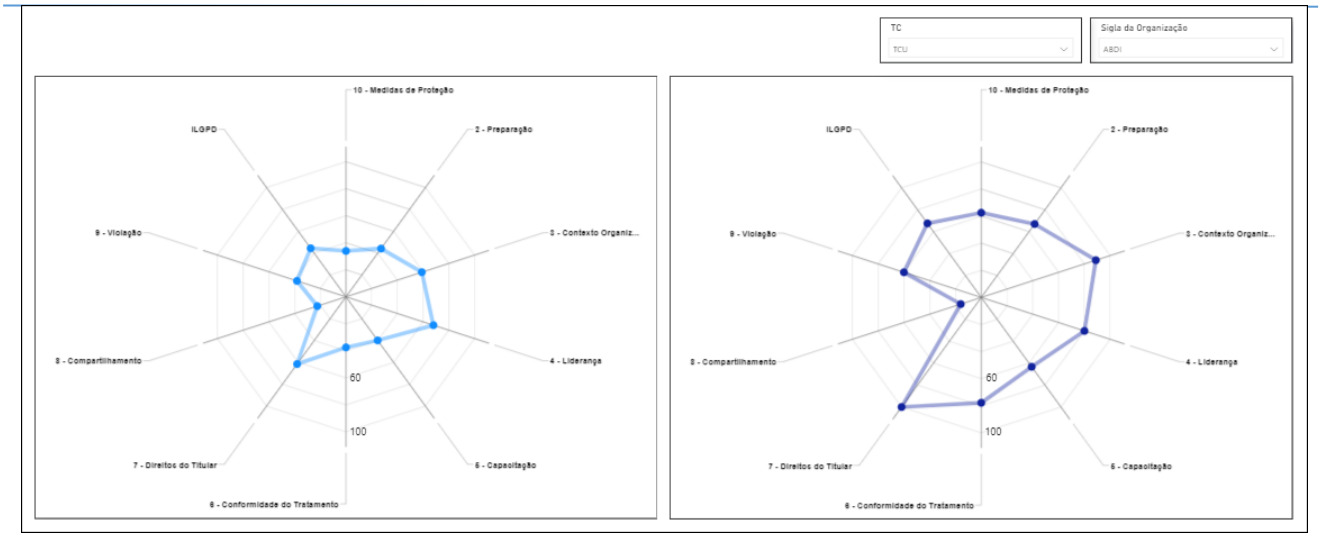


Figura 14 - Painel Nacional - Aba "Radar" (análises comparativas).
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 5])

6. Propósitos da auditoria e relatórios individuais de *feedback*

280. Em 2021, o TCU constatou que 76,7% das organizações públicas federais encontravam-se nos graus inexpressivo ou inicial de adequação à LGPD[1] (TC 039.606/2020-1; Acórdão 1.384/2022-TCU-Plenário, Rel. Min. Augusto Nardes).

Propósitos da auditoria

281. O propósito geral desta auditoria foi realizar um mapeamento amplo das organizações públicas federais quanto à implementação de controles relacionados à LGPD, de modo a dotar o TCU de informação suficiente para poder atuar proativamente no sentido de ajudar tais organizações a alavancarem esses controles, diminuindo, assim, os riscos relativos à privacidade dos cidadãos e à segurança dos respectivos dados custodiados pela APF, em especial aqueles considerados sensíveis.

282. Em síntese, esse panorama é mostrado no Capítulo 2 (Diagnóstico da adequação das organizações públicas federais à LGPD), cujas informações poderão ser levadas em consideração na definição de auditorias baseadas em risco (*e.g.* auditar órgãos com baixos níveis de adequação à LGPD responsáveis por manter sistemas com grandes bases de dados pessoais de cidadãos).

283. Porém, além de gerar esse diagnóstico para o Tribunal, a fiscalização também intencionou conscientizar e orientar os gestores das organizações auditadas em relação aos riscos associados à ausência desses controles e das medidas de proteção associadas, a exemplo de violações e de vazamentos de dados, cada vez mais comuns. Ainda, a partir do cenário percebido, além do próprio TCU, órgãos com jurisdição ou supervisão administrativa sobre outros (*e.g.* CNJ, CNMP, SGD/MGI, Sest/MGI e ANPD) devem atuar com vistas a induzir o aprimoramento desses controles ao longo dos próximos anos.

284. Com isso, o Tribunal espera induzir as organizações públicas federais a elevarem suas maturidades em relação à adequação à LGPD, com reflexos nas respectivas resiliências quanto a incidentes e falhas de segurança que afetem a privacidade dos cidadãos e a proteção dos seus dados.

285. Ademais, esta auditoria municiou os gestores das organizações, bem como as respectivas unidades de controle/auditoria interno/a, com uma sistemática (CSA) e com ferramentas específicas (*e.g.* questionário [**Apêndice D** – Questionário da auditoria], *checklists* [**Apêndices G e H**] e relatórios individuais de *feedback*) para que as próprias organizações possam, ao longo dos próximos anos, continuar se autoavaliando e evoluindo em relação à implementação desses controles.

286. Por fim, a auditoria também serviu para fornecer, aos auditores dos tribunais estaduais participantes, um painel (*dashboard*) construído para permitir a visualização gráfica e interativa das

respostas das organizações auditadas, inclusive com a possibilidade de realização de análises comparativas e de segmentação dos resultados a partir da aplicação de filtros diversos. Ressalte-se que, uma vez que os dados das respostas das organizações foram classificados como públicos (tal aviso constou na primeira página do questionário aplicado), entende-se não haver óbice quanto à publicação do Painel Nacional de Implementação da LGPD na Internet.

Relatórios individuais de *feedback* às organizações auditadas

287. Para motivar os gestores a aperfeiçoarem os controles envolvidos, serão encaminhados às 387 organizações federais auditadas relatórios individuais de *feedback* contendo as respostas fornecidas pela própria organização e comparações com as respostas do conjunto das 387 organizações e com um subconjunto de organizações similares (**Apêndice E** – Organizações federais por área temática).

288. Com isso, espera-se que cada gestor possa comparar os resultados individuais da sua organização com a realidade de um grupo de organizações similares a ela e, assim, ter mais incentivos para continuar evoluindo, ao longo dos próximos anos, em relação à implementação dos controles e das medidas de proteção verificados.

7. Trabalhos futuros

289. Os resultados obtidos nesta fiscalização mostraram que o processo de adequação das organizações públicas federais à LGPD ainda não está completo, tendo em vista que, apesar da perceptível evolução ocorrida em comparação com o cenário verificado na auditoria de 2021 (Seção 2.4 deste relatório), ainda há muita margem para melhoria da maturidade desses órgãos/entidades, sendo possível identificar, inclusive, diversas questões que despertam preocupação e que, portanto, sugere-se que sejam endereçadas por meio de recomendação a alguns OGSs (Capítulo 10).

290. Com vistas a induzir ainda mais avanços no que se refere à implementação da LGPD por parte das organizações auditadas, convém que se avalie a conveniência e a oportunidade da realização de ações de controle voltadas a órgãos/entidades específicos, selecionados com base em critérios de relevância e risco, incluindo o próprio diagnóstico derivado desta auditoria.

291. Ademais, a publicação do "Painel Nacional de Implementação da LGPD" (Capítulo 5) na Internet permitirá que os próprios cidadãos continuem acompanhando o tema, cobrando gestores e organizações específicas e fomentando, assim, o avanço da adequação dos órgãos à LGPD por meio do controle social e da participação cidadã. Nada impede que esse painel continue a ser atualizado, seja em relação às organizações já auditadas ou mesmo para a inclusão de novos órgãos/entidades (por exemplo, há outros TCEs, além daqueles oito que participaram desta auditoria, interessados na aplicação do questionário e no fornecimento dos dados para que constem nesse painel).

292. Por fim, também é preciso continuar acompanhando de perto o processo de estruturação da ANPD, bem como o avanço da sua agenda regulatória, tendo em vista que essa autarquia será responsável, em grande parte, por atuar para assegurar que os direitos dos titulares de dados sejam respeitados e, consequentemente, que os dados pessoais dos cidadãos brasileiros sejam protegidos. O monitoramento do Tribunal mais recente acerca dessa questão foi tratado no TC 013.140/2022-1 (Acórdão 1.563/2024-TCU-Plenário; Rel. Min. Augusto Nardes).

293. No mesmo sentido, convém que seja acompanhada a elaboração e a execução da Política Nacional de Proteção de Dados e Privacidade, cujas diretrizes deverão ser estabelecidas pela ANPD (Resolução CD/ANPD 11/2023[23] [Agenda Regulatória para o biênio 2023-2024], Anexo, item 19).

8. Comentários dos gestores

294. Passa-se à análise da viabilidade de construção participativa das recomendações endereçadas a grandes conjuntos das organizações auditadas (parágrafos 177, 189, 205, 236, 251 e 265), incluindo aquelas que integram o Sistema de Administração dos Recursos de Tecnologia da Informação (Sisp)[24], o que será feito sob dois pontos de vista.

295. Primeiramente, observa-se que o propósito da Seção III da Resolução - TCU 315/2020 é obter informações sobre "consequências práticas da implementação das medidas aventadas e eventuais alternativas". As recomendações em questão propõem a adoção de medidas relacionadas ao processo de adequação à LGPD, na medida em que os gestores entenderem tais controles necessários para mitigar os riscos atinentes à execução das políticas públicas a cargo dos respectivos órgãos/entidades.

296. Visto que essas recomendações têm como pano de fundo o endereçamento das fragilidades apontadas pelas próprias organizações, entende-se que a única "alternativa" a tais sugestões seria o gestor optar por não fazer nada diante das situações de risco detectadas, o que, por óbvio, mostra-se incompatível com o princípio do interesse público.

297. De igual modo, não se vislumbra que alguma consequência prática negativa possa derivar da implementação de medidas de adequação à LGPD que os próprios gestores venham a julgar necessárias e decidam por priorizar, à luz das autoavaliações de riscos que realizaram.

298. Portanto, desse primeiro ponto de vista, conclui-se inexistir propósito prático no envio do relatório preliminar para que este receba comentários dessas centenas de gestores.

299. De outro prisma, como medida compensatória, buscou-se ouvir a ANPD, autoridade central em relação ao tema LGPD, bem como os demais OGSs (CNJ, CNMP, SGD/MGI e Sest/MGI), em face do seu poder de supervisão administrativa sobre os órgãos/entidades envolvidos, acerca da pertinência das propostas de recomendações direcionadas a esses grandes conjuntos das organizações auditadas. De modo geral, os órgãos citados ressaltaram a importância de se avançar no processo de implementação da Lei e não vislumbraram óbices quanto à deliberação aventada.

300. Desta forma, com fundamento na Resolução - TCU 315/2020, art. 14, § 2º, inciso II, tendo em vista a inexistência de alternativas e de aspectos negativos advindos das recomendações em tela, não houve envio do relatório preliminar para comentários dos gestores de cada uma das organizações individualmente endereçadas nos parágrafos 177, 189, 205, 236, 251 e 265.

301. A seguir, passa-se à análise dos comentários apresentados pelos gestores das organizações citadas no parágrafo 299, as quais suscitaram alterações na proposta de encaminhamento presente na versão preliminar do relatório, materializadas no parágrafo 353.2 da versão final do relatório.

8.1.Comentários da SGD/MGI

302. Em resposta ao Ofício 1.011/2024 - AudTI (peça 928), a SGD/MGI, por meio do Ofício SEI 178345/2024/MGI, de 13/12/2024 (peça 941), encaminhou seus comentários na Nota Técnica (NT) SEI 52652/2024/MGI, de mesma data (peça 940). Em relação à implementação das propostas de recomendação direcionadas às organizações auditadas sob sua jurisdição (parágrafo 299), a SGD/MGI apontou as consequências e impactos práticos resumidos na Tabela 19.

Tabela 19 - Consequências e impactos práticos das recomendações às organizações jurisdicionadas à SGD/MGI.
(Fonte: NT SEI 52652/2024/MGI [peça 940, p. 1-4, parágrafos 5-12.2])

Recomendação	Consequência	Impacto Prático
Iniciativas de Identificação, Planejamento e Execução de Medidas Preparatórias (parágrafo 353.1.1 deste relatório)	As 109 organizações precisarão desenvolver um plano estratégico e operacional para se adequarem à LGPD, o que inclui identificar as necessidades de adequação e estabelecer um cronograma de ações	Essa recomendação pode exigir a criação de equipes dedicadas e o envolvimento de diversos departamentos dentro da organização. O custo pode ser significativo, especialmente para organizações com infraestrutura ou processos de gestão de dados pessoais ainda não adequados. Será necessário realizar auditorias internas e implementar novos controles, o que pode gerar resistência por parte das equipes e demandar tempo e recursos
Mapeamento e Adequação ao	As 40 organizações terão que realizar um mapeamento	Este processo pode ser complexo e envolver a revisão de todos os processos de negócios, contratos e atividades

"Contexto Organizacional" (parágrafo 353.1.2)	detalhado sobre o tratamento de dados pessoais, identificando as categorias de dados, as bases legais, os riscos associados e a documentação necessária	relacionadas ao tratamento de dados. As organizações precisarão alocar recursos para garantir a conformidade com as exigências da LGPD, além de possivelmente revisar suas ferramentas de gestão de dados e atualizar contratos com fornecedores e parceiros
Adequação à Dimensão "Liderança" (parágrafo 353.1.3)	As 24 organizações deverão formalizar políticas relacionadas à proteção dedados, como a Política de Segurança da Informação e a nomeação de um Encarregado	Essa medida pode significar mudanças na estrutura de governança das organizações, com a necessidade de contratação ou designação de um profissional especializado para a função de encarregado de proteção de dados. Além disso, as políticas de segurança da informação precisarão ser revisadas, o que pode gerar custos e resistência interna
Plano de Capacitação sobre Proteção de Dados Pessoais (parágrafo 353.1.4)	As 161 organizações devem elaborar e implementar um plano de capacitação, o que implica em criar um programa de treinamentos periódicos para todas as pessoas envolvidas no tratamento de dados pessoais	Esse treinamento será um esforço contínuo, com custos associados à criação de materiais didáticos e à contratação de instrutores especializados. Além disso, as organizações precisam garantir que as informações sobre proteção de dados cheguem de forma clara e eficaz a todos os envolvidos, o que pode ser desafiador, especialmente em entidades maiores ou descentralizadas
Elaboração e Divulgação de Política de Privacidade (parágrafo 353.1.5)	As 146 organizações precisam desenvolver uma política de privacidade e divulgá-la de forma acessível em seus *sites* institucionais	A elaboração da política de privacidade envolve não apenas o desenvolvimento de conteúdo jurídico e informativo, mas também garantir que ela seja clara e compreensível para os titulares dos dados. Sua divulgação exige ferramentas de comunicação eficazes e contínuas atualizações, o que pode gerar custos de manutenção e desenvolvimento de novos canais de comunicação
Implementação de Mecanismos para Atender os Direitos dos Titulares (parágrafo 353.1.6)	As 90 organizações terão que criar processos para responder a solicitações dos titulares de dados, como acesso, retificação e exclusão dos dados, conforme os arts. 9º e 18 da LGPD	Será preciso implementar sistemas e procedimentos para garantir que as solicitações dos titulares sejam atendidas dentro dos prazos legais, o que pode implicar na aquisição de ferramentas específicas e na alocação de pessoal. Além disso, a organização terá que garantir que seus processos estejam alinhados com os direitos dos titulares
Avaliação de Compartilhamento de Dados Pessoais (parágrafo 353.1.7)	As 170 organizações precisam avaliar o compartilhamento de dados pessoais com terceiros e identificar os dados compartilhados, para garantir a conformidade com a LGPD	Isso implica em uma revisão detalhada de contratos e relações com terceiros, além de avaliar os riscos envolvidos no compartilhamento de dados. O processo pode ser trabalhoso e envolver negociações com fornecedores e parceiros, para garantir que a privacidade seja preservada em todas as transações de dados
Liderança, Envolvi-mento da Alta Administração e das Unidades de Controle Interno no Processo de adequação à LGPD (parágrafo 353.1.8)	As organizações precisam garantir que a alta administração lidere o processo de adequação à LGPD e que as unidades de controle/auditoria interno/a se envolvam, com foco no monitoramento e na avaliação de riscos	Isso pode resultar em uma mudança significativa na forma como as organizações abordam a proteção de dados, com a alta administração assumindo um papel ativo. Será necessário garantir que a auditoria interna tenha capacidade e recursos para monitorar a conformidade, o que pode significar um aumento nos custos operacionais e a necessidade de reestruturações

303. No que diz respeito ao acompanhamento e à indução, por parte da SGD/MGI, da implementação dos controles necessários para adequação à LGPD utilizando como referenciais as nove dimensões avaliadas no questionário da auditoria, além de outros guias e modelos existentes, a Secretaria apontou as consequências e impactos práticos listados na Tabela 20:

Tabela 20 - Consequências e impactos práticos da recomendação de que a SGD/MGI acompanhe e induza suas organizações jurisdicionadas.
(Fonte: NT SEI 52652/2024/MGI [peça 940, p. 4-5, parágrafos 13-13.2])

Consequências	A recomendação poderá melhorar a governança dos dados pessoais nas entidades supervisionadas pela SGD/MGI. As organizações estarão mais preparadas para garantir que os dados pessoais sejam tratados conforme as exigências da LGPD
	A medida fortalece a conformidade das organizações com a LGPD, minimizando riscos jurídicos e administrativos relacionados ao tratamento inadequado de dados pessoais
	A recomendação sugere que a SGD/MGI continue induzindo a implementação de controles detalhados, utilizando outros guias como referência. Isso pode gerar um aumento na complexidade operacional das organizações
Impactos Práticos	A implementação de controles específicos sobre dados pessoais, incluindo a definição clara de responsabilidades dos agentes de tratamento, pode exigir a adaptação de processos internos e a criação de novas políticas de privacidade e proteção de dados
	As organizações precisarão revisar e atualizar seus contratos, políticas internas e práticas de coleta e processamento de dados pessoais para estarem em conformidade com a legislação. Isso pode demandar esforços financeiros e operacionais, incluindo treinamento de equipes e investimento em ferramentas tecnológicas
	Implementar controles rigorosos pode ser um desafio para algumas organizações, principalmente as que possuem limitações orçamentárias ou recursos humanos escassos. O acompanhamento constante e a aplicação de boas práticas podem ser difíceis de monitorar, especialmente se as entidades não tiverem uma estrutura sólida de governança de dados. Isso pode resultar em ajustes constantes nos processos e em necessidade de revisões frequentes, aumentando a carga administrativa das organizações

304. Ainda quanto à atuação da SGD/MGI, a nota citou a Portaria SGD/MGI 852/2023, que instituiu o Programa de Privacidade e Segurança da Informação (PPSI), o qual apresenta diretrizes claras quanto aos controles e medidas de privacidade a serem implementados pelas organizações para adequação à LGPD, com metas e prazos de execução de julho de 2023 a dezembro de 2026.

305. Por fim, concluiu que "as medidas propostas oferecem benefícios claros, como a mitigação de riscos jurídicos e administrativos, o aumento da segurança no tratamento de dados e o alinhamento às melhores práticas de privacidade e proteção de dados", que sua implementação é viável, que as recomendações são relevantes e complexas e que "as consequências e impactos práticos destacados indicam que a adequação à LGPD e o fortalecimento da governança de dados pessoais representam um esforço significativo para as organizações" auditadas, envolvendo "ajustes estruturais, operacionais e financeiros, além de mudanças culturais e organizacionais" (peça 940, p. 5-6, parágrafos 14-26).

Análise dos comentários da SGD/MGI

306. A NT SEI 52652/2024/MGI apresentou, de forma objetiva, possíveis consequências e efeitos práticos da implementação das recomendações sugeridas no relatório de auditoria, sinalizando que alguns órgãos podem ter dificuldades em implementá-las.

307. De fato, cumprir a LGPD e garantir a proteção de dados pessoais é um desafio complexo ao qual as organizações precisam se adequar, pois os danos oriundos dos riscos de não o fazerem são imensos para os cidadãos que têm suas informações armazenadas em bases de dados gerenciadas por entes públicos.

308. Entretanto, apesar das dificuldades, isso não pode ser usado, por si só, como justificativa para o cenário identificado na presente auditoria relativamente à evolução da implementação da LGPD em comparação à avaliação realizada em 2021 pelo próprio TCU, que ainda revela um quadro em que

os cidadãos que usam serviços públicos e que são beneficiários de políticas públicas estão expostos a riscos que afetam a privacidade dos seus dados, com consequências que podem ser bem severas.

309. Ademais, tais recomendações visam a preparar as organizações fiscalizadas para o cumprimento de critérios normativos e/ou legais, a exemplo da nomeação do encarregado de dados (Lei 13.709/2018, art. 41) e da liderança dos processos de adequação à LGPD pela alta administração dos órgãos (Decreto 9.203/2017, art. 17).

310. Portanto, apesar do tamanho do desafio, é necessário que os gestores das organizações auditadas, liderados pelas respectivas altas administrações, implementem medidas efetivas para avançarem no sentido de cumprirem os preceitos da LGPD, mitigando, assim, os riscos para os titulares de dados, de acordo com suas capacidades operacionais e contando com o apoio da SGD nesse processo.

311. Dessa forma, entende-se que as recomendações direcionadas às organizações do Sisp, bem como à própria SGD/MGI, devem ser mantidas conforme registrado na versão preliminar do relatório (peça 923, p. 57, parágrafos 313.1 e 313.2).

8.2.Comentários da Sest/MGI

312. Em resposta ao Ofício 1.012/2024 - AudTI (peça 925), a Sest/MGI enviou seus comentários por intermédio do Ofício SEI 173656/2024/MGI, de 5/12/2024 (peça 942). Em relação à pertinência das propostas de recomendação direcionadas às organizações auditadas sob sua jurisdição (parágrafo 299), a Sest/MGI se limitou a informar que as empresas estatais sob sua supervisão "foram devidamente notificadas e cientificadas a respeito das demandas apontadas no relatório" (peça 942, p. 1, parágrafo 2).

313. No tocante ao acompanhamento e indução, por parte da Sest/MGI, da implementação dos controles necessários para adequação à LGPD com base nas nove dimensões avaliadas no questionário da auditoria, além de outros guias e modelos, a Secretaria informou que "continuará a acompanhar a implementação das ações para adequação à LGPD sob o ponto de vista da governança corporativa das empresas estatais, respeitando o limite das competências institucionais que lhe foram atribuídas" (peça 942, p. 1, parágrafo 3).

Análise dos comentários da Sest/MGI

314. Tendo em vista que a Sest/MGI não apresentou consequências práticas da implementação das medidas aventadas nem eventuais alternativas, bem como não se opôs às propostas de recomendação feitas pela equipe de auditoria às empresas estatais e à própria Secretaria, entende-se pela manutenção de tais propostas.

