Avaliação de Conformidade com a LGPD:
Um Modelo de Maturidade de Processos

Jonas Pereira de Andrade Filho

CENTRO DE INFORMÁTICA
UNIVERSIDADE FEDERAL DA PARAÍBA

João Pessoa, 2024

Jonas Pereira de Andrade Filho

Avaliação de Conformidade com a LGPD: Um Modelo de Maturidade de Processos

Dissertação apresentada ao curso Pós-Graduação em Informática do Centro de Informática, da Universidade Federal da Paraíba, como requisito para defesa do mestrado.

Orientador: Prof. Dr. Gustavo Motta

Dezembro de 2024

Catalogação na publicação
Seção de Catalogação e Classificação

F481a Andrade Filho, Jonas Pereira de.
Avaliação de conformidade com a LGPD : um modelo de maturidade de processos / Jonas Pereira de Andrade Filho. - João Pessoa, 2024.
117 f. : il.

Orientação: Gustavo Motta.
Dissertação (Mestrado) - UFPB/PPGI.

1. Informática. 2. LGPD (Lei Geral de Proteção de Dados). 3. Segurança da informação. 4. Dados pessoais - privacidade. I. Motta, Gustavo. II. Título.

UFPB/BC CDU 004(043)

Elaborado por RUSTON SAMMEVILLE ALEXANDRE MARQUES DA SILVA - CRB-15/0386

UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA

Ata da Sessão Pública de Defesa de Dissertação de Mestrado de Jonas Pereira de Andrade Filho, candidato ao título de Mestre em Informática na área de Sistemas de Computação, realizada em 30 de agosto de 2024.

Aos trinta dias do mês de agosto do ano de dois mil e vinte e quatro, às dezesseis horas, no Centro de Informática da Universidade Federal da Paraíba, reuniram-se os membros da Banca Examinadora constituída para julgar o Trabalho Final do discente Jonas Pereira de Andrade Filho, vinculado a esta Universidade sob a matrícula nº 20221004994, candidato ao grau de Mestre em Informática, na área de *"Sistemas de Computação"*, na linha de pesquisa *"Computação Distribuída"*, do Programa de Pós-Graduação em Informática. A comissão examinadora foi composta pelos professores: Gustavo Henrique Matos Bezerra Motta, Orientador e Presidente da banca; Clauirton de Albuquerque Siebra, Examinador Interno; Thiago Pereira da Nóbrega, Examinador Externo à Instituição. Dando início aos trabalhos, o Presidente da Banca cumprimentou os presentes, comunicou a finalidade da reunião e passou a palavra ao candidato para que ele fizesse a exposição oral do trabalho de dissertação intitulado "**Avaliação de Conformidade com a LGPD: Um Modelo de Maturidade de Processos**". Concluída a exposição, o candidato foi arguido pela Banca Examinadora que emitiu o seguinte parecer: "***aprovado***". Do ocorrido, eu, Gilberto Farias de Sousa Filho, coordenador do Programa de Pós-Graduação em Informática, lavrei a presente ata que vai assinada por mim e pelos membros da Banca Examinadora. João Pessoa, 30 de agosto de 2024.

Gilberto Farias de Sousa Filho
Coordenador do Programa de Pós-Graduação em Informática

Prof. Dr. Gustavo Henrique M. Bezerra Motta _____
Orientador (PPGI-UFPB)

Prof. Dr. Clauirton de Albuquerque Siebra _____
Examinador Interno (PPGI-UFPB)

Prof. Dr. Thiago Pereira da Nóbrega _____
Examinador Externo à Instituição (UFCG)

DEDICATÓRIA

À minha esposa e ao nosso filho, por toda a paciência, compreensão e amor nos momentos em que a minha ausência se fez necessária. Vocês foram minha fonte de motivação e força em cada passo dessa jornada.

Aos meus pais, por todo o conhecimento, apoio e valores que me transmitiram ao longo da vida. Vocês plantaram em mim a semente do saber, e por isso, sou eternamente grato.

Ao meu orientador, pela orientação, paciência e compreensão ao longo deste percurso. Sua sabedoria e apoio foram fundamentais para a concretização deste trabalho.

A todos os amigos, colegas de trabalho, de alguma forma, contribuíram para que este momento se tornasse realidade, meu sincero e eterno agradecimento.

RESUMO

O crescimento exponencial das atividades digitais nas últimas décadas, como o comércio eletrônico, o trabalho remoto e o ensino à distância, trouxe inegáveis benefícios econômicos e sociais devido à adoção acelerada de Tecnologias de Informação e Comunicação. Contudo, este desenvolvimento resultou em uma coleção massiva de dados pessoais. O aumento do volume de dados gerados e compartilhados elevou significativamente os riscos de violação da privacidade, tornando essencial a implementação de regulamentações robustas para garantir a proteção desses dados nos serviços digitais públicos e privados. Este trabalho propõe um modelo de maturidade de processos para auxiliar as organizações (públicas e privadas) a atenderem aos requisitos legais de conformidade com a Lei Geral de Proteção de Dados (LGPD), visando estabelecer uma estrutura clara e eficaz para avaliar o nível de maturidade das organizações em relação à LGPD. A falta de conformidade das organizações com esta Lei representa um obstáculo para as ambições do país de ingressar em blocos econômicos e organismos internacionais importantes, como também pode trazer prejuízos para o sistema de proteção de dados nacional. Espera-se que com implementação desse modelo possa oferecer suporte às organizações para alinhar-se aos princípios delineados na LGPD, ao mesmo tempo, em que lhes permita avaliar o grau de maturidade alcançado em relação aos critérios delineados pela legislação.

Palavras-chave: Lei Geral de Proteção de Dados; LGPD; Modelo de Capacidade e Maturidade Integrado; Privacidade; Segurança da Informação.

ABSTRACT

The exponential increase in digital activities, such as e-commerce, remote work, and distance education over the past decades, has brought economic and social benefits through the rapid adoption of Information and Communication Technology. However, this has also led to a rapid accumulation of data. This exponential growth in the volume of data generated and shared has significantly elevated the risk of privacy breaches, making the implementation of robust regulations essential. To achieve a fully digital government, it is crucial that the sharing of personal data in all spheres is both socially appropriate and compliant with regulatory bodies. This paper proposes a process maturity model to assist organizations in meeting these legal compliance requirements with the General Data Protection Law (LGPD). The goal is to establish a clear and effective structure for evaluating an organization's level of maturity in relation to the Law. Non-compliance with this law represents an obstacle to the country's ambitions of joining important economic blocs and international organizations and may also harm the national data protection system. It is expected that the implementation of this model will support organizations in aligning with the principles outlined in the LGPD, while also enabling them to assess the level of maturity achieved concerning the criteria set by the legislation.

Key-words: General Data Protection Law; LGPD; Integrated Capability Maturity Model; Privacy; Information Security

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

ANPD Agência Nacional de Proteção de Dados

BMC Business Model Canvas

BPMN Business Process Model and Notation

BCB Banco Central do Brasil

CMMI *Capability Maturity Model Integration*

CMM *Capability Maturity Model*

CMMPC *Capability Maturity Model for Privacy Concern*

CB Constituição Brasileira

DPD *Data Protection Directive*

DPO *Data Protection Officer*

DMM *Data Maturity Model*

EUA Estados Unidos da América

FOIA Freedom of Information Act

GDPR General Data Protection Regulation

HIPAA Health Insurance Portability and Accountability Act

LAI Lei de Acesso à Informação

LGPD Lei Geral de Proteção dos Dados

POSIN Política de Segurança da Informação

POSIC Política de Segurança da Informação e Comunicação

RNP Rede Nacional de Pesquisa

RGPD Regulamentação Geral de Proteção de Dados

SEI *Software Engineering Institute*

SGSI Sistema de Gestão de Segurança da Informação

TIC Tecnologia da Informação e Comunicação

TCC Trabalho de Conclusão de Curso

UE União Europeia

WIP *Work In Progress*

Sumário

1 INTRODUÇÃO

1.1 Introdução

O aumento exponencial de acesso à internet tem beneficiado bilhões de pessoas nessas duas últimas décadas. A rápida adoção de recursos de Tecnologia da Informação e Comunicação (TIC) promoveu diversas oportunidades econômicas e sociais, originadas do ambiente digital (BRASIL, 2020).

O avanço da conectividade está transformando o cenário digital. Com a proliferação de diversos tipos de dispositivos conectados à internet, a quantidade e os tipos de dados coletados têm crescido rapidamente. À medida que novas tecnologias se aprimoram, as informações do consumidor tornam-se mais acessíveis, valiosas e, consequentemente, mais vulneráveis do que nunca (RAINIE; ANDERSON, 2017).

Mesmo que um excesso de informações tenha sido fornecida de forma voluntária pelos consumidores por meio de atividades diárias, como de visitar um consultório médico, usar aplicativos, dispositivos vestíveis, publicação em redes socais ou interagir com dispositivos de aprendizado de máquina como Alexa[1] – os dados são geralmente coletados de forma clandestina (AGUIRRE et al., 2015)

Informações coletadas sem consentimento colocam os consumidores em risco eminentes de roubo de identidade, discriminação ou até um tipo de perseguição obsessiva. Enquanto aqueles indivíduos que fornecem seus dados pessoais de forma espontânea, criam a expectativa de que suas informações sejam usadas para o propósito acordado, assim como mantido privado e sigilo. Normalmente essa permissão é fornecida na forma de termos de serviço, inscrição por e-mail e/ou políticas de privacidade (WEISS, 2018).

No mundo digital interconectado de hoje, a proliferação das tecnologias digitais e o crescimento exponencial dos dados aumentaram a importância de proteger a privacidade e a segurança dos dados, tornando-se preocupações primordiais para indivíduos, organizações e governos. O ambiente corporativo e tecnológico não se resume mais a apenas às salas de aula ou aos escritórios – ele está em qualquer lugar onde haja conexão com a internet. Soluções de segurança que enxergam a rede da empresa como um mundo interno e sempre confiável não se aplicam mais nesse cenário. O sistema de videoaulas e a colaboração digital no trabalho levam a rede a ambientes inesperados. Foi necessário pensar em abordagens e tecnologias capazes de gerir o risco desses acessos pluralizados, deslocando o foco da segurança da rede para o negócio e do sistema para o monitoramento e validação (FAYAYOLA; OLORUNFEMI; SHOETAN, 2024).

