

INOVAÇÃO E CONFORMIDADE NA ERA DA PROTEÇÃO DE DADOS: O CASO DO MUNICÍPIO DE JOINVILLE

Sahmara Liz Botemberger¹⁵⁷

Resumo: Este artigo explora o processo de adequação do Município de Joinville à Lei Geral de Proteção de Dados Pessoais (LGPD), destacando os desafios enfrentados e as soluções implementadas para garantir a conformidade legal, promover a transparência e fortalecer a confiança dos cidadãos. O estudo detalha a abordagem adotada pela administração pública, que utilizou recursos próprios para iniciar o processo de adequação sem onerar os cofres públicos, implementando uma série de estratégias inovadoras e práticas de governança de dados. Entre os principais desafios, destacam-se o grande volume de dados tratados, a complexidade da estrutura organizacional e a necessidade de capacitação e mudança de cultura entre os servidores públicos. As soluções abordadas incluem a criação de um Comitê Municipal de Proteção de Dados, a implementação de metodologias ágeis e ferramentas como o Project Model Canvas e o Google Forms, além de ações para conscientizar e treinar servidores públicos. O artigo conclui que o caso de Joinville pode servir de modelo para outras administrações públicas no Brasil.

¹⁵⁷ Pós-graduada em Direito Público com ênfase em Gestão Pública pela Damásio Educacional S/A. Pós-graduada em Direito Processual Civil pela Faculdade Guilherme Guimbala. Pós-Graduada em Advocacia no Direito Digital e Proteção de Dados pela Universidade São Judas Tadeu. Graduada em Direito na Faculdade Guilherme Guimbala. Servidora Pública, Coordenadora da Área de Proteção de Dados e Encarregada de Tratamento de Dados do Município de Joinville/SC. Certified Information Privacy Manager pela International Association of Privacy Professionals. Advogada. E-mail: sahmara.botemberger@joinville.sc.gov.br Lattes: <http://lattes.cnpq.br/3081097240826961>

Abstract: This article explores the process of adapting the Municipality of Joinville to the Brazilian General Data Protection Law (LGPD), highlighting the challenges faced and the solutions implemented to ensure legal compliance, promote transparency, and strengthen citizen trust. The study details the approach taken by the public administration, which utilized its own resources to initiate the adaptation process without burdening public finances, implementing a series of innovative strategies and data governance practices. Among the main challenges were the large volume of data processed, the complexity of the organizational structure, and the need for training and cultural change among public servants. The solutions addressed include the creation of a Municipal Data Protection Committee, the implementation of agile methodologies and tools such as the Project Model Canvas and Google Forms, as well as actions to raise awareness and train public servants. The article concludes that the case of Joinville may serve as a model for other public administrations in Brazil.

Palavras-Chave: Lei Geral de Proteção de Dados, LGPD, conformidade, administração pública, proteção de dados, governança de dados, Joinville, adequação legal, segurança da informação.

Keywords: General Data Protection Law, LGPD, compliance, public administration, data protection, data governance, Joinville, legal adaptation, information security.

Sumário: 1. Introdução; 2. Metodologia; 2.1 Desafios Enfrentados; 2.1.1 Volume de dados tratados; 2.1.2 Estrutura organizacional complexa; 2.1.3 Quadro funcional e capacitação; 2.1.4 Cultura organizacional e privacidade de dados; 2.1.5 Mapeamento, Inventário de Dados e Adequação de Processos que tratam dados pessoais; 2.2 Estratégias para a Adequação; 2.2.1 Estrutura mínima de governança; 2.2.2 Publicação de decretos e regulamentações; 2.2.3 Implementação da Área de Proteção de Dados; 2.2.4 Preparando o Projeto; 2.2.5 Avaliação inicial do cenário atual; 2.2.6 Treinamento e sensibilização; 2.2.7 Mapeamento de processos de trabalho que tratam dados pessoais; 2.2.8 Gestão de riscos e análise de impacto; 2.2.9 Relatório de Impacto de Proteção de Dados; 2.10 Execução de outras ações em paralelo à conscientização, mapeamento e gestão de riscos; 3. Resultados; 3.1 Resultados Alcançados; 3.2 Resultados Esperados e Metas a Serem Atingidas; 4. Considerações finais. Referências Bibliográficas.

1. INTRODUÇÃO

A Lei Geral de Proteção de Dados (LGPD)¹⁵⁸ é a legislação brasileira que regula o tratamento de dados pessoais, tanto em meios físicos quanto digitais, por pessoas naturais ou jurídicas, públicas ou privadas, com o objetivo de proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade dos indivíduos.

Desta forma, conforme o artigo 3º, II, a lei se aplica às atividades de tratamento que tenham por objetivo a oferta ou o fornecimento de bens, excluindo-se o tratamento de dados pessoais realizado por pessoa natural para fins exclusivamente particulares e não econômicos.

Nesse sentido, Bioni (2021) destaca a urgência da regulamentação da proteção de dados pessoais, argumentando que, com o desenvolvimento da ciência mercadológica, dados pessoais tornaram-se um recurso vital para a economia da informação. Ele menciona que a capacidade de organizar esses dados em larga escala, por meio de tecnologias como Big Data, criou um novo mercado baseado na extração e comercialização dessas informações, resultando em uma “economia de vigilância” onde o cidadão é reduzido a mero espectador de seus próprios dados.¹⁵⁹

Apesar de órgãos públicos não terem finalidade econômica ou lucrativa, prestam, de forma direta ou indireta, serviços essenciais à população, como saúde, educação, assistência social e infraestrutura urbana. Além disso, todas as fases da vida de um indivíduo, desde o nascimento até o seu falecimento, ficam registradas em órgãos públicos. Portanto, o volume de dados tratados por esses órgãos é elevado e de alta criticidade, o que torna a Administração Pública a maior custodiante de dados pessoais no país.

A adequação à LGPD nas administrações públicas municipais é fundamental para garantir a conformidade legal, promover a transparência e fortalecer a confiança dos cidadãos nas instituições públicas.

Convém mencionar que, conforme estudo realizado pelo Tribunal de Contas da União, o Brasil vem ocupando as primeiras posições dos rankings internacionais no que tange à perpetração de ataques cibernéticos. Ocupou

¹⁵⁸ BRASIL. Presidência da República. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 30/07/2024.