8.3.Comentários da ANPD

315. Em resposta ao Ofício 1.014/2024 - AudTI (peça 926), a ANPD apresentou seus comentários nos documentos acostados às peças 936-939. Em síntese, a Autoridade trouxe três argumentos principais à consideração da equipe de auditoria, quais sejam:

315.1. Em relação à recomendação para que continuasse acompanhando e induzindo as organizações sob sua jurisdição a implementarem os controles necessários para se adequarem à Lei 13.709/2018 (parágrafo 353.2), a Autarquia manifestou que "não detém competência para o exercício do poder de supervisão administrativa sobre qualquer dos demais 386 órgãos ou entidades listados na 'peça 922'" (peça 936, p. 2, parágrafo 3);

315.2. Ainda sobre esse ponto, a ANPD aduziu que o referido acompanhamento implicaria na instauração de processos de fiscalização pela Autoridade perante esses órgãos, o que feriria o poder discricionário da ANPD quanto à definição de critérios e prioridades para suas atividades fiscalizatórias, bem como interromperia a execução do seu planejamento institucional, previsto no Mapa de Temas Prioritários para o biênio 2024-2025 (peça 937, p. 6-7, parágrafo 6.1);

315.3. No tocante à recomendação para elaboração de Política de Privacidade (parágrafo 353.1.5), a ANPD sugeriu a definição precisa dos termos utilizados, com vistas a promover a uniformidade de

entendimentos. Apontou que o relatório preliminar utilizou "Política de Privacidade" e "Aviso de Privacidade" como sendo sinônimos ou indicando se tratarem de documentos de natureza semelhante, enquanto a ANPD tem adotado, em suas discussões normativas/regulatórias, diferentes significados para essas duas expressões (para a Autoridade, "Aviso de Privacidade" denominaria o documento destinado a informar os titulares de dados pessoais acerca do tratamento de seus dados de maneira ostensiva, clara, adequada e acessível, ao passo que "Política de Privacidade" seria o documento que estabelece as regras de boas práticas e de governança, entre outros aspectos relacionados ao tratamento de dados pessoais, como indicado pelo art. 50 da LGPD [*e.g.* condições da organização; regime de funcionamento; procedimentos, incluindo os relacionados às reclamações e petições de titulares; normas de segurança; padrões técnicos; obrigações específicas para os diversos envolvidos no tratamento; ações educativas; mecanismos internos de supervisão e de mitigação de riscos]). Por conseguinte, a ANPD considerou que adotar essa distinção entre "Aviso de Privacidade" e "Política de Privacidade" promoveria "maior clareza e efetividade na comunicação, assegurando precisão conceitual e alinhamento às boas práticas de governança" (peça 938, p. 4-5, parágrafos 2.8-2.12).

316. Com isso, a ANPD sugeriu a avaliação de duas revisões no relatório preliminar: i) retirada da menção à ANPD na recomendação direcionada aos órgãos com supervisão administrativa sobre outros (parágrafo 353.2), tendo em vista que a Autoridade não detém competência para o exercício de tal poder sobre as organizações listadas na peça 922, apenas uma função regulatória e fiscalizatória, positivada, entre outros dispositivos, no art. 55-J da Lei 13.709/2018; ii) adoção dos termos "Aviso de Privacidade" e "Política de Privacidade" de acordo com as definições apresentadas, de modo a privilegiar a transparência e a clareza no processo de comunicação e a aumentar a precisão conceitual e a conformidade com as suas interpretações regulatórias (peça 938, p. 5-6, parágrafo 3.1).

317. Por fim, a ANPD aduziu que, "dada a importância e pertinência do trabalho realizado pelo TCU, os dados, as informações e as recomendações contidos no Relatório de Auditoria TC 009.980/2024-5 (...) serão considerados nas próximas atividades de programação e planejamento" da sua Coordenação de Fiscalização, "em especial na elaboração do Mapa de Temas Prioritários do biênio de 2026-2027, o que deverá ocorrer no segundo semestre" (peça 937, p. 7, parágrafo 6.2).

Análise dos comentários da ANPD

318. Quanto ao primeiro comentário (parágrafo 315.1), conforme amplamente fundamentado no Ofício 524/2024/GABPR/ANPD (peça 936), na NT 219/2024/CON2/CGN/ANPD (peça 938) e no Parecer 18/2021/GAB/ASJUR-ANPD/CGU/AGU (peça 939), a Autoridade efetivamente não detém competência para exercer o poder de supervisão administrativa sobre os órgãos/entidades listados na peça 922, atuando apenas com função tipicamente regulatória e fiscalizatória. Dessa forma, entende-se que deve ser acatado o argumento da Autoridade quanto a esse item e, consequentemente, retirada a menção à ANPD da recomendação prevista no parágrafo 353.2 deste relatório.

319. Em relação ao segundo comentário (parágrafo 315.2), cumpre esclarecer que o objetivo da proposta de recomendação era, sobretudo, no sentido de que a Autoridade continuasse promovendo eventos e elaborando normativos e guias de implementação, a exemplo do "Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado"[9] e do "Guia Orientativo – Tratamento de dados pessoais pelo Poder Público"[10].

320. No que diz respeito ao terceiro ponto (parágrafo 315.3), apesar de reconhecer-se a relevância e a assertividade da sugestão, cumpre informar que o relatório se fundamentou em questionário eletrônico aplicado a 387 organizações públicas federais, o qual utilizou os termos aqui reproduzidos. O questionário (**Apêndice D** – Questionário da auditoria) contém longo texto explicativo sobre o que é, o teor e o conteúdo que se espera de uma Política de Privacidade, mitigando o risco de confusão. Além disso, oito TCEs fizeram auditorias paralelas utilizando essa mesma terminologia, existem 387 relatórios de *feedback* que já estão prontos, apenas aguardando o julgamento do processo para serem encaminhados

aos órgãos auditados, e foi criado um "Painel Nacional de Implementação da LGPD" (Capítulo 5) pelos órgãos fiscalizados, o qual, inclusive, será posteriormente aberto à sociedade.

321. Portanto, entende-se que alterar o termo "Política de Privacidade" para "Aviso de Privacidade" em todos esses documentos e artefatos já elaborados acarretaria um trabalho razoável, com risco adicional de gerar inconsistências em documentos diferentes. Dessa forma, entende-se que não seria produtivo alterar os termos citados no presente relatório.

8.4.Comentários do CNMP

322. Em resposta ao Ofício 1.015/2024 - AudTI (peça 924), o CNMP encaminhou, por meio do Ofício 73/2024/SG/SEC, de 16/12/2024 (peça 943), despacho elaborado pela respectiva encarregada de dados (peça 944), a qual dividiu a sua análise e comentários em duas partes: uma primeira, relativa à recomendação endereçada ao próprio CNMP (parágrafo 353.2), e outra, referente às recomendações direcionadas aos órgãos do Ministério Público da União – MPU (parágrafo 353.1).

323. Em relação ao CNMP, foi informado que o tema proteção de dados pessoais ganhou destaque a partir da publicação da Resolução - CNMP 281/2023[25] [Institui a Política Nacional de Proteção de Dados Pessoais e o Sistema Nacional de Proteção de Dados Pessoais no Ministério Público – MP], a qual "estabeleceu diretrizes para as ações de planejamento e execução das obrigações funcionais e estabeleceu prazos e procedimentos para a adequação e gestão administrativa dos ramos e unidades do [MP] nacional, em alinhamento com as regras e princípios aplicáveis à proteção de dados pessoais" (peça 944, p. 2).

324. Segundo o Conselho, essa "Resolução estabelece (...) que o papel de Autoridade Nacional de Proteção de Dados do Ministério Público (APDP/MP) será desempenhado pela Unidade Especial de Proteção de Dados Pessoais (UEPDAP), vinculada à Comissão de Preservação da Autonomia do Ministério Público (CPAMP) do CNMP" (peça 944, p. 2).

325. À continuação, o despacho destacou uma série de iniciativas desenvolvidas pelo Conselho: relatório de conformidade e cronograma de adequação; ações de capacitação; campanha nacional de divulgação; e atuação finalística na tutela da proteção de dados pessoais (peça 944, p. 4-6).

326. Por fim, citou a realização, em 2024, de "8 (oito) reuniões ordinárias internas, duas reuniões com o [CNJ] e uma reunião com a [ANPD] para fortalecer a cooperação entre as instituições, com o objetivo de aumentar a efetividade na tutela do direito fundamental à proteção de dados pessoais" (peça 944, p. 7).

327. Quanto às recomendações aos órgãos do MPU, argumentou que o apontamento de que o Ministério Público Militar (MPM) e o Ministério Público do Trabalho (MPT) não teriam padronizado a comunicação de incidentes à ANPD não deve prosperar, uma vez que a mencionada Resolução - CNMP 281/2023 estabelece que "quem exerce a função de Autoridade Nacional de Proteção de Dados do Ministério Público (APDP/MP) é a [UEPDAP], por força do art. 4º, inciso V e art. 25", de forma que "eventuais incidentes de segurança ocorridos no âmbito dos ramos e unidades do [MP] deverão ser comunicados à UEPDAP, e não à ANPD, o que justifica[ria] a ausência de padronização de comunicação informada nos autos" (peça 944, p. 9-10).

328. Sobre os pontos de atenção contidos no relatório que noticiam que "a Escola Superior do MPU [ESMPU], o MPDFT e o MPT não possuem Plano de Capacitação" e que "a ESMPU não avaliou se compartilha dados pessoais com terceiros ou ainda não identificou os dados eventualmente compartilhados", o Conselho sinalizou que tais pontos "encontram-se contemplados nos arts. 62 e 100 da Resolução - CNMP 281/[20]23, e serão objeto de acompanhamento e fiscalização por parte da UEPDAP, em cumprimento ao processo de adequação à LGPD já iniciado nos ramos e unidades ministeriais" (peça 944, p. 10).

Análise dos comentários do CNMP

329. As iniciativas descritas pelo CNMP (parágrafos 323-326) mostram que a aplicação da Resolução - CNMP 281/2023 e os compromissos do Conselho e da UEPDAP em garantirem a conformidade regulatória e a tutela do direito fundamental à proteção dos dados pessoais, de certo modo, já vêm surtindo o efeito que se deseja com a recomendação do parágrafo 353.2, uma vez que têm induzido que os órgãos do MP implementem os controles necessários para se adequarem à LGPD.

330. Em todo caso, entende-se pertinente manter aquela recomendação, no sentido de que o CNMP, em conjunto com a UEPDAP, continue acompanhando e induzindo a implementação desses controles ao longo dos próximos anos.

331. Ademais, o fato de a Resolução - CNMP 281/2023 prever que MPM e MPT reportem eventuais incidentes de segurança à UEPDAP não exclui sua obrigação de os reportarem, também, à ANPD, conforme prevê a LGPD (Lei 13.709/2018, art. 48).

332. Quanto ao fato de a ESMPU, o MPDFT e o MPT não possuírem Plano de Capacitação e a ESMPU não ter avaliado se compartilha dados pessoais com terceiros ou ainda não ter identificado os dados compartilhados, a sinalização do Conselho de que tais pontos estão contemplados nos arts. 62 e 100 da Resolução - CNMP 281/2023 e serão acompanhados e fiscalizados pela UEPDAP, apesar de importante, não é suficiente para alterar a situação fática apontada na autoavaliação realizada pelos próprios gestores. Ademais, essa recomendação reforçará a necessidade de que as unidades envolvidas tratem esses pontos de atenção, não se vislumbrando, portanto, óbice quanto à sua manutenção.

333. Dessa forma, entende-se que as recomendações contidas nos subitens do parágrafo 353.1, no que se refere aos órgãos do MP, devem ser mantidas.

8.5.Comentários do CNJ

334. Em resposta ao Ofício 1.016/2024 - AudTI (peça 927), o CNJ encaminhou, por meio do Ofício 1103/2024/SG, de 19/12/2024 (peça 946), despacho da Coordenadoria de Apoio à Governança de TIC (peça 945), a qual também dividiu a sua análise e comentários em duas partes: uma sobre o CNJ como instituição (parágrafo 353.2) e outra referente à atuação do CNJ como OGS (parágrafo 353.1).

335. Em relação à instituição, o Conselho reconheceu a assertividade dos apontamentos do relatório de auditoria e informou que adotará as iniciativas necessárias para implementar as recomendações, ressaltando que "a Política de Privacidade, Uso de Dados e de Cookies no CNJ já se encontra em processo de elaboração (...), bem como uma [SIC] avaliações e diagnósticos sobre mapeamento de dados pessoais, além de avaliações de maturidade visando [a]o atendimento pleno dos requisitos da LGPD" (peça 945, p. 2-3).

336. Quanto ao seu papel como OGS, enalteceu que "o CNJ já possui publicada[s] as Resoluções Nº 363[/2021], que estabelece medidas para o processo de adequação à [LGPD] a serem adotadas pelos tribunais; e (...) 396[/2021], que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário – ENSEC-PJ, citada no próprio relatório de auditoria" (peça 945, p. 4).

337. Por fim, pugnou que, para exercer plenamente o seu papel de OGS, precisa ter acesso aos resultados do esforço até então realizado por cada uma das organizações que atuam sob sua supervisão administrativa, ou seja, precisa receber os relatórios individualizados de *feedback*, "sob pena de terem que envidar novos esforços para realizar os mesmos levantamentos e gastar, assim, um tempo precioso na implementação dos mecanismos necessários para o pleno cumprimento da LGPD" (peça 945, p. 4).

Análise dos comentários do CNJ

338. No que diz respeito ao CNJ enquanto instituição, cumpre louvar o reconhecimento do Conselho sobre os pontos de atenção, bem como a sua disposição em adotar iniciativas para implementação das recomendações, dando importante passo para o cumprimento da LGPD.

339. No tocante à sua atuação como OGS e ao seu pedido de acesso aos relatórios individualizados para melhor atuar no papel de acompanhar e induzir a implementação da LGPD pelos

órgãos do judiciário, cumpre ressaltar que a proposta de encaminhamento já prevê esse compartilhamento (parágrafo 353.7.2), de modo que não se faz necessário nenhum ajuste no relatório.

340. Dessa forma, entende-se pela manutenção das recomendações voltadas ao CNJ.

9. Conclusão

341. Esta auditoria diagnosticou os controles implementados por 387 organizações públicas federais (peça 922) para adequação à LGPD, por meio de um questionário de autoavaliação, subdividido 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".

342. A análise dos resultados obtidos indicou diversos pontos de atenção, incluindo a identificação de sete achados de auditoria (Capítulo 4): i) não conclusão de medidas preparatórias com vistas a se adequar à LGPD; ii) não condução de qualquer iniciativa ligada à dimensão "Contexto organizacional"; iii) não realização de qualquer das ações ligadas à dimensão "Liderança"; iv) ausência de PSI, de nomeação do DPO e de comunicação padronizada à ANPD; v) ausência de Plano de Capacitação; vi) ausência de Política de Privacidade e não atendimento a direitos dos titulares; e vii) desconhecimento dos compartilhamentos de dados pessoais com terceiros. Ademais, de todas as 387 organizações, as instâncias de controle interno de quase metade (159, ou 41,09%) não realizaram trabalho de avaliação sobre a LGPD ou a LAI nos últimos três anos (parágrafo 165).

343. Para permitir a comparação das organizações, foi criado um indicador (iLGPD) capaz de resumir as respostas fornecidas nas nove dimensões do questionário em um valor entre 0 e 100%, relativo ao grau de implementação das medidas de adequação avaliadas. O iLGPD médio das 387 organizações auditadas foi de 44%. As avaliações médias das nove dimensões indicaram carências, sobretudo, quanto à realização de medidas preparatórias para adequação à LGPD (44%), ao compartilhamento de dados pessoais (22%) e à implementação de medidas para proteger esses dados (34%). [Figura 13].

344. De modo geral, considera-se cumprido o objetivo primário da fiscalização (Seção 1.3 deste relatório), tendo-se notícia, inclusive, acerca da implementação de controles pelas organizações durante o próprio curso da auditoria, de modo que estas pudessem responder positivamente determinado item do questionário (*e.g.* nomeação de encarregado pelo tratamento de dados pessoais).

345. Entende-se que os benefícios estimados (Seção 1.8 deste relatório) foram parcialmente alcançados, a partir da conscientização dos gestores das 387 organizações auditadas quanto à necessidade de adequação à LGPD e da disponibilização, a estes e às auditorias internas dos respectivos órgãos/entidades, de ferramenta/sistemática para que possam continuar se autoavaliando.

346. Contudo, a equipe considera que o panorama das 387 organizações públicas federais, identificado a partir desta auditoria, ainda representa riscos à privacidade dos cidadãos e à proteção dos respectivos dados pessoais, fazendo-se necessário que tais órgãos/entidades prossigam implementando os controles/medidas avaliados, bem como outros, de modo a darem pleno cumprimento à LGPD.

347. Diante disso e dos achados identificados, foram propostas recomendações que visam a auxiliar os gestores a se adequarem à LGPD, de modo a cumprir os requisitos de conformidade com a referida lei e, também, atingir os benefícios que as boas práticas de proteção de dados pessoais e de privacidade proporcionam às organizações públicas e, principalmente, aos cidadãos.

348. Além disso, é preciso destacar que boa parte dos achados (4.1, 4.2, 4.3, 4.4 e 4.6) tiveram como causas uma falta de atuação adequada da alta administração no que diz respeito à priorização do tema nas organizações públicas fiscalizadas, motivo pelo qual será proposta recomendação específica para que exerçam suas funções e liderem as ações de implementação da LGPD nos respectivos órgãos em que tais achados foram identificados, considerando o disposto no art. 17 do Decreto 9.203/2017.

349. Para orientar seus progressos individuais nessa jornada, cada uma das 387 organizações auditadas receberá um relatório de *feedback* personalizado. Ademais, propõe-se recomendações de

caráter geral às respectivas unidades de controle/auditoria interno/a e aos principais OGSs (CNJ, CNMP, SGD/MGI e Sest/MGI), de modo que acompanhem a evolução desses órgãos/entidades ao longo dos próximos anos e induzam a continuidade do aumento de maturidade de todos nessa área. Os principais pontos de atenção identificados nas 387 organizações estão sintetizados na peça 922.

350. Adicionalmente, é importante que a ANPD e os OGSs continuem a editar normativos e guias com vistas a, ao longo dos próximos anos, orientar e induzir a continuidade dos processos de adequação à LGPD das organizações sob suas supervisões administrativas.

351. Registre-se que esta auditoria serviu, também, para o compartilhamento de conhecimentos, métodos e ferramentas com auditores dos TCEs (Seção 1.3, tópico "Rede Integrar - Ação 29 do Plano Anual de Trabalho 2024"), bem como para a construção do "Painel Nacional de Implementação da LGPD" (Capítulo 5), o qual, espera-se, servirá para fomentar as organizações públicas federais, estaduais e municipais a continuarem suas ações e projetos de adequação à LGPD.

352. Por fim, considerando a possibilidade de construção participativa das deliberações deste Tribunal, nos termos do art. 14 da Resolução - TCU 315/2020, bem como o previsto nas Normas de Auditoria – NAT (Portaria - TCU 280/2010), foi oportunizado prazo de dez dias aos órgãos/entidades destinatários da recomendação de acordo com o relatório preliminar (CNJ, CNMP, SGD/MGI, Sest/MGI e ANPD) para que, caso quisessem, apresentassem comentários e/ou informações quanto às consequências práticas da implementação das medidas aventadas, bem como eventuais alternativas. Esses comentários dos gestores foram avaliados no Capítulo 8 deste relatório.

10. Propostas de encaminhamento

353. Diante do exposto, submetem-se os autos à consideração do Relator, Ministro Walton Alencar Rodrigues, com as seguintes propostas:

353.1. **recomendar**, com fundamento no art. 11 da Resolução - TCU 315, de 2020 (parágrafo 342):

353.1.1. **às 109 organizações apontadas no achado 4.1** (peça 922, coluna "Q2.1") que realizem iniciativas voltadas à identificação, ao planejamento e à execução de medidas preparatórias para se adequarem à LGPD;

353.1.2. **às 40 organizações apontadas no achado 4.2** (peça 922, coluna "Q3.1") que conduzam iniciativas ligadas à dimensão "Contexto organizacional" (*e.g.* mapear normativos afetos à proteção de dados pessoais aplicáveis ao ente; identificar elementos relacionados aos tratamentos de dados pessoais: dados tratados, categorias de titulares com os quais se relaciona, operadores, controladores conjuntos, processos de negócio, responsáveis, locais de armazenamento dos dados; adequar instrumentos contratuais; avaliar riscos associados aos processos de tratamento de dados);

353.1.3. **às 24 organizações apontadas no achado 4.3** (peça 922, coluna "Q4.1") que realizem iniciativas ligadas à dimensão "Liderança" (*e.g.* formalização de políticas [Segurança da Informação, Classificação da Informação, Proteção de Dados Pessoais], nomeação do encarregado pelo tratamento de dados pessoais e publicação das respectivas informações de contato);

353.1.4. **às 161 organizações apontadas no achado 4.5** (peça 922, coluna "Q5.1", respostas "a1" e "a2") que elaborem Plano de Capacitação (ou instrumento similar) e contemplem nele a temática de proteção de dados pessoais, incluindo a necessidade de treinamento diferenciado para as pessoas que exercem funções com responsabilidades essenciais quanto à proteção de dados pessoais;

353.1.5. **às 146 organizações apontadas no achado 4.6** (peça 922, coluna "Q7.1") que elaborem Política de Privacidade (ou instrumento similar) e a divulguem em seu sítio eletrônico institucional;

353.1.6. **às 90 organizações apontadas no achado 4.6** (peça 922, coluna "Q7.2") que implementem mecanismos para atender os direitos dos titulares (LGPD, arts. 9º e 18);

353.1.7. **às 170 organizações apontadas no achado 4.7** (peça 922, coluna "Q8.1") que avaliem se compartilham dados pessoais com terceiros e identifiquem os dados eventualmente compartilhados;

353.1.8. **às organizações apontadas nos achados 4.1 a 4.7** (peça 922, colunas "Q2.1", "Q3.1", "Q4.1", "Q5.1", "Q7.1", "Q7.2" e "Q8.1"; peças 918, 919 e 920) que:

353.1.8.1. os respectivos processos de adequação à LGPD sejam liderados explicitamente pela sua alta administração, considerando o disposto no art. 17 do Decreto 9.203/2017 (parágrafo 348);

353.1.8.2. envolvam as respectivas unidades de controle/auditoria interno/a no processo de adequação à LGPD, fazendo com que incluam em seus planejamentos atividades de avaliação e monitoramento de riscos relacionados à privacidade e à proteção de dados pessoais, em especial quanto ao endereçamento dos pontos de atenção relacionados nas peças 918, 919, 920 e 922, bem como avaliem periodicamente a efetividade das medidas e das práticas operacionais já implementadas (parágrafo 349);

353.2. **recomendar ao Conselho Nacional de Justiça, à Secretaria de Governo Digital e à Secretaria de Coordenação e Governança das Empresas Estatais, ambas do Ministério da Gestão e da Inovação em Serviços Públicos, bem como ao Conselho Nacional do Ministério Público, este último em conjunto com sua Unidade Especial de Proteção de Dados Pessoais**, com fundamento no art. 11 da Resolução - TCU 315, de 2020, que, considerando suas atuações sobre as organizações sob suas respectivas supervisões administrativas, continuem acompanhando e induzindo a implementação dos controles necessários para adequação à Lei 13.709/2018 (LGPD), em especial quanto ao endereçamento dos pontos de atenção relacionados nas peças 918, 919, 920 e 922 (parágrafo 349), utilizando como referenciais as nove dimensões avaliadas no questionário desta auditoria, além de outros guias e modelos existentes (Resolução CCGD 4/2020: "Guia de Boas Práticas para Implementação da LGPD na APF"; ANPD: "Guia Orientativo – Tratamento de dados pessoais pelo Poder Público", "Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado"; MGI: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/framework-guias-e-modelos);

353.3. **dar ciência**, com fundamento na Resolução - TCU 315/2020, art. 9º, inciso I:

353.3.1. **às 80 organizações listadas na peça 918** de que a ausência de estabelecimento formal de uma Política de Segurança da Informação afronta o disposto no Decreto 9.637/2018, art. 15, inciso II, c/c a Instrução Normativa - GSI/PR 1/2020, art. 9º, bem como na Resolução - CNJ 396/2021, art. 19, inciso II, e na Resolução - CNMP 156/2016, art. 22, inciso III (parágrafo 221.1);