[1] Alexa é uma assistente virtual desenvolvida pela Amazon, que é capaz de interagir com o usuário através da voz, podendo reproduzir música, definir alarmes, fornecer informações sobre o tempo, trânsito, esportes entre outras informações em tempo real, como notícias, além de controlar sistemas e aparelhos inteligentes e conectados

Com todas essas conexões ou hiper conexões, surgem dilemas éticos e morais, além de novos desafios para a necessidade regulamentar o uso indiscriminado de dados no universo virtual. As organizações também tem seu papel no uso de dados pessoais, e assim, em vários países adotaram leis de proteção para gerir este uso. Uma das pioneiras é o General Data Protection Regulation (GDPR), ou Regulamento Geral sobre a Proteção de Dados, adotado nos países da União Europeia e empresas que tratam dados de titulares que moram nessa região (TEAM, 2020).

1.2 Problemática

No Brasil, regulamentação semelhante foi elaborada e promulgada em agosto de 2018 (porém com vigência a partir de 2020), denominada de Lei Geral de Proteção dos Dados. Esta lei impõe a obrigatoriedade de adequação das empresas para a proteção à privacidade em dados pessoais, englobando as organizações em todos os níveis e o não cumprimento das exigências estabelecidas sujeitará em penalidades legais.

Recentemente, o Brasil alcançou uma posição de destaque ao se tornar o 7º país mais digitalizado do mundo, o primeiro em toda a região das Américas, superando inclusive os Estados Unidos da América e o Canadá (DENER et al., 2021). Diante dessa realidade, o amplo fluxo de dados pessoais na internet pode atrair a ocorrência de crimes cibernéticos, exigindo o reforço das medidas técnicas de segurança.

Visando promover a confiança tanto no âmbito nacional quanto internacional em relação às transações digitais, medidas mais efetivas têm sido adotadas para salvaguardar a privacidade e segurança das informações pessoais dos cidadãos brasileiros. Além disso, é de suma importância fortalecer as políticas de segurança cibernética e conscientizar a população sobre práticas seguras na internet. A promulgação da Lei Geral de Proteção dos Dados (LGPD) reforça a relevância dessas iniciativas, ao fornecer um arcabouço jurídico para a proteção dos dados e incentivar a construção de um ambiente digital confiável e resiliente no Brasil.

A implementação de um governo transparente não é tão simples como pode parecer inicialmente. A tarefa de reorganizar os dados por meio de processos novos e aprimorados, abrindo repositórios de dados governamentais de maneira acessível, organizada e imparcial para os cidadãos, sem comprometer a privacidade em informações ou expor dados sensíveis que prejudiquem a função do Estado, torna-se um desafio gigantesco (SANDOVAL-ALMAZÁN, 2015).

A disponibilização de dados, a transparência e o grau de publicidade estão diretamente vinculados ao nível de agregação e à sensibilidade das informações. Além disso, essa relação também está intimamente ligada ao orçamento destinado à segurança da informação. É essencial realizar investimentos adequados em capacitação de equipes,

aquisição de softwares e equipamentos para criptografia, anonimização, estruturação de banco de dados e outras infraestruturas necessárias para garantir o bom funcionamento desses processos (GONÇALVES, 2020).

O princípio fundamental da administração pública é a transparência, assegurada pelo Estado por meio do direito de acesso à informação. O artigo 5º da Lei nº 12.527/2011 (Lei de Acesso à Informação (LAI)) estabelece que esse acesso deve ser concedido de forma clara, transparente e fácil de compreensão, por meio de procedimentos objetivos e rápidos.

Visando garantir a transparência, a administração pública muitas vezes enfrenta dificuldades em discernir o que pode ser divulgado ao público e o que deve ser mantido em sigilo. Esse problema pode afetar diretamente o direito fundamental à privacidade e liberdade das pessoas, previsto no artigo 5º, X e XII da Constituição (MAXIMIANO, 2022).

Um dos principais desafios enfrentados pelas instituições é a necessidade de promover uma mudança cultural interna a sua equipe acerca da relação ao tratamento de dados pessoais. Essas transformações na cultura institucional demandam tempo e investimentos financeiros como em atividades de divulgação, treinamento e conscientização da comunidade envolvida. Alcançar o nível de conformidade com a LGPD exige, principalmente, uma transformação cultural que nem é tão fácil tampouco rápida (CRESPO, 2021). Outrossim, para garantir o cumprimento e conformidade da legislação de proteção de dados, as organizações devem estabelecer um grupo responsável pelo trabalho de adequação à LGPD. Essa equipe será encarregada de gerir o processo de adequação, começando pelo mapeamento dos processos e sistemas que lidam e armazenam dados pessoais e sensíveis. Ressalta-se que, sem esse mapeamento, impossibilita-se tomar decisões sobre os critérios a serem adotados para a proteção dos dados pessoais manipulados pela instituição de ensino (CUNDA et al., 2021).

Além dos fatores já citados, a lei estabelece, ainda, a necessidade de designar um cargo de encarregado pelo tratamento de dados pessoais, também conhecido como *Data Protection Officer*, cuja responsabilidade é de proteger dos dados pessoais da instituição. O *Data Protection Officer* (DPO) precisa ter um perfil que combine conhecimentos das áreas de TI e jurídica, a fim de poder lidar com questões relacionadas à LGPD e Agência Nacional de Proteção de Dados (ANPD). Essa exigência apresenta dificuldades significativas, pois muitas vezes as organizações, sejam empresariais ou públicas, já contam com uma equipe reduzida e muito específica. Este perfil abrange duas áreas distintas, tornando o processo de seleção do profissional ainda mais difícil.

Salienta-se que em algumas organizações, em particular, instituições de ensino, é comum a coleta frequente de dados devido à natureza de suas atividades. Essas coletas abrangem diversos tipos de informações, como dados pessoais, cadastrais, avaliações edu-

cacionais, notas e frequência acadêmicas. No entanto, é perceptível que essas instituições geralmente não têm o costume de solicitar a autorização do titular dos dados para realizar a coleta, tratamento e armazenamento das informações, porém, com a entrada em vigor da nova Lei, esse procedimento será proibido (BARBOSA et al., 2021).

A Rede Nacional de Pesquisa (RNP) é uma organização social vinculada ao Ministério de Ciência, Tecnologia e Inovações (MCTI) e mantida por esse, entre outros ministérios. Em pesquisa recente, realizada no ano de 2022, por esta organização, 30 (trinta) instituições públicas e privadas de ensino e pesquisa, constatou que 50% (cinquenta por cento) ainda não definiu as bases legais para o tratamento de dados pessoais; 44% (quarenta e quatro porcento) admitiu que deveria gerenciar o consentimento dos usuários, mas não o faz e 62% (sessenta e dois por cento) ainda não definiu um processo para responder às solicitações dos titulares de dados pessoais. A maioria, também, não havia definido o encarregado pelo tratamento de dados pessoais (*Data Protection Officer* - DPO), sendo exigência da Lei (RNP, 2022).

A execução de uma política pública é um procedimento que, além de envolver a colaboração de múltiplos intervenientes, também abarca processos organizados que devem estar em sintonia para alcançar seu propósito e, assim, materializar os resultados desejados. Essa fase é definida como as medidas essenciais para que uma política seja posta em prática e funcione de maneira eficaz (RUA, 1997).

Para a implementação de uma de política pública normalmente inclui participantes de vários níveis do governo e organizações com variados interesses, conhecimentos e estruturas institucionais. Isso leva à formação de colaborações inter organizacionais para realizar ações governamentais específicas, e a maneira como essas colaborações se organizam e se relacionam afeta a eficácia de suas ações (BARBOSA, 2016).

Assim, a LGPD, por si só, formaliza o problema público do uso indevido de dados pessoais no âmbito legal. Isso torna a parte das estratégias de implementação mais complexa, pois dependerá da atuação de alguns atores internos e externos para conseguir efetividade (SANTOS, 2020).

A utilização de um modelo de processo para a implantação da LGPD em uma organização desempenha um papel primordial na atividade de adequação. Essa lei preconiza uma abordagem sistemática e abrangente para garantir a conformidade com suas disposições. Ao adotar um modelo de processo, a organização terá à disposição uma estrutura clara e organizada que irá guiar a implementação das medidas necessárias, desde a análise e mapeamento dos dados até a efetivação de políticas e procedimentos de proteção. Além disso, um modelo de processo contribui para assegurar a consistência e uniformidade na aplicação das diretrizes da LGPD, evitando lacunas ou falhas no cumprimento das obrigações legais. Por fim, a utilização de um modelo de processo facilita o monitoramento

contínuo e aprimoramento das práticas de proteção de dados, permitindo uma adaptação eficiente às mudanças regulatórias e às demandas do ambiente empresarial em constante evolução.

Considerando a diversidade de modelos de processos disponíveis na literatura, cada um com suas aplicações específicas, seria vantajoso considerar a adoção de um modelo com as características do *Capability Maturity Model Integration* que é amplamente utilizado na Engenharia de Software. Sua vasta aplicação nessa área torna-o uma opção atrativa a ser considerada. Reconhecido internacionalmente, o *Capability Maturity Model Integration* (CMMI) oferece uma estrutura sólida e estabelecida para avaliar e aprimorar a maturidade dos processos de desenvolvimento de software. Ao propor um modelo com base no CMMI em conjunto com a implantação da LGPD, as organizações podem garantir que seus processos de tratamento de dados pessoais estejam alinhados com as melhores práticas da indústria, resultando em uma abordagem mais robusta e confiável para a conformidade com a LGPD. O modelo CMMI fornece diretrizes específicas para cada estágio do processo de desenvolvimento de software, permitindo a identificação de lacunas, a melhoria dos procedimentos e a integração adequada de medidas de proteção de dados em todas as etapas do ciclo de vida do software. Isso não apenas garante a conformidade legal, mas também fortalece a confiança dos clientes e parceiros em relação ao tratamento de suas informações pessoais.

