Universidade de Brasília

Faculdade de Economia, Administração,Contabilidade e Gestão de Políticas Públicas

Departamento de Administração

BRENDA GOMES DOS SANTOS

ALINHAMENTO DE ORGANIZAÇÕES DO PODER EXECUTIVO FEDERAL ÀS MEDIDAS DE PROTEÇÃO E PREVENÇÃO CONTRA A VIOLAÇÃO DE DADOS PESSOAIS: análise baseada em relatórios emitidos em atendimento ao Tribunal de Contas da União

Brasília – DF

2025

BRENDA GOMES DOS SANTOS

ALINHAMENTO DE ORGANIZAÇÕES DO PODER EXECUTIVO FEDERAL ÀS MEDIDAS DE PROTEÇÃO E PREVENÇÃO CONTRA A VIOLAÇÃO DE DADOS PESSOAIS: análise baseada em relatórios emitidos em atendimento ao Tribunal de Contas da União

Monografia apresentada ao Departamento de Administração como requisito parcial à obtenção do título de Bacharel em Administração.

Professor Orientador: Dr. Carlos André de Melo Alves

Brasília – DF

2025

BRENDA GOMES DOS SANTOS

ALINHAMENTO DE ORGANIZAÇÕES DO PODER EXECUTIVO FEDERAL ÀS MEDIDAS DE PROTEÇÃO E PREVENÇÃO CONTRA A VIOLAÇÃO DE DADOS PESSOAIS: análise baseada em relatórios emitidos em atendimento ao Tribunal de Contas da União

A Comissão Examinadora, abaixo identificada, aprova o Trabalho de Conclusão do Curso de Administração da Universidade de Brasília da aluna BRENDA GOMES DOS SANTOS

Dr. Carlos André de Melo Alves
Professor-Orientador

Mestra, Olinda Maria Gomes Lesses,
Professora-Examinadora

Doutor,Welandro Damasceno Ramalho
Professor-Examinador

Brasília, 19 de fevereiro de 2025

Sinto-me vitoriosa pois, mesmo com as dificuldades e a rotina diária que envolve trabalhar, praticar exercícios físicos e as responsabilidades domésticas, cheguei até este estágio de desenvolvimento deste trabalho. Agradeço ao meu namorado por ser compreensivel e saber que durante esse período precisei concentrar muito do meu tempo livre no desenvolvimento deste TCC. Gratidão a minha mãe e a minha irmã, que sempre estiveram ao meu lado, incondicionalmente, em todas as circunstâncias e ao meu orientador Prof. Carlos André pela paciência e os ensinamentos

RESUMO

A proteção de dados pessoais é um assunto de interesse na atualidade de entidades de diferentes setores, inclusive as do setor público. Sem prejuízo da atuação da Agência Nacional de Proteção de Dados (ANPD) como regulador setorial sobre o tema, cabe ao Tribunal de Contas da União (TCU), na execução de suas atividades de controle externo, auditar a conformidade das entidades públicas federais custeadas pela União (inclusive aquelas integrantes do Poder Executivo Federal) às diretrizes estabelecidas pela Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD). O objetivo geral deste estudo é analisar o grau de alinhamento das entidades do poder executivo federal às medidas de proteção e prevenção contra a violação de dados pessoais, com base em questões dos relatórios de feedback emitidos em atendimento ao TCU. A pesquisa é descritiva com abordagem predominantemente quantitativa. A população contemplou 382 entidades públicas federais que se sujeitaram a Auditoria do TCU. A amostra não probabilística correspondeu a 24 entidades que disponibilizaram publicamente seus relatórios de feedback com as respostas dadas ao TCU. A coleta dos dados priorizou os referidos relatórios de feedback, especialmente as questões 9.1 a 9.5 (medidas contra violação de dados pessoais) e 10.1 a 10.5 (medidas de proteção de dados pessoais). O tratamento dos dados empregou estatística descritiva. Os resultados indicaram alinhamento a 30,8% das respostas sobre as medidas contra violação de dados pessoais e a 22,5% das respostas sobre as medidas de proteção de dados pessoais. Constatou-se, também, que 28,6% dos órgãos do Poder Executivo, 36,0% das Autarquias e 25,7% das outras entidades da amostra exibiram respostas alinhadas às medidas contra violação de dados pessoais, e 37,1% dos órgãos do Poder Executivo, 18,0% das Autarquias e 14,3% das outras entidades da amostra citaram respostas alinhadas às medidas de proteção de dados pessoais. Em geral, constatou-se oportunidade para aprimorar o alinhamento das entidades da amostra às medidas indicadas. Os achados contribuem, também, para melhor entender iniciativas de entidades públicas relativas à proteção e à prevenção contra violação de dados pessoais no País.

Palavras-chave: Proteção de Dados Pessoais, Lei Geral de Proteção de Dados, Poder Executivo Federal, Controle Externo, Tribunal de Contas da União.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ANPD – Autoridade Nacional de Proteção de Dados

LGPD – Lei Geral de Proteção de Dados Pessoais

TCU – Tribunal de Contas da UniãoGDPR – General Data Protection Regulation (Regulamento Geral de Proteção de Dados, na União Europeia)

ONU – Organização das Nações Unidas

N/A – Não Aplicável

SUMÁRIO

1 INTRODUÇÃO

1.1 Contextualização

A proteção de dados emergiu como uma preocupação central na era digital, visto a vasta quantidade de informações pessoais circulando livremente na internet. Este conceito, conforme delineado pelo Solove em sua obra "*Understanding Privacy*" (2008), aborda a necessidade de salvaguardar a privacidade e a segurança dos dados dos indivíduos, diante da proliferação de tecnologias de informação e comunicação. (SOLOVE, 2018, n.p).

Em 1948, a proteção de dados foi abordada na Declaração Universal dos Direitos Humanos, no qual, foi descrito, no art. 12, que: “Ninguém será submetido a interferências arbitrárias em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataques à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques” (ONU, 1948).

Na Europa, o tema proteção de dados também é debatido. Em 2016, a União Europeia divulgou o Regulamento Geral de Proteção de Dados, do *inglês General Data Protection Regulation* – GDPR. Após essa publicação, o tema ganhou ênfase e esse movimento regulatório não apenas ampliou a conscientização sobre a importância da privacidade, mas também influenciou legislações em diversas partes do mundo, como a Lei Geral de Proteção de Dados (LGPD) no Brasil.

A LGPD foi sancionada em 14 de agosto de 2018, no entanto a lei passou a vigorar apenas em setembro de 2020. O órgão responsável por zelar pela proteção de dados pessoais e por regulamentar, implementar e fiscalizar o cumprimento da LGPD no Brasil é a ANPD. (ANPD, 2024).

Mesmo após a entrada em vigor da LGPD, houve casos no Brasil de vítimas que tiveram os dados invadidos. Sendo um deles considerado um mega vazamento, pois foram difundidos dados considerados sensíveis como CPF, nome completo, endereço e telefone, os mesmos foram divulgados pelo Ministério da Saúde (Silva, 2020).

Em vista do exposto, entendeu-se necessário promover a implementação de uma cultura de segurança da informação e proteção de dados pessoais na

Administração Pública Federal. Este contexto motivou o Tribunal de Contas da União - TCU a realizar uma auditoria, com o propósito de avaliar a conformidade das organizações públicas federais com a LGPD e a estruturação da ANPD (Tribunal de Contas da União, 2022).

1.2 Formulação do problema

É importante destacar que cabe ao TCU, como órgão responsável pelo controle externo, a função de auditar os órgãos financiados pela União no que diz respeito às medidas de proteção e prevenção contra a violação de dados pessoais. E, ainda, essa auditoria pode considerar relatórios de feedback gerados pelas organizações custeadas pela união para atender essa demanda de auditoria, inclusive aquelas organizações vinculadas ao Poder Executivo Federal. É adequado dizer, também, que a obrigação de responder o relatório de feedback independe de os respondentes serem órgãos integrantes do poder executivo, serem autarquias federais ou outras entidades federais.

Esses relatórios possuem questões exemplificadas no apêndice desse estudo, segmentadas nos itens 9 e 10, dispondo, respectivamente, sobre 'medidas contra violação de dados pessoais' e 'medidas de proteção de dados pessoais'. Por fim, é adequado indicar que as respostas dessas entidades públicas podem permitir uma análise do grau de alinhamento delas às referidas medidas contidas no relatório de feedback do TCU, o que dá a oportunidade para a realização de estudo empírico.

Diante desse cenário, considerando o que foi apresentado na contextualização e nesta seção, o problema de pesquisa proposto é o seguinte: **Qual é o grau de alinhamento das entidades do poder executivo federal às medidas de proteção e prevenção contra a violação de dados pessoais, com base em questões dos relatorios de feedback emitidos em atendimento ao Tribunal de Contas da União?**

1.3 Objetivo Geral

Analisar o grau de alinhamento das entidades do poder executivo federal às medidas de proteção e prevenção contra a violação de dados pessoais, com base em questões dos relatorios de feedback emitidos em atendimento ao Tribunal de Contas da União.

1.4 Objetivos Específicos

1 - Identificar o grau de alinhamento das medidas de proteção e prevenção contra a violação de dados pessoais segmentados por questões dos relatorios de feedback emitidos em atendimento ao Tribunal de Contas da União.

2 - Comparar o grau de alinhamento previamente identificado, considerando os órgãos do poder executivo, as autarquias federais e outras entidades federais.