353.3.2. **às 48 organizações listadas na peça 919** de que a ausência de nomeação do encarregado pelo tratamento de dados pessoais afronta o disposto na Lei 13.709/2018, art. 41, *caput* (par. 221.2);

353.3.3. **às 250 organizações listadas na peça 920** de que a falta de comunicação à ANPD e aos titulares de dados da ocorrência de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares afronta o disposto na Lei 13.709/2018, art. 48, *caput* (parágrafo 221.3);

353.4. 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 a deliberação contida no parágrafo 353.2, sendo que aquelas contidas no parágrafo 353.1, por serem de caráter mais específico de cada organização auditada, não serão monitoradas;

353.5. **classificar como públicos os dados das respostas individuais das 387 organizações ao questionário da auditoria**, conforme Lei 12.527/2011 (LAI), art. 3º, inciso I, excetuando-se as informações pessoais dos gestores respondentes, as quais devem ser classificadas como sigilosas, em consonância com o art. 31, § 1º, inciso I, dessa mesma lei;

353.6. encaminhar cópias eletrônicas deste relatório e do acórdão decorrente desta fiscalização, bem como do relatório e do voto que o fundamentarem, ao Conselho Nacional de Justiça (CNJ), ao Conselho Nacional do Ministério Público (CNMP), à Unidade Especial de Proteção de Dados Pessoais (UEPDAP) do Ministério Público, à Secretaria de Governo Digital (SGD/MGI) e à Secretaria de Coordenação e Governança das Empresas Estatais (Sest/MGI), ambas do Ministério da Gestão e da Inovação em Serviços Públicos, à Autoridade Nacional de Proteção de Dados (ANPD), à Casa Civil (CC/PR) e ao Gabinete de Segurança Institucional (GSI/PR), ambos da Presidência da República, à

Controladoria-Geral da União (CGU), à Frente Parlamentar Mista pela Transparência Pública, à Comissão de Transparência, Governança, Fiscalização e Controle e Defesa do Consumidor do Senado Federal, ao Instituto Rui Barbosa (IRB), à Associação dos Membros dos Tribunais de Contas do Brasil (Atricon), entidade coordenadora do Programa Nacional de Transparência Pública, aos Tribunais de Contas dos Estados do Amazonas (TCE-AM), da Bahia (TCE-BA), do Ceará (TCE-CE), do Pará (TCE-PA), de Pernambuco (TCE-PE), do Paraná (TCE-PR), do Rio de Janeiro (TCE-RJ) e do Rio Grande do Norte (TCE-RN), os quais conduziram auditorias independentes similares a esta, bem como às demais organizações públicas auditadas (peça 922);

353.7. autorizar a Unidade de Auditoria Especializada em Tecnologia da Informação (AudTI), observada eventual necessidade de reserva quanto a questões específicas, a:

353.7.1. dar ampla divulgação às informações e aos produtos derivados da execução desta auditoria, a fim de contribuir para a melhoria das organizações públicas em relação à adequação à LGPD;

353.7.2. compartilhar os dados das respostas individuais das organizações ao questionário da auditoria, excetuando-se as informações pessoais dos gestores respondentes, com o CNJ, o CNMP, a SGD/MGI, a Sest/MGI e a ANPD, observados os grupos de organizações públicas sob as respectivas supervisões administrativas, de modo que tais órgãos possam orientar e contribuir ativamente para o processo de adequação das suas organizações supervisionadas à LGPD;

353.8. classificar como público o presente processo, nos termos da Resolução - TCU 294/2018, arts. 4º e 8º, com exceção das peças 722, 733, 734, 754, 755, 758, 759, 760, 761, 762, 763, 764, 768, 770, 771, 772, 773, 777, 785, 786, 788, 789, 790, 793, 794, 795, 796, 799, 800, 812, 820, 823, 824, 825, 826, 827, 829, 830, 831, 834, 836, 841, 842, 846, 847, 848, 849, 850, 851, 852, 853, 854, 855, 863, 865, 866, 870, 871, 882, 887, 888, 889, 895, 903, 906, 909, 911, 913 e 921, as quais devem ser classificadas como sigilosas por conterem informações pessoais de gestores, em consonância com a Lei 12.527/2011 (LAI), art. 31, § 1º, inciso I;

353.9. arquivar o presente processo, com base no art. 169, inciso V, do Regimento Interno do TCU.

Audti, 28 de janeiro de 2025.

(assinado eletronicamente)
Regis Soares Machado
AUFC - Mat. 7688-0
Coordenador

(assinado eletronicamente)
Fernando Pereira de Faria
AUFC - Mat. 8118-3
Membro

(assinado eletronicamente)
Sylvio Xavier Júnior
AUFC - Mat. 2423-6
Membro

Apêndice A – Planejamento da fiscalização

Auditoria sobre a implementação dos dispositivos da LGPD na União

Objetivo contido na proposta de fiscalização (TC 007.563/2024-8, peça 2)

De acordo com a proposta de fiscalização do tipo Auditoria de Conformidade (TC 007.563/2024-8), o objetivo do trabalho foi elaborar diagnóstico acerca dos controles implementados por organizações públicas federais para adequação à LGPD, bem como induzir essas organizações a conduzirem iniciativas para providenciar o pleno cumprimento da legislação. A auditoria foi conduzida pela AudTI.

Critérios utilizados para proposição (TC 007.563/2024-8, peça 2)

Riscos

- Organizações públicas não estarem aderentes à LGPD, mesmo após o início de vigência da Lei 13.709/2018 e a realização de fiscalização anterior sobre o tema (TC 039.606/2020-1);

- Dados pessoais tratados em desconformidade com a legislação, com prejuízos aos cidadãos e perda de confiança no governo;

- Danos à imagem das organizações ou mesmo prejuízos ao erário em virtude de eventuais indenizações por descumprimento da legislação.

Oportunidade

A LGPD entrou em vigor em agosto de 2020 e, um ano depois, o TCU constatou que 76,7% das organizações públicas federais encontravam-se nos graus inexpressivo ou inicial de adequação àquela lei (TC 039.606/2020-1). Com isso, o presente momento se mostrava oportuno para a realização de nova fiscalização, com vistas a verificar a evolução do cumprimento da legislação pela Administração Pública, desta vez em conjunto com alguns TCEs (de modo a incluir organizações estaduais e municipais), tendo em vista que essa ação de controle foi incluída no Plano Anual de Trabalho (PAT) 2024 da Rede Integrar (Ação 29). Ademais, os resultados da auditoria poderão guiar os gestores na condução de iniciativas para adequação à legislação.

Materialidade

Apesar de as organizações públicas estarem isentas da aplicação de multas pela ANPD (Lei 13.709/2018, art. 52, § 3º), os impactos causados por eventual divulgação imprópria de dados pessoais podem resultar em ações judiciais e indenizações, com consequentes danos de imagem e/ou pecuniários ao erário. Não há como calcular a materialidade exata.

Relevância

Países que não proveem mecanismos adequados de proteção de dados pessoais estão perdendo oportunidades comerciais. Ademais, lei similar entrou em vigor na União Europeia em 2018 (*General Data Protection Regulation* – GDPR), o que aumentou a relevância do tema proteção de dados na comunidade internacional. Sem proteção de dados, não há privacidade. Com a aceleração da transformação digital do setor público, dados dos cidadãos são cada vez mais utilizados pelo governo, sendo que a violação desses dados pode causar prejuízos enormes à população. Por isso, faz-se necessário ao Tribunal induzir a implementação de medidas por parte das organizações da APF para a proteção e o devido tratamento dos dados pessoais e a garantia de sua privacidade.

Retorno ou benefício(s) esperado(s)

- Conscientização das organizações públicas federais, estaduais e municipais quanto à necessidade de se adequarem à LGPD;

- Conhecimento dos Tribunais de Contas sobre o grau de adequação dessas organizações à LGPD, por meio do "Painel Nacional de Implementação da LGPD";

- Criação de base de conhecimento, aderente à realidade governamental, para auxiliar essas organizações na condução de projetos de adequação à LGPD;

- Disponibilização, a gestores e auditorias internas das organizações auditadas, de ferramenta/sistemática para autoavaliação contínua ao longo dos próximos anos.

Apêndice B – Matriz de Planejamento

TC 009.980/2024-5 **Fiscalização:** 96/2024
TIPO: Auditoria de Conformidade.
ÓRGÃO/ENTIDADE: 387 organizações da Administração Pública federal (peça 922).
OBJETIVOS: Elaborar diagnóstico acerca dos controles implementados por organizações públicas federais para adequação à Lei Geral de Proteção de Dados Pessoais (LGPD) e induzi-las a conduzirem iniciativas para providenciar o pleno cumprimento da Lei 13.709/2018.

Tema	Informações requeridas	Fontes de informação	Procedimento	Detalhamento do procedimento	Possíveis achados
Preparação, Contexto organizacional, Liderança e Capacitação Q1. As organizações se estruturaram para a condução de iniciativas de adequação à LGPD?	IR1. Iniciativas (plano de ação, projeto ou documento similar) da organização para providenciar a adequação à LGPD. IR2. Política (ou documento similar) que considera os princípios e aspectos gerais de tratamento de dados. IR3. Processo de tratamento de dados mapeado. IR4. Normas internas relacionadas a proteção e	FI1. Respostas dos gestores ao questionário. (IR1 a IRxx) FI2. Plano de projeto/ação/ normativo para adequação à LGPD. (IR4) FI3. Políticas/normas sobre a classificação de informações. (IR2) FI4. Política de proteção de dados pessoais. (IR3) FI5. Política de segurança da informação. (IR1)	**Liderança** P1. Verificar se as organizações elaboraram políticas relacionadas ao tratamento de dados pessoais. LGPD, arts. 46 e 50, inciso I, alíneas "a" e "d". ABNT NBR ISO/IEC 27701:2019, itens 6.2, 6.2.1, 6.5.2 e 7.2.1. ABNT NBR ISO/IEC 27002:2019, itens 5.1 e 8.2.	P1.1 Verificar se há política de segurança da informação. P1.2 Verificar se há política de classificação da informação. P1.2.1 Verificar se a política de classificação da informação abrange a categorização de dados pessoais. P1.2.2 Verificar se a política de classificação da informação contempla diretrizes quanto à identificação de dados pessoais sensíveis. P1.2.3 Verificar se a política de classificação da informação contempla diretrizes quanto à identificação de dados de crianças e adolescentes. P1.3 Verificar se há política de proteção de dados pessoais. P1.4 Verificar se há encarregado pelo tratamento de dados pessoais (DPO) e se as informações se encontram devidamente	A1. Poucas organizações possuem políticas que buscam assegurar a proteção de dados pessoais. A2. As políticas de classificação da informação das organizações não abrangem, ou abrangem de maneira insuficiente, a classificação de dados pessoais. A3. As organizações não possuem políticas de proteção de dados pessoais.

	tratamento de dados. IR5. Programa de governança em privacidade de dados. IR6. Dados de identificação do encarregado (DPO). IR7. Iniciativas conduzidas pela organização para conscientização e capacitação de servidores em proteção de dados pessoais. IR8. Partes interessadas relacionadas à proteção de dados pessoais. IR9. Dados pessoais tratados pela organização. IR10. Processos organizacionais que realizam o tratamento de dados pessoais. IR11. Ativos da organização que hospedam dados	FI6. Inventário de normativos relacionados à proteção de dados pessoais que devem ser respeitados pela organização. (IR5) FI7. Ato(s) de nomeação do DPO. (IR6) FI8. Plano de capacitação. (IR7) FI9. Certificados de capacitação dos servidores. (IR7) FI10. Relação de partes interessadas. (IR8) FI11. Inventário(s) de dados pessoais. (IR9) FI12. Fluxogramas. (IR10) FI13. Banco de dados de gestão de configuração. (IR11)		publicadas.	
			Preparação P2. Verificar se as organizações conduziram iniciativas para providenciar a adequação à LGPD. LGPD, arts. 23 e 50, § 2º, inciso I. ABNT NBR ISO/IEC 27701:2019, item 5.2.4.	P2.1 Verificar se as organizações instituíram grupo de trabalho para providenciar a adequação à LGPD. P2.2 Verificar se as organizações instituíram projeto, plano de ação ou iniciativa similar para providenciar a adequação à LGPD. P2.3 Verificar se as organizações publicaram normativos que tratam dos aspectos mais importantes relacionados à proteção de dados e à privacidade. P2.4 Verificar se as organizações mapearam seus processos de tratamento de dados e instituíram programa de governança em privacidade de dados.	A4. Poucas organizações conduziram iniciativas suficientes para adequação à LGPD. A5. Poucas organizações instituíram política (ou documento similar) que considera os princípios e aspectos gerais relacionados ao tratamento de dados. A6. Poucas organizações têm processos de tratamento de dados mapeados. A7. Poucas organizações possuem programa de governança em privacidade de dados.
			Contexto organizacional P3. Verificar se foram identificados outros normativos que abrangem comandos que remetam à proteção de dados pessoais e que também devem ser seguidos pelas organizações. ABNT NBR ISO/IEC 27701:2019, item 5.2.1.	P3.1 Verificar se as organizações identificaram, além da LGPD, outras leis, regulamentos e instruções normativas que abrangem comandos relacionados à proteção de dados pessoais e que também devem ser respeitados. P3.2 Verificar se os riscos relacionados ao processo de tratamento de dados foram identificados.	A8. Poucas organizações consideraram, nas suas iniciativas de adequação, além da LGPD, outros normativos que abrangem a proteção de dados pessoais. A9. As organizações não mantêm relação adequada com os operadores e os controladores conjuntos.
			Liderança P4. Verificar se as organizações indicaram o	P4.1 Verificar se o encarregado foi nomeado. P4.1.1 Verificar se as organizações	A10. Poucas organizações nomearam o encarregado. A11. Poucas organizações deram

	pessoais.		encarregado para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD. LGPD, art. 41. IN SGD/ME 117/2020. ABNT NBR ISO/IEC 27701:2019, item 5.3.3.	definiram as responsabilidades e as competências do encarregado. P4.1.2 Verificar se foi publicizada a nomeação do encarregado (*e.g.*: DOU, portaria e portal). P4.1.3 Verificar a qual setor pertence o encarregado. P4.1.4 Verificar se foi disponibilizado canal (e-mail, telefone etc.) para que agentes externos e internos se comuniquem com o encarregado.	publicidade à identificação e às informações de contato do encarregado.
			Capacitação P5. Verificar se as organizações possuem iniciativas para conscientização e capacitação dos colaboradores em proteção de dados pessoais. LGPD, art. 50. ABNT NBR ISO/IEC 27701:2019, itens 5.5.2, 5.5.3 e 5.5.4.	P5.1 Verificar se as organizações possuem planos de conscientização e de capacitação dos colaboradores. P5.1.1 Verificar se foram considerados diferentes níveis de capacitação, de acordo com o envolvimento do colaborador na temática de proteção de dados pessoais. P5.2 Verificar se os colaboradores envolvidos diretamente em atividades que realizam tratamento de dados pessoais receberam treinamento relacionado à proteção de dados pessoais.	A12. Poucas organizações elaboraram planos de conscientização e de capacitação dos colaboradores. A13. Poucos colaboradores foram capacitados no tema proteção de dados e privacidade. A14. A maioria das iniciativas de capacitação em proteção de dados pessoais não consideram os diferentes níveis de envolvimento dos colaboradores no tema.
			Contexto organizacional P6. Verificar se as organizações identificaram as principais partes interessadas relacionadas à proteção de dados pessoais. LGPD, art. 5º, incisos V, VI e VII, e arts. 26 e 39.	P6.1 Verificar se as organizações identificaram as partes interessadas relacionadas à proteção de dados pessoais. P6.1.1 Verificar se foram identificados os operadores. P6.1.2 Verificar se foram identificadas as categorias de titulares de dados pessoais. P6.1.3 Verificar se foi(foram)	A15. Poucas organizações identificaram as principais partes interessadas relacionadas à proteção de dados pessoais (categorias de titulares de dados pessoais, operadores e controladores conjuntos de dados pessoais). A16. Poucas organizações

			ABNT NBR ISO/IEC 27701:2019, itens 5.2.2, 7.2.6 e 7.2.7.	identificado(s), quando for o caso, controlador(es) conjunto(s).	identificaram os locais de armazenamento dos dados pessoais tratados.
			Contexto organizacional P7. Verificar se foram identificados os dados pessoais que são tratados pelas organizações, bem como os processos que realizam esses tratamentos. LGPD, arts. 11-14 e 37. ABNT NBR ISO/IEC 27701:2019, item 7.2.8.	P7.1 Verificar se foram identificados os processos de negócio que realizam tratamento de dados pessoais. P7.1.1 Verificar se foram identificados os responsáveis pelos processos que realizam tratamento de dados pessoais. P7.2 Verificar se foram identificados os dados pessoais que são tratados pela organização. P7.2.1 Verificar se foram identificados os locais onde os dados pessoais são armazenados (ativos ou nuvem). P7.3 Verificar se foram identificados os riscos associados ao processo de tratamento de dados.	A17. Poucas organizações identificaram os dados pessoais que tratam. A18. Poucas organizações identificaram os processos organizacionais que realizam tratamento de dados pessoais. A19. Poucas organizações identificaram os responsáveis pelos processos organizacionais que realizam tratamento de dados pessoais. A20. Poucas organizações identificaram os ativos nos quais os dados pessoais são armazenados. A21. Poucas organizações identificaram os dados pessoais sensíveis ou de crianças e adolescentes que tratam. A22. Poucas organizações identificaram os riscos relacionados ao processo de tratamento de dados pessoais.
Conformidade do tratamento, Direitos do titular, Compartilha-mento de	IR1. Finalidade dos processos organizacionais que tratam dados pessoais. IR2 Quantitativo	FI1. Respostas dos gestores ao questionário. (IR1, IR2, IR3, IR4, IR5, IR6, IR7, IR8, IR9, IR10, IR11, IR12, IR13)	**Conformidade do tratamento** P1. Verificar se o tratamento de dados pessoais está em conformidade com a	P1.1. Verificar se os processos que realizam tratamento de dados pessoais estão em conformidade com os princípios da finalidade e da necessidade (minimização e tempo de retenção) estabelecidos na LGPD.	A23. Poucas organizações analisaram a conformidade dos seus processos de tratamento de dados pessoais. A24. As organizações analisaram, de maneira

dados pessoais, Violação de dados pessoais e Medidas de proteção Q2. As organizações implementaram medidas e controles de proteção de dados pessoais para adequação à LGPD?	de dados pessoais coletados para a realização dos tratamentos. IR3. Tempo no qual os dados pessoais são armazenados pela organização. IR4. Bases legais que justificam os tratamentos de dados pessoais da organização. IR5. Acordos firmados com operadores para garantir o cumprimento da LGPD. IR6. Responsabilidades dos controladores conjuntos, caso existam. IR7. Entidades com as quais a organização compartilha dados pessoais. IR8. Diretrizes da organização, direcionadas para os titulares de	FI2. Inventário(s) de dados pessoais. (IR1, IR2, IR3, IR4) FI3. Fluxogramas. (IR1, IR2, IR9, IR10, IR13) FI4. Registro de atividades de tratamento de dados pessoais. (IR1, IR2, IR3, IR4) FI5. Ajustes e contratos firmados com operadores. (IR5, IR7) FI6. Ajustes e contratos firmados com controladores conjuntos. (IR6, IR7) FI7. Política de privacidade. (IR8, IR9) FI8. Sistema de Gestão de Requisições. (IR9) FI9. Fluxogramas. (IR9, IR10) FI10. Sistema de Gestão de Incidentes. (IR9, IR10) FI11. Política e	LGPD. LGPD, arts. 6º-7º, art. 9º, inciso II, e arts. 37 e 40. ABNT NBR ISO/IEC 27701:2019, itens 7.2.1, 7.2.2, 7.2.8, 7.4.4, 7.4.5 e 7.4.7.	P1.2. Verificar se há base legal definida que justifique os tratamentos de dados pessoais. P1.3 Verificar se existe(m) inventário(s) de dados pessoais que consolida(m) os registros de atividades de tratamento de dados pessoais. P1.4 Verificar se existe(m) Relatório(s) de Impacto à Proteção de Dados Pessoais (RIPD). P1.5 Verificar se já foram implementados controles para mitigar os riscos identificados na elaboração de RIPD.	insuficiente, a conformidade dos seus processos de tratamento de dados pessoais. A25. Poucas organizações possuem inventário(s) de dados pessoais. A26. Poucas organizações elaboraram RIPD. A27. Poucas organizações implementaram controles para mitigar os riscos identificados na elaboração de RIPD.
			Compartilhamento de dados pessoais P2. Verificar se as organizações identificaram os casos de transferência, compartilhamento ou tratamento conjunto de dados pessoais e se os acordos ou contratos firmados estão com papéis e responsabilidades definidos. LGPD, arts. 33-36 e arts. 42-50. ABNT NBR ISO/IEC 27701:2019, itens 7.2.6 e 7.5.	P2.1 Verificar se houve adequação de contratos ou ajustes firmados com os operadores. P2.2 Verificar se foi avaliada a adequação dos operadores à LGPD. P2.3 Nos casos em que há controladores conjuntos, verificar se os papéis e responsabilidades de cada um foram estabelecidos de forma transparente. P2.4 Verificar se há transferência(s) internacional(is) de dados pessoais. P2.4.1 No caso de transferência internacional de dados pessoais, verificar se foram observados os critérios estabelecidos na LGPD.	A28. Poucos contratos ou ajustes firmados com os operadores ou controladores conjuntos foram atualizados para abranger cláusulas que buscam garantir o tratamento de dados pessoais em conformidade com a LGDP. A29. As transferências internacionais de dados pessoais não estão em conformidade com a LGPD.
			Direitos do titular P3. Verificar se as	P3.1 Verificar se há política de privacidade.	A30. Poucas organizações publicaram a política de

	dados, para o tratamento de dados pessoais. IR9. Processos definidos pela organização para atendimento dos direitos dos titulares. IR10. Mecanismos das organizações utilizados para o tratamento de violações de dados pessoais. IR11. Medidas de segurança, técnicas e administrativas, adotadas pela organização para proteger os dados pessoais. IR12. Análises de impacto de proteção de dados pessoais. IR13. Diretrizes organizacionais para garantir o *privacy by design* e o *privacy by default*.	Planos de Gestão de Riscos. (IR10, IR11, IR12, IR13) FI12. Relatório(s) de Impacto de Proteção de Dados (RIPD). (IR10, IR11, IR12, IR13)	organizações dispõem de mecanismos para informar e dar atendimento aos direitos dos titulares de dados. LGPD, arts. 9º e 17-22, art. 50, inciso I, alíneas "a", "d" e "e". ABNT NBR ISO/IEC 27701:2019, itens 7.3.1-7.3.10.	P3.1.1 Verificar se a política de privacidade está publicada em local de fácil acesso. P3.2 Verificar se há meios para requisição e atendimento dos direitos dos titulares de dados pessoais. P3.2.1 Verificar se foram estipulados prazos para atendimento de cada um dos direitos dos titulares.	privacidade. A31. Poucas organizações possuem mecanismos para atendimento dos direitos dos titulares.
			Violação de dados pessoais P4. Verificar se as organizações possuem mecanismos para o tratamento de violações de dados pessoais. LGPD, arts. 48 e 50, § 2º, inciso I, alínea "g". ABNT NBR ISO/IEC 27701:2019, itens 6.13.1.1 e 6.13.1.15.	P4.1 Verificar se há meios para registro (inclusive pelos próprios titulares) e para resposta a incidentes de segurança da informação que envolvem violação de dados pessoais. P4.2 Verificar se há procedimento definido para notificar os titulares e a ANPD quando houver a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.	A32. Poucas organizações possuem processos definidos para tratamento de violações de dados pessoais. A33. Poucas organizações possuem processos definidos para notificação dos interessados no caso de violação de dados pessoais.
			Medidas de proteção P5. Verificar se as organizações adotam medidas para tratamento de riscos relacionados à proteção de dados pessoais. LGPD, art. 5º, inciso XVII, art. 10, § 3º, e arts. 32, 38 e 46.	P5.1 Verificar se as organizações adotam medidas de segurança, técnicas (soluções de segurança, controle de acesso) e administrativas (medidas organizacionais), para 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. P5.1.1 Verificar se existe um processo	A34. Poucas organizações adotam medidas suficientes de segurança, técnicas e administrativas, para proteger os dados pessoais. A35. Poucas organizações gerenciam e tratam os riscos associados ao tratamento de dados pessoais.