A ideia é de desenvolver um modelo de processo, em conjunto com os requisitos de implantação e/ou adequação à LGPD, assim as organizações podem garantir que seus processos de tratamento de dados pessoais estejam alinhados com as melhores práticas da indústria, resultando em uma abordagem mais robusta e confiável para a conformidade com a LGPD. O modelo CMMI fornece diretrizes específicas para cada estágio do processo de desenvolvimento de software, permitindo a identificação de lacunas, a melhoria dos procedimentos e a integração adequada de medidas de proteção de dados em todas as etapas do ciclo de vida do software. Isso não apenas garante a conformidade legal, mas também fortalece a confiança dos clientes e parceiros em relação a como está sendo o tratamento de suas informações pessoais.

Os vazamentos de dados pessoais constituem um desafio relevante no atual contexto de digitalização das transações e da economia. À medida que as atividades online se tornam mais frequentes, cresce também a preocupação com a proteção adequada dessas informações e a segurança cibernética.

Um incidente que ilustra esse problema ocorreu com a empresa brasileira Netshoes S.A.[2] em janeiro de 2018, quando aproximadamente dois milhões de registros de usuários sofreram um comprometimento, resultando no vazamento de dados pessoais. Segundo

[2]http://www.netshoes.com.br

o Ministério Público do Distrito Federal, foram expostas informações como nome, CPF, e-mail, data de nascimento e histórico de compras de clientes, ainda que dados mais sensíveis como número de cartão de crédito e senhas não tenham sido afetados no caso. Esse vazamento representou uma falha de segurança que expôs indevidamente dados que haviam sido confiados à empresa para fins de transações comerciais pela internet (Assessoria Especial de Imprensa Ministério Público Distrito Federal, 2024).

Instituições financeiras também já sofreram com vazamentos de dados de clientes. De acordo com informações disponibilizadas pelo Banco Central do Brasil (BCB) em sua seção sobre a Lei Geral de Proteção de Dados (Banco Central do Brasil, 2024). Algumas instituições financeiras notificaram incidentes de segurança nos últimos anos que envolveram expostos de informações pessoais em grande escala. A tabela 1 apresenta uma seleção de alguns incidentes de vazamento de dados pessoais catalogados pelo BCB

Tabela 1: Registro de incidentes envolvendo dados pessoais

N.º	Instituição envolvida no incidente	Natureza do incidente	Período do Incidente
1	Banco do Estado do Pará S.A. (Banpará)	Dados cadastrais vinculados a 3.020 chaves Pix	20/03 a 13/04 de 2024
2	Pagcerto Instituição de Pagamento LTDA. (Pagcerto)	Dados cadastrais vinculados a 2.197 chaves Pix	23/04 a 24/04 de 2024
3	Banco BTG Pactual S.A. (BTG Pactual)	Dados cadastrais vinculados a 8.032 chaves Pix	23/07 a 05/08 de 2024
4	99Pay Instituição de Pagamento S.A. (99Pay)	Dados cadastrais vinculados a 39.088 chaves Pix	26/05 a 02/07 de 2024
5	Acesso Soluções de Pagamento S.A. (Acesso)	Dados cadastrais vinculados a 160.147 chaves Pix	03/12 a 05/12 de 2021
6	Unicred do Brasil (Unicred)	Dados cadastrais vinculados a 174 chaves Pix	05/08 a 08/08 de 2024

Fonte: Prórprio autor, adaptado de (Banco Central do Brasil, 2024).

Os casos exemplificados evidenciam os riscos decorrentes de incidentes de segurança que envolvem vazamentos de informações pessoais sensíveis. Tais ocorrências reforçam a importância da implementação e aprimoramento contínuos de mecanismos e protocolos rígidos de segurança e proteção de dados nas organizações. A proteção adequada dos dados fornecidos pelo cidadão em ambiente digital deve ser uma prioridade, tendo em vista o potencial impacto que vazamentos em grande escala podem ocasionar na privacidade do indivíduo e sua dignidade. (Banco Central do Brasil, 2024).

Em todos os casos os vazamentos são de chaves Pix, que por si só já é preocupante, mas também aos dados cadastrais associados à chave, como nome, CPF, telefone, entre outros. Um deles reportou vazamento de 1,4 milhão de CPFs e outros dados em 2019.

Esses casos apontam para a necessidade constante de aprimorar as técnicas de proteção de dados pessoais na intenção de para coibir novas ocorrências que possam colocar em risco a privacidade de seus.

1.3 Objetivos

1.3.1 Objetivo Geral

O objetivo principal deste trabalho é a proposição de um modelo de processo com maturidade visando a adequação à Lei Geral de Proteção dos Dados. O modelo tem como propósito estabelecer uma estrutura clara e eficaz para avaliar o nível de maturidade das organizações em relação às exigências da LGPD, auxiliando com recomendações para avançar para níveis mais elevados de conformidade.

1.3.2 Objetivos Específicos

Com o propósito de alcançar a meta principal deste projeto, foram estabelecidos os seguintes objetivos específicos:

1. Realizar uma revisão bibliográfica abrangente sobre a Lei Geral de Proteção de Dados (LGPD), abordando seus princípios, requisitos legais aplicáveis às organizações e as implicações para a conformidade com a legislação;

2. Investigar e identificar o modelo de maturidade de processos mais adequado para a proposta deste trabalho, considerando sua compatibilidade com os requisitos da LGPD e as melhores práticas do setor;

3. Desenvolver uma proposta de modelo de maturidade de processos que esteja consoante com os requisitos da LGPD, incorporando as melhores práticas e diretrizes recomendadas para garantir a conformidade e a proteção de dados pessoais.

1.4 Justificativa

A falta de conformidade das organizações, sejam elas públicas ou privadas, com a LGPD representa um obstáculo para as ambições do país de ingressar em blocos econômicos e organismos internacionais importantes. Além disso, essa falta de conformidade pode trazer prejuízos para o sistema de proteção de dados nacional, potencialmente resultando em conflitos de interesse. A fim de alcançar a implementação completa de um governo totalmente digital, é fundamental que o compartilhamento de dados pessoais em todas as esferas seja tanto esperado quanto exigido pela sociedade e pelos órgãos de controle.

Para garantir uma implantação adequada, são necessários procedimentos e controles para o compartilhamento de dados pessoais com terceiros, sejam eles organizações públicas ou privadas, porém devem incluir, além das nacionais, as internacionais (TCU, 2022).

A implementação de um modelo de processos com maturidade para adequação aos requisitos da Lei Geral de Proteção de Dados (LGPD) constitui uma abordagem estratégica para assegurar a conformidade e elevar o nível de maturidade organizacional no tratamento de dados pessoais. Este modelo não apenas garante que as organizações cumpram as exigências legais, mas também impulsiona uma evolução contínua na gestão de processos, capacitando as empresas a atingir padrões superiores de excelência operacional e segurança da informação.

Para ser efetivo, o modelo deve ser adaptável a qualquer tipo de organização, independentemente do porte, setor ou estágio de maturidade. Sua flexibilidade é crucial para possibilitar ajustes conforme as necessidades e especificidades de diferentes ambientes organizacionais. Dessa forma, o modelo pode ser implementado tanto por pequenas empresas quanto por grandes corporações, assegurando que todas possam alcançar conformidade com a LGPD.

Além disso, é imperativo que o modelo seja sistematizado, ou seja, estruturado de forma a proporcionar um processo claro, coerente e repetível para a avaliação e aprimoramento da conformidade. A sistematização envolve a definição de etapas bem delineadas, critérios de avaliação objetivos e mecanismos de monitoramento contínuo, permitindo que as organizações possam mapear seu progresso, identificar áreas de melhoria e implementar ações corretivas de maneira eficiente.

Em suma, um modelo de processos com maturidade para a adequação à LGPD deve atuar como um instrumento robusto e versátil, capaz de ser aplicado em qualquer organização e sistematizado para garantir uma conformidade consistente e um aprimoramento contínuo na proteção de dados pessoais

Justifica-se este estudo tendo em vista a necessidade de aprendizado cada vez mais aprofundado acerca das legislações pertinentes, em especial no que tange a um tema de tão grande relevância acadêmica e profissional dos dias atuais que é a proteção de dados. Nesse sentido, evidencia-se a importância acadêmica, vez que o desenvolvimento de processos que garantam eficiência e eficácia nas atividades administrativas faz parte do desenvolvimento científico em busca de melhoras para a sociedade na totalidade. Além disto,e vidência-se a importância social do tema, tendo em vista a completa inserção da sociedade atual em todo o mundo no meio cibernético, local onde antes não existiam regras, nem tampouco proteção de direitos, fator este que deixava pessoas e Estados vulneráveis aos mais diversos tipos de desrespeito a direitos e garantias.

1.5 Estrutura do Trabalho

Este trabalho de dissertação de mestrado está dividido em vários capítulos, seguindo uma estrutura lógica e coerente. Na seção 1, Introdução, é apresentada a contextualização do problema de pesquisa, a relevância do estudo e os objetivos da pesquisa.

Na Fundamentação Teórica, seção 2, é apresentada uma revisão da literatura relacionada ao tema da pesquisa, incluindo conceitos fundamentais de Leis e processos organizacionais, além de destacar trabalhos anteriores relevantes.

A Metodologia adotada é descrita na seção 3, onde se expõem a abordagem de pesquisa adotada, a justificativa para a escolha da metodologia, a descrição dos participantes ou sujeitos do estudo, dos instrumentos de coleta de dados e da análise de dados.

No capítulo dedicado à Proposta do Trabalho, apresentado na seção 4, é descrito o modelo de processos com maturidade desenvolvido nesta pesquisa. Esse modelo visa fornecer uma estrutura sistemática para avaliar e melhorar a conformidade das organizações com as exigências legais, especialmente no contexto da proteção de dados.