¹⁵⁹ BIONI, Bruno Ricardo. Proteção de Dados Pessoais: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021.

a 8ª posição do mundo em número de ataques a dispositivos da internet das coisas (IOT) no período de abril a junho de 2021 e o 5º lugar em ataques de sequestro de dados em meados de 2021.¹⁶⁰

Sendo assim, este artigo apresenta o início do processo de adequação à LGPD – um case bem-sucedido – no Município de Joinville, de forma orgânica, aproveitando os recursos existentes sem onerar os cofres públicos e gerando valor.

Destacamos os principais desafios, estratégias adotadas e os resultados alcançados.

2. METODOLOGIA

O processo de adequação à Lei Geral de Proteção de Dados (LGPD) no Município de Joinville exigiu uma abordagem detalhada e estruturada. Nesta seção, serão apresentados os principais desafios enfrentados pela administração pública durante a implementação, bem como as estratégias adotadas para superar esses obstáculos. A metodologia baseou-se em ferramentas ágeis, capacitação de servidores e um mapeamento rigoroso dos processos, buscando garantir a conformidade legal sem sobrecarregar os cofres públicos. A seguir, detalhamos cada um desses aspectos.

2.1. Desafios enfrentados

2.1.1. Volume de dados tratados

O Município de Joinville, com cerca de 700 mil habitantes e serviços de saúde que operam 24 horas por dia, enfrenta o desafio de gerenciar um grande volume de dados pessoais e dados sensíveis diariamente.

2.1.2. Estrutura organizacional e complexa

A estrutura organizacional da administração pública municipal de Joinville é extensa e diversificada, composta por 18 órgãos da administração direta, 56 Unidades Básicas de Saúde, 11 Unidades de Referência, 17 equipamentos de Assistência Social, 76 Centros de Educação Infantil, 85

¹⁶⁰ TRIBUNAL DE CONTAS DA UNIÃO (TCU). TCU analisa segurança cibernética de instituições federais. Disponível em: <https://portal.tcu.gov.br/imprensa/noticias/tcu-analisa-seguranca-cibernetica-de-instituicoes-federais.htm#:~:text=A%20fiscaliza%C3%A7%C3%A3o%20do%20TCU%20apurou,dados%20em%20meados%20de%202021>. Acesso em: 02/08/2024.

Escolas de Ensino Fundamental, 8 Unidades de Cultura e 8 Subprefeituras. A administração indireta inclui 4 autarquias: o Instituto de Previdência dos Servidores Públicos do Município de Joinville (IPREVILLE), o Hospital São José, o Departamento de Trânsito (Detrans) e a Companhia Águas de Joinville.

A complexidade dessa estrutura aumentou o desafio de adequação à LGPD, especialmente em termos de coordenação e conformidade entre os diferentes órgãos.

2.1.3. Quadro funcional e capacitação

Outro desafio foi o grande número de colaboradores. O quadro funcional do Município conta com aproximadamente 13.500 pessoas, incluindo servidores, contratados, estagiários e jovens aprendizes. A necessidade de capacitar todos esses agentes públicos sobre a importância da proteção de dados seria crucial para o sucesso do projeto, especialmente considerando que muitos nunca haviam recebido treinamento sobre privacidade e governança de dados.

2.1.4. Cultura organizacional e privacidade de dados

A cultura organizacional do Município também precisava ser transformada para valorizar a privacidade e a proteção de dados pessoais.

Historicamente, a governança corporativa e o investimento em treinamento para áreas que não envolviam saúde, educação e segurança pública eram mínimos, o que tornava o processo de adequação à LGPD ainda mais desafiador. Além disso, a dispersão geográfica dos órgãos municipais dificultava a comunicação e a implementação de uma cultura única de proteção de dados.

De acordo com Lanzer (2017), a cultura organizacional é definida como um conjunto de valores e normas que fornecem a um grupo de pessoas uma noção clara sobre o que é certo ou errado, aceito ou não aceito no grupo. Ela é considerada *perene*, com mudanças mais lentas, sendo menos suscetível à influência, especialmente por parte de gestores.¹⁶¹ Essa característica torna a cultura organizacional crucial no processo de adequação à proteção de dados pessoais, já que não se trata de uma proposta de governo, mas de uma política de Estado que deve perdurar, independentemente de quem esteja no comando da organização.

¹⁶¹ LANZER, Fernando. *Clima e Cultura Organizacional: entender, manter e mudar*. 2. ed. 2017.

2.1.5. Mapeamento, inventário de dados e adequação de processos que tratam dados pessoais

Esse quesito era considerado o ponto crucial para o sucesso de todo o processo de adequação, pois qualquer falha nessa etapa comprometeria o restante.

O mapeamento dos processos que tratam dados pessoais é o “raio X” dos órgãos no que tange à conformidade. É a partir dele que se torna possível realizar a análise de riscos, elaborar o relatório de impacto (uma exigência legal), e propor soluções para a aderência à legislação.

No início do processo existiam muitas dúvidas, muitas teorias, pouca prática e um template disponibilizado pelo Governo Federal, que se mostrou inadequado para a realidade local. O modelo era uma planilha Excel com aproximadamente 144 linhas de questionamentos. O Município de Joinville não faz uso da aplicação Excel, utilizando o software livre e de código aberto LibreOffice, que, devido à quantidade de informações e necessidade de compartilhamento, não seria a ferramenta ideal.

Outro problema relevante era o fato de que nem todos os servidores tinham facilidade em trabalhar com planilhas, o que aumentaria o tempo necessário para a conclusão do processo de mapeamento e tornaria a análise dos processos pouco funcional para a realidade. Diante disso, como um time bem alinhado, tivemos que usar nossa criatividade para adaptar o processo e garantir que ele fosse funcional.

Como mencionado, a Prefeitura de Joinville é um órgão de porte, relativamente grande, em uma cidade de médio porte, com cerca de 700 mil habitantes. São 18 órgãos da administração direta e 4 autarquias, sendo uma delas um hospital de alta complexidade sob gestão municipal, o que significa que um grande volume de dados é tratado, com um nível de criticidade elevado. Isso traz a certeza de que há uma infinidade de processos a serem analisados e, muito possivelmente, adequados para garantir a conformidade com a LGPD.

2.2. Estratégias para a adequação

O Município de Joinville adotou as estratégias para superar esses desafios abaixo listadas.

2.2.1. Estrutura mínima de governança

Para enfrentar esses desafios, o Município iniciou com a criação de uma estrutura mínima de governança.