1.5 Justificativas

A proteção de dados no Brasil, tornou-se um tema valorizado, inclusive no setor público. Pesquisas realizadas têm buscado evidenciar a importância, os benefícios e as punições da LGPD nos órgãos públicos, conforme pode ser observado na pesquisa de Saraiva e Brito (2020). No entanto, esse trabalho teve como objetivo principal avaliar o que deve ser feito em conformidade com a lei.

Numa perspectiva teórica, a presente pesquisa amplia os achados de pesquisa citada no parágrafo anterior, pois, ela permite a utilização de técnicas estatísticas diferenciadas de outras pesquisas e uma análise descritiva de dados obtidos em questões do relatório de feedback, permitindo apurar o que está sendo divulgado por orgãos públicos do Poder Executivo Federal.

Sob uma perspectiva prática, os resultados desta pesquisa podem beneficiar diversos atores, como, por exemplo, o próprio TCU e a ANPD, pois a pesquisa fornece, por meio de estatísticas descritivas, uma visão sobre os resultados dos itens 9 e 10 do relatório de feedback. Além disso, os órgãos públicos e seus gestores poderão identificar as áreas com maior necessidade de aprimoramento, permitindo a realização de treinamentos e investimentos adequados, dessa forma, evitando os gastos nas questões que estão sendo conduzidas corretamente.

Por fim, as pessoas interessadas no assunto proteção de dados em órgãos públicos’ poderão verificar se todos os órgãos e entidades incluídos na amostra desta pesquisa, estão cumprindo ou não as normas estabelecidas para proteção de dados pessoais. Além disso, poderão contribuir para reflexões que levem ao aprimoramento da prevenção e proteção de dados pessoais em organizações públicas.

2. REFERENCIAL TEÓRICO

2.1 Tratamento de Dados Pessoais – Histórico e Contexto Internacional

O processo de criação de leis gerais de proteção de dados evoluiu em diferentes gerações. Sabe-se que a proteção de dados tem sido um tema abordado desde o século XX, conforme pesquisa realizada por Lugati e Almeida (2020). O tema teve um aumento em sua remissão decorrente das evoluções tecnológicas, acompanhado da necessidade de serem criadas leis que regulamentem o tema citado. Em maio de 1973, a Suécia aprovou sua Lei de Proteção de Dados, a primeira norma em nível federal a tratar especificamente sobre proteção de dados. Não muito depois, em janeiro de 1977, a Alemanha também publicou uma lei referente à proteção de dados (Palhares, 2021).

Em 1995, foi criada a Diretiva 95/46/CE, da União Europeia, contendo o primeiro regulamento, trazendo conceitos de proteção de dados similares aos das legislações atuais (Brasil, 2024). Em 2018, entrou em vigor, substituindo a Diretiva 95/46/CE, o Regulamento Geral sobre Proteção de Dados, uma das primeiras consequências dessa regulação foi obrigar empresas como o Facebook e o Google a mudar a forma como coletam e tratam dados (Brasil, 2024).

Conforme as informações mencionadas, pode-se verificar que já era possível notar as movimentações em relação ao tema, pois os países foram enxergando a necessidade e a importância de leis específicas sobre a proteção de dados. No Brasil, é possível constatar leis que tangenciam o tema desde a Constituição de 1988, a qual, no artigo 5º, diz: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação” (Brasil, 1988).

Outro exemplo é o Código de Defesa do Consumidor, consubstanciado na Lei nº 8.078, de 11 de setembro de 1990, que estabelece diretrizes sobre o acesso e a correção de informações nos bancos de dados de consumidores. O artigo 43 da lei citada neste parágrafo, por exemplo, assegura que:

> [...] o consumidor [...] terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele. [...]

> Além disso, o artigo determina que essas informações devem ser "objetivas, claras, verdadeiras e em linguagem de fácil compreensão", não podendo conter "informações negativas referentes a período superior a cinco anos (Brasil, 1990).

Dando sequência às leis que mencionam a proteção de dados, a Lei Federal nº 9.296, de 1996, é um marco importante, pois a mesma, diz que “é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal” (Brasil, 1996). Ou seja, a lei aborda proteção para os meios de comunicação citados, dando poder apenas à justiça poder verificar o caso, e apenas para investigação criminal ou instrução processual penal.

Já no ano de 2013, foi implementado o Marco Civil da Internet, que se destacou como um ponto de partida importante principalmente para o sistema judiciário brasileiro compreender melhor a internet. A legislação menciona importantes conceitos como a neutralidade de rede, garantindo que todos os dados trafegados na internet sejam tratados de forma igualitária, sem discriminação ou preferência por conteúdo, origem, destino ou serviço. Além disso, o Marco Civil da Internet fortaleceu a liberdade de expressão, assegurando que os usuários possam se expressar livremente no ambiente digital, sem censura prévia (Brasil, 2014).

Vale mencionar também, por sua vez, que o Decreto nº 7.962, de 2013, acrescenta orientações importantes ao Código de Defesa do Consumidor, reforçando a proteção dos dados pessoais. O mesmo diz sobre a autodeterminação, privacidade, confidencialidade e segurança das informações de dados pessoais prestados ou coletados, garantindo que os consumidores tenham mais controle sobre suas informações. O decreto complementa a legislação existente, e fortalece a proteção, assegurando que as empresas adotem práticas responsáveis na gestão dos dados pessoais dos consumidores (Brasil, 2013).

Em 2018, entrou em vigor o Regulamento 679/2016, conhecido como GDPR (General Data Protection Regulation) ou RGPD (Regulamento Geral de Proteção de Dados). Aprovado pelo Parlamento Europeu em abril de 2016, sua aplicação efetiva teve início em 25 de maio de 2018, permitindo às empresas um período de adaptação

às novas exigências. Como regulamento, sua implementação é obrigatória em todos os países membros da União Europeia. (Comissão Europeia, 2024).

O Brasil, assim como diversos outros países, inspirou-se na GDPR europeia para a formulação de sua própria legislação de proteção de dados, a LGPD. Esta inspiração resultou em leis semelhantes, incluindo os benefícios e penalidades. A GDPR destaca a preocupação com situações de desequilíbrio entre o titular dos dados e o responsável pelo seu tratamento, particularmente quando este último é uma autoridade pública, buscando garantir que o tratamento de dados seja realizado de maneira justa e equitativa. (Vergili; Lima, 2020).

É possível que empresas públicas e privadas solicitem dados pessoais para realizar cadastros variados, desde os mais simples até os mais abrangentes, ou mesmo para permitir o acesso das pessoas e entidades a determinados conteúdos e sites. A GDPR europeia estabeleceu normas que devem ser seguidas por ambos os tipos de organizações. Isso permitiu que a tecnologia avançada fosse utilizada para proteger os dados tanto de pessoas físicas quanto jurídicas (Monteiro; Araújo, 2021).

Na GDPR, nos Artigos 2º e 3º, fica estabelecido que essa lei deve ser aplicada tanto a empresas públicas como privadas da União Europeia:

> Artigo 2º
>
> [...] 3. O Regulamento (CE) n.º 45/2001 aplica-se ao tratamento de dados pessoais pelas instituições, órgãos, organismos ou agências da União. O Regulamento (CE) n.º 45/2001, bem como outros atos jurídicos da União aplicáveis ao tratamento de dados pessoais, são adaptados aos princípios e regras do presente regulamento nos termos previstos no artigo 98.º
>
> Artigo 3º 1. O presente regulamento aplica-se ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União. (União Européia, 2001)

O GDPR traz comandos normativos que buscam assegurar que tanto organizações públicas quanto privadas estão sujeitas às normas de proteção de dados, contribuindo para dar uniformidade ao tratamento da proteção dos dados pessoais no âmbito da União Europeia.

Sendo assim, no ambiente contemporâneo, considerando que o setor de tecnologia é predominante em praticamente todas as atividades, ter leis que oferecem proteção e segurança se torna importante para a convivência, dando inclusive mais liberdade para que de fato, as pessoas possam realizar as tarefas do dia a dia. A proteção da fonte de onde a informação é obtida é uma regra que fortalece a liberdade de divulgação da informação, assegurando que os dados e informações sejam tratados de forma ética e responsável, conforme destacado por (Tavares, 2012)

Desde 1970, era realizada uma coleta de dados e a necessidade de implementar leis específicas para tratar esses dados já era uma demanda emergente. Nesse período citado era usado o sistemas de computação do tipo mainframe. Dessa forma, criaram as regras jurídicas que foram desenvolvidas tanto em nível europeu quanto na Alemanha. Dado que grandes quantidades de dados estavam sendo processadas nesses sistemas de forma sequencial, percebeu-se a necessidade de controlar os diversos passos do processamento de dados, incluindo a coleta, o armazenamento e o uso dessas informações. Assim, a atenção foi direcionada para a regulamentação de todas as etapas envolvidas no processamento de dados (Albers, 2017).

Conforme mencionado, pode-se entender que a Europa destaca-se mundialmente por seu desenvolvimento em diversas áreas, e a proteção de dados não é exceção. Desde cedo, o continente abordou e discutiu essa questão de maneira avançada. O Conselho Europeu, através da Convenção de Strasbourg de 1981, ofereceu uma definição ao tema. Nela, informação pessoal é descrita como “qualquer informação relativa a uma pessoa singular identificada ou suscetível de identificação.” Fica entendido, portanto, a forma de caracterizar determinada informação como pessoal: o fato de estar vinculada a uma pessoa, revelando algum aspecto objetivo desta.