A seção 5 é dedicada ao Estudo de Caso, onde o modelo de processos com maturidade é aplicado em três organizações distintas. O objetivo deste capítulo é validar a aplicabilidade do modelo em cenários reais, analisando o posicionamento de cada organização em relação aos diferentes níveis de maturidade propostos.

Finalmente, na seção 6, que corresponde à Conclusão, são recapitulados os objetivos da pesquisa e discutidas as implicações dos resultados para a área de estudo. Além disso, são apresentadas as limitações do estudo e sugeridas direções para futuras pesquisas.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo, será apresentado, na primeira seção 2.1, Leis de Privacidade, uma análise das primeiras iniciativas de ordem jurídica que lidam com a questão da privacidade no mundo. Em seguida será listada e comentada as mesmas iniciativas jurídicas, porém voltado para o Brasil, na seção 2.2, Leis sobre Privacidade no Brasil.

Na sequência, a seção 2.3, Processos Organizacionais, abordará as atividades e operações realizadas em uma organização para atingir seus objetivos e metas. Posteriormente, seção 2.4, Modelo de Processo com Níveis de Maturidade, será apresentado processos com níveis de maturidade e como este poderá otimizar a qualidade, reduzir custos e acelerar o desenvolvimento de processos organizacionais

Por fim, a seção 2.5 trará uma revisão dos trabalhos relacionados, destacando estudos e pesquisas que contribuíram para o desenvolvimento do tema abordado. Esta seção visa contextualizar a pesquisa dentro do campo acadêmico mais amplo, demonstrando como outros estudiosos têm tratado questões semelhantes e quais lacunas a presente dissertação busca preencher.

2.1 Leis de Privacidade

2.1.1 Primeiras Iniciativas no Mundo

As iniciativas e manifestações de proteção e privacidade da informação é bem mais antiga, remetendo para o século XVIII, na Suécia. Foi em 1766, mais precisamente, onde foi desenvolvido um marco legal sobre o acesso à informação. Já nos Estados Unidos da América (EUA), foi aprovada a Lei de Liberdade de Informação, do inglês Freedom of Information Act (FOIA), dois séculos depois, em 1966. Na América do Sul, a Colômbia foi a pioneira a elaborar e estabelecer um código, em 1888, que franqueou o acesso a documentos de Governo (BRASIL, 2011).

Os dados pessoais podem ser utilizados das mais diferentes formas, tantas assim que o proprietário perde o controle. Muitas informações circulam entre as empresas, são armazenados em locais virtuais, fora do alcance. Então, dentro deste contexto, observa-se a necessidade da proteção destas informações pessoais, pois além do uso desenfreado, os dados pessoais podem revelar a identidade do indivíduo, possibilitando atingir sua privacidade. De posso dessas informações é possível revelar seus gostos, suas particularidades, sua rotina, tornando o indivíduo parte vulnerável diante de quem faz uso de suas informações pessoais (MAGALHÃES; OLIVEIRA, 2021).

A preocupação com o direito à proteção dos dados pessoais tem sua origem bem remota, datada no século XIX, no ano 1890 para ser mais preciso. Há um marco histórico

neste ano, com a publicação do artigo *The Right to Privacy* (WARREN; BRANDEIS, 1890), onde os juristas americanos *Samuel Warren* e *Louis Brandeis* entenderam a privacidade como o "direito de ser deixado só", no sentido de que todos deveriam respeitar a vida privada, o espaço íntimo de cada um, incluindo o conteúdo, intimidade, honra e as informações pessoais.

Com o passar dos anos, esse conceito foi se modificando e se atualizando até ser reconhecido como direito fundamental na Declaração Universal dos Direitos Humanos, em 1948, onde garantiu a não intromissão na vida privada, na família, no domicílio e nas correspondências. Após alguns anos, várias cartas normativas internacionais (Convenção Europeia de Direitos Humanos (1953); Carta de Direitos Fundamentais da União Europeia (2000); tratado sobre o Funcionamento da União Europeia (2007) foram elaboradas no sentido de fortalecer o estabelecimento do direito à privacidade, ampliando seu sentindo, acrescentando além de informações pessoais, o direito ao controle dos dados, no conjunto de valores a serem protegidos pelo direito à privacidade.

Devido à necessidade de interpretar sistematicamente outros direitos como a dignidade, a liberdade e o acesso à informação, a proteção de dados pessoais tem como valor central a privacidade no sentido mais amplo, incluindo em seu conceito todos os direitos inerentes ao desenvolvimento da personalidade do indivíduo, desde a esfera íntima indisponível, como a honra, até os elementos negociáveis, como a imagem, além do controle sobre a informação (autodeterminação informativa) (RODOTÀ, 2015).

2.1.2 Origem do GDPR

A *General Data Protection Regulation* (GDPR) aplica-se a todos os Estados Membros da União Europeia, mas seu alcance é muito maior, abrange qualquer organização em qualquer lugar do mundo que preste serviços para a UE que envolvam o processamento de dados pessoais. Isso significa que o GDPR é provavelmente, é agora, a lei de segurança de dados mais importante do mundo. Embora se baseie no trabalho da Diretiva de Proteção de Dados da UE (*Data Protection Directive* (DPD)), da Health Insurance Portability and Accountability Act (HIPAA)[3] dos EUA e de vários outros instrumentos de proteção de dados, o GDPR pode ser considerado uma compilação e atualização abrangente dos objetivos da UE na proteção dos direitos e liberdades de seus residentes (TEAM, 2020).

A elaboração GDPR foi um marco importante para o reconhecimento global e contínuo na preservação das informações pessoais. Apesar da economia da informação[4]

[3]Health Insurance Portability and Accountability Act é uma lei federal americana, de 1996, que exigia a criação de padrões nacionais para proteger informações confidenciais de saúde do paciente de serem divulgadas sem o consentimento ou conhecimento do paciente.

[4]A economia da informação é uma economia com maior ênfase nas atividades que geram informação do que naquelas de manufatura; a informação é vista como um bem de capital.

estar presente há algum tempo, o valor real dos dados pessoais só se tornou evidente mais recentemente com a regulamentação deste instrumento. O roubo cibernético de dados pessoais expõe as pessoas a riscos pessoais significativos. As técnicas de análise de *big data*[5] permitem que as organizações rastreiem e prevejam o comportamento individual e podem ser implantadas na tomada de decisão automatizada. A combinação de todas essas questões, juntamente com o avanço contínuo da tecnologia e as preocupações com o uso indevido de dados pessoais por governos e empresas, resultou em uma nova lei aprovada pela União Europeia (UE) para esclarecer os direitos de dados dos residentes da UE e garantir um nível de proteção de dados pessoais em toda a UE (TEAM, 2020).

O motivo que inspirou o surgimento de regulamentações de proteção de dados pessoais de forma mais consistente e consolidada a partir dos anos 1990 está diretamente relacionado ao próprio desenvolvimento do modelo de negócios da economia digital, que passou a ter uma dependência muito maior dos fluxos internacionais de bases de dados, especialmente os relacionados às pessoas, viabilizados pelos avanços tecnológicos e pela globalização.

A essência deste pacto é a liberdade, mas o equilíbrio se dá na transparência. Assim, as leis de proteção de dados pessoais têm a particularidade de elaborar princípios e vinculá-los a indicadores mais assertivos, de natureza técnica, que permitam uma avaliação verificável do cumprimento do acordo. Assim, através da análise de trilhas de auditoria e da implementação de um conjunto de controles. elementos para uma melhor governança de dados pessoais.

O debate sobre este tema surgiu União Europeia , sendo abordado pelo partido *The Greens*, onde foi consolidado com a publicação do General Data Protection Regulation (tradução Regulamento Geral Europeu de Proteção de Dados Pessoais) No. 679, aprovado em 27 de abril de 2016. Sua finalidade era de abordar a proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, conhecido pela expressão *free data flow* (do inglês, fluxo de dados livre). O GDPR concedeu um prazo de até dois anos para as empresas de adequarem ao regulamento, e após este prazo, iniciaram-se as aplicações de multas e penalidades.

Isto criou um efeito dominó nos demais países que desejavam manter as relações comerciais com a UE, pois também deveriam possuir legislação no mesmo nível do GDPR. Assim, aqueles que não tivessem leis no mesmo patamar que a GDPR passaria a ter mais dificuldades na concretização dos negócios com os países da UE. Tal imposição não era favorável para a maioria das nações, em especial, as da América Latina (PINHEIRO, 2020).

[5] *Big Data* são dados com maior variedade que chegam em volumes crescentes e com velocidade cada vez maior (GARCIA, 2022)

A União Européia até tinha leis relacionadas à privacidade, mas eram de 1995 (Diretiva n.º 95/46 CE) e não correspondiam ao cenário tecnológico atual. O projeto do GDPR foi iniciado em 2012 e aprovado em 2016, iniciando discussões sobre a proteção de dados em vários cantos do Planeta. Inspirou, por exemplo, a criação da CCPA – Lei de Privacidade do Consumidor da Califórnia – e da LGPD – Lei Geral de Proteção de Dados – no Brasil (SANTOS, 2021a).

A intensificação das demandas tornou-se evidente após a implementação das novas regulamentações estabelecidas pelo Regulamento Geral de Proteção de Dados (RGPD) da União Européia. Isso se deu em virtude da ausência dos requisitos necessários no Brasil para cumprir as exigências, tais como obter o consentimento dos usuários, estabelecer contratos e cláusulas-padrão, adotar normas corporativas vinculantes, acordos e tratados bilaterais. Como resultado, o Brasil não era reconhecido pela União Européia (UE) como um Estado apto para efetuar transferências internacionais de dados. O RGPD, no contexto da transferência internacional de dados pessoais, possui aplicação extraterritorial, ou seja, abrange empresas localizadas em qualquer um dos países da UE, assim como aquelas que prestam serviços a indivíduos situados nesses países (GONÇALVES, 2020).

2.2 Leis sobre Privacidade no Brasil

No Brasil, diversas iniciativas do governo vêm sendo feita nos últimos anos na intenção de normatizar e proteger a informação, a privacidade e o direito à intimidade. Em todos os textos constitucionais há menção a esses direitos, como, direito à inviolabilidade do domicílio e ao sigilo de correspondência, porém, apenas na Constituição Brasileira (CB) de 1988 que foi contemplado o direito à intimidade e à proteção privada (FINKELSTEIN; FINKELSTEIN, 2020).