Representantes das secretarias com o maior volume e criticidade de dados (Secretarias da Fazenda, Gestão de Pessoas, Assistência Social, Saúde, Educação, de Governo, Administração e Planejamento, Controladoria-geral, Procuradoria-geral e Companhia Águas de Joinville) foram convocados para formar o Comitê Municipal de Proteção de Dados. Esse grupo desempenhou um papel crucial na elaboração das regulamentações municipais sobre a LGPD

2.2.2. Publicação de decretos e regulamentações

Como parte do processo de adequação, o Município publicou os seguintes decretos: nº 44.844/2021, regulamentando a LGPD em Joinville; nº 46.169/2022, nomeando os membros do Comitê Municipal de Proteção de Dados; nº 48.597/2022, nomeando o Encarregado de Tratamento de Dados; e nº 47.858/2022, nomeando a Coordenação da Área de Proteção de Dados.

2.2.3. Implementação da Área de Proteção de Dados

A criação da Área de Proteção de Dados foi outra etapa essencial no processo de adequação, subordinada à Secretaria de Administração e Planejamento. Inicialmente, a área contava com apenas uma Coordenação, mas, no início de 2024, foi reforçada com a chegada de dois estagiários de Direito.

O cargo de Coordenação foi remanejado de outra área e a escolha da Secretaria, se deu pela necessidade de alocar a área o mais próximo das Unidades de Tecnologia da Informação e do Escritório de Processos num primeiro momento, para conhecer os processos e procedimentos já existentes e aproveitar a expertise dos servidores dessas unidades.

Com a implementação da Área de Proteção de Dados e a criação de uma equipe dedicada, o Município de Joinville estava preparado para iniciar a fase seguinte: o planejamento detalhado das ações necessárias para garantir a conformidade com a LGPD. Nesse contexto, a escolha das metodologias e ferramentas adequadas foi fundamental para assegurar a eficiência do processo.

2.2.4. Preparando o projeto

No segundo semestre de 2022, foi iniciado o processo de adequação.

O primeiro passo foi escolher as metodologias e ferramentas que seriam utilizadas. Assim, optou-se pelo uso do Project Model Canvas para

estruturar o projeto e apresentá-lo à Diretoria, destacando os objetivos, premissas, riscos, stakeholders, custos, entre outras informações relevantes.

Para organizar as tarefas e determinar prazos e responsáveis foi utilizado o Gráfico de Gantt, que permitiu visualizar o tempo de conclusão de cada etapa.

A metodologia ágil também foi aplicada com o uso do Kanban¹⁶², adaptado ao Trello para garantir um melhor controle e condução das tarefas e entregáveis

Na gestão de risco, a metodologia da norma ISO 31000 se mostrou a mais adequada. Quanto à Matriz de Risco, trabalhou-se com uma matriz qualitativa combinada com uma matriz 3x3 para avaliar a probabilidade e o impacto.

Na produção de conteúdos, aplicou-se o Legal Design e o Visual Law, buscando tornar as informações jurídicas e técnicas mais acessíveis por meio de elementos visuais e linguagem simples e clara.

Para a fase de mapeamento, a metodologia LGPD Model Canvas foi aproveitada durante a fase de conscientização, com o objetivo de trazer clareza sobre o conceito de mapeamento de processos que tratam dados pessoais e na fase de execução do mapeamento, foi empregado o Google Forms e o Google Sheets, que fazem parte dos serviços do Google Workspace contratados pelo Município.

Com as metodologias e ferramentas definidas, o próximo passo foi realizar uma avaliação detalhada do cenário atual, mapeando o volume de dados tratados e a maturidade das práticas de segurança da informação. Este diagnóstico foi essencial para fundamentar as etapas seguintes do processo de adequação.

¹⁶² Kanban é um método de gerenciamento de trabalho que visa melhorar a eficiência e a produtividade através da visualização do fluxo de trabalho e da limitação do trabalho em andamento (WIP - Work In Progress). Originado na Toyota nos anos 1950, o Kanban foi desenvolvido por Taiichi Ohno como parte do sistema de produção enxuta (Lean Manufacturing). Ele utiliza cartões visuais em um quadro para representar tarefas e seu progresso, ajudando as equipes a identificar gargalos e melhorar continuamente seus processos.

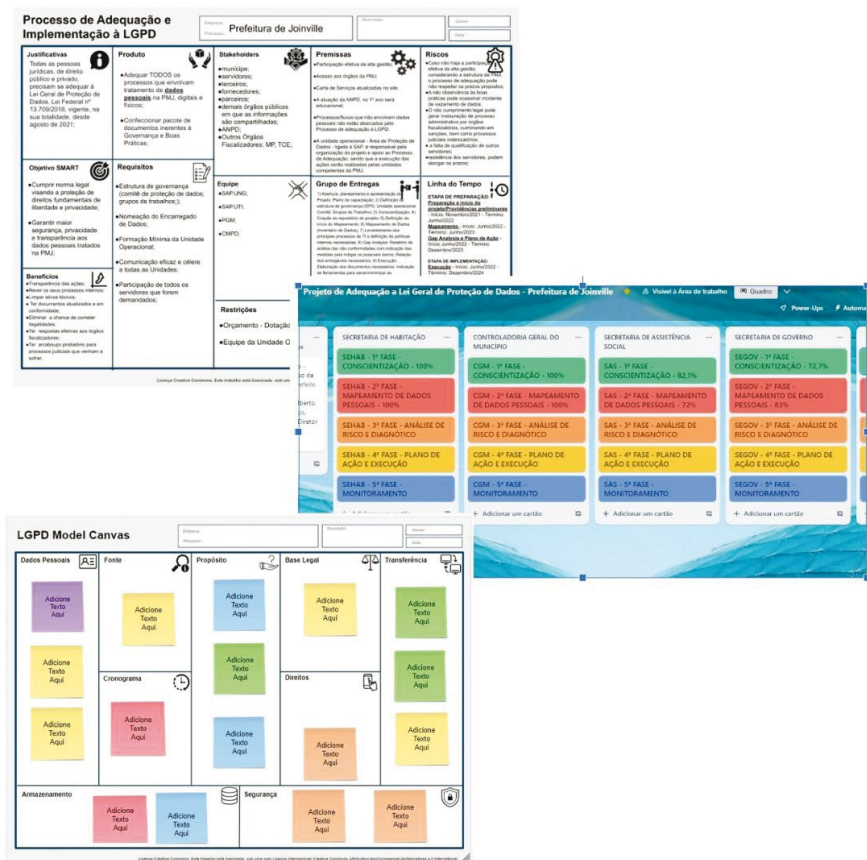


Imagem 2 – Diversas Metodologias aplicadas na fase de conscientização

2.2.5. Avaliação inicial do cenário atual

Para entender o cenário inicial, foi necessário realizar um levantamento abrangente sobre o volume de dados tratados pelos órgãos municipais, a quantidade de servidores e a maturidade das práticas de segurança da informação. Foi essencial mapear os sistemas em uso e identificar potenciais riscos e vulnerabilidades. Esse diagnóstico inicial permitiu determinar ações prioritárias e fundamentar o planejamento das etapas seguintes do processo de adequação.