Dessa forma, conforme apresentado, as leis tiveram fases e suas evoluções, e os cidadãos também foram se adequando a essas regulamentações. A proteção de dados é vista, por tais leis, como um processo complexo, que envolve a participação ativa do indivíduo na sociedade e considera o contexto em que seus dados são solicitados. Essas normas estabelecem meios de proteção para ocasiões em que a liberdade de decidir livremente é restringida (Doneda, 2011).

Sendo assim, diante da evolução tecnológica e o emprego de tecnologias que manipulavam os dados, tornou-se necessário aprimorar leis e regulamentações sobre a proteção de dados evoluir para poder acompanhar essa evolução. As referidas leis e regulamentações, entre elas a citada GDPR, podem, inclusive, contribuir para que as pessoas possam invocar a proteção de direitos específicos sobre seus dados pessoais. Medidas elaboradas pelo Estado podem ser contestadas por meio de recursos jurídicos adequados. Essa abordagem legal e regulatória assegura que o avanço tecnológico não comprometa os direitos fundamentais dos indivíduos, proporcionando um equilíbrio entre inovação e proteção dos dados pessoais (Albers, 2017).

Por fim, o setor público e o setor privado são responsáveis pela coleta de uma vasta quantidade de dados. Em virtude disso, ambos necessitam seguir as leis e regras sobre proteção de dados. A colaboração entre esses setores é essencial para a criação de comandos e técnicas normativas em setores suscetíveis à regulação, garantindo a proteção e a privacidade das informações pessoais coletadas (Zanatta, 2015). Dessa maneira, tanto o setor privado quanto o setor público respondem pela implementação e cumprimento das legislações e regulamentações de proteção de dados.

2.2 Proteção e Prevenção contra violação de dados pessoais no Brasil e no setor público

Diante das situações e das evoluções observadas e mencionadas tanto no Brasil quanto no Exterior, especialmente das leis mencionadas na Alemanha e da GDPR na União Europeia, no Brasil floresceu no legislativo iniciativa para formular uma lei especificamente para a proteção de dados. A citada ‘Lei Geral de Proteção de Dados Pessoais’ ou LGPD, está consubstanciada pela Lei nº 13.709/2018, tendo sido promulgada com o objetivo de proteger os direitos fundamentais de liberdade e privacidade, e também garantir a formação livre da personalidade de cada indivíduo. A lei aborda o tratamento de dados pessoais, no meio físico e digital, realizado por pessoas físicas ou jurídicas de direito público ou privado. Ela engloba um amplo conjunto de operações que podem ocorrer em formatos manuais ou digitais (Brasil, 2024).

O Artigo 1º da LGPD dispõe sobre o tratamento de dados pessoais em meios digitais. De acordo com esse artigo, o titular dos dados é responsável por autorizar explicitamente o uso de suas informações pessoais por uma entidade ou empresa, para que esses dados sejam inseridos no sistema de armazenamento, tanto por pessoas físicas quanto jurídicas de direito público ou privado (Monteiro; Araújo, 2021).

> [...] Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (Brasil, 2018)

Com base no referido Artigo 1º, fica entendido que a lei deve ser seguida por todos, pessoa física, pessoa jurídica e inclusive órgãos públicos. A LGPD traz consigo clara inspiração na GDPR europeia, que no caso, impõe medidas para infrações aos que não obedecem às suas normas, inclusive consequências operacionais para os que devem seguir a lei, no caso, tanto as empresas privadas quanto o governo.

Em adição, a LGPD dita os deveres para o tratar os dados pessoais, daqueles que permitem a identificação de um indivíduo, com o objetivo de garantir os direitos fundamentais à privacidade, à liberdade de expressão, de informação, de comunicação e de opinião (Almeida; Soares 2022), conforme previsto no Art. 2º da LGPD, citado na sequência.

> [...] Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
>
> I - O respeito à privacidade;
>
> II - A autodeterminação informativa;
>
> III - A liberdade de expressão, de informação, de comunicação e de opinião;
>
> IV - A inviolabilidade da intimidade, da honra e da imagem; O desenvolvimento econômico e tecnológico e a inovação;
>
> V - A livre iniciativa, a livre concorrência e a defesa do consumidor; e
>
> VI - Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (Brasil, 2018).

É adequado reiterar que os serviços digitais aumentaram no País. Segundo uma pesquisa realizada pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação, entre março e julho de 2023 foram coletados dados de 23.975 domicílios e 21.271 indivíduos. Em 2023, 73% dos usuários de Internet com 16 anos ou mais utilizaram serviços de governo eletrônico, tendo sido observado um crescimento de 8% em relação a 2022. Outra mudança foi no aumento de pagamentos no meio digital de impostos e taxas, entre 2021 e 2023, ou seja, as pessoas estão aumentando o uso de serviços digitais.

> [...] Os órgãos públicos vêm aumentando a oferta de serviços digitais, como mostra a pesquisa TIC Governo Eletrônico. O aumento verificado em 2023 do número de pessoas que acessaram serviços públicos pela Internet é algo positivo, tanto para os cidadãos quanto para os governos", comenta Fabio Storino, coordenador da TIC Domicílios.

Percentual (%)		Sim	Não	Não sabe	Não respondeu
TOTAL		84	16	0	0
ÁREA	Urbana	86	14	0	0
	Rural	74	26	0	0
REGIÃO	Sudeste	85	15	0	0
	Nordeste	80	20	0	0
	Sul	89	11	0	0
	Norte	79	21	0	0
	Centro-Oeste	87	11	1	1
RENDA FAMILIAR	Até 1 SM	70	29	0	0
	Mais de 1 SM até 2 SM	84	16	0	0
	Mais de 2 SM até 3 SM	93	7	0	0
	Mais de 3 SM até 5 SM	97	3	0	0
	Mais de 5 SM até 10 SM	98	2	0	0
	Mais de 10 SM	93	7	0	0
	Não tem renda	74	26	0	0
	Não sabe	84	15	1	0
	Não respondeu	85	15	0	0
CLASSE SOCIAL	A	98	2	0	0
	B	98	2	0	0
	C	91	9	0	0
	DE	67	33	0	0

Figura 1 - Domicílios com acesso à internet

Fonte: CGI.br/NIC.br

Dessa forma, ao observar o crescimento do meio digital para a utilização de plataformas, principalmente para a realização de serviços que englobam o setor público, verifica-se a importância da LGPD. Em adição, o artigo 46 da LGPD trata das

medidas de segurança que devem ser adotadas para proteger os dados pessoais, conforme descrito a seguir.

> [...] Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. (Brasil, 2018).

Vale salientar que o órgão fiscalizador da LGPD é a Autoridade Nacional de Proteção de Dados - ANPD. Segundo a definição dada pela própria ANPD:

> [...] a ANPD é uma autarquia de natureza especial, vinculada ao Ministério da Justiça e Segurança Pública, responsável por zelar pela proteção de dados pessoais e por regulamentar, implementar e fiscalizar o cumprimento da LGPD no Brasil. (Brasil, 2024).

A missão institucional da ANPD é assegurar a mais ampla e correta observância da LGPD no país e, nessa medida, garantir a devida proteção aos direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade dos indivíduos.

Vale destacar que o art. 55-J da LGPD, estabelece as principais competências da ANPD referentes a proteção de dados pessoais, dentre as quais se destacam as seguintes:

Quadro 1 - Art 55-J da LGPD

●Elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;
●Fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
●Promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;
●Estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis;

●Promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;
●Editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD;
●Ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento;
●Editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclararem startups ou empresas de inovação, possam adequar-se à Lei;
●Deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação da LGPD, as suas competências e os casos omissos;
●Articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e
●Implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com a LGPD.

Fonte: Brasil, 2018.

A literatura apresenta argumentos indicando que foi necessário atribuir a tarefa de fiscalização referente a proteção de dados pessoais não apenas ao Estado e aos seus gestores. A criação da ANPD, como uma nova entidade governamental, foi necessária para mediar, de forma independente, as tensões ainda pouco conhecidas pelo poder público, na ocasião de criação da LGPD. Destaca-se, portanto, a importância de fornecer conhecimento especializado aos responsáveis por assumir e desempenhar adequadamente essa função (Sarlet; Rodriguez 2022).

Conforme o artigo 55-C da LGPD, a ANPD é composta pelo Conselho Diretor, Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, Corregedoria, Ouvidoria, órgão de assessoramento jurídico próprio e unidades administrativas e especializadas.

Sem prejuízo da atuação da ANPD, é adequado lembrar, conforme citado na introdução, que as organizações públicas, especialmente aquelas custeadas pela União, estão sujeitas a serem auditadas pelo TCU. Dessa forma, o TCU pode elaborar pedidos para preenchimento de questionários sobre o cumprimento da LGPD de organizações públicas, bem como elaborar relatórios de feedback buscando inclusive fomentar o processo de fiscalização nas organizações auditadas que não estão cumprindo as normas estabelecidas pela LGPD, propondo, inclusive, melhorias ou recomendações no tocante ao cumprimento dessa legislação.

No decorrer do relatório de feedback elaborado pelo TCU, foram citados no Apêndice desse estudo as questões dos itens 9 e 10, que tratam, respectivamente, da 9 - Violação de Dados Pessoais e 10 - Medidas de Proteção, contêm cinco perguntas e cinco respostas cada, totalizando dez perguntas e dez respostas. Essas questões são particularmente importantes para o desenvolvimento da parte empírica deste estudo, cujo método de elaboração será melhor descrito no Capítulo 3 desta pesquisa.