Para se compreender melhor e de forma mais ampla como a privacidade tornou-se um direito fundamental, acerca dos instrumentos jurídicos, a seguir estão os principais instrumentos legais desenvolvidos nos últimos, em ordem cronológica.

Remetemos para o século XIX (dezenove) ainda na Constituição do Império, datada em 1824, reconhecia o direito à privacidade ao amparar o **"segredo da carta"** como também a "inviolabilidade da casa", porém não mencionava o sigilo em si, estando mais pautada ao direto de propriedade uma vez que não protegia o conteúdo, mas sim a invasão e obstrução (DANIEL, 2022).

Já no século XX, no ano de 1948, temos a **Declaração Universal dos Direitos Humanos** tratando da privacidade, mais especificamente do "Direito ao Respeito pela Vida Privada e Familiar" e ainda que "ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques, toda a pessoa tem direito à

proteção da lei". (MALDONADO; BLUM, 2022)

A Constituição Federal de 1998 dispõe a privacidade e os dados pessoais no rol dos direitos e garantias fundamentais, sendo protegidos pela inviolabilidade e sigilo. Este direito vem adquirindo progressivamente maior relevância com o crescimento de técnicas de comercialização e comunicação eletrônica, e se apresenta como defesa natural do homem contra as investidas tecnológicas, com a necessidade de locomoção, do círculo relacional do homem, muitas vezes expondo-o diante dos mais diversos públicos, como sociais, comerciais ou de lazer. Está bem nítido que as esferas da intimidade reduziram drasticamente com o uso da internet e novas formas de se relacionar (BITTAR, 2017).

Avançando um pouco mais, na atual **Constituição Federal** de 1988, trouxe mais garantias sobre o tema, onde, em seu artigo 5º, X, prever que "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" (PINHEIRO, 2020).

No início da década de 90 a Lei n.º 8.078/90, conhecida como **Código de Defesa do Consumidor**, previu o direito do acesso a "informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele", mais especificamente em banco de dados e cadastros dos consumidores. Assim, o usuário poderá ter acesso às suas informações além das fontes nas quais estão armazenadas, como cadastros e fichas (VALESI RAQUEL; AOKI, 2021).

Em seguida foi a vez da **Lei de Interceptação Telefônica e Telemática** (Lei n.º 9.296/96), que regulamenta a interceptações das comunicações e fluxo de comunicações em sistemas informatizados e também de telemática, reconhecendo o direito à privacidade, restringindo o uso desse método investigativo sempre sob o amparo de uma ordem judicial (OLIVEIRA, 2020).

A pressão da sociedade civil para que o Estado cumpra suas obrigações de divulgar dados governamentais - tornando-os abertos - e de proteger os usuários de Internet no processamento de seus dados pessoais por entidades públicas e privadas foi de grande importância para surgir um instrumento regulamentário chamado Marco Civil da Internet. Foi no ano de 2014 através da Lei No. 12.965/14, que foi promulgado o marco onde há artigos que visa a proteção à confidencialidade e inviolabilidade da vida privada digital e os fluxos de tráfego da Internet, além de garantir que a guarda e disponibilização de registros de conexão e de acesso a aplicações a internet protejam a intimidade, honra e imagem de seus usuários (BRASIL, 2014).

Esta lei surgiu como alternativa a diversas propostas legislativas que visavam criminalizar determinadas práticas na Internet, muitas delas quer eram consideradas triviais ou até mesmo socialmente aceitas. A lei não apenas contém algumas disposições progressistas, como o princípio da neutralidade da rede, mas também é um importante padrão

internacional, pois o projeto submetido ao parlamento foi moldado por várias rodadas de consulta pública (AUGUSTO; FRANCISCO; VENTURINI, 2017).

Foi neste marco regulatório onde a palavra privacidade surgiu pela primeira vez, passando a constar no sistema jurídico brasileiro, estabelecendo princípios, garantias, diretos e deveres a serem observados no ambiente digital (DANIEL, 2022).

Verdadeiros impérios de marketing foram criados a partir da captação de dados de usuários dos provedores de internet, principalmente na segmentação de produtos de consumo (marketing direcionado) e sua promoção (publicidade). Os dados pessoais desses cidadãos se tornaram de vital importância no mecanismo motor da economia da informação; com a possibilidade de se organizar tais dados de maneira de fácil escalabilidade, um novo mercado foi criado, cuja base de sustentação é sua extração (BIONI, 2018).

Em função dessas práticas, assim como outras que já vinham ocorrendo, a **Lei Geral de Proteção dos Dados** - aprovada em agosto de 2018, mas com vigência só a partir de agosto de 2020, com uma proposta mais atual em relação ao paradigma da privacidade na era digital. Foi a partir desta lei que se começou a ter uma discussão madura em relação à proteção de dados (COTS; OLIVEIRA, 2018).

2.2.1 Origem da Lei Geral de Proteção de Dados (LGPD)

Os sistemas e serviços de software exigem uma conectividade constante entre indivíduos e entidades corporativas, sejam públicas ou privadas, o que leva à coleta, processamento e divulgação regulares de grandes volumes de dados. É crucial destacar que a falta de conformidade com políticas de privacidade pode acarretar graves consequências, resultando em danos tanto individuais quanto sociais. Além disso, os dados gerados por esses sistemas frequentemente contêm um excesso de informações pessoais, que podem ser utilizadas para fins distintos daqueles originalmente previstos. A divulgação não autorizada dessas informações pode gerar sérios problemas de privacidade para as organizações (ALVES; NEVES, 2021).

Para garantir a privacidade dos usuários, diversos países implementaram legislações rigorosas para regulamentar o uso de dados pessoais. Um exemplo proeminente é o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia. No Brasil, essa preocupação se materializou na Lei 13.709, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), sancionada em 14 de agosto de 2018. Embora a LGPD tenha sido criada em 2018, ela só entrou em vigor em 18 de setembro de 2020, com sanções administrativas aplicáveis a partir de 1º de agosto de 2021 (VASCONCELOS, 2021).

A LGPD representa um marco legal importante no Brasil, impactando profundamente tanto instituições privadas quanto públicas. Seu alcance é vasto, estabelecendo normas para a proteção de dados pessoais em qualquer contexto que envolva o trata-

mento dessas informações, independentemente do meio utilizado, seja por pessoas físicas ou jurídicas (PINHEIRO, 2020).

Um dos aspectos mais notáveis da LGPD é a atribuição da propriedade dos dados aos próprios indivíduos, conferindo-lhes maior controle sobre suas informações pessoais. A lei estabelece regras claras para o uso desses dados, assegurando a proteção de direitos fundamentais, como a liberdade, a privacidade e o desenvolvimento pessoal (OKANO et al., 2022).

Para o cumprimento das diretrizes da LGPD demanda não apenas o entendimento e a aplicação correta das normas por parte das organizações, mas também a participação de profissionais qualificados para lidar com questões relacionadas à proteção de dados pessoais (BARBOSA, 2019). Assim, o tratamento dos dados pessoais pode ser realizado por agentes de tratamento divididos em duas categorias:

- O **Controlador** é definido pela Lei como a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, tais como as finalidades e os meios do tratamento (art. 5º, VI da LGPD). No âmbito da Administração Pública, o Controlador será a pessoa jurídica do órgão ou entidade pública sujeita à Lei, representada pela autoridade imbuída de adotar as decisões acerca do tratamento de tais dados.
- O **Operador** é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (art. 5º, VII da LGPD), aí incluídos agentes públicos no sentido amplo que exerçam tal função, bem como pessoas jurídicas diversas daquela representada pelo Controlador, que exerçam atividade de tratamento no âmbito de contrato ou instrumento congênere.

É preciso compreender alguns conceitos centrais da LGPD para uma aplicação efetiva da legislação. O **titular dos dados** é a pessoa física a quem os dados pessoais se referem, sendo fundamental garantir seus direitos e proteção durante o tratamento dessas informações. Os**dados pessoais**, por sua vez, englobam qualquer informação relacionada a uma pessoa natural identificada ou identificável, abrangendo desde dados básicos como nome e endereço até informações mais sensíveis, como orientação sexual ou religiosa. Já os **dados pessoais sensíveis** constituem uma categoria especial de dados que requerem cuidados adicionais em seu tratamento, devido ao potencial de causar danos significativos à privacidade ou à liberdade do titular. Esses dados incluem informações sobre origem racial ou étnica, opiniões políticas, convicções religiosas, saúde, vida sexual, entre outras. A compreensão e o correto manejo desses conceitos são essenciais para garantir a conformidade com a LGPD e proteger os direitos dos indivíduos em relação ao tratamento de seus dados pessoais (FERNANDES; NUZZI, 2022).

A Autoridade Nacional de Proteção de Dados Pessoais (ANPD), órgão federal vinculado à Presidência da República, será responsável pela regulação, fiscalização e aplicação de penalidades relacionadas ao tratamento de dados pessoais por pessoas físicas e jurídicas, conforme estabelecido pela LGPD. Sua autonomia técnica e decisória é garantida pela lei, e suas características, finalidades e competências são definidas pelo Decreto nº 10.474, de 26 de agosto de 2020 (SARLET; RODRIGUEZ, 2022).