			ABNT NBR ISO/IEC 27701:2019, itens 6.2.2.1, 6.2.2.2, 6.9.4.1, 6.7, 7.2.5 e 7.4.	formal de registro, cancelamento e provisionamento de acesso de usuários a sistemas que realizam tratamento de dados pessoais. P5.1.2 Verificar se há rastreabilidade (*logs*) dos tratamentos de dados efetuados. P5.1.3 Verificar se é utilizada criptografia para proteger os dados pessoais, em especial os dados pessoais sensíveis. P5.2 Verificar se as organizações tomaram providências para que processos e sistemas sejam projetados (desde a concepção) de forma que a coleta e o tratamento de dados pessoais estejam limitados ao que é estritamente necessário para o propósito identificado (*Privacy by design* e *Privacy by default*).	A36. Poucas organizações adotaram providências para que os tratamentos de dados pessoais ocorram "*by design* e *by default"*.

Apêndice C – Respostas aos questionamentos da Matriz de Planejamento

1. Neste apêndice, o objetivo é verificar se, em razão da aplicação dos procedimentos detalhados na Matriz de Planejamento e das análises realizadas ao longo deste relatório, foi possível responder adequadamente as questões de auditoria propostas.

QST-1: As organizações se estruturaram para a condução de iniciativas de adequação à LGPD?

2. A resposta à QST-1 envolve, em essência, um resumo das informações prestadas pelas 387 organizações federais auditadas em resposta às perguntas das primeiras quatro dimensões do questionário ("Preparação", "Contexto Organizacional", "Liderança" e "Capacitação" – Seções 2.1.1 a 2.1.4 deste relatório).

3. Dessa análise, percebe-se que, dessas 387 organizações, quase um terço (109, ou 28,16%) ainda não concluíram qualquer medida preparatória para se adequarem à LGPD, muitas ainda não realizaram medidas básicas relacionadas ao contexto organizacional (*e.g.* verificar se há tratamento de dados envolvendo controlador conjunto [248, ou 64,08%], avaliar os riscos relativos aos seus processos de tratamento de dados pessoais [228, ou 58,92%]), quase 70% (270) ainda não têm uma política que englobe a classificação de dados pessoais e quase dois terços (244, ou 63,05%) não possuem plano de capacitação ou não incluíram nesse plano a necessidade de treinamentos especificamente direcionados à proteção de dados pessoais (achados 4.1 a 4.5).

4. De modo geral, não se pode dizer que os órgãos/entidades federais tenham se estruturado adequadamente para conduzirem iniciativas de adequação à LGPD, havendo, ainda, muito a ser feito, mesmo em questões relativamente básicas. Os subindicadores médios das 387 organizações auditadas relativos a essas quatro dimensões são: "Preparação" (iPrep) = 44%, "Contexto Organizacional" (iOrg) = 59%, "Liderança" (iLid) = 68% e "Capacitação" (iCap) = 40% (Figura 13).

QST-2: As organizações implementaram medidas e controles de proteção de dados pessoais para adequação à LGPD?

5. A seu turno, a resposta à QST-2 baseia-se nas respostas das 387 organizações federais auditadas às perguntas das demais cinco dimensões ("Conformidade do Tratamento", "Direitos do Titular", "Compartilhamento de Dados Pessoais", "Violação de Dados Pessoais" e "Medidas de Proteção" – Seções 2.1.5 a 2.1.9 deste relatório).

6. Das 387 organizações públicas federais, quanto a aspectos de conformidade, tem-se que quase 70% (270) disseram não manter registro adequado das suas operações de tratamento de dados e 72,35% (280) afirmaram que nunca elaboraram um RIPD. Muitos dos direitos dos titulares também não são atendidos, sendo que 146 organizações (37,73%) não possuem política de privacidade e noventa (23,26%) sinalizaram que não atendem os direitos previstos nos arts. 9º e 18 da LGPD. Quase metade dessas organizações (184, ou 47,55%) não avaliaram se compartilham dados pessoais com terceiros ou ainda não identificaram os dados compartilhados. Menos de um décimo das organizações (36) avaliaram riscos em relação aos tratamentos de dados realizados na nuvem (achados 4.6 e 4.7).

7. No que se refere aos incidentes de segurança envolvendo violação de dados pessoais, apenas 127 órgãos/entidades (32,82%) possuem planos de resposta e só 132 (34,11%) registram em sistema próprio as ações adotadas para tratar/responder a esses incidentes (Tabela 13). A adoção de medidas de proteção também é insuficiente: somente 100 organizações (25,84%) criptografam os dados armazenados, apenas 81 (20,93%) normatizaram a obrigatoriedade de mascarar/tarjar dados pessoais em documentos e só 125 (32,3%) disponibilizam ferramentas para isso (Tabela 14).

8. Ou seja, de igual modo não se pode afirmar que as organizações federais implementaram medidas e controles suficientes para se adequarem à LGPD. Os subindicadores médios dos 387 entes relativos a essas cinco dimensões são: "Conformidade do Tratamento" (iConf) = 37%, "Direitos do

Titular" (iDir) = 62%, "Compartilhamento de Dados Pessoais" (iComp) = 22%, "Violação de Dados Pessoais" (iResp) = 38% e "Medidas de Proteção" (iProt) = 34%.

Conclusão

9. Apesar de ter havido evolução em relação ao cenário verificado em auditoria anterior (Seção 2.4 deste relatório), quase metade dessas organizações (173, ou 44,7%) ainda se encontram nos níveis/faixas "Inexpressivo" (52, ou 13,44%) ou "Iniciando" (121, ou 31,27%) de adequação à LGPD (Figura 13).

10. Ou seja, é preciso que tanto o TCU quanto alguns OGSs (CNJ, CNMP, SGD/MGI, Sest/MGI e ANPD) permaneçam induzindo melhorias nos órgãos/entidades públicos federais e acompanhando as respectivas evoluções ao longo dos próximos anos.

Apêndice D – Questionário da auditoria

Auditoria para avaliar a adequação das organizações públicas à LGPD

A Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), que entrou em vigor em agosto de 2020, dispõe sobre o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica de direito público ou privado. Um ano após o início de sua vigência, o Tribunal de Contas da União (TCU) constatou que 76,7% das organizações públicas federais ainda permaneciam nos graus inexpressivo ou inicial de adequação à LGPD (TC 039.606/2020-1; Acórdão 1.384/2022-TCU-Plenário, relator Ministro Augusto Nardes).

Com isso, o presente momento mostra-se oportuno para a realização de nova ação de controle, com vistas a verificar a evolução do cumprimento da legislação por parte dos órgãos e entidades da Administração Pública. De acordo com previsão incluída na Ação 29 do Plano Anual de Trabalho (PAT) 2024 da Rede Integrar, essa nova auditoria será realizada em parceria com os Tribunais de Contas Estaduais (TCEs) que aderiram à ação, de modo a ampliar o escopo da avaliação para incluir, além das organizações federais, também um conjunto de organizações públicas estaduais e municipais. No total, tribunais de oito estados da federação aderiram à fiscalização (TCE-AM, TCE-BA, TCE-CE, TCE-PA, TCE-PE, TCE-PR, TCE-RJ e TCE-RN).

O método utilizado é denominado autoavaliação de controles internos (do inglês *Control Self-Assessment* – CSA), no qual disponibiliza-se um questionário para que os gestores preencham as respostas que melhor reflitam a situação atual das respectivas organizações com relação à implementação de controles e medidas para assegurar a conformidade com a LGPD, anexando-se as evidências correspondentes. Cada organização federal, estadual e municipal fiscalizada deverá designar uma pessoa para responder as perguntas a seguir em nome da instituição, realizando o respectivo envio (clique no botão "Enviar" disponível na última página do questionário) até às 23h59 do dia 19/7/2024 (sexta-feira).

Espera-se que esta fiscalização sirva para conscientizar e orientar gestores e unidades de auditoria interna de diferentes níveis federativos na condução de iniciativas para que seus órgãos e entidades se adequem à legislação e, também, possam continuar se autoavaliando ao longo dos próximos anos. A partir dos resultados levantados junto às organizações fiscalizadas, planeja-se, também, construir um painel nacional de implementação da LGPD.

Este código de acesso (*token*: {TOKEN:TOKEN}) corresponde às respostas da organização **{TOKEN:LASTNAME}**.

Observações importantes:

1) Todos os textos do questionário foram previamente validados com o intuito de minimizar dúvidas de interpretação em relação às perguntas e às opções de resposta correspondentes. Aconselha-se que o questionário seja preenchido o quanto antes, idealmente logo nos primeiros dias do prazo disponível (a partir de 24/6/2024), frisando-se que eventuais solicitações de esclarecimentos (a serem encaminhadas para o e-mail **auditoria.lgpd@tcu.gov.br**) podem não ser respondidas a tempo e que isso não justifica o não preenchimento completo e envio do questionário **até às 23h59 do dia 19/7/2024 (sexta-feira)**.

2) O questionário não contempla todas as medidas e controles possíveis de serem implementados para a adequação das organizações à LGPD, podendo, ainda, abranger questões e opções de resposta que tratam de medidas e controles que podem não ser aplicáveis a algumas organizações, por diversas razões (*e.g.* contexto específico, porte, objetivos institucionais, características particulares da instituição).

3) A partir deste questionário, esta Corte de Contas pretende diagnosticar a maturidade das organizações em relação aos critérios questionados, ciente de que uma maturidade maior implica em custos mais elevados e que, portanto, a definição do grau de maturidade mais adequado a cada organização é, essencialmente, uma decisão de gestão (tomada com base no tipo de negócio, apetite a riscos, custo e expectativa de retorno da implementação de controles internos específicos etc.), a qual deve estar amparada por análises devidamente fundamentadas.

4) As questões tiveram como referência a própria legislação (sobretudo a Lei 13.709/2018), normas e códigos de boas práticas, em especial a norma ABNT NBR ISO/IEC 27701:2019 ("Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e diretrizes").

5) O questionário envolve a solicitação de informações e, em casos pontuais, solicita o envio/anexação de arquivos capazes de evidenciar as respostas fornecidas. Nas questões que permitem a marcação de uma única opção de resposta (TIPO A), as diferentes opções disponíveis refletem um aumento gradativo da maturidade da organização em relação às práticas e aos controles envolvidos. Para essas questões, o respondente deve decidir qual, dentre as opções disponíveis, melhor reflete a situação atual da sua organização. Nas questões que permitem a marcação de múltiplas opções de resposta (TIPO B), o respondente deve marcar todas as opções atendidas pela sua organização.

6) Nas questões do TIPO A, além de marcar a opção que melhor reflete a situação da sua organização em relação ao tópico questionado, o gestor **DEVE** complementar textualmente a sua resposta, no respectivo campo de comentário (que aceita texto aberto). Caso marque a opção "Não se aplica", o gestor deve justificar nesse campo o seu entendimento pela não aplicação daquela medida/controle à sua organização. Caso marque alguma das demais opções de resposta, o gestor deve

fornecer nesse campo detalhes que permitam compreender melhor a escolha por aquela opção, considerando o contexto específico da sua organização. Por exemplo, o gestor deve utilizar esse campo para descrever, quando aplicável, datas, períodos, responsáveis, projetos e iniciativas, bem como referenciar artefatos, evidências, atas e outros documentos internos, indicando os respectivos nomes, datas e números de identificação, se houver. A qualquer momento, inclusive após encerrado o prazo para o preenchimento do questionário, os auditores poderão requisitar informações adicionais, bem como o envio desses elementos (artefatos, evidências, atas, documentos) eventualmente mencionados pelo gestor.

7) O respondente pode navegar à vontade entre os grupos de questões por meio dos botões "Próximo" e "Anterior" localizados no rodapé das páginas. O botão "Próximo", no entanto, só permitirá o avanço se as perguntas obrigatórias do grupo/página (marcadas com um asterisco vermelho) estiverem preenchidas. No ponto onde estiver, o respondente também pode clicar em "Retomar mais tarde" para salvar as respostas marcadas até então e voltar a preencher o questionário em outro momento. Após clicar em "Próximo" no último grupo de questões, haverá uma última tela com o intuito de fornecer ao respondente mais uma oportunidade de voltar e revisar todas as respostas fornecidas no questionário.

8) Para eventuais consultas, uma cópia completa deste questionário (em PDF), bem como outras informações relacionadas, estão disponíveis na página da fiscalização, hospedada no portal do TCU (https://portal.tcu.gov.br/fiscalizacao-de-tecnologia-da-informacao/atuacao/fiscalizacoes/auditoria-sobre-lgpd). Recomenda-se, também, imprimir esta página, tendo em vista que estas orientações poderão ser úteis ao longo do preenchimento de todo o questionário.

9) Esta Corte de Contas comunica que, assim como ocorreu na fiscalização anterior (Acórdão 1.384/2022-TCU-Plenário, item 9.10), à exceção das informações pessoais dos gestores respondentes e dos textos fornecidos nos campos de comentário, os dados das respostas individuais das organizações ao questionário da auditoria serão classificados como públicos, à luz do art. 3º, inciso I, da Lei 12.527/2011 (Lei de Acesso à Informação – LAI; https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm).

10) Incluindo a identificação do respondente (Q1.1), este questionário contém, no total, 22 questões, sendo que algumas só abrem de forma condicionada a respostas anteriores e algumas destinam-se apenas à anexação de documentos. Para esses casos, é aceito o *upload* de um único arquivo, em formato PDF (se o arquivo original estiver em outro formato, será necessário imprimi-lo em PDF), com tamanho máximo de 20MB.

11) Este questionário foi avaliado pela Autoridade Nacional de Proteção de Dados (ANPD).

1. Identificação do respondente

De acordo com o ofício de comunicação de fiscalização enviado previamente, a organização deve indicar um servidor responsável pela resposta ao questionário.

1.1 Dados do servidor responsável pela resposta ao questionário:

[Help: Os dados pessoais solicitados se limitam ao que é estritamente necessário para que a equipe de auditoria possa entrar em contato com o respondente, caso haja necessidade.]

Nome completo:

E-mail:

Telefone (com DDD):

Cargo/Função:

Lotação:

2. Preparação

Antes de iniciar o processo de adequação à LGPD, a organização deve adotar medidas e realizar ações no sentido de construir um ambiente propício para o sucesso dessa empreitada.

A questão desta seção, então, aborda aspectos relacionados à identificação, ao planejamento e à concretização dessas medidas preparatórias.

Um exemplo de medida preparatória pode ser a instituição de um comitê ou de um grupo de trabalho para tratar do tema. Ademais, mesmo antes de formalizar qualquer normativo interno especificamente relacionado à proteção e à privacidade de dados, a organização pode produzir determinados artefatos iniciais, tais como estudos, planos de ação, atas de reuniões, trocas de e-mails com propostas a respeito etc.

É importante que, desde o início, essas iniciativas contem com o apoio e, idealmente, até mesmo com a participação direta da alta direção da organização. Ademais, convém que sejam envolvidas pessoas da organização pertencentes a unidades que exercem atividades relevantes para o tratamento de dados pessoais (*e.g.* Segurança da Informação, Tecnologia da Informação, Direito, Auditoria/Conformidade, Ouvidoria).

Em um primeiro estágio de maturidade, a organização terá apenas documentado informações relacionadas aos objetivos dessas iniciativas de adequação e às ações necessárias para alcançá-los, possivelmente especificando os recursos necessários, os responsáveis e os prazos previstos.

Avançando, em um estágio intermediário, a organização já terá normatizado as principais questões relacionadas ao tema tratamento de dados (*e.g.* política de proteção de dados pessoais, plano de capacitação associado, política de privacidade), levando em consideração os princípios gerais ou todos os elementos elencados na LGPD.

Por fim, no nível mais maduro em relação ao tema, a organização possuirá programa de governança em privacidade de dados implementado, amplamente divulgado a todas as partes interessadas e sendo periodicamente avaliado e revisado, com vistas à melhoria contínua.

Referências úteis:

- Lei 13.709/2018, art. 50, em especial § 2º, inciso I (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm);

- ABNT NBR ISO/IEC 27701:2019, item 5.4 (Planejamento).

2.1 (TIPO A) A organização conduziu iniciativas para identificar, planejar e executar medidas preparatórias com vistas a se adequar à LGPD?

[Help: **Questão TIPO A:**

Esta questão permite a marcação de uma única opção de resposta, sendo que as diferentes opções disponíveis refletem um aumento gradativo da maturidade da organização em relação às práticas e aos controles envolvidos. No caso, o respondente deve assinalar qual, dentre as opções disponíveis, melhor reflete a situação atual da sua organização.

Além de marcar a opção que melhor reflete a situação da sua organização em relação ao tópico questionado, o gestor **DEVE** complementar textualmente a sua resposta, no respectivo campo de comentário (que aceita texto aberto). Caso marque a opção "Não se aplica", o gestor deve justificar nesse campo o seu entendimento pela não aplicação daquela medida/controle à sua organização. Caso marque alguma das demais opções de resposta, o gestor deve fornecer nesse campo detalhes que permitam compreender melhor a escolha por aquela opção, considerando o contexto específico da sua organização. Por exemplo, o gestor deve utilizar esse campo para descrever, quando aplicável, datas, períodos, responsáveis, projetos e iniciativas, bem como referenciar artefatos, evidências, atas e outros documentos internos, indicando os respectivos nomes, datas e números de identificação, se houver. A qualquer momento, inclusive após encerrado o prazo para o preenchimento do questionário, os auditores poderão requisitar informações adicionais, bem como o envio desses elementos (artefatos, evidências, atas, documentos) eventualmente mencionados pelo gestor.]

Favor escolher apenas uma das opções a seguir:

- Não se aplica (justificar no campo de comentário);
- Não (a organização não realizou medidas preparatórias com vistas a se adequar à LGPD);
- A organização iniciou, mas ainda não concluiu iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD;
- A organização concluiu iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD (possui plano de ação, plano de projeto ou documento similar para direcionar os esforços nesse sentido), porém ainda não formalizou normativo interno relacionado à proteção e à privacidade de dados;
- A organização concluiu iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD e já publicou uma política (ou documento similar) que considera os princípios e aspectos gerais relacionados ao tratamento de dados;
- A organização já mapeou seus principais processos de tratamento de dados (natureza, escopo, finalidade, benefícios, probabilidade e gravidade dos riscos associados) e publicou normativos internos que tratam dos aspectos mais importantes relacionados à proteção e à privacidade de dados, porém ainda não possui um programa de governança em privacidade de dados implementado;
- A organização já mapeou todos os processos de tratamento de dados (natureza, escopo, finalidade, benefícios, probabilidade e gravidade dos riscos associados), publicou normativos internos que tratam dos temas proteção e privacidade de dados de forma abrangente e possui programa de governança em privacidade de dados implementado, periodicamente monitorado/avaliado e atualizado continuamente.

3. Contexto organizacional

Para alcançar os resultados pretendidos pelas iniciativas de adequação à LGPD, a organização deve avaliar uma série de fatores internos e externos relevantes para atingir os objetivos associados.

A questão desta seção, então, aborda aspectos relacionados ao mapeamento dos normativos correlatos à proteção de dados pessoais que devem ser respeitados pela organização, à identificação das partes interessadas e às análises dos diferentes tipos de dados pessoais tratados pela organização e dos processos organizacionais que realizam o tratamento desses dados. (Obs.: por dado pessoal, entende-se qualquer informação relacionada à pessoa natural identificada ou identificável [*e.g.* nome, RG, CPF, telefone, e-mail]; por tratamento de dados, entende-se qualquer operação [*e.g.* coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão, extração] realizada com dados pessoais).

Por exemplo, o Decreto-Lei 5.452/1943 (Consolidação das Leis do Trabalho – CLT) e as Leis 8.078/1990 (Código de Defesa do Consumidor – CDC), 12.414/2011 (Cadastro Positivo), 12.527/2011 (Lei de Acesso à Informação – LAI) e 13.787/2018 (digitalização e utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuários de pacientes) contém diversos dispositivos que, eventualmente, podem se aplicar à organização.

Além dessas leis, também podem existir normas infralegais, regulamentos, portarias, instruções normativas, decisões judiciais/administrativas e requisitos contratuais que tragam comandos relacionados à proteção de dados pessoais e que também devem ser respeitados pela organização.

Convém, ainda, que a organização identifique todas as partes que possuem interesses ou responsabilidades associadas ao tratamento de dados pessoais, tais como os titulares de dados pessoais, os controladores conjuntos e os operadores. O titular é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (*e.g.* cidadão, cliente, servidor público, representante de fornecedor, terceirizado). O controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (controlador conjunto é aquele que determina os propósitos e as formas do tratamento de dados pessoais junto com outro controlador). A seu turno, o operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Considerando que o controlador é obrigado a reparar danos causados em razão da atividade de tratamento de dados pessoais (LGPD, art. 42), a organização deve ter contrato firmado com os agentes contratados que realizam tratamento de dados em seu nome (operadores), bem como com os controladores conjuntos, contendo cláusulas com vistas a definir papéis e responsabilidades e a assegurar que estes adotem medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais compartilhados com eles.

Ademais, tanto o controlador quanto o operador devem manter registro das operações de tratamento de dados pessoais realizadas (LGPD, art. 37), sendo que a ANPD poderá determinar ao controlador que elabore Relatório de Impacto à Proteção de Dados Pessoais (RIPD) com descrição, dentre outros elementos, dos dados coletados e das metodologias de coleta e de garantia da segurança das informações (art. 38).

A organização deve, ainda, estabelecer políticas e salvaguardas adequadas, com base em avaliações sistemáticas dos impactos e dos riscos à privacidade, relativamente aos dados pessoais tratados, com vistas a mitigar possíveis probabilidades e impactos da ocorrência de situações indesejadas (art. 50, § 2º, inciso I, alínea “d”). Esses riscos devem ser avaliados sob o prisma das diversas operações realizadas com os dados (*e.g.* coleta, produção, acesso, transmissão, armazenamento, eliminação). Inclusive, tais avaliações devem nortear a organização quanto a eventual necessidade de priorizar as iniciativas de adequação à LGPD em relação a processos de negócio específicos, de mais alto risco.

Referências úteis:

- Lei 13.709/2018, art. 5º, em especial incisos I, V, VI, VII e X, art. 7º, § 5º, e arts. 37, 39, 42-46 e 50, § 1º e § 2º, inciso I, alínea “d” (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm);

- ABNT NBR ISO/IEC 27701:2019, itens 5.2.1 (Entendendo a organização e seu contexto), 5.2.2 (Entendendo as necessidades e as expectativas das partes interessadas), 5.4.1.2 (Avaliação de riscos de segurança da informação), 6.5.1 (Responsabilidade pelos ativos), 6.5.2 (Classificação da informação), 7.2.6 (Contratos com operadores de dados pessoais), 7.2.7 (Controlador conjunto de dados pessoais) e 7.2.8 (Registros relativos ao tratamento de dados pessoais).