3. MÉTODOS E TÉCNICAS DE PESQUISA

Este capítulo apresenta os métodos e técnicas utilizados para a produção da presente pesquisa. O capítulo está dividido em 4 subseções, que apresentam: a tiplolgia da pesquisa (3.1), caracterização das organizações ou setor objeto de estudo (3.2), população e amostra (3.3) e procedimentos de coleta e análise de dados (3.4).

3.1. Tipologia de pesquisa

A pesquisa é descritiva, conforme definido por Sampieri (2012), o qual a caracteriza como um tipo de pesquisa que busca especificar propriedades e características importantes de qualquer fenômeno que se analise. Do ponto de vista abordagem, trata-se de uma pesquisa predominantemente quantitativa, a qual consiste no uso de coleta de dados para testar hipóteses com base na medição numérica e na análise estatística para estabelecer padrões de comportamento. A abordagem do estudo predominante é a quantitativa, buscando-se apresentar frequencias e percentuais para evidenciar o atingimento dos objetivos da pesquisa.

3.2. Caracterização do setor objeto do estudo

O setor abordado nesta pesquisa engloba as organizações públicas. Segundo dados do TCU, especial atenção foram dadas àquelas que estão sob controle do Poder Executivo Federal, totalizando 382 organizações. Essas entidades estão sujeitas a adequação à LGPD e às medidas implementadas para atender às exigências estabelecidas pela legislação. Além disso, estão sujeitas a avaliação da ANPD referentes à estrutura organizacional, a condução de suas atribuições e a regulamentação de aspectos citados na LGPD (ACÓRDÃO Nº 1384, 2022).

3.3. População e amostra ou Participantes da pesquisa

A população desta pesquisa abrange as entidades presentes no relatório de feedback emitido pelo Tribunal de Contas da União (TCU) em 2022, que auditou 382 organizações públicas, conforme o Acórdão n° 1384/2022 – TCU – Plenário. Dentre

essas organizações, a amostra foi composta por 24 entidades que disponibilizaram publicamente seus relatórios de feedback, contendo as respostas fornecidas ao TCU.

Inicialmente, foi realizado uma análise documental no ACÓRDÃO Nº 1384, 2022 e nos relatórios de fedeback, posterialmente elaborado uma planilha contendo o nome das 382 organizações públicas auditadas, conforme a lista oficial divulgada pelo Tribunal de Contas da União. Em seguida, realizou-se uma busca detalhada nos sites institucionais de cada órgão para verificar a acessibilidade dos relatórios de feedback. Foram encontrados 40 relatórios publicados, que foram baixados, organizados e catalogados em uma nova planilha. Nessa etapa, também foram adicionadas informações complementares, como estado da sede de cada órgão, links de acesso aos documentos e a natureza jurídica de cada instituição (Poder Executivo, Poder Judiciário, Poder Legislativo, Autarquia Federal, Fundação Pública e outros).

Após a análise dos 40 relatórios inicialmente coletados, foi identificada a disponibilidade de relatórios abrangendo as questões abrangidas nos itens 9 e 10 dos relatórios do poder executivo, excluindo entidades do poder judiciário e do legislativo. Com isso, a amostra final foi definida em 24 organizações, descritas no Apêndice 1, abrangendo três grupos de entidades: órgãos do poder executivo federal, autarquias federais e outras entidades públicas federais (que incluem outras entidades da administração pública indireta).

3.4. Procedimentos de coleta e de análise de dados

A coleta de dados foi realizada por meio de pesquisa documental, considerando relatórios de feedback elaborados em atendimento ao pedido do TCU. Para realizar a coleta, foi necessário acessar o site de cada entidade da amostra e buscar os PDF dos relatórios de feedback. Esses relatórios abrangem questões respondidas pelas entidades.

O início do período a que se refere a solicitação do TCU para elaboração de relatórios de feedbacks foi outubro de 2020, conforme descrito no acordão 2.909/2020-tcu-plenário. A coleta de dados desses relatórios de feedbacks para o atigimento dos objetivos dessa pesquisa abrangeu o período de 08/02/2024 a 23/11/2024.

Neste estudo foram coletados dados de dez questões descritas conforme extrato do questionário citado no Anexo 1. Verificam-se neste apêndice cinco questões de 9.1 a 9.5, referentes medidas para prevenção contra a violação de dados pessoais e cinco questões de 10.1 a 10.5, relacionadas a medidas de proteção de dados pessoais. Considerando as 24 organizações da amostra, foi possível coletar 120 respostas vinculadas às questões 9.1 a 9.5 e outras 120 respostas vinculadas às questões 10.1 a 10.5. No total, foram coletadas 240 respostas.

Para análise de dados, nesta pesquisa, foi utilizada estatística descritiva, com o objetivo de organizar e interpretar os resultados, possibilitando uma melhor compreensão das medidas adotadas para proteção de dados pessoais e prevenção contra violações de dados pessoais.

Foram analisadas as respostas do relatório de feedback dadas para as questões referentes às medidas contra violação de dados pessoais (questões 9.1 a 9.5) categorizados como ‘sim’ ou ‘não’. Para as questões sobre medidas de proteção de dados pessoais, as respostas foram apuradas conforme segue: questões 10.1 e 10.5 foram categorizadas como ‘sim’ ou ‘não’, e as questões 10.2 a 10.4 foram categorizadas como ‘sim’, ‘não’ ou ‘parcialmente’.

Sobre o emprego da estatística descritiva, foram empregados procedimentos de contagem de frequências, cálculo de percentuais e elaboradas tabelas de contingência. Esses procedimentos permitiram comparar o alinhamento de medidas segundo as respostas de cada questão.

Quanto mais as frequências e percentuais dessas respostas enfatizaram a resposta ‘sim’, denotou-se neste estudo maior alinhamento às medidas previstas nas questões. Em oposição, quanto mais as frequências e percentuais dessas respostas enfatizaram a resposta ‘não’, denotou-se neste estudo menor alinhamento ao que dispunha sobre as medidas descritas nas questões.

Em adição, foi possível fazer comparações entre as citadas frequências e percentuais de resposta considerando as análises no tocante ao alinhamento das medidas por grupos de entidades da amostra segmentadas em ‘poder executivo’, ‘autarquia’ e ‘outras entidades’, aproveitando os dados citados na segunda coluna do Apêndice 1, dispondo sobre a amostra do estudo.

Por fim, a metodologia empregada permitiu uma análise dos dados coletados, assegurando que as informações obtidas estivessem alinhadas ao atingimento dos objetivos específicos da pesquisa. Para auxiliar a elaboração das análises dos dados foram empregadas planilha eletrônica e o software SPSS.

4. DESCRIÇÃO E ANÁLISE DOS RESULTADOS

Este capítulo apresenta uma descrição e análise dos resultados. Inicialmente, a Seção 4.1 dispõe sobre a identificação do grau de alinhamento das medidas de proteção e prevenção contra a violação de dados pessoais segmentados por questões dos relatorios de feedback emitidos em atendimento ao TCU. Em seguida, a Seção 4.2 apresenta uma comparação do referido grau de alinhamento, considerando os órgãos do poder executivo, as autarquias federais e outras entidades federais.

4.1 Identificação do grau de alinhamento segmentado por questão

Inicialmente, a Tabela 1 apresenta os resultados estatísticos para as respostas das questões 9.1 ao 9.5. Os enunciados de cada uma dessas questões constam do Anexo 1 deste estudo.

Tabela 1 - Resultados da identificação do grau de alinhamento (questões 9.1 a 9.5)

	Questão	**'Não' Freq. (%)**	**'Sim' Freq. (%)**	**'Total' Freq. (%)**
Medidas contra violação de dados pessoais	9.1	19 (79,2%)	5 (20,8%)	24 (100,0%)
	9.2	16 (66,7%)	8 (33,3%)	24 (100,%)
	9.3	17 (70,8%)	7 (29,2%)	24 (100,0%)
	9.4	14 (58,3%)	10 (41,7%)	24 (100,0%)
	9.5	17 (70,8%)	7 (29,2%)	24 (100,0%)
	Total	83 (69,2%)	37 (30,8%)	120 (100,0%)

Fonte: dados da pesquisa.

Legenda: ‘9.1’ a ‘9.5’ são as questões, cujos enunciados estão descritos no Anexo 1 deste estudo. ‘Freq.’ Indica a contagem de frequencia da resposta da questão. ‘(%)’ indica o percentual de respostas da contagem de frequencia, com relação ao total de 24 respostas.

No item 9.1, sobre a existência de um plano de resposta a incidentes, a Tabela 1 exibe 79,2% das organizações afirmaram não possuir um documento formalizado para lidar com violações, enquanto apenas 20,8% declararam contar com esse recurso. A ausência desse planejamento pode comprometer a capacidade de reação a ataques e falhas, aumentando a vulnerabilidade das instituições diante de incidentes de segurança.

O item 9.2 trata da existência de um sistema para registrar incidentes de segurança envolvendo dados pessoais. Segundo a Tabela 1, apenas 33,3% das organizações afirmaram possuir esse controle, enquanto 66,7% não têm um sistema estruturado. Isso dificulta a identificação de recorrências em ataques cibernéticos, acessos não autorizados e vazamentos de dados, comprometendo a prevenção e resposta a incidentes.