2.3 Processos Organizacionais

Os processos organizacionais referem-se às atividades e operações realizadas em uma organização para atingir seus objetivos e metas. Eles são as ações sequenciais e interrelacionadas que transformam insumos (como recursos, informações e conhecimento) em produtos ou serviços finais. Os processos organizacionais abrangem diversas áreas e níveis da organização, desde a produção e operações até o marketing, vendas, recursos humanos, financeiro, entre outros. Esses processos são essenciais para o funcionamento eficaz de uma organização, pois ajudam a garantir a consistência, eficiência e qualidade das atividades realizadas. Ao mapear, analisar e otimizar os processos organizacionais, as empresas podem identificar oportunidades de melhoria, reduzir custos, aumentar a produtividade e a satisfação dos clientes, e manter-se competitivas no mercado. (GOMES; GOMES, 2014)

Com a quebra das barreiras geográficas e maior abertura comercial, que antes limitavam as empresas a uma região ou a uma nação, a competição agora se eleva para um nível global. Essas disputas exigem das organizações, uma melhoria contínua em seus processos organizacionais, buscando sempre os melhores padrões de qualidade e eficiência. Isso só é alcançado por meio de ferramentas e metodologias adequadas para sua posição e consolidação no mercado em que atuam. (POMPEU et al., 2022)

Processos bem estruturados são a espinha dorsal de uma organização, proporcionando a base para a eficiência, qualidade e consistência em todas as operações e áreas organizacionais. São cruciais para o bom funcionamento de qualquer empresa, permitindo que as equipes executem suas tarefas de maneira eficiente e resultando em um fluxo de trabalho suave e produtivo. A padronização estabelecida também é essencial, garantindo que todos os departamentos e colaboradores sigam práticas uniformes, evitando, erros e inconsistências que poderiam prejudicar o desempenho geral da organização. Além disso, os processos bem definidos incluem etapas de controle de qualidade, o que é fundamental para garantir a entrega de produtos ou serviços que atendam aos padrões desejados. Isso não apenas aumenta a satisfação dos clientes, mas também fortalece a reputação da organização no mercado (POMPEU et al., 2022).

Outro benefício significativo é a agilidade que os processos claros proporcionam. Em um ambiente competitivo, a capacidade de tomar decisões rapidamente pode ser

crucial para o sucesso. Quando os processos são bem documentados e compreendidos, as decisões podem ser tomadas com mais rapidez e eficácia, permitindo que a organização se adapte às mudanças do mercado de forma ágil e eficiente.

Com o avanço tecnológico, os sistemas de informação gerencial adquirem uma importância em destaque na orientação das decisões nas organizações, tornando os processos de obtenção e fornecimento de informações mais ágeis e precisos. Com a sofisticação desses sistemas, as mudanças nos processos se tornam mais frequentes, enquanto os recursos tecnológicos e computacionais exercem um impacto direto na estrutura e estratégia de negócios. O desenvolvimento e a evolução das organizações são, assim, diretamente influenciados pelo progresso da informação e do conhecimento. Diante desse cenário, as organizações buscam por meios mais dinâmicos para se adaptarem a essa nova era, conhecida como a "Era da Informação". Com isso, torna-se indispensável o uso da tecnologia da informação e dos sistemas de informação, considerados como os principais facilitadores para agregar valor às organizações no processo decisório (PARAGUAI; DELAZERI; RIBEIRO, 2023).

2.4 Modelo de Processo com Níveis de Maturidade

O Instituto de Engenharia de Software (*Software Engineering Institute* (SEI)) dos Estados Unidos foi criado para melhorar as capacidades da indústria de software americana. Na metade da década de 1980, o SEI iniciou um estudo sobre maneiras de avaliar as capacidades das empresas que eram contratadas para desenvolverem software para o governo americano. O resultado dessa avaliação de capacidade foi o Modelo de Maturidade de Capacidade de Software ou *Capability Maturity Model* (CMM) do SEI (PAULK et al., 1993).

Isso teve um impacto significativo ao ser apresentado à comunidade de engenharia de software, levando-a a considerar seriamente a melhoria de processos. Esse modelo foi tão amplamente aceito que serviu de base para uma série de outros modelos de maturidade de capacidade, como o Modelo de Maturidade de Capacidade de Pessoas (P-CMM) e o Modelo de Maturidade de Capacidade de Engenharia de Sistemas (CURTIS; HEFLEY; MILLER, 2001) (BATE et al., 1995). Esses modelos desempenham um papel crucial ao promover uma abordagem estruturada para avaliar e aprimorar as capacidades das organizações em relação à engenharia de software, gestão de pessoas e engenharia de sistemas, respectivamente.

Com a quantidade de diversos modelos criados, o SEI iniciou um novo programa para desenvolver um modelo de capacidade integrado, surgindo o CMMI. O framework do CMMI substitui os CMMs de Engenharia de Software e Engenharia e integra outros modelos de maturidade de capacidade. Ele possui duas instanciações, uma em estágios e

outra contínua, e aborda algumas das fraquezas relatadas no Software CMM. Este modelo é baseado em um conjunto de capacidades de engenharia de sistemas e software, que deve estar presente à medida que as organizações atingem diferentes níveis de capacidade e maturidade de processos. (PRESSMAN; MAXIM, 2021)

A melhoria de processos é uma atividade de longo prazo que visa compreender e modificar os processos existentes para aumentar a qualidade do produto, reduzir custos e diminuir o tempo de desenvolvimento. Essa abordagem permite otimizar os processos de desenvolvimento e reduzir despesas. É uma atividade contínua, considerando que o ambiente de negócios está em constante mudança, e os novos processos precisam evoluir para incorporar essas alterações. Para facilitar essa jornada, uma escala de maturidade de processo é necessária, fornecendo uma referência clara e compreensível da qualidade do processo para possibilitar o planejamento de estratégias para uma evolução e melhoria contínua.

O modelo CMMI é utilizado na indústria de software há décadas e provou ser eficaz na melhoria dos processos e na garantia da qualidade. Ele estabelece práticas e diretrizes claras para a gestão de projetos, desenvolvimento de software e governança, o que pode ser aplicado em outras áreas, de forma análoga as já existentes.

2.4.1 *Capability Maturity Model Integration (CMMI)*

A gestão de dados visa otimizar o uso de informações de forma segura e eficiente, alinhada às políticas e regulamentações. Nesse contexto, a governança de dados, conforme (PLOTKIN, 2020), define as regras e responsabilidades para o tratamento dos dados, enquanto a administração de dados, aspecto operacional da governança, garante a execução dessas regras no dia a dia. A administração de dados é fundamental para a governança, sendo responsável pela gestão dos metadados e pela designação de responsáveis pelos dados.

Assim, entende-se que o gerenciamento de dados é a prática de coletar, organizar, armazenar, proteger e usar os dados de uma organização. A maneira conforme a qual se organiza, acessa e protege os dados influencia diretamente a capacidade de uma empresa tomar decisões informadas e estratégicas.

No atual contexto da era digital, tem-se que dados são as principais ferramentas de desenvolvimento e incremento para a inovação, vez que a eficiência e a competitividade são aspectos cada vez mais fortes e inerentes ao mercado na totalidade. Um bom gerenciamento de dados permite melhores tomadas de decisão, aumento de eficiência das atividades desenvolvidas, automatização de processos, melhoria da experiência dos clientes, redução de custos e gerenciamento de riscos (PROENÇA; BORBINHA, 2018).

Para que o gerenciamento de dados ocorra de maneira eficaz e eficiente, etapas

devem ser seguidas para obter-se melhores resultados. As etapas consistem em coleta, armazenamento, processamento, análise, visualização e governança, sendo esta última de grande importância, tendo em vista a necessidade de definição de políticas e processos para garantir a qualidade, segurança e conformidade dos dados (PROENÇA; BORBINHA, 2018).

Tendo como foco o gerenciamento de dados, o uso de ferramentas tecnológicas para a melhor obtenção de resultados tem sido diferencial na busca pela alta qualidade na gestão e gerenciamento de dados, em especial no setor público, tendo em vista a aplicabilidade da LGPD.

Nesse contexto, evidencia-se o CMMI (Capability Maturity Model Integration), criado pelo SEI da Universidade Carnegie Mellon, é um framework que oferece um conjunto de práticas e diretrizes para aprimorar os processos organizacionais. Seu objetivo é ajudar empresas de diversos setores a alcançar níveis mais elevados de maturidade em suas operações. Adquirido pela ISACA em 2016, o CMMI tem sido continuamente aprimorado e disseminado globalmente, tornando-se um referencial importante para a melhoria contínua.

Entende-se, assim, que o CMMI é um *framework* aplicável a diversas áreas, desde desenvolvimento de software até gestão de serviços, auxiliando organizações a evoluírem seus processos, transformando-os de imprevisíveis e caóticos em processos disciplinados e com resultados previsíveis. Ele oferece um conjunto de práticas comprovadas e um caminho estruturado para a melhoria contínua. O CMMI é composto por diferentes constelações, como o CMMI-DEV para desenvolvimento de produtos, que fornecem diretrizes específicas para cada área de atuação.

De acordo com (NASCIMENTO, 2023), o modelo enfatiza dois conceitos essenciais: Capacidade e Maturidade. A Capacidade se relaciona com os objetivos estabelecidos para cada área de processos isoladamente. Essa capacidade é considerada atingida quando cada área de processos consegue operar efetivamente conforme o planejado, ou seja, quando as práticas idealizadas para essas áreas são implementadas de maneira satisfatória. Por outro lado, a Maturidade se refere ao nível geral de desenvolvimento organizacional. Ela é alcançada quando todas as áreas de processos, em suas respectivas categorias, atingem as capacidades esperadas. Isso significa que, ao atingir a maturidade, a organização demonstra um nível de desenvolvimento mais elevado, refletido em um gerenciamento de dados mais sofisticado e eficaz. Quanto mais elevado o estágio de maturidade, mais avançado e robusto é o gerenciamento de dados dentro da organização.