2.2.6. Treinamento e sensibilização

Xavier (2022) ressalta que o elo humano frequentemente é negligenciado em ações institucionais. No contexto da Lei Geral de Proteção de Dados

(LGPD), ele enfatiza a importância da Instituição promover treinamentos contínuos, capacitações, campanhas de sensibilização e outras ações voltadas para servidores, contratados, jurisdicionados e parceiros. Essas medidas são fundamentais para garantir a segurança da informação, a privacidade e o adequado tratamento dos dados pessoais.¹⁶³

Coadunando com o referido autor, a capacitação dos servidores foi uma prioridade no processo de adequação à LGPD.

O treinamento começou com as equipes de gestão e foi gradualmente ampliado para todos os servidores, independente de suas funções.

Em pouco mais de 18 meses, cerca de 11 mil servidores foram conscientizados, sendo 2.195 presencialmente e o restante na forma online. Para a capacitação presencial, os auditórios do Corpo de Bombeiros Voluntários de Joinville, da Associação de Municípios do Nordeste de Santa Catarina - AMUNESC, e do Hospital Municipal São José foram utilizados, não representando nenhum custo adicional para o Município.

A ferramenta OBS Studio foi utilizada para gravação da conscientização, e o conteúdo foi disponibilizado na plataforma gratuita Moodle, configurada e adequada para o Município.

Atualmente, a cada início de mês, são identificados os servidores que ainda não passaram pela conscientização, e enviado a orientação para a devida realização. Novos servidores, estagiários, contratados, jovens aprendizes, quando iniciam suas atividades na Prefeitura, passam pela capacitação assim que entram.

Outra ação realizada foi a elaboração do guia orientativo para os servidores sobre a LGPD. O Guia está disponibilizado na forma online no sítio eletrônico do Município de Joinville¹⁶⁴. O material foi elaborado internamente, utilizando a ferramenta Canvas.com, também gratuita.

¹⁶³ XAVIER, Fábio Correa. LGPD no Setor Público: boas práticas para a jornada de adequação. 1. ed. Publicação Independente, 2022.

¹⁶⁴ MUNICÍPIO DE JOINVILLE. Cartilha Lei Geral de Proteção de Dados Pessoais - Lei Federal nº 13.709/2018. Disponível em: <https://www.joinville.sc.gov.br/wp-content/uploads/2022/05/Cartilha-Lei-Geral-de-Prote%C3%A7%C3%A3o-de-Dados-Pessoais-Lei-Federal-n%C2%BA-13.7092018-v2.pdf>. Acesso em: 05/08/2024.



Imagem 3 – Guia Orientativo para Servidores sobre LGPD – Comitê Municipal

Como evidências para o Processo de Adequação, foram realizadas listas de presenças, fotos, testes de conhecimento e emissão de certificados, o que possibilitou ter métricas conforme dashboard abaixo.

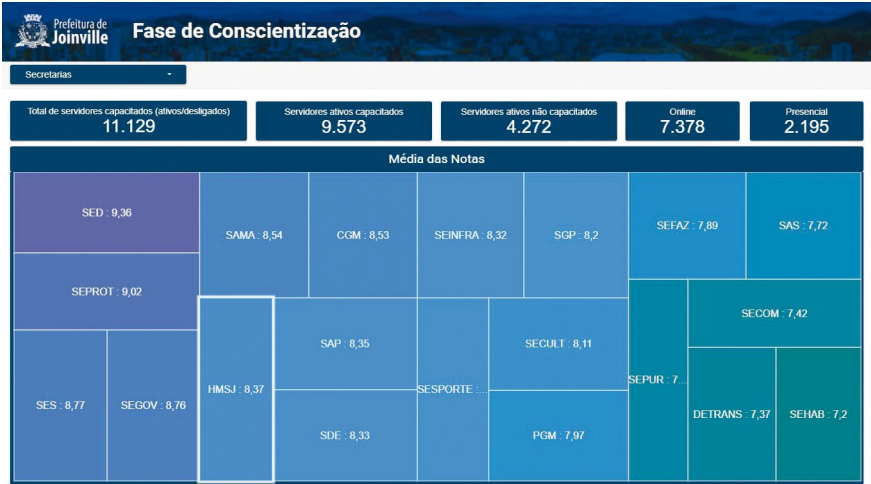


Imagem 4 – Dashboard do Processo de Adequação – Fase de Conscientização

Após a capacitação e sensibilização de boa parte dos servidores, o Município estava pronto para uma das etapas mais críticas do processo de adequação: o mapeamento dos processos que tratam dados pessoais. Esse mapeamento não só forneceu uma visão clara das atividades de cada órgão, como também permitiu a identificação de riscos e vulnerabilidades, preparando o terreno para a análise de riscos e a conformidade plena com a LGPD.

2.2.7. Mapeamento de processos de trabalho que tratam dados pessoais

No segundo semestre de 2023, com a maior parte dos servidores já conscientizados, deu-se início à fase de mapeamento. Essa etapa demandou considerável esforço, pois representava um momento crucial para a obtenção de um diagnóstico preciso das atividades dos órgãos. A partir dessa fase, tornou-se possível realizar a análise de riscos, elaborar o relatório de impacto, conforme exigido pela legislação, e propor soluções para garantir a aderência à Lei Geral de Proteção de Dados (LGPD).