No item 9.3, que avalia o registro das ações adotadas para solucionar incidentes, a Tabela 1 mostra que apenas 29,2% das organizações relataram documentar essas medidas, enquanto 70,8% não documenta. A ausência de registro de ações pode prejudicar a transparência e a melhoria contínua dos processos internos de segurança. Sem um histórico detalhado, torna-se mais difícil avaliar a eficácia das respostas adotadas e implementar correções para evitar reincidências.

O item 9.4 refere-se ao monitoramento de eventos suspeitos, que permite detectar ameaças antes que causem danos. Conforme a Tabela 1, cerca de 41,7% das entidades da amostra indicaram que realizam essa medida, enquanto 58,3% evidenciaram que não adotam essa medida. A falta de monitoramento contínuo pode facilitar a ocorrência de incidentes e comprometer a integridade das informações armazenadas.

Já o item 9.5 aborda a comunicação de violações à ANPD e aos titulares, uma exigência da LGPD. Apesar dessa obrigatoriedade, a Tabela 1 mostra que 70,8% das organizações indicaram que ainda não possuem diretrizes claras para esse processo, o que pode gerar penalizações e afetar a credibilidade institucional. Apenas 29,2% das instituições relataram seguir protocolos para essa comunicação.

No total, conforme os resultados exibidos na Tabela 1, 69,2% das respostas indicam que medidas avaliadas ainda não são adotadas, enquanto 30,8% dessas respostas indicam que as medidas foram implementadas. De maneira geral, as evidências indicam existir oportunidade para que as entidades da amostra busquem maior alinhamento às medidas contra violação de dados pessoais.

A Tabela 2 apresenta os resultados estatísticos para as respostas das questões 10.1 a 10.5. Os enunciados de cada uma dessas questões constam do Anexo 1 deste estudo, com base nas respostas das entidades da amostra ao TCU.

Tabela 2 - Resultados da identificação do grau de alinhamento (questões 10.1 a 10.5)

	Questão	**'Não' Freq. (%)**	**'Parcialmente' Freq. (%)**	**'Sim' Freq. (%)**	**'Total' Freq. (%)**
Medidas de Proteção de Dados Pessoais	10.1	8 (33,3%)	N/A[1]	16 (66,7%)	24 (100,0%)
	10.2	10 (41,7%)	11 (45,8%)	3 (12,5%)	24 (100,0%)
	10.3	8 (33,3%)	13 (54,2%)	3 (12,5%)	24 (100,0%)
	10.4	13 (54,2%)	9 (37,5%)	2 (8,3%)	24 (100,0%)
	10.5	21 (87,5%)	N/A[1]	3 (12,5%)	24 (100,0%)
	Total	60 (50,0%)	33[2] (27,5%)[2]	27 (22,5%)	120 (100,0%)

Fonte: dados da pesquisa

Legenda: '10.1' a '10.5' são as questões, cujos enunciados estão descritos no Anexo 1 deste estudo. 'Freq.' Indica a contagem de frequencia da resposta da questão. '(%)' indica o percentual de respostas da contagem de frequencia, com relação ao total de 24 respostas. N/A indica 'Não Aplicável'.

Observação: 1. 'N/A' indica 'não aplicável'. 2. A frequencia e o percentual total para a resposta 'Parcialmente' considerou as respostas das Questões 10.2 a 10.4.

A Questão 10.1 serve para avaliar se a organização pode comprovar a adoção de medidas de segurança técnicas e administrativas para proteger dados pessoais. Verifica-se, na Tabela 2, que 66,7% das entidades da amostra afirmaram possuir essas práticas, enquanto 33,3% relataram não adotá-las. Isso demonstra alinhamento da maioria dos respondentes à implementação de medidas protetivas, embora ainda exista um terço de entidades da amostra que não evidenciaram esse alinhamento.

A Questão 10.2 ajuda a analisar a existência de processos formais para registro, cancelamento e provisionamento de usuários em sistemas que tratam dados pessoais. Segundo a Tabela 2, apenas 12,5% das organizações implementaram esse controle em todos os sistemas, 45,8% adotaram parcialmente e 41,7% não possuem processos estruturados. A falta de uma gestão eficaz de acessos pode expor informações sensíveis a riscos desnecessários.

A Questão 10.3 possibilita verificar se a organização registra eventos das atividades de tratamento de dados pessoais. Conforme a Tabela 2, apenas 12,5% das entidades da amostra afirmaram manter esse controle em todas as operações, enquanto 54,2% fazem esse registro parcialmente e 33,3% não possuem essa prática. O monitoramento de atividades é essencial para auditorias e conformidade com a LGPD, sendo um aspecto que precisa ser reforçado na maioria das entidades da amostra.

A Questão 10.4 aborda o uso de criptografia para proteção de dados pessoais. De acordo com a Tabela 2, apenas 8,3% das entidades da amostra utilizam criptografia em todas as situações necessárias, enquanto 37,5% aplicam essa medida parcialmente e 54,2% não a utilizam. A criptografia é uma das estratégias para garantir a segurança das informações, e o percentual de respostas ‘Sim’ demonstra baixo alinhamento às medidas citadas na referida questão.

Já a Questão 10.5 analisa a implementação de princípios como ‘*Privacy by Design’ e ‘Privacy by Default’*, que garantem que a privacidade seja considerada desde a concepção dos sistemas. De acordo com a Tabela 2, apenas 12,5% das organizações adotam essa abordagem, enquanto 87,5% ainda não implementaram essa prática. Ou seja, sobre a privacidade dos dados, trata-se de uma medida ainda desalinhada às práticas da maioria das entidades avaliadas.

Com base na Tabela 2, verificou-se o alinhamento à reposta ‘Sim’ igual ou inferior a 22,5% em quatro questões (10.2 a 10.5). A única exceção foi a Questão 10.1, sobre a capacidade de comprovar que adotou medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais, a qual indicou um percentual de respostas ‘Sim’ de 66,7%.

No total, a Tabela 2 mostra que 50,0% das respostas das entidades da amostra indicam que medidas analisadas não são adotadas, 27,5% das respostas indicam que

as medidas são aplicadas de forma parcial (considerando, neste caso, as questões 10.2 a 10.4) e apenas 22,5% das respostas indicam medidas implementadas. Com base no total das respostas das questões, de forma geral as evidências indicam que as entidades da amostra podem aprimorar o alinhamento às medidas de proteção de dados pessoais.

4.2 Comparação do grau de alinhamento segundo tipo de entidade

A Tabela 3 apresenta os resultados estatísticos para as respostas das questões 9.1 a 9.5, comparando o grau de alinhamento segundo o tipo de entidade. Os enunciados de cada uma dessas questões constam do Anexo 1 deste estudo, com base nas respostas das entidades da amostra ao TCU. A descrição dessa amostra, no Apêndice 1, segmenta as 24 entidades em três grupos: órgãos do Poder Executivo Federal, autarquias federais e outras entidades da Administração Pública indireta do Poder Executivo Federal.

No que se refere à Questão 9.1, que trata da existência de um plano de resposta a incidentes, a Tabela 3 mostra que 30,2% das autarquias federais e 28,6% das outras entidades indicaram alinhamento a esta questão. Por sua vez, para órgãos do Poder Executivo apurou-se 100,0% de respostas ‘não’, indicando que nenhum dos órgãos do Poder Executivo Federal que integram a amostra declarou que possui documento estruturado para lidar com incidentes de segurança da informação envolvendo dados pessoais. A falta desse documento pode dificultar a reação das instituições em emergências, tornando mais difícil reduzir os danos causados por tais incidentes.

Sobre a Questão 9.2, que avalia a existência de um sistema para o registro de incidentes de segurança da informação, verifica-se na Tabela 3 que 40,0% das Autarquias adotam essa medida. Apenas 28,6% dos órgãos do Poder Executivo e 28,6% das outras entidades da amostra indicaram adoção a essa medida. Esse resultado demonstra que a maioria das instituições desse grupo não está alinhada à formalização de incidentes, o que pode comprometer a rastreabilidade e a capacidade de análise posterior para aprimoramento das práticas de segurança.

A Questão 9.3 dispõe sobre o sistema para registro das ações adotadas para solucionar incidentes de segurança da informação que envolvem violação de dados

pessoais, conforme Anexo 1. Os resultados da Tabela 3 indicam que 30,0% das Autarquias, 28,6% dos órgãos do Poder Executivo e 28,6% das outras entidades da amostra registram tais medidas, refletindo um alinhamento das entidades da amostra que ainda pode ser aprimorado, referente a esta questão.