O CMMI oferece um caminho evolutivo para as organizações, permitindo que elas avancem de níveis de maturidade mais baixos para níveis mais altos, sendo um modelo adaptável que pode ser aplicado a diferentes tipos de organizações e setores. O desenvol-

vimento adequado do CMMI possibilita o acesso a um nível organizacional de excelência, desde que cumpridos seus níveis de maturidade. Os cinco níveis de maturidade podem ser entendidos da seguinte forma:

1. Nível 1 — Inicial: No primeiro nível de maturidade do CMMI, conhecido como Inicial, os projetos são caracterizados por uma grande imprevisibilidade. Prazos e orçamentos são frequentemente ultrapassados, devido à falta de processos definidos e à abordagem reativa aos problemas. Neste nível, os projetos são caóticos e com resultados incertos. A falta de planejamento e controle leva a frequentes atrasos e extrapolações orçamentárias, comprometendo a entrega e a qualidade dos produtos. (NASCIMENTO, 2023);

2. Nível 2 — Gerenciado: No segundo nível de maturidade do CMMI, os projetos passam por um processo de gestão mais estruturado. Isso significa que cada projeto possui um planejamento detalhado, é executado de acordo com esse plano, e seu desempenho é medido e controlado continuamente. Ao atingir o nível 2, as organizações evoluem de uma abordagem *ad hoc* para uma gestão mais proativa dos projetos. Os projetos são planejados e controlados de forma mais rigorosa, reduzindo o risco de atrasos e desvios. (NASCIMENTO, 2023);

3. Nível 3 — Definido: O nível 3 do CMMI se caracteriza pela definição de padrões de processo detalhados e documentados para toda a organização. Esses padrões servem como guia para todos os projetos, garantindo consistência e previsibilidade nos resultados. Ao contrário dos níveis anteriores, a organização passa a ser mais proativa, antecipando problemas e tomando ações preventivas. A principal característica do nível 3 é a institucionalização de padrões de processo organizacionais. Esses padrões, que englobam desde o planejamento até a execução e o controle dos projetos, proporcionam uma base sólida para a melhoria contínua e a otimização dos resultados. (NASCIMENTO, 2023);

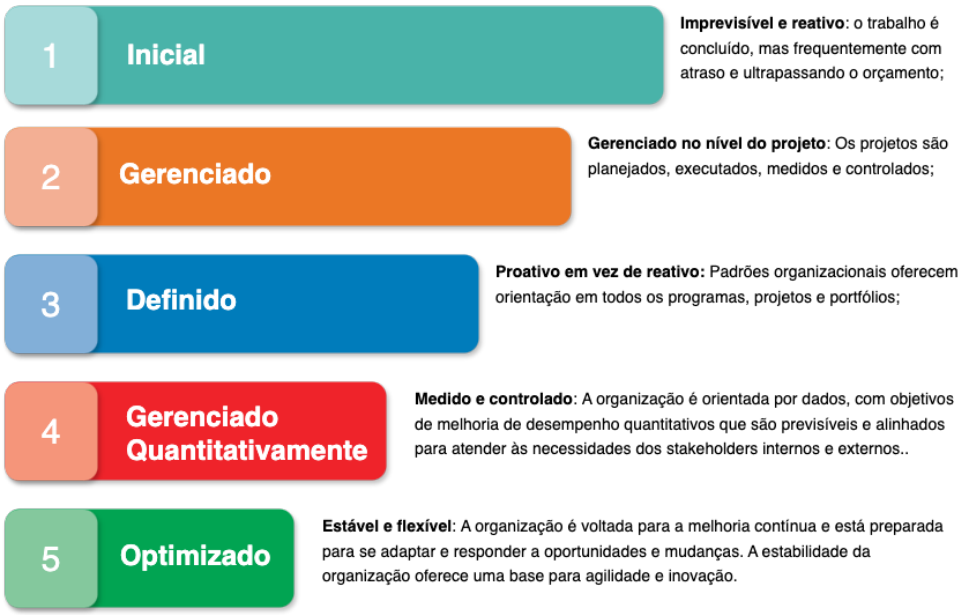
4. Nível 4 — Gerenciado Quantitativamente: No nível 4, as organizações adotam uma abordagem baseada em dados para a gestão de seus processos. Através da análise estatística, é possível identificar tendências, variações e pontos de melhoria, permitindo otimizar o desempenho e alcançar os objetivos de qualidade. Ao atingir o nível 4, as organizações demonstram alto grau de maturidade ao utilizar dados quantitativos para tomar decisões mais precisas e embasadas. A análise estatística permite entender a estabilidade e a capacidade dos processos, possibilitando a identificação de oportunidades de melhoria e a implementação de ações corretivas. (NASCIMENTO, 2023);

5. Nível 5 — Otimização: este nível caracteriza-se por uma busca incessante pela melhoria contínua. As organizações neste nível possuem processos altamente flexíveis,

capazes de se adaptar rapidamente às mudanças do mercado e às novas oportunidades. No Nível 5, as organizações vão além da mera conformidade com os processos. Elas buscam a inovação contínua e a otimização dos processos, visando alcançar um desempenho superior e uma vantagem competitiva. (NASCIMENTO, 2023).

A imagem que se segue apresenta os níveis de maturidade do CMMI,

Figura 1: CMMI – Níveis de Maturidade



Fonte: Próprio autor, 2024.

A implementação dos cinco níveis de maturidade de uma organização tem como foco principal estabilizar os processos organizacionais e consequentemente melhorar seus resultados, possibilitando desta forma o desenvolvimento de ambientes propícios à inovação tecnológica. É importante ressaltar que a aplicação contínua dos níveis de maturidade mencionados acima permite que empresas de todos os portes, desde pequenas e médias até grandes corporações, obtenham os melhores resultados em seus processos organizacionais.

2.5 Trabalhos Relacionados

Segundo (FERREIRA; OKANO, 2021) em sua pesquisa acerca de implementação da LGPD no Brasil, avalia a utilização de um método visual que destacasse as principais preocupações ligadas à privacidade, proteção e conformidade das organizações com os requisitos da LGPD. Foi proposta a LGPD Model Canvas, que é uma ferramenta visual cujo objetivo é auxiliar as organizações na elaboração de estratégias para a conformidade com

a Lei Geral de Proteção de Dados (LGPD) no Brasil. O *framework* LGPD *Model Canvas* é dividido em nove blocos que incluem Dados Pessoais, Finalidade, Consentimento, Transferência Internacional de Dados, Tratamento Seletivo, Direitos do Titular dos Dados, Responsabilidades, Plano de Ação, e Segurança. Esta ferramenta foi inspirada no Business Model Canvas (BMC) que oferece uma representação visual para simplificar estruturas organizacionais complexas. Na mesma linha de pensamento, as imagens têm a capacidade de transformar suposições não expressas em informações explícitas, as quais auxiliam a pensar e comunicar de maneira mais eficaz. (OSTERWALDER; PIGNEUR; CLARK, 2013)

Outro trabalho propõe um *framework* denominado de LGPD4BP, que consiste em um método para avaliar e modelar processos de negócio conforme a LGPD utilizando a notação Business Process Model and Notation (BPMN). A modelagem deste trabalho é composta por: um questionário de avaliação de conformidade dos processos em relação à LGPD, que permite avaliar se um processo de negócio está em conformidade com a Lei; um catálogo de padrões e modelagens criado para modelar requisitos específicos da Lei que serve para ser usados por analistas como referência para modelar processos de negócio e assim atingir a conformidade LGPD e por fim um método de modelagem utilizado para orientar o modelador de negócio em modelar um processo, ou corrigir algum modelo não compatível com a LGPD (ARAÚJO et al., 2021).

O estudo conduzido por (LABADIE; LEGNER, 2019) em um contexto semelhante, porém aplicado à Regulamentação Geral de Proteção de Dados (GDPR) da União Europeia, destaca a importância do controle individual e da responsabilidade organizacional. O trabalho introduz um novo paradigma que exige mudanças significativas na forma como as organizações gerenciam dados pessoais, mas também ressalta os desafios enfrentados na implementação eficaz da regulamentação, principalmente devido à falta de alinhamento entre o conhecimento jurídico sobre a Lei e as práticas de gestão de dados. Nesse contexto, o estudo apresenta um modelo de capacidades desenvolvido em um processo iterativo de design científico (*interactive design science*), que integra tanto a interpretação de textos legais quanto percepções práticas obtidas de grupos focais com mais de 30 especialistas e de 3 projetos relacionados à GDPR da UE. O principal objetivo desse modelo é orientar as organizações na implementação dos requisitos da GDPR em suas práticas existentes. Conclui-se que o uso desse modelo contribuiu para mitigar esses desafios, ajudando a identificar lacunas de conformidade, além de definir e priorizar ações necessárias.

Uma outra abordagem encontrada foi o trabalho de (NASCIMENTO, 2023) onde a avaliação e a melhoria do nível de maturidade na gestão de dados em um órgão público de trânsito, utilizando o Modelo de Maturidade de Gestão de Dados (Data Maturity Model, DMM) do CMMI Institute. O objetivo foi de diagnosticar o nível de maturidade do órgão analisado, identificar seus aspectos positivos e negativos, e propor melhorias que possam

ser implementadas para atender às recomendações do DMM, com foco na administração pública e recursos humanos. Para traçar este caminho de melhoria, propõe-se a utilização de um modelo de maturidade para gestão de dados, de modo que seja possível medir e propor ações para que políticas e práticas de gerenciamento de dados sejam implantadas na organização. Quanto mais maduro for esse gerenciamento, melhor será o planejamento e a visão ao nível estratégico para o uso e consumo dos dados existentes em uma organização.

Semelhante ao trabalho anterior, (MARQUES, 2020), também apresenta o modelo DMM para gestão dos dados e como pode ser utilizado para adequação e conformidade com a LGPD. Conforme o autor, a maturidade de uma organização se reflete na experiência em gerenciar seus dados de maneira eficiente, ou seja, na sua capacidade de controlar e administrar estrategicamente seus ativos de dados. As organizações que implementam uma filosofia e práticas maduras de gerenciamento de projetos de segurança da informação estarão mais preparadas para ter sucesso em um mercado competitivo do que aquelas que mantêm práticas tradicionais. O gerenciamento de informações está se tornando cada vez mais relevante nos modelos de administração, estabelecendo-se como um fator crucial para proporcionar agilidade, robustez, consistência e excelência operacional no desenvolvimento de sistemas mais seguros (KERZNER, 2010).