3.1 (TIPO B) A organização conduziu iniciativa com vistas a IDENTIFICAR:

[Help: **Questão TIPO B:**

Esta questão permite a marcação de múltiplas opções de resposta. No caso, o respondente deve marcar todas as opções que contém iniciativas que já foram realizadas pela sua organização.]

Por favor, escolha as opções que se aplicam:

- OUTROS NORMATIVOS (*e.g.* leis, regulamentos, portarias, instruções normativas, decisões judiciais/administrativas, requisitos contratuais), além da LGPD, que abrangem comandos relacionados à proteção de dados pessoais, os quais a organização deve respeitar;
- AS DIFERENTES CATEGORIAS DE TITULARES de dados pessoais com os quais se relaciona (*e.g.* cidadão, cliente, servidor público, representante de fornecedor, terceirizado);
- OS OPERADORES que realizam tratamento de dados pessoais em seu nome;
- Se há tratamento de dados que envolva CONTROLADOR CONJUNTO;
- E ADEQUAR OS INSTRUMENTOS CONTRATUAIS (*e.g.* contrato, convênio, acordo de cooperação) firmados com os operadores e os controladores conjuntos identificados, de forma a estabelecer suas respectivas responsabilidades e papéis com relação à proteção de dados pessoais;
- OS PROCESSOS DE NEGÓCIO que realizam tratamento de dados pessoais e os respectivos RESPONSÁVEIS (*e.g.* pessoas, departamentos, operadores, controladores conjuntos);
- OS DADOS PESSOAIS TRATADOS pela organização;
- OS LOCAIS DE ARMAZENAMENTO dos dados pessoais tratados pela organização (*e.g.* servidor de arquivos, nuvem, dispositivo USB, *storage*, fita de *backup*, arquivos físicos [pastas, armários]);
- E AVALIAR OS RISCOS associados aos processos de tratamento de dados pessoais que foram identificados;
- A organização AINDA NÃO CONDUZIU INICIATIVA com vistas a identificar qualquer dos objetos mencionados nos itens anteriores.

4. Liderança

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

Nesse sentido, a elaboração e a ampla divulgação de políticas relacionadas à proteção de dados pessoais, bem como a nomeação de um encarregado pelo tratamento de dados pessoais (normalmente chamado de DPO, do inglês *Data Protection Officer*), são ações fundamentais para o processo de adequação à LGPD. O encarregado nomeado deve ter independência (não ser gestor responsável por sistema de informação e não fazer parte de setor/departamento que possa gerar conflito de interesses quanto à sua atuação, a exemplo das unidades de TI [IN SGD/ME 117/2020, art. 1º, § 1º, inciso II]) e autonomia suficientes para reportar à alta administração, servindo como canal de comunicação efetivo entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Deve, ainda, além de profundo entendimento da própria LGPD (Lei 13.709/2018), possuir conhecimentos multidisciplinares relativos a uma série de temas correlatos (*e.g.* Direito, Governança Corporativa e de Dados, Gestão de Riscos, Tecnologia da Informação, Segurança da Informação, Privacidade e Proteção de Dados).

A questão desta seção, então, aborda aspectos atinentes à nomeação desse encarregado e à formalização de políticas (ou documentos similares) que busquem assegurar, no âmbito da organização, a segurança das informações e a proteção dos dados pessoais. A título de exemplo, citam-se:

- Política de Segurança da Informação (PSI): aprovada pela alta direção, estabelece a abordagem da organização para gerenciar os objetivos nessa área, em linha com os requisitos do negócio e com leis e regulamentações aplicáveis; é obrigatória para os órgãos e entidades da Administração Pública federal (Decreto 9.637/2018, art. 15, inciso II);

- Política de Classificação da Informação (PCI): fornece diretrizes para assegurar que as diferentes informações recebam níveis adequados de proteção, de acordo com a sua importância para a organização e os riscos associados; documento importante para direcionar a implementação de controles adequados para a proteção de dados pessoais;

- Política de Proteção de Dados Pessoais (PPDP): alinhada à PSI e à PCI, estabelece regras e diretrizes para o tratamento e para a governança de dados pessoais dentro da organização (público interno), reforçando seu compromisso para alcançar a conformidade com os normativos de proteção de dados pessoais [ver https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/modelo_ppdp.docx].

Em especial no que tange à classificação das informações, a LGPD demanda que sejam adotados cuidados específicos para o tratamento de dados pessoais sensíveis (que envolvem 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) e de dados pessoais de crianças e de adolescentes (Lei 13.709/2018, art. 5º, inciso II, e arts. 11-14).

Referências úteis:

- Lei 13.709/2018, em especial art. 5º, incisos I, II e VIII, arts. 11-14, art. 23, inciso III, e arts. 41, 46 e 50, § 2º, inciso I, alíneas "a" e "d" (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm);

- IN SGD/ME 117/2020 (Dispõe sobre a indicação do Encarregado pelo Tratamento dos Dados Pessoais na APF), em especial art. 1º, § 1º, incisos I e II, e art. 2º (https://www.in.gov.br/en/web/dou/-/instrucao-normativa-sgd/me-n-117-de-19-de-novembro-de-2020-289515596);

- ABNT NBR ISO/IEC 27701:2019, itens 5.3.2 (Política), 6.2 (Políticas de segurança da informação), 6.2.1 (Orientação da Direção para segurança da informação), 6.3.1 (Organização interna) e 6.5.2 (Classificação da informação), 6.5.2.2 (Rótulos e tratamento da informação);

- Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado (https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf).

4.1 (TIPO B) A organização:

[Help: **Questão TIPO B:**

Esta questão permite a marcação de múltiplas opções de resposta. No caso, o respondente deve marcar todas as opções que são atendidas pela sua organização.

Caso marque alguma das opções relativas às políticas, no campo de comentário associado especifique o documento interno e informe, se houver, o endereço da internet (URL) onde este está publicado. Por exemplo, no caso do TCU, a Política de Proteção de Dados Pessoais foi estabelecida por meio da Portaria-TCU 163/2023 (https://pesquisa.apps.tcu.gov.br/documento/norma/*/KEY%253ANORMA-23222/score%2520desc/0). Caso marque alguma das outras opções, nos campos de comentário associados informe os endereços da internet (URLs) onde podem ser verificadas a publicação da nomeação do encarregado em veículo de comunicação oficial e/ou as suas respectivas informações de contato.]

[no campo de comentário, informar o endereço da internet (URL) onde a política está publicada]

Por favor, escolha as opções que se aplicam:

- Instituiu formalmente e mantém atualizada POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (ou instrumento similar);
- Instituiu formalmente e mantém atualizada POLÍTICA DE CLASSIFICAÇÃO DA INFORMAÇÃO (ou instrumento similar), sendo que abordou nesse documento questões específicas relacionadas à classificação de dados pessoais, de dados pessoais sensíveis e de dados pessoais de crianças e de adolescentes;
- Instituiu formalmente e mantém atualizada POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS (ou instrumento similar);
- Nomeou o ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS (*Data Protection Officer* – DPO) e publicou essa nomeação em veículo de comunicação oficial (*e.g.* Diário Oficial da União – DOU);
- DIVULGA EM SEU SÍTIO ELETRÔNICO INSTITUCIONAL a identidade e as informações de contato (nome, e-mail, telefone) do encarregado pelo tratamento de dados pessoais, em local de fácil acesso aos titulares de dados pessoais;
- AINDA NÃO ATENDE NENHUM dos itens anteriores.

4.1.1 Anexe a Política de Proteção de Dados Pessoais (ou documento similar) da organização:

Só responder essa pergunta sob a seguinte condição:

A opção 'Instituiu formalmente e mantém atualizada POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS (ou instrumento similar)' foi marcada na questão anterior. [Obs.: ((Q41_SQ003.NAOK == "Y"))]

Por favor, carregar um arquivo.
Kindly attach the aforementioned documents along with the survey.
Só é aceito o *upload* de um único arquivo no formato PDF, com tamanho máximo de 20MB.

5. Capacitação

É necessário que todas as pessoas da organização estejam cientes da importância dos temas privacidade e proteção de dados pessoais, bem como dos impactos e prejuízos que podem ser causados devido às violações desses dados (*e.g.* sanções aplicadas pela ANPD, indenizações, danos financeiros e à imagem da instituição). Com isso, a organização deve conduzir iniciativas tanto para conscientizar quanto para capacitar seus colaboradores nessas áreas. A conscientização é

importante para que os colaboradores conheçam a legislação, bem como as políticas e normativos institucionais relacionados à proteção de dados pessoais, e para que reconheçam como as suas decisões e ações podem afetar a preservação da privacidade dos titulares de dados.

Nesse sentido, é conveniente que a organização elabore um Plano de Capacitação que contemple ações de conscientização e que determine os conhecimentos e as competências necessárias para os recursos humanos relativamente a essa temática, sobretudo no que tange aos colaboradores diretamente envolvidos em atividades que realizam o tratamento de dados pessoais. Assim, o Plano de Capacitação deve mapear as lacunas de conhecimentos e habilidades associadas ao tema e planejar ações de treinamento para sua redução gradual.

As ações de capacitação devem considerar diferentes níveis de envolvimento dos colaboradores com essa temática, de forma que aquelas pessoas envolvidas em atividades críticas relacionadas ao tratamento de dados pessoais e que ocupam funções com responsabilidades essenciais relacionadas à proteção de dados pessoais recebam treinamento diferenciado, além do nível básico fornecido aos demais colaboradores.

Por fim, vale ressaltar que tanto a LGPD, ao focar na proteção dos dados pessoais e na privacidade dos indivíduos, quanto a Lei 12.527/2011 (Lei de Acesso à Informação – LAI), ao promover a transparência e o acesso às informações públicas, buscam garantir direitos fundamentais relacionados à informação em sentido amplo. Ambas (LGPD e LAI) atuam para fortalecer a proteção dos direitos dos cidadãos e exigir das entidades, públicas e privadas, maior zelo quanto à gestão e ao tratamento das informações. Para isso, embora tenham finalidades distintas, essas normas se complementam de forma harmônica, sendo que a conformidade com ambas é fundamental para as organizações.

As questões desta seção, então, abordam aspectos atinentes à avaliação, ao planejamento e à realização de ações de capacitação relacionadas à privacidade e à proteção de dados pessoais, bem como à necessidade de harmonização entre a LGPD e a LAI.

Referências úteis:

- Lei 12.527/2011 (https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm);

- ABNT NBR ISO/IEC 27701:2019, itens 5.5.2 (Competência), 5.5.3 (Conscientização) e 5.5.4 (Comunicação).

5.1 (TIPO A) Acerca da capacitação dos seus colaboradores em proteção de dados pessoais, a organização:

[Help: **Questão TIPO A:**

Esta questão permite a marcação de uma única opção de resposta, sendo que as diferentes opções disponíveis refletem um aumento gradativo da maturidade da organização em relação às práticas e aos controles envolvidos. No caso, o respondente deve assinalar qual, dentre as opções disponíveis, melhor reflete a situação atual da sua organização.

Além de marcar a opção que melhor reflete a situação da sua organização em relação ao tópico questionado, o gestor **DEVE** complementar textualmente a sua resposta, no respectivo campo de comentário (que aceita texto aberto). Caso marque a opção "Não se aplica", o gestor deve justificar nesse campo o seu entendimento pela não aplicação daquela medida/controle à sua organização. Caso marque alguma das demais opções de resposta, o gestor deve fornecer nesse campo detalhes que permitam compreender melhor a escolha por aquela opção, considerando o contexto específico da sua organização. Por exemplo, o gestor deve utilizar esse campo para descrever, quando aplicável, datas, períodos, responsáveis, projetos e iniciativas, bem como referenciar artefatos, evidências, atas e outros documentos internos, indicando os respectivos nomes, datas e números de identificação, se houver. A qualquer momento, inclusive após encerrado o prazo para o preenchimento do questionário, os auditores poderão requisitar informações adicionais, bem como o envio desses elementos (artefatos, evidências, atas, documentos) eventualmente mencionados pelo gestor.]

Favor escolher apenas uma das opções a seguir:

- Não se aplica (justificar no campo de comentário);
- Não possui PLANO DE CAPACITAÇÃO (ou instrumento similar) e seus colaboradores ainda não realizaram treinamento em proteção de dados pessoais;
- Não possui PLANO DE CAPACITAÇÃO (ou instrumento similar), mas colaboradores específicos já realizaram treinamento em proteção de dados pessoais;
- Possui PLANO DE CAPACITAÇÃO (ou instrumento similar) e, apesar de este não contemplar a temática de proteção de dados pessoais de maneira específica, já realizou treinamento abrangente (não direcionado apenas a determinados colaboradores) nessa área;
- Possui PLANO DE CAPACITAÇÃO (ou instrumento similar), contemplou nesse documento a temática de proteção de dados pessoais e já realizou treinamento da maioria dos colaboradores nessa área;
- Possui PLANO DE CAPACITAÇÃO (ou instrumento similar), contemplou nesse documento a temática de proteção de dados pessoais, incluindo a necessidade de treinamento diferenciado para as pessoas

que exercem funções com responsabilidades essenciais quanto à proteção de dados pessoais, e já realizou treinamento de todos os colaboradores nessa área.

5.1.1 Anexe o Plano de Capacitação (ou instrumento similar) da organização:

Só responder essa pergunta sob as seguintes condições:

Alguma das duas últimas opções foi marcada na questão anterior.

Por favor, carregar um arquivo.
Kindly attach the aforementioned documents along with the survey.
Só é aceito o *upload* de um único arquivo no formato PDF, com tamanho máximo de 20MB.

5.2 (TIPO B) Acerca das ações de capacitação em proteção de dados pessoais realizadas nos últimos 3 (três) anos, a organização:

[Help: **Questão TIPO B:**

Esta questão permite a marcação de múltiplas opções de resposta. No caso, o respondente deve marcar todas as opções que são atendidas pela sua organização.]

Só responder essa pergunta sob as seguintes condições:

Alguma das quatro últimas opções foi marcada na questão 5.1.

Por favor, escolha as opções que se aplicam:

- Levou em consideração a necessidade de COMPLEMENTAR A CAPACITAÇÃO dos participantes nesses treinamentos COM CONTEÚDO SOBRE TRANSPARÊNCIA da gestão relativa às informações de interesse coletivo ou geral (Lei 12.527/2011 – Lei de Acesso à Informação);
- Efetivamente CAPACITOU NO TEMA TRANSPARÊNCIA da gestão relativa às informações de interesse coletivo ou geral (LAI) MAIS DE 50% dos colaboradores que receberam treinamento em proteção de dados pessoais;
- OFERECEU AÇÃO DE CAPACITAÇÃO QUE TENHA ABORDADO CONJUNTAMENTE, de forma integrada, as temáticas da proteção de dados pessoais (LGPD) e da transparência da gestão (LAI);
- ORIENTOU OS PARTICIPANTES nesses treinamentos, mesmo que *a posteriori*, sobre a necessidade de observarem os Enunciados da CGU divulgados por meio da PORTARIA NORMATIVA CGU 71/2023 (https://www.in.gov.br/en/web/dou/-/portaria-normativa-cgu-n-71-de-10-de-abril-de-2023-477406468);
- ORIENTOU OS PARTICIPANTES nesses treinamentos, mesmo que *a posteriori*, sobre a necessidade de observarem as diretrizes e orientações publicadas pela CGU por meio do “PARECER SOBRE ACESSO À INFORMAÇÃO para atender ao Despacho Presidencial de 1º de janeiro de 2023” (https://www.gov.br/acessoainformacao/pt-br/entendimentos-e-estudos-sobre-a-lai/copy_of_parecerfinalsobreacessoinformao_cgu_fev2023.pdf);
- NÃO ATENDEU NENHUM dos itens anteriores.

6. 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 no art. 6º da LGPD são seguidos e que os tratamentos são fundamentados em, ao menos, uma das bases legais descritas na legislação.

A questão desta seção, então, aborda aspectos atinentes à conformidade das atividades de tratamento de dados pessoais realizadas pela organização frente a alguns dos princípios da LGPD, a exemplo de possuir propósitos legítimos, específicos, explícitos e informados aos titulares, de modo que estes sejam capazes de compreender claramente a(s) finalidade(s) para a(s) qual(is) os seus dados pessoais são tratados.

Ademais, a coleta deve se restringir aos dados pessoais estritamente necessários para cumprir com as finalidades de tratamento informadas, a retenção (armazenamento) dos dados deve durar apenas o tempo estritamente necessário para cumprir com essas mesmas finalidades, bem como devem ser identificadas e documentadas as bases legais que fundamentam todas as atividades de tratamento de dados pessoais da organização. As possíveis bases legais são relacionadas nos incisos I a X do art. 7º da Lei 13.709/2018 (consentimento, cumprimento de obrigação legal/regulatória, execução de políticas públicas pela Administração Pública, estudos por parte de órgão de pesquisa, execução de contratos,

exercício regular de direitos em processo judicial/administrativo/arbitral, proteção da vida ou da incolumidade física do titular ou de terceiro, tutela da saúde, interesse legítimo do controlador ou de terceiro e proteção do crédito).

A organização também deve manter registro detalhado (*e.g.* inventário) das operações de tratamento de dados pessoais que realiza, especialmente quando baseado no legítimo interesse (LGPD, art. 37). Esse registro pode contemplar, por exemplo: a identificação do tratamento, sua finalidade, a base legal que o fundamenta, a descrição das categorias dos titulares de dados pessoais envolvidos, os dados pessoais coletados, o tempo de retenção dos dados, o local de armazenamento dos dados, o responsável pelo processo de tratamento e as medidas de segurança adotadas.

Por fim, relativamente às suas operações de maior risco (ver Resolução CD/ANPD 2/2022 [https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/regulamentacoes-da-anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022], Anexo I, art. 4º), a organização deve elaborar Relatório de Impacto à Proteção de Dados Pessoais (RIPD), inclusive de dados sensíveis, para avaliar os possíveis riscos associados (LGPD, art. 38). Por meio do RIPD, a organização descreverá os tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações, identificará a probabilidade de ocorrência de cada fator de risco e o seu impacto sobre as liberdades e direitos fundamentais dos titulares de dados e avaliará as medidas, as salvaguardas e os mecanismos de mitigação de risco apropriados a cada hipótese (https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd).

Referências úteis:

- Lei 13.709/2018, art. 5º, inciso XVII, art. 6º, em especial incisos I, II e III, e arts. 7º, 37, 38 e 40 (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm);

- ABNT NBR ISO/IEC 27701:2019, itens 7.2.1 (Identificação e documentação do propósito), 7.2.2 (Identificação de bases legais), 7.2.5 (Avaliação de impacto de privacidade), 7.2.8 (Registros relativos ao tratamento de DP), 7.4.1 (Limite de coleta) e 7.4.7 (Retenção).

6.1 (TIPO B) A organização:

[Help: **Questão TIPO B:**

Esta questão permite a marcação de múltiplas opções de resposta. No caso, o respondente deve marcar todas as opções que contém iniciativas que já foram realizadas pela sua organização.]

Por favor, escolha as opções que se aplicam:

- Identificou e DOCUMENTOU AS FINALIDADES de todas as suas principais atividades de tratamento de dados pessoais;
- Avaliou se COLETA APENAS OS DADOS ESTRITAMENTE NECESSÁRIOS para cumprir com as finalidades de tratamento de dados pessoais que foram identificadas;
- 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;
- Identificou e DOCUMENTOU AS BASES LEGAIS que fundamentam todas as suas principais atividades de tratamento de dados pessoais;
- POSSUI REGISTRO(S) (*e.g.* INVENTÁRIO[S] DE DADOS PESSOAIS) instituído(s) para consolidar informações relacionadas às características das atividades de tratamento de dados pessoais;
- CATALOGOU NO(S) REGISTRO(S)/INVENTÁRIO(S) DE DADOS PESSOAIS informações que abrangem todas as suas principais atividades de tratamento de dados pessoais;
- Mantém REGISTRO DAS OPERAÇÕES de tratamento de dados pessoais que realiza, em especial quando o tratamento se baseia no legítimo interesse;
- JÁ ELABOROU ALGUM RIPD – Relatório de Impacto à Proteção de Dados Pessoais (LGPD, art. 5º, inciso XVII);
- JÁ IMPLEMENTOU CONTROLES para mitigar os riscos identificados por meio da elaboração de RIPD (Relatório de Impacto à Proteção de Dados Pessoais);
- AINDA NÃO ATENDE NENHUM dos itens anteriores.

6.1.1 Anexe o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) elaborado pela organização:

Só responder essa pergunta sob a seguinte condição:

A opção 'ELABOROU RIPD (Relatório de Impacto à Proteção de Dados Pessoais)' foi marcada na questão anterior.

Por favor, carregar um arquivo.
Kindly attach the aforementioned documents along with the survey.
Só é aceito o *upload* de um único arquivo no formato PDF, com tamanho máximo de 20MB.

7. 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 (arts. 9º e 17-22), em especial aqueles previstos no art. 18.

O art. 9º da LGPD, por exemplo, prevê o direito, aos titulares de dados, de acesso facilitado a uma série de informações: finalidade do tratamento; formas e duração do tratamento; identificação e dados de contato do controlador; informações acerca do uso compartilhado de dados e sua finalidade; responsabilidades dos agentes que realizam o tratamento; e direitos do titular. Além disso, a organização deve informar as hipóteses em que, no exercício de suas competências, realiza tratamento de dados pessoais, fornecendo informações sobre a finalidade, a base legal, os procedimentos e as práticas utilizadas para a execução dessas atividades.

As questões desta seção, então, abordam aspectos atinentes à elaboração da Política de Privacidade (também chamada de "Aviso de Privacidade") e ao atendimento dos direitos do titular de dados pessoais (*e.g.* confirmação da existência de tratamento; acesso aos dados; correção de dados incompletos/inexatos/desatualizados; revogação do consentimento; anonimização, bloqueio ou eliminação de dados desnecessários/excessivos ou que dependam de consentimento do titular; portabilidade dos dados; informações sobre compartilhamento de dados).

A Política/Aviso de Privacidade é um documento endereçado aos usuários de um site, serviço ou sistema (titulares de dados – público externo), com o propósito de dar visibilidade ao tratamento de dados pessoais que ocorre no âmbito desse site/serviço/sistema, de modo a demonstrar que os princípios da LGPD são atendidos (ver https://www.serpro.gov.br/lgpd/noticias/2019/elabora-politica-privacidade-aderente-lgpd-dados-pessoais). Além de fornecer acesso ao documento no momento da coleta dos dados pessoais, convém que a organização o divulgue de forma permanente em seu sítio institucional, em local de fácil acesso aos titulares de dados pessoais.

Referências úteis:

- Lei 13.709/2018, art. 6º, em especial incisos IV e VI, arts. 9º e 17-22, art. 23, inciso I, e art. 50, inciso I, alíneas "a", "d" e "e" (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm);

- ABNT NBR ISO/IEC 27701:2019, itens 7.3 (Obrigações dos titulares de dados pessoais), 7.3.2 (Determinando as informações para os titulares de dados pessoais) e 7.3.3 (Fornecendo informações aos titulares de dados pessoais).

7.1 (TIPO A) A organização elaborou e divulga em seu sítio eletrônico institucional Política de Privacidade (ou instrumento similar)?

[Help: **Questão TIPO A:**

Esta questão permite a marcação de uma única opção de resposta, sendo que as diferentes opções disponíveis refletem um aumento gradativo da maturidade da organização em relação às práticas e aos controles envolvidos. No caso, o respondente deve assinalar qual, dentre as opções disponíveis, melhor reflete a situação atual da sua organização.