Tabela 3 – Resultados da comparação do grau de alinhamento segundo tipo de entidade (Questões 9.1 a 9.5)

	Questão	**Tipo de entidade[4]**	**'Não' Freq. (%)**	**'Sim' Freq. (%)**	**'Total' Freq. (%)**
Medidas contra violação de dados pessoais	9.1	Poder Executivo[1]	7 (100,0%)	0 (0,0%)	7 (100,0%)
		Autarquia[2]	7 (70,0%)	3 (30,0%)	10 (100,0%)
		Outras Entidades[3]	5 (71,4%)	2 (28,6%)	7 (100,0%)
		Total	19 (79,2%)	5 (20,8%)	24 (100,0%)
	9.2	Poder Executivo[1]	5 (71,4%)	2 (28,6%)	7 (100,0%)
		Autarquia[2]	6 (60,0%)	4 (40,0%)	10 (100,0%)
		Outras Entidades[3]	5 (71,4%)	2 (28,6%)	7 (100,0%)
		Total	16 (66,7%)	8 (33,3%)	24 (100,0%)
	9.3	Poder Executivo[1]	5 (71,4%)	2 (28,6%)	7 (100,0%)
		Autarquia[2]	7 (70,0%)	3 (30,0%)	10 (100,0%)
		Outras Entidades[3]	5 (71,4%)	2 (28,6%)	7 (100,0%)
		Total	17 (70,8%)	7 (29,2%)	24 (100,0%)
	9.4	Poder Executivo[1]	3 (42,9%)	4 (57,1%)	7 (100,0%)
		Autarquia[2]	6 (60,0%)	4 (40,0%)	10 (100,0%)
		Outras Entidades[3]	5 (71,4%)	2 (28,6%)	7 (100,0%)
		Total	14 (58,3%)	10 (41,7%)	24 (100,0%)
	9.5	Poder Executivo[1]	5 (71,4%)	2 (28,6%)	7 (100,0%)
		Autarquia[2]	6 (60,0%)	4 (40,0%)	10 (100,0%)
		Outras Entidades[3]	6 (85,7%)	1 (14,3%)	7 (100,0%)
		Total	17	7	24

			(70,8%)	(29,2%)	(100,0%)
	Total	Poder Executivo[1]	25 (71,4%)	10 (28,6%)	35 (100,0%)
		Autarquia[2]	32 (64,0%)	18 (36,0%)	50 (100,0%)
		Outras Entidades[3]	26 (74,3%)	9 (25,7%)	35 (100,0%)
		Total	83 (69,2%)	37 (30,8%)	120 (100,0%)

Fonte: dados da pesquisa

Legenda: ‘9.1’ a ‘9.5’ são as questões, cujos enunciados estão descritos no Anexo 1 deste estudo. ‘Freq.’ Indica a contagem de frequencia da resposta da questão. ‘(%)’ indica o percentual de respostas da contagem de frequencia, com relação ao total de respostas indicado na coluna ‘Total’.

Observações: 1. ‘Poder Executivo’ indica órgãos do Poder Executivo Federal; 2. ‘Autarquia’ indica autarquias federais; 3. ‘Outras Entidades’ incluem outras entidades da administração pública indireta do Poder Executivo Federal; 4. A descrição das entidades da amostra segundo o tipo de entidade consta do Apêndice 1.

Já na Questão 9.4, que aborda o monitoramento proativo da ocorrência de eventos que possam estar associados à violação de dados pessoais. Segundo a Tabela 3, o Poder Executivo apresentou 57,1% das respostas, indicando alinhamento da maioria das entidades desse grupo a essa medida. Por sua vez, Autarquias Federais apresentaram 40,0% de respostas ‘Sim’ e Outras Entidades apresentaram 14,3% de respostas ‘Sim’. Exceto pelo Poder Executivo, para maioria das Autarquias e de outras entidades da amostra o referido monitoramento pode ser aprimorado.

Na Questão 9.5, que examina a comunicação de incidentes à ANPD e aos titulares dos dados pessoais, verificou-se na Tabela 3 que 40,0% das Autarquias Federais, 28,6% dos órgãos do Poder Executivo e 14,3% de outras entidades possuem aderência a essa medida. A falta de um processo organizado para notificar incidentes pode fazer com que esses órgãos sofram punições e prejudiquem sua imagem, já que informar rapidamente sobre problemas de segurança é uma exigência da LGPD.

Por fim, a Tabela 3 mostra que, no total, 71,4% das respostas das entidades do Poder Executivo, 64,0% das respostas Autarquias e 74,3% das respostas das outras entidades da amostra não estão alinhadas às medidas citadas nas questões 9.1 a 9.5, sugerindo que há oportunidade, com algumas variações pontuais, para aprimoramentos no tocante a medidas contra violação de dados pessoais para todos os três tipos de entidades segmentados na amostra citada no Apêndice 1.

Dando sequência às análises, a Tabela 4 apresenta os resultados estatísticos para as respostas das questões 10.1 a 10.5, comparando o grau de alinhamento segundo o tipo de entidade. Os enunciados de cada uma dessas questões constam do Anexo 1.

Tabela 4: Resultados da comparação do grau de alinhamento segundo tipo de entidade (Questões 10.1 a 10.5)

	Questão	**Tipo de entidade[4]**	**'Não' Freq. (%)**	**'Parcialmente' Freq. (%)**	**'Sim' Freq. (%)**	**'Total' Freq. (%)**
Medidas de Proteção de Dados Pessoais	10.1	Poder Executivo[1]	1 (14,3%)	N/A[5]	6 (85,7%)	7 (100,0%)
		Autarquia[2]	4 (40,0%)	N/A[5]	6 (60,0%)	10 (100,0%)
		Outras Entidades[3]	3 (42,9%)	N/A[5]	4 (57,1%)	7 (100,0%)
		Total	8 (33,3%)	N/A[5]	16 (66,7%)	24 (100,0%)
	10.2	Poder Executivo[1]	2 (28,6%)	3 (42,9%)	2 (28,6%)	7 (100,0%)
		Autarquia[2]	3 (30,0%)	6 (60,0%)	1 (10,0%)	10 (100,0%)
		Outras Entidades[3]	5 (71,4%)	2 (28,6%)	0 (0,0%)	7 (100,0%)
		Total	10 (41,7%)	11 (45,8%)	3 (12,5%)	24 (100,0%)
	10.3	Poder Executivo[1]	1 (14,3%)	4 (57,1%)	2 (28,6%)	7 (100,0%)
		Autarquia[2]	4 (40,0%)	6 (60,0%)	0 (0,0%)	10 (100,0%)
		Outras Entidades[3]	3 (42,9%)	3 (42,9%)	1 (14,3%)	7 (100,0%)
		Total	8 (33,3%)	13 (54,2%)	3 (12,5%)	24 (100,0%)
	10.4	Poder Executivo[1]	3 (42,9%)	3 (42,9%)	1 (14,3%)	7 (100,0%)
		Autarquia[2]	6 (60,0%)	3 (30,0%)	1 (10,0%)	10 (100,0%)
		Outras Entidades[3]	4 (57,1%)	3 (42,9%)	0 (0,0%)	7 (100,0%)
		Total	13 (54,2%)	9 (37,5%)	2 (8,3%)	24 (100,0%)
	10.5	Poder Executivo[1]	5 (71,4%)	N/A[5]	2 (28,6%)	7 (100,0%)
		Autarquia[2]	9 (90,0%)	N/A[5]	1 (10,0%)	10 (100,0%)
		Outras Entidades[3]	7 (100,0%)	N/A[5]	0 (0,0%)	7 (100,0%)

		Total	21 (87,5%)	N/A[5]	3 (12,5%)	24 (100,0%)
	Total	Poder Executivo[1]	12 (34,3%)	10[6] (28,6%)[6]	13 (37,1%)	35 (100,0%)
		Autarquia[2]	26 (52,0%)	15[6] (30,0%)[6]	9 (18,0%)	50 (100,0%)
		Outras Entidades[3]	22 (62,9%)	8[6] (22,9%)[6]	5 (14,3%)	35 (100,0%)
		Total	60 (50,0%)	33 (27,5%)	27 (22,5%)	120 (100,0%)

Legenda: ‘10.1’ a ‘10.5’ são as questões, cujos enunciados estão descritos no Anexo 1 deste estudo. ‘Freq.’ Indica a contagem de frequencia da resposta da questão. ‘(%)’ indica o percentual de respostas da contagem de frequencia, com relação ao total de respostas indicado na coluna ‘Total’.

Observações: 1. ‘Poder Executivo’ indica órgãos do Poder Executivo Federal; 2. ‘Autarquia’ indica autarquias federais; 3. ‘Outras Entidades’ incluem outras entidades da administração pública indireta do Poder Executivo Federal; 4. A descrição das entidades da amostra segundo o tipo de entidade consta do Apêndice 1; 5. ‘N/A’ indica ‘não aplicável’; 6. Frequencias e percentuais totais apurados para a resposta ‘parcialmente’ a partir das questões 10.1 a 10.5

Referente aos resultados da Questão 10.1, indicando se a organização foi capaz de comprovar que adotou medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais, segundo a Tabela 4 verifica-se que 85,7% das respostas das entidades do Poder Executivo, 60,0% das Autarquias e 57,1% das respostas de outras entidades da amostra indicaram alinhamento às citadas medidas.

Por sua vez, para a Questão 10.2, que indaga se a organização implementou processo para registro, cancelamento e provisionamento de usuários em sistemas que realizam tratamento de dados pessoais, a Tabela 4 mostra que 42,9% das entidades do Poder Executivo e 60,0% das Autarquias indicaram alinhamento parcial, e 71,4% das outras entidades não indicaram alinhamento ao teor da indagação, o que sinaliza a oportunidade de aprimoramento a respeito do processo citado neste parágrafo, especialmente para outras entidades da amostra.

Já na questão 10.3, que trata do processo de registro e controle de ações para mitigação de problemas, observou-se que 57,1% das entidades do Poder Executivo e 60,0% das Autarquias, 42,9% das outras entidades alinham-se parcialmente a esse processo, e outras 42,9% dessas outras entidades, também, não se alinham ao referido processo. Então, embora haja evidência sobre o referido processo, a implementação dessa medida ainda é limitada.