Inicialmente, a equipe se deparou com a aplicação de um template disponibilizado pelo Governo Federal, que consistia em uma planilha Excel com aproximadamente 144 linhas de questionamentos. No entanto, esse modelo apresentou diversos problemas para a realidade local. Em primeiro lugar, a Prefeitura utiliza o LibreOffice, o que, dada a grande quantidade de informações e a necessidade de compartilhamento, não se mostrou a melhor opção. Outro problema, talvez o mais relevante, foi a complexidade do uso de planilhas por parte dos servidores, o que exigiria a criação de várias guias, uma para cada processo mapeado. Tal abordagem acarretaria um aumento significativo no tempo necessário para completar o mapeamento, além de dificultar a análise posterior dos dados, tornando o processo menos funcional para o contexto municipal.

Apesar das dificuldades, realizou-se um teste piloto com a Secretaria da Fazenda com o template do Governo Federal. E como previsto, restou inexitosa. Com este resultado, a equipe composta pelas Coordenações das Áreas de Indicadores, Desenvolvimento e Proteção de Dados, optou por adaptar o template do Governo Federal para um Google Forms, considerando que essa ferramenta seria mais intuitiva, acessível e atrativa aos servidores.

Ao contrário de algumas consultorias externas, nas quais os consultores preenchem as ferramentas de mapeamento, optou-se por um modelo

em que os próprios servidores analisariam seus processos e preencheriam o formulário, dada a estrutura descentralizada e robusta da Prefeitura.

O template original de 144 questionamentos foi reduzido para 41 perguntas objetivas, em sua maioria de múltipla escolha, a fim de facilitar o preenchimento. Após a definição da ferramenta, estudou-se a melhor estratégia de execução dessa fase nos órgãos.

Inicialmente, foram formados grupos de trabalho com, no mínimo, quatro servidores de cada órgão. O objetivo era realizar uma reunião de alinhamento e apresentar a ferramenta, para que esses servidores pudessem disseminar as informações em seus respectivos órgãos. A estratégia funcionou bem em órgãos menores, como a Secretaria da Habitação, Controladoria-Geral e Secretaria de Governo, mas não teve o mesmo sucesso em órgãos maiores, como a Secretaria de Gestão de Pessoas e a Secretaria da Fazenda.

Diante desse cenário, a estratégia foi reformulada, optando-se por realizar reuniões de alinhamento diretamente com os coordenadores de cada setor. Ao todo, foram realizadas 40 reuniões de alinhamento. Em Joinville, a maioria das unidades e setores possuem um coordenador ou líder de área, profissionais que atuam no nível intermediário da Instituição, entre o operacional e o tático. Com a nova abordagem, cada coordenador ficou responsável pelo mapeamento de sua unidade, o que resultou em um processo mais eficiente. O Hospital São José e as Secretarias de Educação e Saúde, que são as mais robustas, foram as últimas a receberem as orientações e iniciarem o mapeamento. O entendimento é de que a ferramenta e a dinâmica utilizada precisariam estar maduras, ou melhor, testadas, para chegar às Secretarias de maior porte.

À medida que os formulários eram enviados por meio da plataforma *GoogleForms*®, uma planilha centralizada era alimentada, servindo como base para o início das análises de risco.



Imagem 5 – Cruzamento de dados no Mapeamento dos Processos com Googleforms®

Vencida mais uma fase, uma nova etapa iniciava - a análise do mapeamento dos processos de trabalho que tratam dados pessoais, os riscos envolvidos, diagnóstico e planejamento de ações para garantir a aderência à legislação federal.

Com o mapeamento completo dos processos de trabalho que envolvem dados pessoais, o próximo desafio foi realizar uma gestão eficaz dos riscos associados. Nesse ponto, a aplicação da metodologia da Norma ABNT NBR ISO/IEC 31000:2018 foi crucial para garantir que todas as não conformidades fossem devidamente identificadas e classificadas.

2.2.8. Gestão de riscos e análise de impacto

Com os processos de trabalho devidamente mapeados, foi possível realizar uma gestão eficaz de riscos. A metodologia constante da Norma

ABNT NBR ISO/IEC 31000:2018 foi utilizada para identificar e classificar as ações que não estavam em conformidade com a LGPD. Assim, a partir do mapeamento e da análise de riscos, um novo documento começou a ser estruturado, o Relatório de Impacto de Proteção de Dados (RIPD). Tal documento é essencial, obrigatório e descreve os processos de tratamento de dados de alto risco e as medidas de mitigação adotadas.

2.2.9. Relatório de Impacto de Proteção de Dados

Conforme a ANPD, o RIPD é a documentação que contém a descrição dos processos de tratamento de dados pessoais que podem gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais do titular de dados. Deve conter as medidas, salvaguardas e mecanismos de mitigação de risco, nos termos dos artigos 5º, inciso XVII, e 38 da Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD).¹⁶⁵

A LGPD lista, ainda, situações específicas em que o RIPD poderá ser exigido pela ANPD, como nas operações de tratamento efetuadas para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (art. 4º, § 3º); quando o tratamento tiver como fundamento a hipótese de interesse legítimo (art. 10, § 3º); para agentes do Poder Público, incluindo determinação quanto à publicação do RIPD (art. 32); e para controladores em geral, quanto às suas operações de tratamento, incluindo as que envolvam dados pessoais sensíveis (art. 38).¹⁶⁶

No Município de Joinville, que utiliza o Sistema Eletrônico de Informação - SEI¹⁶⁷, foi instituído um Processo Eletrônico exclusivo para a elaboração do RIPD, com um modelo padrão autoexplicativo de documento.

¹⁶⁵ AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Relatório de Impacto à Proteção de Dados Pessoais (RIPD). Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd#p1. Acesso em: 05/08/24.

¹⁶⁶ BRASIL. Presidência da República. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 02/08/2024.

¹⁶⁷ Sistema Eletrônico de Informações (SEI) é um sistema desenvolvido pelo Tribunal Regional Federal da 4ª Região (TRF4). Usada também em outras instituições públicas brasileiras, como sistema de gestão de processos e documentos eletrônicos.

Desta forma, os relatórios ficaram em ambiente seguro, com acesso através de login e senha e segmentação por unidade de trabalho, tendo assinatura eletrônica.