Além de marcar a opção que melhor reflete a situação da sua organização em relação ao tópico questionado, o gestor **DEVE** complementar textualmente a sua resposta, no respectivo campo de comentário (que aceita texto aberto). Caso marque a opção "Não se aplica", o gestor deve justificar nesse campo o seu entendimento pela não aplicação daquela medida/controle à sua organização. Caso marque alguma das demais opções de resposta, o gestor deve fornecer nesse campo detalhes que permitam compreender melhor a escolha por aquela opção, considerando o contexto específico da sua organização. Por exemplo, o gestor deve utilizar esse campo para descrever, quando aplicável, datas, períodos, responsáveis, projetos e iniciativas, bem como referenciar artefatos, evidências, atas e outros documentos internos, indicando os respectivos nomes, datas e números de identificação, se houver. A qualquer momento, inclusive após encerrado o prazo para o preenchimento do questionário, os auditores poderão requisitar informações adicionais, bem como o envio desses elementos (artefatos, evidências, atas, documentos) eventualmente mencionados pelo gestor.]

Favor escolher apenas uma das opções a seguir:

- Não se aplica (justificar no campo de comentário);
- A organização NÃO ELABOROU POLÍTICA DE PRIVACIDADE (ou instrumento similar);
- A organização ELABOROU A POLÍTICA DE PRIVACIDADE (ou instrumento similar), MAS NÃO A DIVULGA em seu sítio eletrônico institucional;

- A organização ELABOROU A POLÍTICA DE PRIVACIDADE (ou instrumento similar) E A DIVULGA em seu sítio eletrônico institucional [no campo de comentário, informar o endereço da internet (URL) onde a política está publicada].

7.1.1 Anexe a Política de Privacidade (ou instrumento similar) da organização:

Só responder essa pergunta sob as seguintes condições:

Alguma das duas últimas opções foi marcada na questão anterior.

Por favor, carregar um arquivo.
Kindly attach the aforementioned documents along with the survey.

Só é aceito o *upload* de um único arquivo no formato PDF, com tamanho máximo de 20MB.

7.2 (TIPO A) Foram implementados mecanismos para atender os direitos dos titulares aplicáveis à organização, relacionados à obtenção de informações sobre o tratamento dos dados, de modo geral (LGPD, art. 9º), bem como sobre os seus dados específicos e o respectivo tratamento (art. 18)?

[Help: **Questão TIPO A:**

Esta questão permite a marcação de uma única opção de resposta, sendo que as diferentes opções disponíveis refletem um aumento gradativo da maturidade da organização em relação às práticas e aos controles envolvidos. No caso, o respondente deve assinalar qual, dentre as opções disponíveis, melhor reflete a situação atual da sua organização.

Além de marcar a opção que melhor reflete a situação da sua organização em relação ao tópico questionado, o gestor **DEVE** complementar textualmente a sua resposta, no respectivo campo de comentário (que aceita texto aberto). Caso marque a opção "Não se aplica", o gestor deve justificar nesse campo o seu entendimento pela não aplicação daquela medida/controle à sua organização. Caso marque alguma das demais opções de resposta, o gestor deve fornecer nesse campo detalhes que permitam compreender melhor a escolha por aquela opção, considerando o contexto específico da sua organização. Por exemplo, o gestor deve utilizar esse campo para descrever, quando aplicável, datas, períodos, responsáveis, projetos e iniciativas, bem como referenciar artefatos, evidências, atas e outros documentos internos, indicando os respectivos nomes, datas e números de identificação, se houver. A qualquer momento, inclusive após encerrado o prazo para o preenchimento do questionário, os auditores poderão requisitar informações adicionais, bem como o envio desses elementos (artefatos, evidências, atas, documentos) eventualmente mencionados pelo gestor.]

Favor escolher apenas uma das opções a seguir:

- Não se aplica (justificar no campo de comentário);
- Não foram implementados mecanismos para atender os direitos dos titulares (LGPD, arts. 9º e 18);
- Foram implementados mecanismos para atender alguns dos direitos dos titulares (LGPD, arts. 9º e 18), mas não todos;
- Foram implementados mecanismos para atender todos os direitos dos titulares (LGPD, arts. 9º e 18) aplicáveis à organização.

8. Compartilhamento de dados pessoais

A organização deve identificar, avaliar e documentar detalhes relacionados aos compartilhamentos de dados pessoais com terceiros.

A realização de compartilhamento de dados pessoais demanda a adoção de controles adequados com vistas a mitigar os riscos que possam comprometer a segurança e a proteção desses dados. Diante disso, a LGPD defende, por exemplo, que as partes envolvidas no compartilhamento adotem determinadas precauções, inclusive, em certos casos, exigindo a formalização de contrato, convênio ou instrumento congênere (LGPD, art. 26, § 1º, inciso IV) e a sua respectiva comunicação à ANPD (art. 26, § 2º). Nos casos de eventual transferência internacional dos dados, a LGPD também apregoa, além da conformidade com os princípios, os direitos e o regime de proteção de dados previsto em seu escopo geral, a adoção de uma série de requisitos e cuidados especiais (arts. 33-36), os quais a organização precisa avaliar e cumprir.

No caso de eventual utilização de solução de computação em nuvem (*cloud computing*), a IN GSI/PR 5/2021 prevê requisitos mínimos de segurança da informação, obrigatórios para órgãos e entidades da Administração Pública federal, porém que servem de parâmetro de boas práticas para qualquer organização que se preocupe com a segurança e a proteção dos dados e informações que trata. Essa norma traz uma série de medidas com vistas a proteger a confidencialidade, a integridade e a disponibilidade dos dados (*e.g.* definição de responsabilidades para os diferentes atores envolvidos na gestão da nuvem, gerenciamento de identidades e de registros/*logs*, adoção de criptografia), além de abordar a prevenção e a resposta a incidentes de segurança.

As questões desta seção, então, abordam aspectos atinentes à identificação dos dados pessoais que são compartilhados com terceiros, à devida avaliação e adequação dessas operações frente aos critérios previstos na LGPD, em especial nos arts. 26 (finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos/entidades públicos, respeitados, ainda, os princípios de proteção de dados pessoais elencados no art. 6º) e 27 (compartilhamento de dados pessoais com pessoa de direito privado), ao registro dos eventos relacionados a esses compartilhamentos (quais dados foram compartilhados, com quem foram compartilhados e quando foram compartilhados), às transferências internacionais de dados pessoais e ao tratamento de dados pessoais em solução de computação em nuvem.

Referências úteis:

- Lei 13.709/2018, art. 5º, inciso XVI, arts. 26-27 e 30, arts. 33-36 e 39, arts. 44 e 50, § 2º, inciso I, alínea "d" (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm);

- IN GSI/PR 5/2021 (Dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da APF), em especial arts. 17 e 18 (https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-5-de-30-de-agosto-de-2021-341649684);

- ABNT NBR ISO/IEC 27701:2019, itens 7.5.1 (Identificando as bases para a transferência de dados pessoais entre jurisdições), 7.5.2 (Países e organizações internacionais para os quais os dados pessoais podem ser transferidos), 7.5.3 (Registros de transferência de dados pessoais) e 7.5.4 (Registro de divulgação de dados pessoais para terceiros);

- Guia Orientativo – Tratamento de dados pessoais pelo Poder Público (https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf).

8.1 (TIPO A) Quanto aos compartilhamentos de dados pessoais com terceiros, a organização:

[Help: **Questão TIPO A:**

Esta questão permite a marcação de uma única opção de resposta, sendo que as diferentes opções disponíveis refletem um aumento gradativo da maturidade da organização em relação às práticas e aos controles envolvidos. No caso, o respondente deve assinalar qual, dentre as opções disponíveis, melhor reflete a situação atual da sua organização.

Além de marcar a opção que melhor reflete a situação da sua organização em relação ao tópico questionado, o gestor **DEVE** complementar textualmente a sua resposta, no respectivo campo de comentário (que aceita texto aberto). Caso marque a opção "Não se aplica", o gestor deve justificar nesse campo o seu entendimento pela não aplicação daquela medida/controle à sua organização. Caso marque alguma das demais opções de resposta, o gestor deve fornecer nesse campo detalhes que permitam compreender melhor a escolha por aquela opção, considerando o contexto específico da sua organização. Por exemplo, o gestor deve utilizar esse campo para descrever, quando aplicável, datas, períodos, responsáveis, projetos e iniciativas, bem como referenciar artefatos, evidências, atas e outros documentos internos, indicando os respectivos nomes, datas e números de identificação, se houver. A qualquer momento, inclusive após encerrado o prazo para o preenchimento do questionário, os auditores poderão requisitar informações adicionais, bem como o envio desses elementos (artefatos, evidências, atas, documentos) eventualmente mencionados pelo gestor.]

Favor escolher apenas uma das opções a seguir:

- Não se aplica (justificar no campo de comentário);
- AINDA NÃO AVALIOU se os realiza ou AINDA NÃO IDENTIFICOU todos os dados eventualmente compartilhados;
- AVALIOU se há esses compartilhamentos e, nos casos detectados, IDENTIFICOU todos os dados eventualmente compartilhados;
- IDENTIFICOU todos os dados pessoais compartilhados com terceiros e INICIOU A AVALIAÇÃO desses compartilhamentos, porém ainda não pode atestar que todos estejam em conformidade com os critérios legais (LGPD, arts. 26-27);
- IDENTIFICOU todos os dados pessoais compartilhados, AVALIOU os compartilhamentos e ATESTA que todos ESTÃO EM CONFORMIDADE COM OS CRITÉRIOS LEGAIS (LGPD, arts. 26-27), apesar de ainda não manter registro dos eventos relacionados a cada compartilhamento;
- IDENTIFICOU todos os dados pessoais compartilhados, AVALIOU os compartilhamentos, ATESTA que todos ESTÃO EM CONFORMIDADE COM OS CRITÉRIOS LEGAIS (LGPD, arts. 26-27), DISPONIBILIZA INFORMAÇÕES acerca do uso compartilhado de dados e sua finalidade (art. 9º, inciso V) e MANTÉM REGISTRO DETALHADO dos eventos relacionados a cada compartilhamento, incluindo a identificação de quais dados foram compartilhados, com quem foram compartilhados e quando foram compartilhados.

8.1.1 (TIPO A) A organização realiza transferência internacional de dados pessoais?

[Help: **Questão TIPO A:**

Esta questão permite a marcação de uma única opção de resposta, sendo que as diferentes opções disponíveis refletem um aumento gradativo da maturidade da organização em relação às práticas e aos controles envolvidos. No caso, o respondente deve assinalar qual, dentre as opções disponíveis, melhor reflete a situação atual da sua organização.

Além de marcar a opção que melhor reflete a situação da sua organização em relação ao tópico questionado, o gestor **DEVE** complementar textualmente a sua resposta, no respectivo campo de comentário (que aceita texto aberto). Caso marque a opção "Não se aplica", o gestor deve justificar nesse campo o seu entendimento pela não aplicação daquela medida/controle à sua organização. Caso marque alguma das demais opções de resposta, o gestor deve fornecer nesse campo detalhes que permitam compreender melhor a escolha por aquela opção, considerando o contexto específico da sua organização. Por exemplo, o gestor deve utilizar esse campo para descrever, quando aplicável, datas, períodos, responsáveis, projetos e iniciativas, bem como referenciar artefatos, evidências, atas e outros documentos internos, indicando os respectivos nomes, datas e números de identificação, se houver. A qualquer momento, inclusive após encerrado o prazo para o preenchimento do questionário, os auditores poderão requisitar informações adicionais, bem como o envio desses elementos (artefatos, evidências, atas, documentos) eventualmente mencionados pelo gestor.]

Só responder essa pergunta sob as seguintes condições:

Alguma das quatro últimas opções foi marcada na questão anterior.

Favor escolher apenas uma das opções a seguir:

- Até o momento, não foi identificada transferência internacional de dados, porém a organização AINDA NÃO AVALIOU TODOS OS CASOS de compartilhamento de dados pessoais;
- Todos os compartilhamentos foram avaliados e NÃO HÁ transferência internacional de dados;
- Todos os compartilhamentos foram avaliados e HÁ TRANSFERÊNCIA INTERNACIONAL DE DADOS.

8.1.1.1 (TIPO A) As transferências internacionais de dados pessoais estão de acordo com os princípios, direitos e requisitos previstos na LGPD, em especial no art. 33?

[Help: **Questão TIPO A:**

Esta questão permite a marcação de uma única opção de resposta, sendo que as diferentes opções disponíveis refletem um aumento gradativo da maturidade da organização em relação às práticas e aos controles envolvidos. No caso, o respondente deve assinalar qual, dentre as opções disponíveis, melhor reflete a situação atual da sua organização.

Além de marcar a opção que melhor reflete a situação da sua organização em relação ao tópico questionado, o gestor **DEVE** complementar textualmente a sua resposta, no respectivo campo de comentário (que aceita texto aberto). Caso marque a opção "Não se aplica", o gestor deve justificar nesse campo o seu entendimento pela não aplicação daquela medida/controle à sua organização. Caso marque alguma das demais opções de resposta, o gestor deve fornecer nesse campo detalhes que permitam compreender melhor a escolha por aquela opção, considerando o contexto específico da sua organização. Por exemplo, o gestor deve utilizar esse campo para descrever, quando aplicável, datas, períodos, responsáveis, projetos e iniciativas, bem como referenciar artefatos, evidências, atas e outros documentos internos, indicando os respectivos nomes, datas e números de identificação, se houver. A qualquer momento, inclusive após encerrado o prazo para o preenchimento do questionário, os auditores poderão requisitar informações adicionais, bem como o envio desses elementos (artefatos, evidências, atas, documentos) eventualmente mencionados pelo gestor.]

Só responder essa pergunta sob a seguinte condição:

A opção 'Todos os compartilhamentos foram avaliados e HÁ TRANSFERÊNCIA INTERNACIONAL DE DADOS' foi marcada na questão anterior.

Favor escolher apenas uma das opções a seguir:

- A organização AINDA NÃO AVALIOU os princípios, direitos e requisitos previstos na LGPD, em especial no art. 33, em relação a todos os casos de transferência internacional de dados;
- Todos os casos de transferência internacional de dados foram avaliados, porém AINDA NÃO ATENDEM integralmente os requisitos legais (LGPD, em especial art. 33);
- Todos os casos de transferência internacional de dados foram avaliados e ATENDEM INTEGRALMENTE OS REQUISITOS LEGAIS (LGPD, em especial art. 33).

8.1.2 (TIPO B) Acerca de tratamento de dados pessoais em solução de computação em nuvem (*cloud computing*), a organização:

[Help: **Questão TIPO B:**

Esta questão permite a marcação de múltiplas opções de resposta. No caso, o respondente deve marcar todas as opções que são atendidas pela sua organização.]

Por favor, escolha as opções que se aplicam:

- REALIZA O TRATAMENTO DE DADOS PESSOAIS EM NUVEM (ainda que apenas armazenamento);
- Avaliou e PODE ASSEGURAR QUE NÃO HÁ ARMAZENAMENTO DE DADOS PESSOAIS EM TERRITÓRIO ESTRANGEIRO;
- Realizou AVALIAÇÃO DE RISCOS relativamente a esse tratamento, amparada em análise e em relatório de impacto que foram devidamente submetidos à apreciação das instâncias competentes;
- INCLUIU, NOS INSTRUMENTOS CONTRATUAIS COM OS PROVEDORES DE NUVEM, CLÁUSULAS e mecanismos que garantem, ao menos, o sigilo dos dados no armazenamento e em trânsito, a não transferência dos dados a terceiros, a remoção incondicional dos dados após o término do contrato e a não utilização dos dados, para quaisquer fins, pelo provedor ou por terceiros;
- NÃO REALIZA NENHUM TRATAMENTO DE DADOS PESSOAIS EM NUVEM.

9. Violação de dados pessoais

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

Convém, ainda, que a organização possua um sistema de informação de gestão de incidentes próprio/adequado para registrar tanto os incidentes em si quanto o histórico de todas as ações adotadas para solucioná-los/tratá-los, desde a eventual adoção inicial de uma solução de contorno, previamente à atuação para efetivamente analisar e erradicar as causas-raízes do incidente.

Ademais, tendo em vista que a identificação/detecção precoce pode diminuir significativamente os impactos causados por esses incidentes, a organização deve adotar mecanismos para monitorar proativa e continuamente os eventos que podem sinalizar (sinais precursores e indicadores) a ocorrência de incidentes de segurança associados à violação de dados pessoais, de modo que seja capaz de agir rapidamente nesses casos.

Por fim, a organização deve comunicar tanto à Autoridade Nacional de Proteção de Dados (ANPD) quanto ao(s) próprio(s) titular(es) de dados a ocorrência de incidente de segurança da informação que possa acarretar risco ou dano relevante a estes últimos. Essa notificação deve ser feita no prazo de 3 (três) dias úteis e mencionar, entre outras coisas: a descrição da natureza e da categoria dos dados pessoais afetados; as informações sobre os titulares afetados, incluindo seu número e a discriminação de crianças, adolescentes e idosos, se houver; a indicação das medidas técnicas e de segurança adotadas para a proteção dos dados, antes e após o incidente; os riscos relacionados ao incidente; as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente sobre os titulares; a data da ocorrência do incidente e a de seu conhecimento pelo controlador; os dados do encarregado; a descrição do incidente, incluindo sua causa. Caso a organização não encaminhe a comunicação tempestivamente, deverá expor, também, os motivos que levaram à demora (Resolução CD/ANPD 15/2024, art. 6º).

A questão desta seção, então, aborda aspectos atinentes à identificação, ao registro e ao tratamento/resposta a incidentes de segurança da informação que envolvem a violação de dados pessoais, bem como à existência de mecanismos e procedimentos padronizados para notificação da ANPD e dos titulares de dados envolvidos nos casos de incidentes que possam representar risco ou causar dano relevante aos titulares.

Referências úteis:

- Lei 13.709/2018, arts. 48 e 50, § 2º, inciso I, alínea “g” (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm);

- Resolução CD/ANPD 15/2024 (Regulamento de Comunicação de Incidente de Segurança), em especial arts. 6º-10 (https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024);

- ABNT NBR ISO/IEC 27701:2019, itens 6.13.1.1 (Responsabilidades e procedimentos), 6.13.1.4 (Avaliação e decisão dos eventos de segurança da informação) e 6.13.1.5 (Resposta aos incidentes de segurança da informação).

9.1 (TIPO B) A organização:

[Help: **Questão TIPO B:**

Esta questão permite a marcação de múltiplas opções de resposta. No caso, o respondente deve marcar todas as opções que são atendidas pela sua organização.]

Por favor, escolha as opções que se aplicam:

- Elaborou e mantém atualizado PLANO DE RESPOSTA A INCIDENTES (ou documento similar), sendo que abordou nesse documento questões específicas relacionadas ao tratamento/resposta a incidentes de segurança da informação que envolvem violação de dados pessoais;
- REGISTRA TODOS OS INCIDENTES de segurança da informação que envolvem violação de dados pessoais em sistema próprio/adequado a esse propósito;
- Sempre registra no sistema próprio/adequado a esse propósito TODAS AS AÇÕES QUE FORAM ADOTADAS PARA TRATAR/RESPONDER AO INCIDENTE de segurança da informação que envolve violação de dados pessoais, incluindo a eventual adoção de solução de contorno em um primeiro momento;
- MONITORA PROATIVA E CONTINUAMENTE a ocorrência de eventos (sinais precursores e indicadores) que podem ser associados a incidentes de segurança da informação que envolvem violação de dados pessoais;
- Estabeleceu e executa PROCEDIMENTOS PADRONIZADOS PARA COMUNICAR À ANPD E AO TITULAR DE DADOS a ocorrência de incidente de segurança da informação que possa acarretar risco ou dano relevante ao(s) titular(es);
- AINDA NÃO ATENDE NENHUM dos itens anteriores.

9.1.1 Anexe o Plano de Resposta a Incidentes (ou documento similar) da organização:

Só responder essa pergunta sob a seguinte condição:

A primeira opção foi marcada na questão anterior.

Por favor, carregar um arquivo.
Kindly attach the aforementioned documents along with the survey.
Só é aceito o *upload* de um único arquivo no formato PDF, com tamanho máximo de 20MB.

10. Medidas de proteção

A organização deve adotar amplas medidas de segurança, técnicas e administrativas com vistas a proteger os dados pessoais que trata de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (LGPD, art. 46), sobretudo, se houver, os dados pessoais sensíveis (que envolvem 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) e os dados pessoais de crianças e de adolescentes.

Para isso, convém, inclusive, que a organização defina claramente papéis, responsabilidades e procedimentos voltados à proteção desses dados e implemente controles específicos que sejam capazes de mitigar riscos que possam resultar em violações de privacidade. Entre tais controles, pode-se citar a definição de processo formal para registro e cancelamento de usuários nos sistemas que realizam tratamento de dados pessoais, de modo a viabilizar a atribuição dos direitos de acesso adequados nesses sistemas. O mesmo deve ser feito com o processo de provisionamento para conceder ou revogar os direitos de acesso, os quais devem observar os princípios de "necessidade de conhecer" (o colaborador só deve ter permissão para acessar informações que necessita para desempenhar suas tarefas) e "necessidade de uso" (o colaborador só deve ter permissão para acessar recursos de TI [*e.g.* equipamentos, aplicações, procedimentos, salas] que necessita para desempenhar suas tarefas).

Adicionalmente, convém que a organização registre e monitore os eventos (*logs*) relacionados às 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 ocorrerem mudanças nos dados, também deve ser registrada a ação realizada (*e.g.* inclusão, alteração ou exclusão). Convém, ainda, que a organização faça uso de soluções criptográficas para proteger de acessos indevidos os dados pessoais armazenados (em repouso) e quando estes estiverem trafegando (em trânsito), seja na rede interna da organização ou mesmo na Internet (durante o envio para um servidor na nuvem, por exemplo).

A organização também deve fornecer aos seus colaboradores diretrizes e orientações a respeito do uso de técnicas e ferramentas tecnológicas capazes de anonimizar, pseudonimizar, ocultar, mascarar e/ou tarjar dados pessoais, em especial no que se refere a temas transversais e comuns das organizações públicas (*e.g.* licitações, contratos, gestão de recursos humanos), o que atua para evitar a negação indevida de pedidos de acesso solicitados com base na LAI, com prejuízo à transparência das informações e ao controle social da Administração Pública.

Por fim, a organização deve assegurar que seus processos e sistemas sejam projetados, desde a concepção, de forma que os tratamentos de dados pessoais associados estejam limitados ao que é estritamente necessário para o alcance das finalidades pretendidas (*Privacy by Design* e *Privacy by Default*).

A questão desta seção, então, aborda aspectos atinentes à implementação de controles adequados para proteger os dados pessoais e mitigar o risco de violação, a exemplo da restrição e do rastreamento das atividades e dos acessos aos sistemas que realizam o tratamento desses dados, da utilização de criptografia para evitar acessos indevidos (seja aos dados armazenados ou mesmo em trânsito), do uso de técnicas e ferramentas de mascaramento/ocultação/tarjamento de dados pessoais e da concepção de processos e sistemas que estejam conformes com a LGPD.

Referências úteis:

- Lei 12.527/2011, arts. 3º e 7º, § 2º, arts. 10-14, e arts. 31 e 40 (https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm);

- Lei 13.709/2018, art. 13, § 4º, arts. 44 e 46, em especial § 2º, e arts. 49 e 50, § 2º, inciso I, alíneas “c” e “d” (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm);

- Decreto 7.724/2012, arts. 11-20, 55, 57, 58, inciso III, e arts. 67 e 68 (https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7724.htm);

- Portaria Normativa CGU 71/2023 (Aprova enunciados referentes à aplicação da Lei nº 12.527, de 18 de novembro de 2011), em especial Enunciado 12 (https://www.in.gov.br/en/web/dou/-/portaria-normativa-cgu-n-71-de-10-de-abril-de-2023-477406468);

- ABNT NBR ISO/IEC 27002:2013, item 6.1 (Organização interna), em especial item 6.1.1 (Responsabilidades e papéis pela segurança da informação);

- ABNT NBR ISO/IEC 27701:2019, itens 6.6.2.1 (Registro e cancelamento de usuário), 6.6.2.2 (Provisionamento para acesso de usuário), 6.7 (Criptografia), 6.9.4.1 (Registros de eventos [logs]) e 7.4 (*Privacy by Design* e *Privacy by Default*).