Sobre a questão 10.4, dispondo se a organização utiliza criptografia para proteger os dados pessoais, a Tabela 4 mostra que 60,0% das Autarquias, 57,1% dos órgãos do Poder Executivo, e 42,9% de outras entidades não estão alinhadas a esta medida. Tais evidências indicam a necessidade de explicitar melhor as medidas de segurança referente a criptografia de dados pessoais.

A questão 10.5, indagando se a organização adotou medidas para assegurar que processos e sistemas sejam projetados, desde a concepção, em conformidade com a LGPD, os resultados da Tabela 4 indicaram que 71,4% das entidades do Poder Executivo, 90,0% das Autarquias e 100,0% das outras entidades não demonstraram alinhamento às medidas citadas pela questão, sinalizando, também, oportunidade para aprimoramentos.

Por fim, a Tabela 4 mostra que, no total, 37,1% entidades do Poder Executivo, 18,0% das Autarquias e 14,3% das outras entidades da amostra não estão alinhadas às medidas, sugerindo que há oportunidade para aprimoramentos no tocante a medidas contra violação de dados pessoais para todos os três tipos de entidades da amostra citada no Apêndice 1, mas para órgãos do Poder Executivo essa necessidade de aprimoramento ficou menos evidenciada do que para as demais entidades da amostra.

5. CONCLUSÕES E RECOMENDAÇÕES

O objetivo geral deste estudo foi analisar o grau de alinhamento das entidades do poder executivo federal às medidas de proteção e prevenção contra a violação de dados pessoais, com base em questões dos relatorios de feedback emitidos em atendimento ao TCU.

Realizou-se pesquisa descritiva com abordagem quantitativa. A partir de população com 382 entidades públicas federais sujeitas a Auditoria do TCU, chegou-se a amostra não probabilística de 24 entidades (órgãos do Poder Executivo, Autarquias Federais e Outras Entidades) que disponibilizaram publicamente seus relatórios de feedback com respostas dadas ao TCU. A coleta dos dados priorizou dez questões, sendo cinco sobre medidas de violação de dados pessoais e cinco sobre medidas de proteção de dados pessoais (Anexo 1). O tratamento dos dados empregou estatística descritiva exibindo contagem de frequências e percentuais.

Dois objetivos específicos foram propostos neste estudo. O primeiro deles foi identificar o grau de alinhamento das medidas de proteção e prevenção contra a violação de dados pessoais segmentados por questões dos relatorios de feedback emitidos em atendimento ao TCU. Este objetivo específico foi alcançado com a exibição dos resultados na Seção 4.1, apurando-se, conforme mostrou a Tabela 1, que 69,2% das respostas das entidades indicaram que as medidas contra violação de dados pessoais ainda não são adotadas, enquanto 30,8% dessas respostas indicam que as medidas foram adotadas. Baseado no total das respostas das questões, de forma geral as evidências indicaram que as entidades da amostra podem aprimorar o alinhamento às medidas contra violação de dados pessoais.

Ainda com relação ao primeiro objetivo específico, a Tabela 2 mostrou que 50,0% das respostas das entidades da amostra indicam que medidas analisadas não são adotadas, 27,5% das respostas indicam que as medidas são aplicadas de forma parcial (considerando, neste caso, as questões 10.2 a 10.4) e 22,5% das respostas

indicam medidas implementadas. As respostas indicam que as medidas de proteção de dados pessoais, também, podem ser aprimoradas pelas entidades da amostra.

Por sua vez, o segundo objetivo específico foi comparar o grau de alinhamento previamente identificado, considerando os órgãos do poder executivo, as autarquias federais e outras entidades da administração indireta federal. Este objetivo específico foi alcançado com a exibição da Seção 4.2. A Tabela 3 mostra, em geral, que 28,6% entidades do Poder Executivo, 36,0% das Autarquias e 25,7% das outras entidades da amostra estão alinhadas às medidas citadas nas questões 9.1 a 9.5, sugerindo que há oportunidade para aprimoramentos no tocante a medidas contra violação de dados pessoais para todos os tipos de entidades segmentados da amostra.

Em complemento, com referência ao segundo objetivo específico, a Tabela 4 mostra que, no total, 37,1% entidades do Poder Executivo, 18,0% das Autarquias e 14,3% das outras entidades da amostra estão alinhadas às medidas de proteção de dados pessoais para todos os três tipos de entidades da amostra, mas para órgãos do Poder Executivo essa necessidade de aprimoramento foi menos evidenciada do que para as demais entidades da amostra.

O atingimento dos objetivos específicos permite informar que o objetivo geral proposto nesta pesquisa foi alcançado. A análise mostrou que 30,8% das respostas sobre as medidas contra violação de dados pessoais e 22,5% das respostas sobre das medidas de proteção de dados pessoais são adotadas. Ao comparar os resultados por tipo de entidade, as evidencias indicaram, também, que 28,6% das entidades do Poder Executivo, 36,0% das Autarquias e 25,7% das outras entidades da amostra estão alinhadas às medidas contra violação de dados pessoais, e 37,1% entidades do Poder Executivo, 18,0% das Autarquias e 14,3% das outras entidades da amostra estão alinhadas às medidas de proteção de dados pessoais, sugerindo, em geral, oportunidade para aprimoramentos para todos os três tipos de entidades da amostra.

A pesquisa, também, avaliou medidas técnicas para proteger dados pessoais (Questões 10.1 a 10.5), verificando que 50,0% das organizações não adotam boas práticas de segurança, enquanto 27,5% aplicam parcialmente e apenas 22,5% possuem medidas bem estabelecidas. Apesar de 66,7% das instituições afirmarem

possuir alguma política de proteção, muitas ainda apresentam falhas graves, como a falta de criptografia (54,2%) e a ausência de controle adequado de acessos (87,5%).

Em que pese o que foi descrito de forma geral no parágrafo anterior, dentre os três grupos de entidades analisados verificou-se, também, na Questão 10.1, que 85,7% das respostas das entidades do Poder Executivo, 60,0% das Autarquias e 57,1% das respostas de outras entidades da amostra indicaram alinhamento à medida indicativa se a organização foi capaz de comprovar que adotou medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais.

Este trabalho tratou tema atual e de interesse para entes públicos federais, para ANPD e para o TCU. Adicionalmente, pode ser de interesse de acadêmicos e especialistas na aplicação da LGPD em organizações públicas, bem como nas medidas adotadas contra a violação de dados pessoais e que promovam a proteção desses dados. De notar que algumas delimitações devem ser lembradas: 1. os dados analisados referem-se exclusivamente àqueles coletados com base nas questões presentes no relatório de feedback do TCU que consta do Anexo 1. 2. As análises limitaram-se a empregar recursos de estatística descritiva, sem emprego de outras análises, como as inferenciais. Os resultados devem ser atribuídos ao conjunto de entidades da amostra que consta do Apêndice 1.

O fortalecimento da segurança da informação não deve ser visto apenas como uma exigência legal, mas como um compromisso essencial para proteger os dados pessoais e garantir a integridade das instituições públicas, sendo um esforço de ação contínua. Dessa forma, entendendo que o tema desta pesquisa não se esgota neste trabalho, são propostas as seguintes sugestões para estudos futuros:

- estender as análises a outras questões do relatório de feedback não contempladas neste estudo;
- ampliar a análise para outras entidades que não sejam apenas do poder executivo federal, abrangendo, por exemplo, entidades do judiciário ou do legislativo; e
- verificar a possibilidade de ocorrerem outras pesquisas similares em outros períodos, as quais podem trazer mais subsídios e possibilidades de comparações com os achados deste estudo.

- Comparar o grau de alinhamento das entidades da administração direta e indireta do poder executivo federal às medidas de proteção e prevenção contra a violação de dados pessoais.

REFERÊNCIAS

ALBERS, Marion. A complexidade da proteção de dados. Direito e Fronteiras Journal, [S.l.], v. 1, n. 1, p. 93-105, 2016. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/93/19. Acesso em: 04 maio. 2024.

ALMEIDA, Siderly do Carmo Dahle de; SOARES, Tania Aparecida. Os impactos da Lei Geral de Proteção de Dados – LGPD no cenário digital. SciELO, jul./set. 2022. https://www.scielo.br/j/pci/a/tb9czy3W9RtzgbWWxHTXkCc/?format=pdf&lang=pt. Acesso em: 24 jun. 2024.

BIONI, Bruno Ricardo et al. Os dados e o vírus: pandemia, proteção de dados e democracia. Data Privacy Brasil, 2020.Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2020/09/eBook_selecoes_osdados_eo_virus.pdf. Acesso em: 21 maio. 2024.

BRASIL. Artigo 55 da Lei Geral de Proteção de Dados (LGPD). Disponível em: https://lgpd-brasil.info/capitulo_09/artigo_55c. Acesso em: 24 jun. 2024.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes-2013-anpd. Acesso em: 12 abril. 2024.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal, 1988. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/518231/CF88_Livro_EC91_2016.pdf. Acesso em: 12 maio. 2024.

BRASIL. Decreto nº 7.962, de 15 de março de 2013. Dispõe sobre a contratação no comércio eletrônico. Diário Oficial da União, Brasília, DF, 15 mar. 2013. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7962.htm. Acesso em: 26 maio 2024.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 23 maio 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 26 maio 2024.