O intuito de criar um processo eletrônico era evitar que os RIPDs ficassem armazenados em simples arquivos de texto, vez que podem indicar vulnerabilidade de alguns processos de trabalho

2.2.10. Outras ações de adequação à LGPD

De acordo com um estudo divulgado pelo Cetic.br, três medidas principais poderiam reduzir 80% dos incidentes de segurança reportados ao Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (CERT.br), baseando-se na Regra de Pareto 80/20, que sugere que 80% dos problemas podem ser resolvidos ao corrigir 20% das causas. As soluções destacadas pelo estudo incluem: manter todos os softwares e dispositivos atualizados com as últimas versões e correções de segurança; realizar o *hardening* de sistemas, desabilitando serviços desnecessários, alterando senhas padrão e configurando os serviços expostos na Internet de maneira segura; e melhorar os processos de identificação e autenticação, implementando múltiplos fatores de autenticação e promovendo a educação sobre a gestão de senhas, com foco na não reutilização de senhas.¹⁶⁸

Com esta preocupação, o Município de Joinville, assim como muitos outros municípios brasileiros, já seguia protocolos de segurança da informação, como segurança de rede, atualizações de sistemas, backups, controle de acessos e gestão de incidentes.

No entanto, não existiam políticas específicas ou ações de conscientização sobre como agir, por exemplo, diante de um e-mail de *phishing*.

Segundo Pinheiro (2023), apesar de a internet e as ferramentas tecnológicas já não serem novidade, ainda há incerteza sobre o que é correto ou incorreto no seu uso, especialmente em ambientes corporativos. Por isso, cabe às empresas definir políticas e diretrizes de segurança da informação

¹⁶⁸ CENTRO REGIONAL DE ESTUDOS PARA O DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO (Cetic.br). Estudos setoriais de segurança digital. Disponível em: <https://cetic.br/media/docs/publicacoes/7/20210514123130/estudos-setoriais-seguranca-digital.pdf>. Acesso em: 12 set. 2024.

que protejam tanto o negócio quanto os empregados, evitando riscos que possam gerar responsabilidade jurídica ou até demissões.¹⁶⁹

Conforme a norma ABNT NBR ISO/IEC 27002:2013, a segurança da informação é obtida por meio da aplicação de controles adequados, que envolvem políticas, processos, procedimentos, além de uma estrutura organizacional e funções de software e hardware.¹⁷⁰

Diante dessa realidade, foram iniciadas tratativas para a elaboração de documentos prioritários, como o termo de uso e política de privacidade, já que o sítio eletrônico do Município não possuía uma política de privacidade, mesmo com o aumento dos serviços eletrônicos ofertados à população. Além disso, foi criado o termo de compromisso, sigilo e confidencialidade para servidores públicos, contratados, cargos em comissão e estagiários. Durante o levantamento dos sistemas utilizados pelo Município, constatou-se o uso de aproximadamente 300 sistemas, entre governamentais, próprios, contratados e gratuitos. Diante disso, optou-se por conscientizar os servidores sobre a importância de não utilizar dados pessoais sem autorização para benefício próprio. O termo de compromisso, sigilo e confidencialidade foi discutido em reunião com o Comitê Municipal de Proteção de Dados, revisado pela Procuradoria-Geral do Município e distribuído para assinatura individual de todos os servidores através dos Núcleos de Gestão de Pessoas de cada órgão, pelo Sistema SEI. Apesar de algumas dificuldades e reuniões adicionais para esclarecimentos, cerca de 11 mil termos foram assinados. Tal documento agora faz parte do processo de admissão de novos servidores e estagiários.

Para garantir que os direitos dos titulares de dados pessoais fossem respeitados, o canal de Ouvidoria do Município foi ajustado para integrar a solicitação desses direitos, com uma carta de serviço específica detalhando os direitos garantidos pela LGPD.

¹⁶⁹ PINHEIRO, Patrícia Peck. Direito Digital. 7ª ed. São Paulo: SaraivaJur, 2023.

¹⁷⁰ ABNT NBR ISO/IEC 27002:2013. Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação. Rio de Janeiro: ABNT, 2013.

Registrar Pedido de Informação sobre dados pessoais

Carta de Serviço publicada conforme Processo SEI nº 23.0.117081-5, em atendimento à Lei nº 13.460/2017. Última atualização: 08/07/2024 às 12:20.

Registre Pedido de Informação

O que é?
 Quem pode fazer?
 Onde e quando fazer?
 Como fazer?
 1) Registrar Pedido
 2) Consultar tramitação
 3) Receber parecer
 Quanto custa?
 Quanto tempo leva?
 Sobre estas informações
 Manifestar-se

Imagem 6 - Interface de acesso à Ouvidoria – Site Institucional Prefeitura de Joinville

Foi também realizada a escolha e divulgação do Encarregado de Tratamento de Dados nas plataformas do Município. Optou-se inicialmente pela centralização do Encarregado, com um titular e um suplente, até que o processo de adequação estivesse mais amadurecido. Para a seleção do titular e do suplente, foram considerados fatores como o conhecimento das áreas de negócios do Município, graduação, domínio técnico e jurídico sobre o tema, interesse em certificações e habilidades de comunicação. Até o momento, não há previsão de gratificação pecuniária para a função de Encarregado de Tratamento de Dados.

Outra ação importante foi a criação de um decreto para o compartilhamento de dados pessoais entre os órgãos da administração direta e indireta, que formalizou as práticas já existentes e garantiu que os requisitos legais da ANPD fossem seguidos. O compartilhamento de dados é crucial para atividades como a análise de aposentadoria, fiscalização de saneamento básico, políticas públicas voltadas à saúde, assistência social, educação, entre outras.

Acerca do tema a ANPD se pronunciou no Guia de Tratamento de Dados Pessoais pelo Poder Público:

“O uso compartilhado de dados é um mecanismo relevante para a execução de atividades típicas e rotineiras do Poder Público, a exemplo de pagamento de servidores e prestação de serviços públicos. A lgpd reconhece essa relevância ao estabelecer, em seu art. 25, que os dados devem ser mantidos “em formato interoperável e estruturado

para o uso compartilhado”, visando, entre outras finalidades, “à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral”¹⁷¹

Diante da quantidade de contratos e convênios do Município que envolvem dados pessoais, foi necessário desenvolver cláusulas padrão de LGPD para os referidos instrumentos. Entre os contratos mais relevantes estão os de empresas que realizam regularização fundiária, clínicas médicas que complementam o atendimento ao SUS e centros de educação infantil particulares. As cláusulas foram elaboradas em conjunto com o Comitê Municipal de Proteção de Dados e a Procuradoria-Geral do Município.