10.1 (TIPO B) A organização:

[Help: **Questão TIPO B:**

Esta questão permite a marcação de múltiplas opções de resposta. No caso, o respondente deve marcar todas as opções que são atendidas pela sua organização.]

Por favor, escolha as opções que se aplicam:

- É capaz de comprovar que ADOTA AMPLAS MEDIDAS DE SEGURANÇA, TÉCNICAS E ADMINISTRATIVAS aptas a proteger os dados pessoais que trata, tendo, inclusive, definido e atribuído papéis, responsabilidades e procedimentos específicos com esse propósito;
- Implementou PROCESSO FORMAL PARA REGISTRO, CANCELAMENTO E PROVISIONAMENTO DE USUÁRIOS nos sistemas que realizam tratamento de dados pessoais;
- REGISTRA E MONITORA EVENTOS (*LOGS*) relacionados às atividades de tratamento de dados pessoais;
- Utiliza criptografia para proteger os dados pessoais quando estes estão em repouso, ou seja, a chamada CRIPTOGRAFIA DE ARMAZENAMENTO;
- Utiliza criptografia para proteger os dados pessoais quando estes estão em trânsito na rede interna da organização ou na Internet, ou seja, a chamada CRIPTOGRAFIA DE PONTA-A-PONTA;
- Possui NORMA(S) INTERNA(S) que orientam os colaboradores quanto à obrigatoriedade do uso de MASCARAMENTO/OCULTAÇÃO/TARJAMENTO em documentos de interesse coletivo ou geral que contenham dados pessoais, de modo a possibilitar dar acesso a tais documentos sem comprometer esses dados;
- Disponibiliza aos colaboradores FERRAMENTA/SOLUÇÃO TECNOLÓGICA PARA REALIZAÇÃO DO MASCARAMENTO/OCULTAÇÃO/TARJAMENTO em documentos de interesse coletivo ou geral que contenham dados pessoais;
- Adota medidas para assegurar que seus processos e sistemas sejam projetados, desde a concepção, em conformidade com a LGPD (*PRIVACY BY DESIGN* E *PRIVACY BY DEFAULT*);
- AINDA NÃO ATENDE NENHUM dos itens anteriores.

11. Questões finais

OBSERVAÇÃO 1: Ao gestor, é relevante compreender cada uma das nove dimensões avaliadas nesta auditoria (Preparação; Contexto organizacional; Liderança; Capacitação; Conformidade do tratamento; Direitos do titular; Compartilhamento de dados pessoais; Violação de dados pessoais; e Medidas de proteção), bem como as subpráticas específicas que foram questionadas no bojo de cada uma dessas dimensões. Deste modo, o gestor pode se programar para, ao longo dos próximos meses/anos, implementar na sua organização as medidas e controles faltantes, frisando-se que o questionário não contempla todas as medidas e controles possíveis de serem implementados para a adequação das organizações à LGPD.

OBSERVAÇÃO 2: A ação do controle interno/auditoria interna é muito importante para que as leis, as normas gerais e as normas internas sejam efetivamente observadas, bem como para avaliar riscos em relação aos processos de trabalho da organização. No âmbito do Poder Executivo federal, as instâncias do sistema de controle interno, nos órgãos estrito senso, são as Assessorias Especiais de Controle Interno (AECI) e, nos outros tipos de organizações, são as auditorias internas, conforme estabelecem o Decreto 3.591/2000 (https://www.planalto.gov.br/ccivil_03/decreto/d3591.htm) e as Instruções Normativas CGU 3/2017 (https://repositorio.cgu.gov.br/handle/1/33409) e 13/2020 (https://repositorio.cgu.gov.br/handle/1/44989).

Q11.1 (TIPO B) Nos últimos 3 (três) anos, a instância do "sistema de controle interno governamental" da organização realizou avaliação relacionada com o tema:

[Help: **Questão TIPO B:**

Esta questão permite a marcação de múltiplas opções de resposta. No caso, o respondente deve marcar todas as opções que são atendidas pela sua organização.

No caso de ente público estadual, municipal ou federal de outro Poder que não o Executivo, favor responder em relação à instância que desempenha o papel de controle interno/auditoria interna da organização, ou que mais se aproxima desse papel.]

Por favor, escolha as opções que se aplicam:

- PROTEÇÃO DE DADOS PESSOAIS (Lei Geral de Proteção de Dados Pessoais – LGPD);
- TRANSPARÊNCIA DA GESTÃO relativa às informações de interesse coletivo ou geral (Lei de Acesso à Informação – LAI);
- AINDA NÃO FOI REALIZADA AVALIAÇÃO DE NENHUM DESSES TEMAS (LGPD ou LAI).

Q11.2 (texto aberto) Por favor, registre aqui os principais desafios, deficiências e pontos de atenção relacionados à adequação da sua organização à LGPD, bem como quaisquer outras considerações, comentários ou críticas que considerar pertinentes:

[Help: **ATENÇÃO:**

CONFIRA TODAS AS SUAS RESPOSTAS ANTES DE CLICAR NO BOTÃO "ENVIAR".

Caso ainda exista alguma pendência ou dúvida, utilize a opção "Retomar mais tarde" (localizada no canto superior direito da página) para salvar as respostas fornecidas até então. Desse modo, até 19/7/2024 (sexta-feira), por meio do mesmo código de acesso (*token*: {TOKEN:TOKEN}), é possível retornar para alterar ou complementar as respostas fornecidas.

Ao final, depois do envio, aparecerá, na página de confirmação, uma opção para salvar/imprimir as respostas. Entretanto, alertamos que **ESSA OPÇÃO SÓ APARECE NESSE MOMENTO** e não será possível acessar o questionário após o dia 19/7/2024 para ver ou imprimir as respostas enviadas.]

Esta Corte de Contas agradece a sua participação.

19/7/2024 – 23h59

Enviar questionário

Obrigado por ter preenchido o questionário.

Apêndice E – Organizações federais por área temática

As 387 organizações (peça 922) foram distribuídas por área temática da seguinte forma:
- 11 “Agências Reguladoras”: ANA, ANAC, ANATEL, ANCINE, ANEEL, ANM, ANP, ANS, ANTAQ, ANTT, ANVISA;
- 6 “Bancos”: BANCO DA AMAZÔNIA, BB, BNB, BNDES, CAIXA, EMGEA;
- 2 “Casas Legislativas”: CD, SF;
- 29 “Conselhos de Profissão”: CAU/BR, CFA, CFB, CFBio, CFBM, CFC, CFED, CFESS, CFF, CFFA, CFM, CFMV, CFN, CFO, CFP, CFQ, CFT, CFTA, Cofeci, Cofecon, Cofem, Coffito, Confe, Confea, Confef, Confen, Confere, Conferp, Conter;
- 117 “Instituições de Ensino”: CAPES, CEFET-MG, CEFET-RJ, CPII, ENAP, FOSORIO, FUB, Fundaj, FURG, IBC, IF Baiano, IF Farroupilha, IF Goiano, IF Sudeste, IFAC, IFAL, IFAM, IFAP, IFB, IFBA, IFC, IFCE, IFES, IFF, IFG, IFMA, IFMG, IFMS, IFMT, IFNMG, IFPA, IFPB, IFPE, IFPI, IFPR, IFRJ, IFRN, IFRO, IFRR, IFRS, IFS, IFSC, IFSertãoPE, IFSP, IFSul, IFSULDEMINAS, IFTM, IFTO, INEP, INES, UFABC, UFAC, UFAL, UFAM, UFAPE, UFBA, UFC, UFCA, UFCAT, UFCG, UFCSPA, UFDPar, UFERSA, UFES, UFF, UFFS, UFG, UFGD, UFJ, UFJF, UFLA, UFMA, UFMG, UFMS, UFMT, UFNT, UFOB, UFOP, UFOPA, UFPA, UFPB, UFPE, UFPel, UFPI, UFPR, UFR, UFRA, UFRB, UFRGS, UFRJ, UFRN, UFRPE, UFRR, UFRRJ, UFS, UFSB, UFSC, UFSCar, UFSJ, UFSM, UFT, UFTM, UFU, UFV, UFVJM, UNIFAL-MG, UNIFAP, UNIFEI, UNIFESP, UNIFESSPA, UNILA, UNILAB, UNIPAMPA, UNIR, UniRIO, Univasf, UTFPR;
- 12 “Instituições de Saúde”: APS, CHS-UFRJ, Conceição, EBSERH, FIOCRUZ, FUNASA, HCPA, HEMOBRÁS, HFA, HU-UNIFESP, IEC, INCA;
- 9 “Militares”: AMAZUL, CCCPM, CEX, CFIAe, CM, COMAER, EMGEPRON, FHE, IMBEL;
- 32 “Ministérios”: CGU, MAPA, MCID, MCom, MCTI, MD, MDA, MDHC, MDIC, MDS, MEC, MESP, MFAZ, MGI, MIDR, MinC, MIR, MJSP, MMA, MME, MMULHERES, MPA, MPI, MPO, MPOR, MPS, MRE, MS, MTE, MTR, MTur, PR;
- 6 organizações do “Ministério Público”: CNMP, ESMPU, MPDFT, MPF, MPM, MPT;
- 75 “Outras”: ABGF, ABIN, AEB, AGU, ANPD, BCB, BN, CADE, CBTU, CDC, CDP, CDRJ, CEAGESP, CEASAMINAS, CMB, CNEN, CNPQ, CODEBA, CODERN, CODEVASF, CONAB, CPRM, CVM, DATAPREV, DNIT, DNOCS, DPU, EBC, ECT, ELETRONUCLEAR, EMBRAPA, ENBPAR, EPE, FCP, FCRB, FINEP, FNDE, FUNAG, FUNAI, FUNARTE, Fundacentro, Funpresp-Exe, Funpresp-Jud, Ibama, IBGE, IBRAM, ICMBIO, INB, INCRA, Infra S/A, INFRAERO, INMETRO, INPI, INSS, IPEA, IPHAN, ITI, JBRJ, NAV Brasil, NUCLEP, PETROBRAS, PGFN, PPSA, PREVIC, RFB, SERPRO, SPA, STN, SUDAM, SUDECO, SUDENE, SUFRAMA, SUSEP, Telebras, TRENSURB;
- 5 organizações da “Segurança Pública”: CBMDF, PCDF, PF, PMDF, PRF;
- 16 “Serviços Sociais Autônomos”: ABDI, AgSUS, ANATER, APEX Brasil, EMBRATUR, Sebrae/DN, Senac/DN, Senai/DN, SENAI-CETIQT, Senar/Adm. Central, Senat/CN, SESC, Sescoop/UN, Sesi/CN, Sesi/DN, Sest/CN;
- 1 “Tribunal de Contas”: TCU;
- 66 “Tribunais do Judiciário”: CJF, CNJ, CSJT, STF, STJ, STM, TJDFT, TRE-AC, TRE-AL, TRE-AM, TRE-AP, TRE-BA, TRE-CE, TRE-DF, TRE-ES, TRE-GO, TRE-MA, TRE-MG, TRE-MS, TRE-MT, TRE-PA, TRE-PB, TRE-PE, TRE-PI, TRE-PR, TRE-RJ, TRE-RN, TRE-RO, TRE-RR, TRE-RS, TRE-SC, TRE-SE, TRE-SP, TRE-TO, TRF1, TRF2, TRF3, TRF4, TRF5, TRF6, TRT1, TRT2, TRT3, TRT4, TRT5, TRT6, TRT7, TRT8, TRT9, TRT10, TRT11, TRT12, TRT13, TRT14, TRT15, TRT16, TRT17, TRT18, TRT19, TRT20, TRT21, TRT22, TRT23, TRT24, TSE, TST.

Apêndice F – Indicador de adequação à LGPD (iLGPD)

De modo a consolidar os dados obtidos e a possibilitar a realização de comparações entre as diferentes organizações auditadas, no que tange ao nível de adequação à LGPD, fez-se necessário definir, para cada organização, um indicador derivado das respectivas respostas fornecidas às perguntas do questionário. Esse "indicador de adequação à LGPD" (iLGPD) é capaz, então, de resumir as respostas da organização em um único valor, entre 0 e 100%, o qual representa, em última instância, o grau de implementação das medidas de adequação avaliadas na auditoria.

Em seguida, a partir do cálculo desse indicador, podem ser definidos os chamados "níveis/faixas de adequação à LGPD". Na auditoria realizada em 2021 (TC 039.606/2020-1; Acórdão 1.384/2022-TCU-Plenário, Rel. Min. Augusto Nardes), por exemplo, foram definidos quatro níveis: "Inexpressivo" ($0 \leq$ indicador $\leq 0{,}15$), "Inicial" ($0{,}15 <$ indicador $\leq 0{,}5$), "Intermediário" ($0{,}5 <$ indicador $\leq 0{,}8$) e "Aprimorado" ($0{,}8 <$ indicador ≤ 1)[1]. Assim, conforme o valor final do indicador obtido pela organização, esta podia ser enquadrada em um desses níveis.

O questionário aplicado (**Apêndice D** – Questionário da auditoria) foi composto, basicamente, por questões do "Tipo A" (resposta única) e por questões do "Tipo B" (múltiplas respostas). Para as primeiras, a atribuição das notas (entre 0 e 100%) seguiu uma escala exponencial fixa, com taxa de crescimento de 0.35, a qual foi definida após a realização de simulações diversas sobre os dados reais das respostas das 387 organizações federais (Tabela 21).

Tabela 21 – Gradação das notas (arredondadas) nas questões do "Tipo A" (resposta única).
(Fonte: elaboração própria)

Qtde. de opções de resposta*	Exemplos	Gradação da nota (arredondada)
3	Q7.1, Q7.2	0 – 60% - 100%
5	Q5.1, Q8.1	0 – 16% - 36% - 63% - 100%
6	Q2.1	0 – 11% - 24% - 42% - 67% - 100%

*Para todos os efeitos, nas questões do "Tipo A", também foi atribuída nota "0" às respostas "Não se aplica".

A seu turno, para as questões do "Tipo B" (múltiplas respostas), as notas foram atribuídas por meio de uma escala linear simples, ou seja, dividiu-se 100% pela quantidade de itens disponíveis na questão (desconsiderando-se a opção de resposta que correspondia à ausência de implementação de qualquer dos controles/medidas mencionados) e, a cada um dos itens marcados, a nota era gradativamente incrementada, de 0 (nenhum item marcado) até 100% (todos os itens marcados).

Em consenso com os auditores dos TCEs que aderiram à fiscalização e que, por isso, também fariam uso do mesmo questionário, algumas questões foram excluídas da regra de formação do subindicador da respectiva dimensão e, consequentemente, também do cômputo do indicador geral (iLGPD). A questão 5.2, por exemplo, foi excluída por conter itens que fazem referência a documentos da CGU, cuja observância não seria cogente para as organizações públicas estaduais e municipais. As questões 8.1.1 e 8.1.1.1 foram excluídas porque o fato de o órgão/entidade realizar ou não transferência internacional de dados está relacionado à sua atuação, não sendo indicativo, por si só, de que esteja mais ou menos adequado à LGPD. A questão 8.1.2 (tratamento de dados pessoais em nuvem) foi excluída do cálculo do iComp (e do iLGPD) a pedido dos auditores dos TCEs.

Por fim, as atribuições de notas às diferentes questões (e, consequentemente, aos subindicadores das nove dimensões) ficaram conforme mostra a Tabela 22. Quanto aos níveis de adequação à LGPD, por uma questão de padronização das escalas adotadas pelo TCU em suas fiscalizações, a equipe decidiu adotar as mesmas faixas utilizadas no levantamento iESGo 2024[xxvi], ou seja: "Inexpressivo" ($0 \leq$ iLGPD $< 15\%$), "Iniciando" ($15\% \leq$ iLGPD $< 40\%$), "Intermediário" ($40\% \leq$ iLGPD $\leq 70\%$) e "Aprimorado" ($70\% <$ iLGPD $\leq 100\%$) [Figura 15].

Tabela 22 - Resumo da metodologia de cálculo do indicador de adequação à LGPD (iLGPD).
(Fonte: elaboração própria)

Aspecto	Regra adotada
Questões do "Tipo A" (resposta única)	Notas (arredondadas) atribuídas a partir da aplicação de escala gradativa com taxa exponencial de 0.35
Questões do "Tipo B" (múltiplas respostas)	Notas (arredondadas) atribuídas a partir da aplicação de escala linear simples
Subindicadores de cada dimensão (iPrep, iOrg, iLid, iCap, iConf, iDir, iComp, iResp e iProt)	A nota do subindicador corresponde à nota da respectiva questão, à exceção da dimensão "Direitos do titular", cujo subindicador recebe a fórmula: iDir = 0,4*Q7.1 + 0,6*Q7.2
Indicador de adequação à LGPD	iLGPD = (iPrep + iOrg + iLid*2 + iCap*1,5 + iConf*2 + iDir*2 + iComp*2 + iResp*1,5 + iProt*2) / 15

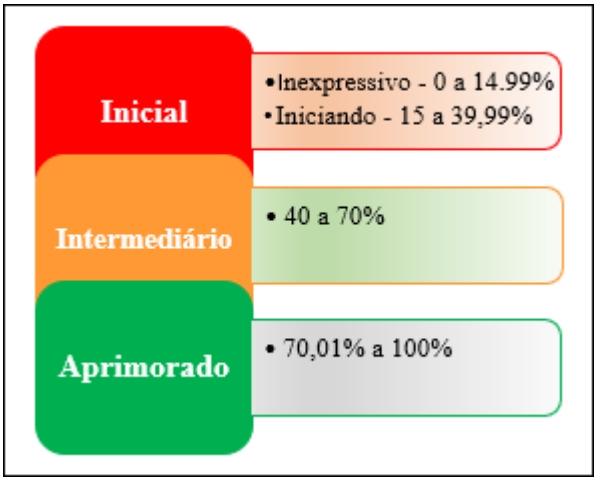


Figura 15 - Quatro níveis de adequação à LGPD (definidos com base no iESGo 2024).
(Fonte: iESGo 2024)

Apêndice G – *Checklist* para verificação de Política de Proteção de Dados Pessoais

As normas ABNT NBR ISO/IEC 27001:2013, 27002:2013 e 27701:2019 fornecem diretrizes para gestão de segurança da informação e sua relação com a proteção de dados pessoais, levando em consideração os ambientes de risco das organizações. Essas normas foram projetadas para serem usadas como referência na seleção e na implementação de controles de segurança da informação e proteção de dados pessoais comumente aceitos.

De acordo com o item 5.1 da ABNT NBR ISO/IEC 27701:2019 c/c o item 5.2 da ABNT NBR ISO/IEC 27001:2013 e o item 5.1 da ABNT NBR ISO/IEC 27002:2013, a alta direção deve estabelecer um conjunto de políticas de segurança da informação, entre as quais sugere-se uma política de proteção de dados pessoais. Este *checklist* para verificação de POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS foi definido conforme as diretrizes para implementação relacionadas nos referidos itens.

#	**Verificar se**	**S/N**	**Observações/ evidências**
1	Existe uma política de proteção de dados pessoais (ou instrumento normativo equivalente) formalmente estabelecida		
2	A política de PD foi publicada para as partes interessadas (públicos interno e externo)		
3	A política de PD é assinada pela alta direção, refletindo o comprometimento em satisfazer os requisitos legais aplicáveis relacionados com a proteção de dados pessoais		
4	A política de PD prevê a relação com outros normativos associados (*e.g.* Política de Segurança da Informação)		
5	A política de PD regulamenta os agentes de tratamento no âmbito da organização		
6	A política de PD define gestores e estruturas, atribuindo-lhes papeis e responsabilidades pela proteção de dados pessoais		
7	A política de PD abrange e é aplicável aos fornecedores da organização (que tratem dados pessoais)		
8	A política de PD regulamenta os principais aspectos para a proteção de dados pessoais na organização (tratando, no mínimo, das hipóteses de tratamento de dados pessoais utilizadas, do exercício dos direitos dos titulares, das transferências e compartilhamentos de dados e da interação com a ANPD)		
9	A política de PD prevê a necessidade de comunicação/conscientização aos interessados		
10	A política de PD prevê a sua revisão periódica ou quando ocorrerem mudanças significativas		

Apêndice H – *Checklist* para verificação de Política de Privacidade

A Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) estabeleceu diretrizes para a proteção de dados pessoais, levando em consideração os ambientes de risco das organizações. Essa norma definiu novas formas de interação com os titulares de dados, bem como obrigações adicionais de transparência sobre o tratamento de dados pessoais.

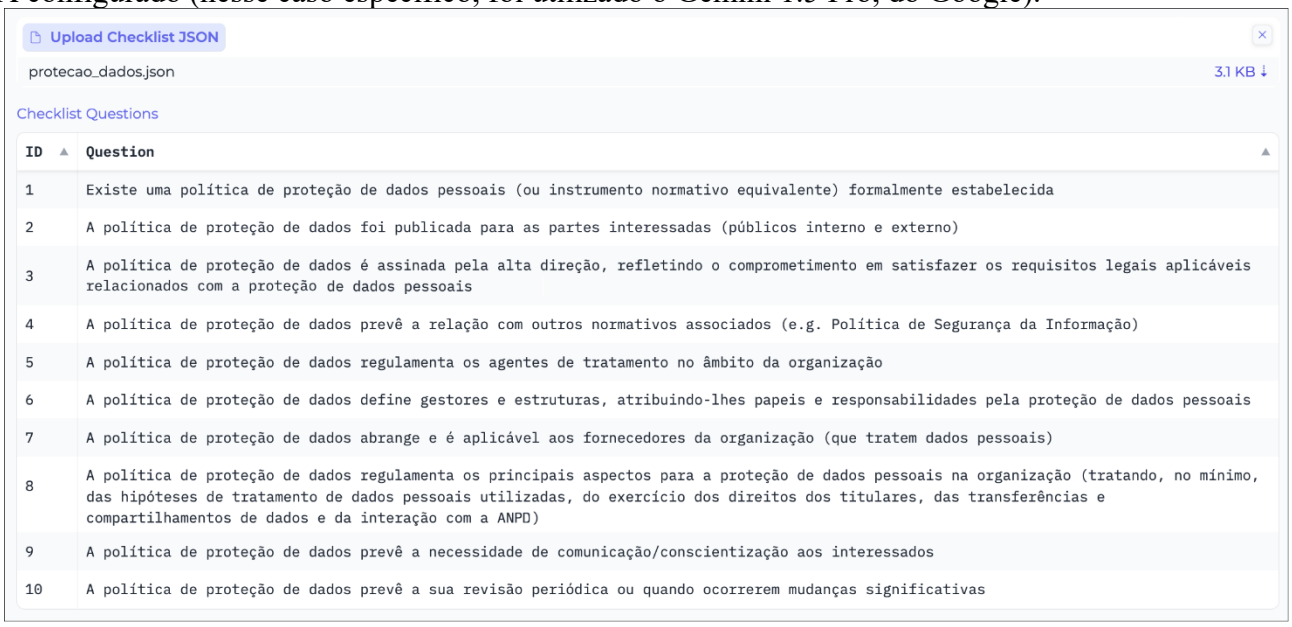
Este *checklist* para verificação de POLÍTICA DE PRIVACIDADE foi definido conforme as exigências previstas na LGPD.