BRASIL. Lei nº 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Diário Oficial da União, Brasília, DF, 25 jul. 1996. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 26 maio 2024.

Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação. Pesquisa TIC Domicílios 2023: acesso e uso das tecnologias de informação e comunicação nas residências brasileiras. São Paulo: Comitê Gestor da Internet no Brasil, 2023. Disponível em: https://cetic.br/pesquisa/domicilios/indicadores. Acesso em: 26 maio 2024.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico: Journal of Law, 2011. Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 20 abril. 2024.

LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de. Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. Revista de Direito da Universidade Federal de Viçosa, 2020. Disponível em: https://periodicos.ufv.br/revistadir/article/view/10597. Acesso em: 18 abril. 2024.

MONTEIRO, André; ARAÚJO, Fernanda. Proteção de dados e privacidade no Brasil: da teoria à prática. Revista Jurídica de Tecnologia, Rio de Janeiro, v. 9, n. 1, p. 50-72, 2021. Disponível em: https://rjt.org.br/protecao-de-dados. Acesso em: 26 maio 2024.

MONTEIRO, Renato Leite et al. Lei Geral de Proteção de Dados e GDPR: histórico, análise e impacto. Baptistaluz, 2019. Disponível em: https://baptistaluz.com.br/wp-content/uploads/2019/01/RD-DataProtection-ProvF.pdf. Acesso em: 08 maio. 2024.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Declaração Universal dos Direitos Humanos. Paris, 1948. Disponível em: https://www.un.org/en/about-us/universal-declaration-of-human-rights. Acesso em: 15 maio 2024.

PALHARES, Joana. Leis de proteção de dados: uma análise comparativa. Revista de Direito Internacional, Lisboa, v. 15, n. 4, p. 102-121, 2021. Disponível em: https://rdi.pt/leis-protecao-dados. Acesso em: 26 maio 2024.

SAMPIERI, Roberto Hernández. Metodologia de pesquisa. 5. ed. São Paulo: McGraw-Hill, 2012.

SARLET, G. B. S.; RODRIGUEZ, D. P. A autoridade nacional de proteção de dados (ANPD): elementos para uma estruturação independente e democrática na era da governança digital. Revista Direitos Fundamentais & Democracia, [S. l.], v. 27, n. 3, p. 217–253, 2022. DOI: 10.25192/issn.1982-0496.rdfd.v27i32285. Disponível em:

https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2285. Acesso em: 24 jun. 2024.

SILVA, Ricardo. O mega vazamento de dados no Brasil: causas e consequências. Revista Brasileira de Segurança da Informação, São Paulo, v. 10, n. 3, p. 85-110, 2020. Disponível em: https://rbsi.org.br/mega-vazamento. Acesso em: 26 maio 2024.
SOLOVE, Daniel. Understanding Privacy. Maio de 2018. Disponível em: https://pt.scribd.com/document/491622718/daniel-en-pt. Acesso em: 27 jun. 2024.

TAVARES, Ana. Ética e privacidade na era digital. Revista de Ética e Sociedade, Porto Alegre, v. 7, n. 2, p. 44-66, 2012. Disponível em: https://res.org.br/etica-e-privacidade. Acesso em: 26 maio 2024.

TRIBUNAL DE CONTAS DA UNIÃO (TCU). Fiscalização sobre a implementação dos dispositivos da LGPD na União, nos Estados e nos Municípios. Disponível em: https://portal.tcu.gov.br/fiscalizacao-de-tecnologia-da-informacao/atuacao/fiscalizacoes/auditoria-sobre-lgpd/. Acesso em: 27 jun. 2024.

TRIBUNAL DE CONTAS DA UNIÃO. Acórdão nº 1384/2022 – Plenário. Auditoria sobreadequação das organizações públicas federais à Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 2022. Disponível em: https://www.tcu.gov.br/contasgov/acordaos/acordao-1384-2022.pdf. Acesso em: 07 abril 2024.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Regulamento Geral sobre a Proteção de Dados (GDPR). Jornal Oficial da União Europeia, L 119, p. 1-88, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 26 maio 2024.

VERGILI, Renata; LIMA, Pedro. GDPR e LGPD: um estudo comparado. Revista de Direito Digital, São Paulo, v. 6, n. 1, p. 77-99, 2020. Disponível em: https://rdd.org.br/gdpr-lgpd. Acesso em: 26 julho 2024.

ZANATTA, Rafael. Proteção de dados no Brasil: desafios e perspectivas. Revista Brasileira de Direito Privado, Curitiba, v. 11, n. 2, p. 12-34, 2015. Disponível em: https://rbdp.org.br/protecao-de-dados. Acesso em: 12 novembro 2024.

APÊNDICE 1 – AMOSTRA

Nome da entidade	**Tipo da entidade**
Controladoria Geral da União	Poder Executivo
Hospital Federal dos Servidores do Estado	Autarquia
Instituto Nacional de Meteorologia	Autarquia
Polícia Rodoviária Federal	Poder Executivo
Secretaria Especial da Receita Federal do Brasil	Poder Executivo
Ministério da Economia	Poder Executivo
Ministério da Educação	Poder Executivo
Ministério do Turismo	Poder Executivo
Ministério do Meio Ambiente	Poder Executivo
Universidade Federal da Bahia	Autarquia
Universidade Federal de Juiz de Fora	Autarquia
Universidade Federal de Lavras	Autarquia
Banco Central do Brasil	Autarquia
Companhia Brasileira de Trens Urbanos	Empresa Pública
Centro Federal de Educação Tecnológica de Minas Gerais	Autarquia
Companhia Nacional de Abastecimento	Empresa Pública
Empresa de Planejamento e Logística S.A	Empresa Pública
Fundação Biblioteca Nacional	Fundação Pública
Fundação Oswaldo Cruz	Fundação Pública
Instituto Patrimônio Histórico e Artístico Nacional	Autarquia
Petrobras	Empresa Pública
Fundação Universidade Federal do Pampa	Autarquia
VALEC	Empresa Pública
Agência Nacional de Saúde Suplementar	Autarquia

Fonte: dados da pesquisa.

ANEXO 1 – QUESTIONÁRIO TCU (Questões Selecionadas)

TRIBUNAL DE CONTAS DA UNIÃO

Auditoria para avaliar a adequação das organizações públicas federais à LGPD

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

- ○ Sim
- ○ Não

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

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

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

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

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

- ○ Sim
- ○ Não

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

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

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

- ○ Sim
- ○ Não

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

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

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

- ○ Sim
- ○ Não

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

Convém que a organização adote mecanismo para monitorar proativamente os eventos de segurança da informação que são associados à violação de dados pessoais para adotar medidas necessárias caso ocorram.

A identificação precoce de incidentes pode diminuir significativamente os impactos causados por eles.

9.5 A organização estabeleceu procedimentos para comunicar à Autoridade Nacional de Proteção de Dados e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares?

- ○ Sim
- ○ Não

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

A organização deve comunicar à ANPD e ao titular a ocorrência de incidente de segurança da informação que possa acarretar risco ou dano relevante aos titulares. A notificação deve ser feita em prazo razoável e mencionar, no mínimo: a descrição da natureza dos dados pessoais afetados; as informações sobre os titulares envolvidos; a indicação das medidas técnicas e de segurança adotadas para a proteção dos dados; os riscos relacionados ao incidente; e as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. Caso a organização não encaminhe a comunicação tempestivamente, deverá ser exposto, também, os motivos que levaram à demora.

Medidas de proteção

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

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

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

- ○ Sim
- ○ Não

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

A organização deve adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

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

- ○ Sim (a organização implementou processo formal para registro, cancelamento e provisionamento de usuários em todos os sistemas que realizam tratamento de dados pessoais).
- ○ Parcialmente (a organização implementou processo formal para registro, cancelamento e provisionamento de usuários em alguns sistemas que realizam tratamento de dados pessoais).
- ○ Não (a organização não implementou processo formal para registro, cancelamento e provisionamento de usuários em sistemas que realizam tratamento de dados pessoais).

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

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

Convém que a concessão de direitos de acesso observem os princípios de "necessidade de conhecer" e "necessidade de uso".

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

- ○ Sim (a organização registra os eventos de todas as atividades de tratamento de dados pessoais).
- ○ Parcialmente (a organização registra os eventos de algumas atividades de tratamento de dados pessoais).

- ○ Não (a organização não registra os eventos de atividades de tratamento de dados pessoais).

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

Convém que a organização registre os eventos (*logs*) das atividades de tratamento de dados pessoais de forma que seja possível identificar por quem, quando e quais dados pessoais foram acessados. Nos casos em que ocorrem mudanças nos dados, também deve ser registrada a ação realizada (*e.g.*: inclusão, alteração ou exclusão).

10.4 A organização utiliza criptografia para proteger os dados pessoais?

- ○ Sim (a organização utiliza criptografia para proteger todos os dados pessoais).
- ○ Parcialmente (a organização utiliza criptografia para proteger alguns dados pessoais).
- ○ Não (a organização não utiliza criptografia para proteger os dados pessoais).

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

A utilização de criptografia pode proteger a confidencialidade, a autenticidade e/ou a integridade da informação.

Por exemplo, devido à criticidade dos dados sensíveis, a adoção de mecanismos para criptografá-los em trânsito e no armazenamento pode mitigar riscos associados à violação de dados pessoais.

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

- ○ Sim
- ○ Não

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

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