O Município também enviou ofícios aos stakeholders externos, em especial fornecedores, para entender o grau de adequação à LGPD e as práticas de segurança da informação adotadas por esses parceiros. Foram priorizados os fornecedores de tecnologia, visto que muitos sistemas críticos para o Município são geridos por essas empresas, e, em alguns casos, os contratos já foram ajustados.

Quanto à Política de Segurança da Informação, o Município está finalizando a revisão das práticas de retenção e descarte de dados pessoais, controle de acesso a sistemas, uso da internet, backup, trabalho remoto e uso de VPN, além de outras medidas como o Privacy by Design¹⁷². A criação de um plano de resposta a incidentes e remediação também está em fase final, e o protocolo TLP (Traffic Light Protocol), utilizado pelo Governo Federal, está sendo considerado para classificação de informações.

Por fim, foram promovidas outras ações, como a redução de dados desnecessários publicados no sítio eletrônico do Município, incluindo listas de presenças de reuniões, e a pseudoanonimização das listas públicas de vagas em Centros de Educação Infantil (CEIs). A Controladoria-Geral do Município também lidera a elaboração do Código de Ética do Servidor Público de Joinville, alinhado às novas exigências da LGPD.

¹⁷¹ ANPD. Guia Orientativo: Tratamento de Dados Pessoais pelo Poder Público. Versão 2.0, junho de 2023, Brasília. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes>. Acesso em: 16 de setembro de 2024.

¹⁷² O conceito de Privacy by Design (Privacidade desde a Concepção) foi desenvolvido nos anos 90 pela especialista em privacidade de dados, Ann Cavoukian. Ele se tornou um padrão internacional em 2010 e é uma abordagem que visa incorporar a privacidade e a proteção de dados pessoais desde o início de qualquer projeto ou sistema.

3. RESULTADOS

De acordo com o Comitê Gestor da Internet no Brasil (CGI.br, 2024), a pesquisa TIC Governo Eletrônico tem monitorado, desde 2021, as ações voltadas à privacidade e proteção de dados pessoais em órgãos públicos federais, estaduais e municipais. Os resultados mais recentes, de 2023, mostram um crescimento significativo de iniciativas nas prefeituras de grandes municípios, especialmente nas capitais, em relação à implementação da LGPD. No entanto, ainda há desafios, principalmente em municípios de menor porte, onde muitas prefeituras não possuem estruturas adequadas para atender plenamente as exigências da legislação.¹⁷³

A referida pesquisa revela um crescimento expressivo nas iniciativas de privacidade e proteção de dados em prefeituras de capitais e municípios com mais de 100 mil habitantes. O percentual de prefeituras de capitais com áreas ou pessoas responsáveis pela implementação da LGPD subiu de 66% em 2021 para 82% em 2023, enquanto nas cidades de mais de 500 mil habitantes esse número aumentou de 62% para 82%. No entanto, em cidades menores, especialmente nas do interior, o crescimento foi mais modesto, com um aumento de 28% para 36% no mesmo período. Ainda assim, as prefeituras do Nordeste apresentaram os menores índices de conformidade, com apenas 33% contando com áreas específicas para proteção de dados.¹⁷⁴

O processo de adequação à LGPD no Município de Joinville gerou uma série de resultados significativos, tanto no que diz respeito à conformidade legal quanto à melhoria da governança de dados. Nesta seção, serão apresentados os principais resultados alcançados até o momento, bem como os objetivos futuros que a administração municipal espera atingir. Serão discutidos aspectos como a economia gerada, a capacitação de servidores,

¹⁷³ COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). Privacidade e proteção de dados pessoais 2023: perspectivas de indivíduos, empresas e organizações públicas no Brasil = Privacy and personal data protection 2023: perspectives of individuals, enterprises and public organizations in Brazil. São Paulo: CGI.br, 2024. Disponível em: <https://cetic.br/media/docs/publicacoes/2/20240901120340/privacidade-e-protecao-de-dados-2023.pdf>. Acesso em: 11 de setembro de 2024.

¹⁷⁴ COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). Privacidade e proteção de dados pessoais 2023: perspectivas de indivíduos, empresas e organizações públicas no Brasil = Privacy and personal data protection 2023: perspectives of individuals, enterprises and public organizations in Brazil. São Paulo: CGI.br, 2024. Disponível em: <https://cetic.br/media/docs/publicacoes/2/20240901120340/privacidade-e-protecao-de-dados-2023.pdf>. Acesso em: 11 de setembro de 2024.

o impacto na cultura organizacional e os benefícios para os cidadãos. Esses resultados demonstram o sucesso da iniciativa e as oportunidades de aprimoramento contínuo.

3.1. Resultados Alcançados

Um dos principais resultados alcançados foi a conformidade legal, com a estruturação de processos que garantem o tratamento adequado dos dados pessoais. A publicação de decretos, a criação da Área de Proteção de Dados e a nomeação do Encarregado de Tratamento de Dados foram passos fundamentais que consolidaram essa conformidade dentro da administração pública municipal.

Outro resultado significativo foi a transparência no tratamento de dados, que foi aprimorada com a criação de canais específicos para que os cidadãos pudessem exercer seus direitos como titulares de dados pessoais, conforme previsto na LGPD. Isso aumentou a confiança dos servidores e da população nas práticas adotadas pelo Município.

A segurança da informação também foi reforçada, com a implementação de controles de acessos, backup de dados e a criação de um plano de resposta a incidentes, o que reduziu consideravelmente os riscos de vazamentos de dados ou ataques cibernéticos. A introdução de práticas de Privacy by Design também garantiu que novos sistemas e processos já considerassem a proteção de dados desde o início.

No âmbito da cultura organizacional, houve um avanço notável com o engajamento dos servidores no processo de adequação à LGPD. Mais de 11 mil servidores foram conscientizados sobre a importância da proteção de dados, por meio de treinamentos presenciais e online, o que resultou em um aumento significativo da cultura de privacidade entre os funcionários públicos municipais.

A participação do Município em grupos de discussão e fóruns sobre proteção de dados públicos também trouxe benefícios, como a colaboração com outras prefeituras e a elaboração do Guia Prático para a fase de conscientização e treinamento da adequação à LGPD¹⁷⁵, em parceria com as cidades de Recife, Londrina e Paulista. Isso fortaleceu o ecossistema de proteção de dados, facilitando a disseminação de boas práticas.