#	**Verificar se**	**S/N**	**Observações/ evidências**
1	Existe uma política de privacidade (ou instrumento equivalente) estabelecida		
2	A política de privacidade foi publicada para as partes interessadas (públicos interno e externo)		
3	A política de privacidade informa o titular de dados sobre os princípios aplicáveis ao tratamento de dados pessoais		
4	A política de privacidade fornece informações sobre o controlador, o operador e o encarregado		
5	A política de privacidade informa como se dá a custódia de dados pessoais		
6	A política de privacidade informa sobre como o titular de dados pode obter as informações previstas no art. 18 da LGPD, quando aplicáveis		
7	A política de privacidade informa sobre como o titular de dados pode exercer seus direitos		
8	A política de privacidade informa quais são as hipóteses em que, no exercício de suas competências, a organização realiza o tratamento de dados pessoais		
9	A política de privacidade fornece informações claras sobre a previsão legal, a finalidade, as informações de contato do controlador, os procedimentos e as práticas utilizadas no tratamento de dados		
10	A política de privacidade fornece informações acerca do uso compartilhado de dados pelo controlador e sua finalidade		
11	A política de privacidade informa a data de sua última atualização		

Apêndice I – Análise de evidências com uso de IA (GabiChecks)

O GabiChecks é uma ferramenta automatizada para verificação de documentos, desenvolvida pelo auditor Fernando Lima Gama Júnior, a qual utiliza inteligência artificial (IA) para automatizar a verificação de conformidade em documentos no formato *Portable Document Format* (PDF), podendo ser utilizada em processos de auditoria. Essa ferramenta se propõe a solucionar a ineficiência e a propensão a erros inerentes à análise humana de grandes volumes de documentos, buscando garantir a aderência a normas e a regulamentações, aumentar a precisão dos resultados das análises e possibilitar, quando necessário, a avaliação de todo o universo de documentos auditados.

O processo de funcionamento do GabiChecks se inicia com a inserção, no sistema, dos documentos no formato PDF, a partir dos quais os respectivos textos das páginas são extraídos. Em seguida, esses textos são processados em conjunto com um arquivo *JavaScript Object Notation* (JSON) contendo os parâmetros do *checklist* de auditoria predefinido (Figura 16), com base no qual a ferramenta realiza a geração automática de perguntas (*prompts*), as quais são enviadas ao modelo de IA configurado (nesse caso específico, foi utilizado o Gemini 1.5 Pro, do Google).


Upload Checklist JSON

protecao_dados.json 3.1 KB

Checklist Questions

ID	Question
1	Existe uma política de proteção de dados pessoais (ou instrumento normativo equivalente) formalmente estabelecida
2	A política de proteção de dados foi publicada para as partes interessadas (públicos interno e externo)
3	A política de proteção de dados é assinada pela alta direção, refletindo o comprometimento em satisfazer os requisitos legais aplicáveis relacionados com a proteção de dados pessoais
4	A política de proteção de dados prevê a relação com outros normativos associados (e.g. Política de Segurança da Informação)
5	A política de proteção de dados regulamenta os agentes de tratamento no âmbito da organização
6	A política de proteção de dados define gestores e estruturas, atribuindo-lhes papeis e responsabilidades pela proteção de dados pessoais
7	A política de proteção de dados abrange e é aplicável aos fornecedores da organização (que tratem dados pessoais)
8	A política de proteção de dados regulamenta os principais aspectos para a proteção de dados pessoais na organização (tratando, no mínimo, das hipóteses de tratamento de dados pessoais utilizadas, do exercício dos direitos dos titulares, das transferências e compartilhamentos de dados e da interação com a ANPD)
9	A política de proteção de dados prevê a necessidade de comunicação/conscientização aos interessados
10	A política de proteção de dados prevê a sua revisão periódica ou quando ocorrerem mudanças significativas

Figura 16 - Arquivo JSON contendo os parâmetros do *checklist* para avaliação dos documentos PDF.
(Fonte: elaboração própria [ver **Apêndice G** – *Checklist* para verificação de Política de Proteção de Dados Pessoais])

O modelo de IA, então, analisa o conteúdo de cada um dos documentos PDF e fornece, de forma automatizada, as respostas às perguntas de cada um dos itens do *checklist* predefinido, as quais, em seguida, são salvas em um banco de dados e compiladas em relatórios detalhados e individualizados, contendo, cada um, a análise do documento PDF correspondente de acordo com as perguntas do *checklist* fornecido.

Cada um desses relatórios incluem, para cada pergunta do *checklist* (campo "*question*"), a respectiva resposta de acordo com o padrão solicitado (campo "*answer*", contendo "1" para "Sim" e "0" para "Não"), as evidências encontradas no documento caso a resposta seja "Sim" ou a sinalização de sua ausência caso a resposta seja "Não" (campo "*evidence*"), além de breves justificativas para o fato de o modelo ter considerado aquela resposta para aquele item de verificação, permitindo, assim, a rastreabilidade e a revisão posterior pelos auditores (campo "*justification*") [Figura 17].

Processed Answers

Filename	ID	Question	answer	evidence	justification
ANA	1	Existe uma política de proteção de dados pessoais (ou instrumento normativo equivalente) formalmente estabelecida	1	O próprio documento em questão, intitulado Aviso de Privacidade, atualizado em fevereiro de 2023, configura a política de proteção de dados da ANA (Agência Nacional de Águas e Saneamento Básico).	O documento apresentado detalha as práticas da ANA em relação à coleta, armazenamento, tratamento e compartilhamento de dados pessoais, demonstrando o compromisso da agência com a transparência e o respeito à privacidade de seus usuários. Adicionalmente, o documento cita a legislação brasileira relevante, incluindo a Lei Geral de Proteção de Dados (LGPD), indicando a conformidade da ANA com a regulamentação vigente. Embora o nome do documento seja Aviso de Privacidade, seu conteúdo abrange todos os aspectos essenciais de uma política de proteção de dados completa, configurando-se como tal.
ANA	2	A política de proteção de dados foi publicada para as partes interessadas (públicos interno e externo)	0	Não há menção explícita no documento sobre a publicação da política para as partes interessadas.	O texto apresentado descreve o Aviso de Privacidade da ANA, detalhando os tipos de dados coletados, como são utilizados, protegidos e os direitos dos titulares. Apesar de ser um documento público por estar disponível, não há nenhuma menção explícita afirmando que este aviso foi publicado ou distribuído para seus públicos interno e externo como uma política de proteção de dados.
ANA	3	A política de proteção de dados é assinada pela alta direção, refletindo o comprometimento em satisfazer os requisitos legais	0	Não foi possível encontrar tal informação no documento fornecido.	O texto apresentado descreve o Aviso de Privacidade da Agência Nacional de Águas e Saneamento Básico (ANA). Apesar de mencionar a importância da proteção de dados e detalhar os procedimentos relacionados a este tema, o documento não menciona se a política de proteção de dados é assinada pela alta direção ou apresenta qualquer informação similar que indique

JSON file '/private/var/folders/f7/c32nbgc516lfp9xm0zcjclj80000gn/T/gradio/0dd3cd821d236239fd28d141d7f75cc7f4ba2525a0ee50de0f55e8aee5e8fc79/protecao_dados.json' loaded successfully.

Figura 17 - Exemplo do banco de dados gerado a partir da execução da ferramenta GabiChecks.
(Fonte: elaboração própria)

A aplicação do GabiChecks nesta auditoria apresentou diversas vantagens em relação à alternativa de análise humana e não automatizada dessas evidências. A automatização da verificação de conformidade por meio do processamento simultâneo de múltiplos arquivos e da análise de dados com base em *checklists* predefinidos permitiu otimizar enormemente o tempo e os recursos alocados para a fiscalização. Caso não tivesse feito uso dessa solução de IA, certamente a equipe não teria tido condições de analisar a quantidade de documentos que a utilização do GabiChecks permitiu, tendo que, necessariamente, selecionar para análise uma amostra reduzida dos documentos em questão.

No caso, o uso do GabiChecks possibilitou a rápida verificação dos documentos submetidos, além de ter gerado relatórios detalhados, os quais ofereceram uma visão mais abrangente do processo de auditoria, facilitaram a identificação de possíveis falhas e permitiram que os auditores, então, direcionassem seus esforços para áreas de maior risco. A partir do banco de dados criado pela ferramenta, também foi possível, de modo facilitado, sistematizar as respostas dessas análises.

Tendo em vista que a realização de cada verificação, naturalmente, possui um custo associado (devido à utilização do modelo de IA do Google) e que o desenvolvimento do GabiChecks ainda se encontra em fase experimental, considerou-se suficiente, para os fins pretendidos nesta auditoria, a análise de uma amostra aleatória de 145 documentos, cerca de um terço do total. Em todo caso, frisa-se que, apesar de não ser desprezível, esse custo de utilização da ferramenta ainda representa uma pequena fração do custo que derivaria da análise manual pelos auditores da equipe.

Também é importante destacar que, quando se faz uso de uma ferramenta automatizada como é o caso do GabiChecks, os auditores precisam estar cientes das restrições envolvidas e, consequentemente, devem estabelecer procedimentos para mitigar os riscos relacionados à confiabilidade das análises realizadas. Para tanto, aspectos cruciais são a qualidade dos dados de entrada fornecidos ao sistema, o quanto o modelo de IA configurado é capaz de compreender nuances de linguagem e interpretar normas e o quanto os algoritmos desse modelo estão sujeitos à ocorrência de vieses, pois todos esses fatores podem comprometer a precisão das análises resultantes.

Os auditores, então, precisaram definir critérios de aceitabilidade dos riscos envolvidos em relação às informações geradas pelo GabiChecks. Para isso, utilizaram métodos como a revisão amostral dos resultados e, principalmente, o seu julgamento profissional para validar as conclusões obtidas por meio da ferramenta, à medida que o seu desenvolvimento era aperfeiçoado. Em todo caso, tendo em vista que a realização dessas análises não possuía nenhum objetivo sancionatório em relação às organizações envolvidas, tal questão não foi considerada como uma limitação da auditoria.

Por fim, é crucial destacar que qualquer ferramenta automatizada, por melhor e mais bem configurada que seja, dificilmente será capaz de substituir à altura a análise crítica e a tomada de decisão por parte dos auditores. Portanto, a revisão das respostas, das evidências e das justificativas

fornecidas pelo GabiChecks se mostraram fundamentais para garantir a qualidade e a confiabilidade do processo de auditoria.

Em suma, o GabiChecks foi considerado uma ferramenta valiosa para auditores que buscam otimizar o processo de verificação de conformidade em documentos, com potencial para gerar ganhos significativos em termos de produtividade e de redução de custos. A capacidade de processar grandes volumes de documentos em tempo reduzido pode diminuir a necessidade de formação de grandes equipes para lidar com demandas extensas, otimizando o uso de recursos em auditorias e acelerando a entrega de resultados, bem como sua precisão.

Embora a ferramenta não seja capaz de eliminar totalmente a necessidade de supervisão e de julgamento profissional, a automação proporcionada pelo GabiChecks certamente liberou os auditores para que estes pudessem se dedicar a análises mais complexas, à gestão de riscos e à tomada de decisões estratégicas, elevando a eficiência e a qualidade do processo de auditoria como um todo.

Apêndice J – Listas de Siglas, de Figuras e de Tabelas

Lista de Siglas

ABNT	Associação Brasileira de Normas Técnicas
AECI	Assessoria Especial de Controle Interno
ANPD	Autoridade Nacional de Proteção de Dados
APDP/MP	Autoridade Nacional de Proteção de Dados do Ministério Público
APF	Administração Pública Federal
Atricon	Associação dos Membros dos Tribunais de Contas do Brasil
AudGovernança	Unidade de Auditoria Especializada em Governança e Inovação
AudTI	Unidade de Auditoria Especializada em Tecnologia da Informação
AUFC	Auditor Federal de Controle Externo
BI	*Business Intelligence*
CCGD	Comitê Central de Governança de Dados
CD	Conselho Diretor [da ANPD]
CDC	Código de Defesa do Consumidor (Lei 8.078/1990)
CGU	Controladoria-Geral da União
CLT	Consolidação das Leis do Trabalho (Decreto-Lei 5.452/1943)
CNJ	Conselho Nacional de Justiça
CNMP	Conselho Nacional do Ministério Público
Confe	Conselho Federal de Estatística
CPAMP	Comissão de Preservação da Autonomia do Ministério Público
CSA	*Control Self-Assessment* (Autoavaliação de Controles Internos)
DOU	Diário Oficial da União
DPO	*Data Protection Officer* (encarregado pelo tratamento de dados pessoais)
DPU	Defensoria Pública da União
Embratur	Agência Brasileira de Promoção Internacional do Turismo
ENSEC-PJ	Estratégia Nacional de Segurança Cibernética do Poder Judiciário
ESMPU	Escola Superior do MPU
FNAS	Fundo Nacional de Assistência Social
FUNAG	Fundação Alexandre de Gusmão
FUNASA	Fundação Nacional de Saúde
GSI	Gabinete de Segurança Institucional [da PR]
HFA	Hospital das Forças Armadas
IA	inteligência artificial
iCap	subindicador [do iLGPD] relativo à dimensão “Capacitação”
iComp	subindicador [do iLGPD] relativo à dimensão “Compartilhamento de Dados Pessoais”
iConf	subindicador [do iLGPD] relativo à dimensão “Conformidade do Tratamento”
iDir	subindicador [do iLGPD] relativo à dimensão “Direitos do Titular”
IEC	*International Electrotechnical Commission*
IFS	Instituto Federal de Educação, Ciência e Tecnologia de Sergipe
iLGPD	indicador de adequação à LGPD
iLid	subindicador [do iLGPD] relativo à dimensão “Liderança”
IN	Instrução Normativa
iOrg	subindicador [do iLGPD] relativo à dimensão “Contexto Organizacional”
iPrep	subindicador [do iLGPD] relativo à dimensão “Preparação”
iProt	subindicador [do iLGPD] relativo à dimensão “Medidas de Proteção”
IRB	Instituto Rui Barbosa
iResp	subindicador [do iLGPD] relativo à dimensão “Violação de Dados Pessoais”

ISO	*International Organization for Standardization*
ISSAI	*International Standards of Supreme Audit Institutions* (Normas Internacionais das Entidades Fiscalizadoras Superiores)
LAI	Lei de Acesso à Informação (Lei 12.527/2011)
LGPD	Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018)
MDS	Ministério do Desenvolvimento e Assistência Social, Família e Combate à Fome
MGI	Ministério da Gestão e da Inovação em Serviços Públicos
MME	Ministério de Minas e Energia
MP(U)	Ministério Público (da União)
NAT	Normas de Auditoria do TCU
NBR	Norma Técnica Brasileira
NT	Nota Técnica
OGS	Órgão Governante Superior
PAT	Plano Anual de Trabalho [da Rede Integrar]
PCI	Política de Classificação da Informação
PD	Proteção de Dados [Pessoais]
PPDP	Política de Proteção de Dados Pessoais
PPSI	Programa de Privacidade e Segurança da Informação
PPT	pessoas, processos e tecnologia
PR	Presidência da República
PSI	Política de Segurança da Informação
RIPD	Relatório de Impacto à Proteção de Dados Pessoais
Segecex	Secretaria-Geral de Controle Externo
Senai/DN	Serviço Nacional de Aprendizagem Industrial - Departamento Nacional
Senat/CN	Serviço Nacional de Aprendizagem do Transporte - Conselho Nacional
Sesi/DN	Serviço Social da Indústria - Departamento Nacional
Sest	Secretaria de Coordenação e Governança das Empresas Estatais [do MGI]
Sest/CN	Serviço Social do Transporte - Conselho Nacional
SGD	Secretaria de Governo Digital [do MGI]
Sisp	Sistema de Administração dos Recursos de Tecnologia da Informação
TCE	Tribunal de Contas Estadual
TCU	Tribunal de Contas da União
TI(C)	tecnologia da informação (e comunicações)
UEPDAP	Unidade Especial de Proteção de Dados Pessoais
UFFS	Universidade Federal da Fronteira Sul
UFPI	Fundação Universidade Federal do Piauí
USB	*Universal Serial Bus* (Porta Serial Universal)

Lista de Figuras

Lista de Tabelas

APÊNDICE A - Matriz de Achados

DESCRIÇÃO DO ACHADO	SITUAÇÃO ENCONTRADA	OBJETOS	CRITÉRIO	EVIDÊNCIA	CAUSA	EFEITO	ENCAMINHAMENTO
F/I - Ausência de PSI, de nomeação do DPO e de comunicação padronizada à ANPD	- 80 organizações (peça 918) que não formalizaram uma Política de Segurança da Informação, em afronta ao disposto no Decreto 9.637/2018, art. 15, inciso II, c/c a Instrução Normativa GSI/PR 1/2020, art. 9º, bem como na Resolução - CNJ 396/2021, art. 19, inciso II, e na Resolução - CNMP 156/2016, art. 22, inciso III; - 48 organizações (peça 919) que não nomearam o encarregado pelo tratamento de dados pessoais, em afronta ao disposto na Lei 13.709/2018, art. 41, caput; - 250 organizações (peça 920) que não padronizaram a comunicação à ANPD e aos titulares de dados da ocorrência de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares, em afronta ao disposto na Lei 13.709/2018, art. 48, caput.	Base de Dados - Base de dados extraída da ferramenta LimeSurvey	Decreto 9637/2018, art. 15, inciso 2º Instrução Normativa 1/2020, Gabinete de Segurança Institucional da Presidência da República (GSI/PR), art. 9º Lei 13709/2018, art. 41; art. 48 Resolução 396/2021, Conselho Nacional de Justiça (CNJ), art. 19, inciso 2º Resolução 156/2016, Conselho Nacional do Ministério Público	Evidência sem referência	O questionário solicitou que os respondentes fornecessem, no respectivo campo de comentário, mais detalhes sobre alguns dos itens que marcassem. Tendo em vista que este achado se refere a itens das questões 4.1 (formalização da PSI e nomeação do DPO) e 9.1 (comunicação à ANPD) que não foram marcados pelos gestores, consequentemente eles não possuem justificativas associadas por parte dos respondentes.	A PSI é o documento basilar que norteia a abordagem de alto nível da organização para gerenciar os objetivos relacionados à segurança da informação. Sua ausência, portanto, prejudica sobremaneira o atingimento desse propósito. A falta de nomeação do encarregado pelo tratamento de dados pessoais priva o órgão/entidade de alguém cuja missão está diretamente relacionada à implementação da LGPD, o que contribuiria para alavancar as	Dar ciência Dar ciência Dar ciência

DESCRIÇÃO DO ACHADO	SITUAÇÃO ENCONTRADA	OBJETOS	CRITÉRIO	EVIDÊNCIA	CAUSA	EFEITO	ENCAMINHAMENTO
			(CNMP), art. 22, inciso 3º			iniciativas nesse sentido. Além disso, também faz com que a organização não mantenha um canal de comunicação efetivo com a ANPD e mesmo com os titulares dos dados. A ausência de processo padronizado de comunicação dos incidentes que possam acarretar risco ou dano relevante aos titulares de dados afeta negativamente alguns dos pilares nos quais se baseia a própria LGPD, a exemplo dos princípios da transparência (fornecimento de informações claras e precisas acerca dos tratamentos de	

DESCRIÇÃO DO ACHADO	SITUAÇÃO ENCONTRADA	OBJETOS	CRITÉRIO	EVIDÊNCIA	CAUSA	EFEITO	ENCAMINHAMENTO
						dados) e da prevenção (adoção de medidas para prevenir a ocorrência de danos em virtude desses tratamentos) [Lei 13.709/2018, art. 6º, incisos VI e VIII].	

Notas de fim

[1] Disponível em: <https://portal.tcu.gov.br/data/files/41/A2/F4/D5/2F8BA8108DD885A8F18818A8/Avaliacao%20sobre%20a%20LGPD.pdf>. Acesso em: 28/1/2025.

[2] Disponível em: <https://redeintegrar.irbcontas.org.br>. Acesso em: 28/1/2025.

[3] Disponível em: <https://redeintegrar.irbcontas.org.br/wp-content/uploads/2024/01/PLANO_ANUAL_DE_TRABALHO_2024.pdf>. Acesso em: 28/1/2025.

[4] Disponível em: <https://portal.tcu.gov.br/data/files/80/04/47/3A/C1DEF610F5680BF6F18818A8/ISSAI_100_principios_fundamentais_auditoria_setor_publico.pdf>. Acesso em: 28/1/2025.

[5] Disponível em: <https://portal.tcu.gov.br/fiscalizacao-de-tecnologia-da-informacao/atuacao/fiscalizacoes/auditoria-sobre-lgpd>. Acesso em: 4/10/2024.

[6] Disponível em: <https://www.in.gov.br/en/web/dou/-/instrucao-normativa-sgd/me-n-117-de-19-de-novembro-de-2020-289515596>. Acesso em: 28/1/2025.

[7] Disponível em: <https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-5-de-30-de-agosto-de-2021-341649684>. Acesso em: 28/1/2025.

[8] Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024>. Acesso em: 28/1/2025.

[9] Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf>. Acesso em: 28/1/2025.

[10] Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 28/1/2025.

[11] Disponível em: <https://portal.tcu.gov.br/data/files/2C/64/E1/89/408BC710D79E7EB7F18818A8/QuestionarioLGPDVPublicacao%20_1_.pdf>. Acesso em: 28/1/2025.

[12] Disponível em: <https://www.gov.br/gsi/pt-br/ssic/legislacao/copy_of_IN01_consolidada.pdf>. Acesso em: 28/1/2025.

[13] Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3975>, <https://atos.cnj.jus.br/files/original122608202109246l4dc3e072cca.pdf>. Acesso em: 28/1/2025.

[14] Disponível em: <https://www.cnmp.mp.br/portal/images/Normas/Resolucoes/RESOLUO_156.pdf>. Acesso em: 28/1/2025.

[15] Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-normativa-cgu-n-71-de-10-de-abril-de-2023-477406468>. Acesso em: 28/1/2025.

[16] Disponível em: <https://www.gov.br/acessoainformacao/pt-br/entendimentos-e-estudos-sobre-a-lai/copy_of_parecerfinalsobreacessoinformao_cgu_fev2023.pdf>. Acesso em: 28/1/2025.

[17] Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/regulamentacoes-da-anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022>. Acesso em: 28/1/2025.

[18] Disponível em: <https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd>. Acesso em: 28/1/2025.

[19] Disponível em: <https://www.serpro.gov.br/lgpd/noticias/2019/elabora-politica-privacidade-aderente-lgpd-dados-pessoais>. Acesso em: 28/1/2025.

[20] Disponível em: <https://repositorio.cgu.gov.br/handle/1/33409>. Acesso em: 28/1/2025.

[21] Disponível em: <https://repositorio.cgu.gov.br/handle/1/44989>. Acesso em: 28/1/2025.

[22] Disponível em: <https://www.poder360.com.br/opiniao/mau-uso-da-lgpd-cria-apagao-de-prestacoes-de-contas-de-convenios>. Acesso em: 28/1/2025.

[23] Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-11-de-27-de-dezembro-de-2023-534947737>. Acesso em: 28/1/2025.

[24] Disponível em: <https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/sisp/sobre-o-sisp/orgaos-do-sisp>. Acesso em: 28/1/2025.

[25] Disponível em: <https://www.cnmp.mp.br/portal/images/CALJ/resolucoes/Resoluo-n-281-de-2023-com-anexo.pdf>. Acesso em: 28/1/2025.

[xxvi] Iniciativa para avaliar o nível de adesão das organizações públicas federais em relação às práticas ESG (*Environmental, Social and Governance*). Disponível em: <https://iesgo.tcu.gov.br>. Acesso em: 28/1/2025.