¹⁷⁵ <https://municipioslgpd.com.br/documentos/>

Por fim, o Município conseguiu gerar uma economia significativa ao realizar o processo de adequação internamente, sem a contratação de consultorias externas. A capacitação dos próprios servidores para conduzir o processo resultou numa economia de mais de um milhão e meio de reais, conforme as estimativas iniciais de contratação de serviços externos.

3.2. Resultados Esperados e Metas a serem atingidas

Embora muitos avanços tenham sido realizados, ainda existem áreas que precisam ser aprimoradas. Um dos resultados esperados no futuro é o aumento da maturidade dos processos de proteção de dados, especialmente em relação à automação de algumas tarefas e à melhoria dos sistemas de monitoramento.

O Município ainda busca aprimorar o controle sobre o uso compartilhado de dados entre os órgãos da administração direta e indireta, e espera que, com o tempo, possa indicar um Encarregado de Dados para cada órgão, à medida que a equipe se qualificar adequadamente.

Outro ponto que precisa ser trabalhado é o engajamento dos cidadãos. Embora a transparência tenha sido reforçada, o Município ainda espera que os cidadãos utilizem de forma mais ativa os canais de exercício de seus direitos de dados, e que o nível de conhecimento da população sobre a LGPD aumente. Para isso, são necessárias ações de comunicação mais amplas e campanhas de conscientização voltadas para o público externo. De um modo geral, o engajamento do cidadão também proporcionará um nível de educação diferenciado reduzindo o número de ocorrências de golpes, principalmente cibernéticos.

No que tange à segurança da informação, espera-se finalizar e formalizar a política de segurança da informação, incluindo a implementação de um protocolo para a classificação de informações. Além disso, o plano de resposta a incidentes precisa ser completamente implementado e testado, para garantir que, em caso de um incidente, as respostas sejam rápidas e eficazes.

A consolidação da cultura de proteção de dados também é uma meta de longo prazo, especialmente em áreas onde a adesão às boas práticas de privacidade ainda é desafiadora. O Município espera continuar promovendo capacitações regulares e atualizações para os servidores, além de desenvolver novos materiais educativos para reforçar os princípios da LGPD e garantir que a conformidade se mantenha sólida ao longo do tempo.

Por fim, espera-se que a integração com stakeholders externos seja ampliada. Embora o Município tenha iniciado tratativas com fornecedores e outros parceiros, ainda é necessário que todos estejam plenamente adequados à LGPD, com contratos devidamente ajustados e práticas de segurança de dados bem estabelecidas

4. CONSIDERAÇÕES FINAIS

O processo de adequação à LGPD no Município de Joinville demonstra que, com uma abordagem estratégica e o comprometimento de todos os envolvidos, é possível implementar mudanças significativas no setor público, garantindo a conformidade legal e a proteção dos dados pessoais dos cidadãos. O case de Joinville mostrou-se inovador ao utilizar recursos internos, sem onerar os cofres públicos, e ao adotar práticas de governança de dados alinhadas com a legislação vigente.

Além disso, a criação de uma cultura organizacional voltada para a privacidade e segurança de dados foi um dos grandes marcos dessa jornada, com mais de 11 mil servidores treinados e conscientizados. A implementação de políticas e práticas de segurança da informação também foi essencial para garantir a mitigação de riscos e a prevenção de incidentes.

Embora muitos desafios tenham sido enfrentados ao longo do processo, como o grande volume de dados tratados e a complexidade da estrutura organizacional, as estratégias adotadas pelo Município, como o mapeamento de processos, a gestão de riscos e a criação de um Comitê Municipal de Proteção de Dados, foram fundamentais para o sucesso da iniciativa.

A experiência de Joinville serve como inspiração para outras administrações públicas no Brasil, mostrando que, com planejamento e inovação, é possível atender às exigências da LGPD de forma eficiente e eficaz. No entanto, o trabalho de adequação à proteção de dados é contínuo, e a manutenção dessas práticas será essencial para garantir a conformidade a longo prazo e fortalecer ainda mais a confiança da população nas instituições públicas.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT NBR ISO/IEC 27002:2013. **Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação**. Rio de Janeiro: ABNT, 2013.

ALURA. **Kanban**: o que é, Método Kanban e como funciona. Disponível em: <https://www.alura.com.br/artigos/metodo-kanban>. Acesso em: 16 set. 2024.

ANPD. **Guia Orientativo**: Tratamento de Dados Pessoais pelo Poder Público. Versão 2.0, junho de 2023, Brasília. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes>. Acesso em: 16 de setembro de 2024.

ANPD. **Relatório de Impacto à Proteção de Dados Pessoais (RIPD)**. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd#p1. Acesso em: 05 ago. 2024.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: [05 ago.2024].

CETIC.br. **Estudos Setoriais de Segurança Digital**. Disponível em: <https://cetic.br/media/docs/publicacoes/7/20210514123130/estudos-setoriais-seguranca-digital.pdf>. Acesso em: 12 set. 2024.

CGI.br. **Privacidade e proteção de dados pessoais 2023**: perspectivas de indivíduos, empresas e organizações públicas no Brasil. São Paulo: CGI.br, 2024.

CORRÊA, Fábio Xavier. **LGPD no Setor Público**: boas práticas para a jornada de adequação. 1. ed. Publicação Independente, 2022.

LANZER, Fernando. **Clima e Cultura Organizacional**: entender, manter e mudar. 2. ed. 2017.

PINHEIRO, Patrícia Peck. **Direito Digital**. 7ª ed. São Paulo: SaraivaJur, 2023.

SISPRO. **Privacy by Design: Incorporando a Privacidade desde a Concepção**. Disponível em: <<https://www.sispro.com.br>> Acesso em: 16 set. 2024.

BRASIL, Tribunal de Contas da União. **TCU analisa segurança cibernética de instituições federais**. Disponível em: <https://portal.tcu.gov.br/imprensa/noticias/tcu-analisa-seguranca-cibernetica-de-instituicoes-federais.htm#:~:text=A%20fiscaliza%C3%A7%C3%A3o%20do%20TCU%20apurou,dados%20em%20meados%20de%202021>. Acesso em: 02 ago. 2024.

Enviado em 23.09.2024.

Aprovado em 21.10.2024.



Este trabalho está licenciado sob uma licença Creative Commons Attribution-NonCommercial 4.0 International License.

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.