O trabalho apresentado por (ZITOUN et al., 2021) aborda um modelo de avaliação de maturidade que visa diagnosticar o nível atual de maturidade de uma empresa, especialmente no que se refere à gestão de dados e informações. Além disso, o modelo sugere recomendações para promover a evolução da maturidade organizacional. Este artigo explora uma metodologia para desenvolver modelos de maturidade, visando avaliar a maturidade empresarial em termos de gestão de dados e análises avançadas. O foco está na criação de um conjunto de ferramentas que não apenas simplifiquem a aplicação do modelo, mas também estabeleçam um roteiro evolutivo fundamentado em evidências. O Modelo de Maturidade de Gestão de Dados (DMMM) proposto foi concebido para apoiar a transformação digital, desde os estágios iniciais até a otimização completa. O modelo abrange uma série de aspectos essenciais, como a estrutura organizacional, os sistemas de informação, as dimensões dos dados e as operações.

Os trabalhos citados abordam temas relacionados à implementação da LGPD e gestão de dados pessoais, porém não tratam especificamente de processos de maturidade visando a adequação à conformidade com a LGPD.

Os trabalhos propõem ferramentas como *canvas*, *frameworks* e modelos para auxiliar organizações na conformidade com requisitos da LGPD, mas não avaliam o amadurecimento dessas organizações por meio de processos iterativos visando atender integralmente à legislação. Já os trabalhos que citam o Modelo de Maturidade de Gestão de Dados (DMM) o fazem no contexto mais amplo da gestão de dados em geral, sem focalizar a maturação de processos especificamente para adequação à LGPD.

Diferentemente, esta dissertação irá diagnosticar o nível de maturidade de processos corporativos com aplicação de um modelo de maturidade, para identificar aqueles processos que necessitam de maior atenção para a conformidade com os requisitos da Lei Geral de Proteção de Dados.

3 METODOLOGIA

Para o desenvolvimento de uma pesquisa científica, tem-se como primordial a determinação dos aspectos metodológicos a ela inerentes, tendo em vista a necessidade de traçar os planos a serem executados para possibilitar o desenvolvimento de análises adequadas e consequente alcance de resultados cientificamente comprovados.

Este estudo tem como objeto de análise a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n.º 13.709/2018, legislação brasileira que objetiva proteger os direitos fundamentais de liberdade e privacidade e a livre formação da personalidade de cada indivíduo. Em outras palavras, a LGPD estabelece as regras para a coleta, o uso, o armazenamento e o compartilhamento de dados pessoais.

Para a realização deste estudo, utilizaram-se os métodos de pesquisa bibliográfica, descritiva, exploratória, aliadas ao estudo de caso para o desenvolvimento apropriado do modelo de processo com maturidade para a adequação da Lei Geral de Proteção dos Dados (LGPD).

Em se tratando de pesquisa bibliográfica, tem-se que esta se caracteriza por ser um tipo de estudo que se baseia na coleta, análise e interpretação de informações presentes em diversas fontes bibliográficas, como livros, artigos científicos, teses, dissertações, documentos oficiais e outros materiais relevantes para o tema em questão, tendo como objetivo principal aprofundar o conhecimento sobre um determinado assunto, identificando diferentes perspectivas, teorias e dados sobre ele. A revisão bibliográfica foi realizada de maneira sistemática e estruturada, tendo como objeto de estudo materiais científicos já tornados públicos, bem como análise rigorosa das legislações pertinentes (MARCONI; LAKATOS, 2006). A revisão bibliográfica aqui desenvolvida proporcionou uma compreensão aprofundada do assunto e permitiu embasar teoricamente a pesquisa.

No que se refere a pesquisa exploratória, conforme objetivos específicos deste estudo, esta tem como fundamento aprofundar o conhecimento sobre determinado tema. Assim, entende-se que a pesquisa exploratória é uma ferramenta fundamental para o pesquisador que busca entender melhor um tema/fenômeno complexo e pouco conhecido, permitindo que o pesquisador se familiarize com o tema, identifique lacunas no objeto de estudo e tenha a possibilidade de formular novas perguntas de pesquisa. Assim, a pesquisa exploratória se conceitua como sendo a "que se caracteriza pelo desenvolvimento e esclarecimento de ideias, visando oferecer uma visão panorâmica, uma primeira aproximação a um determinado fenômeno pouco explorado" (OLIVEIRA et al., 2006). Esta ferramenta metodológica possui a função de fornecer informações e conhecimento suficientes para que se chegue ao entendimento pleno acerca de determinado objeto de estudo, tendo como pressuposto a garantia de preservação das características deste objeto.

Somando aos métodos acima citados, tem-se a pesquisa descritiva, cujo principal objetivo metodológico é descrever as características inerentes a determinado objeto de estudo, buscando identificar todos os aspectos relacionados à sua existência. Ou seja, a pesquisa descritiva é um método de estudo que visa descrever as características de um objeto de estudo, pois fornece dados concretos que podem ser usados para embasar decisões e planejar ações estratégicas (MARCONI; LAKATOS, 2006).

Em se tratando do método de estudo de caso, entendido como ferramenta metodológica de pesquisa que se concentra na análise profunda de um fenômeno particular, seja ele um indivíduo, um grupo, um evento, uma organização ou um sistema. Ao invés de buscar generalizações amplas, o estudo de caso busca entender a complexidade e a singularidade de um caso específico, explorando suas características, contextos e relações causais (MARCONI; LAKATOS, 2006).

O estudo de caso geralmente combina diferentes métodos de coleta de dados, como entrevistas, observação, análise de documentos e dados quantitativos, buscando compreender o fenômeno na totalidade, considerando suas múltiplas dimensões e interações. Suas características principais são: aprofundamento intensivo e detalhado no objeto de estudo, vez que o caso é analisado dentro de seu contexto específico, considerando as variáveis e fatores que influenciam o fenômeno em questão (GIL, 2010).

Por fim, tem-se o método de pesquisa-ação, que consiste em um método de investigação que combina a pesquisa com a ação, visando à transformação de uma determinada realidade. É uma abordagem participativa, onde os pesquisadores e os participantes de um grupo social trabalham juntos para compreender e solucionar problemas, buscando a melhoria de uma situação (OLIVEIRA et al., 2006).

Assim, verificou-se que este estudo adotou procedimentos metodológicos abrangentes para investigar e propor um modelo de processo de maturidade para adequação à Lei LGPD de forma que possa ser adotado em organizações públicas e privadas. Inicialmente, será realizada uma análise bibliográfica do tema por meio de consultas em artigos científicos, sites especializados, livros, revistas da área e também a publicações provenientes de congressos nacionais e internacionais.

4 MODELO DE MATURIDADE E CAPACIDADE PARA PRIVACIDADE

Este capítulo apresenta o Modelo de Maturidade e Capacidade para Privacidade (CMMPC), uma estrutura desenvolvida para avaliar e orientar organizações no cumprimento dos requisitos previstos na Lei Geral de Proteção de Dados (LGPD).

O capítulo inicia com a seção 4.1, na qual o modelo é introduzido e contextualizado. Em seguida, a seção 4.2 descreve os níveis de maturidade que os processos organizacionais podem alcançar, definindo as etapas evolutivas do modelo. Na sequência, a seção 4.3 detalha os processos específicos que compõem o modelo, com foco na adequação às exigências legais.

A seção Avaliando processos e níveis de maturidade (4.4) integra os conceitos discutidos nas seções anteriores, apresentando uma visão consolidada da avaliação dos processos em relação aos níveis de maturidade. Nessa seção, são introduzidos um índice de maturidade e uma representação gráfica, visando facilitar a interpretação dos resultados.

Para exemplificar a aplicação prática do modelo, a seção Exemplo de aplicação do modelo CMMPC (4.5) apresenta um caso ilustrativo que demonstra sua utilização em um cenário real. Por fim, o capítulo é concluído com as Considerações Finais (4.6), que sintetizam os principais pontos discutidos e avaliam a contribuição do modelo para a conformidade da privacidade em relação aos requisitos da LGPD.

4.1 O Modelo CMMPC

Um modelo de capacidade e maturidade define um conjunto de métricas para medir a competência ou maturidade organizacional em termos de um conjunto de práticas, habilidades ou padrões reconhecidos. As métricas são organizadas em categorias e quantificadas em uma escala de desempenho. Utilizando critérios de avaliação específicos, as organizações podem medir seu desempenho em relação a esses níveis de maturidade (ALIYU et al., 2020).

A proposta deste trabalho visa apresentar um modelo de maturidade de processo adequado para avaliar a conformidade de organizações com a Lei Geral de Proteção de Dados (LGPD). Inspirados pelos fundamentos do *Capability Maturity Model Integration* (CMMI), decidimos criar o *Capability Maturity Model for Privacy Concern* (CMMPC) - Modelo de Maturidade e Capacidade para Privacidade (ou voltado para questões de privacidade) para abordar os desafios específicos relacionados à proteção de dados nas organizações.

O CMMPC pretende fornecer uma ferramenta sistemática e estruturada que permita às organizações avaliarem e melhorarem continuamente suas práticas de proteção de

dados. A estrutura do modelo é baseada em níveis de maturidade que refletem a evolução das capacidades de privacidade da organização, desde a conformidade inicial até a excelência em proteção de dados.

O CMMPC se baseia nos princípios do CMM/CMMI, integrando-os aos requisitos específicos da LGPD. Seu foco central é fornecer uma estrutura de avaliação sistemática e eficaz, considerando práticas recomendadas, políticas organizacionais e requisitos legais. Para atingir esse objetivo, o modelo será desenvolvido considerando as práticas recomendadas, políticas organizacionais e requisitos legais, com ênfase especial nas etapas de coleta, processamento, armazenamento e descarte de dados pessoais, sejam digitais ou não.

Ainda, a aplicação deste modelo buscará identificar áreas que necessitarão de maior atenção, permitindo que a própria organização fortaleça sua postura frente aos desafios emergentes no cenário da privacidade em dados. Este trabalho contribuirá significativamente para a capacitação das organizações na gestão eficaz de dados pessoais, promovendo uma cultura de responsabilidade e conformidade com as regulamentações vigentes.

4.2 Níveis de maturidade do modelo

O modelo CMMPC, abrange cinco níveis de escala de maturidade organizacional e diversos processos relacionados às práticas necessárias para a conformidade com a LGPD. Cada processo foi organizado de maneira a abranger requisitos semelhantes contidos na lei. Então, cada nível de maturidade no modelo CMMPC representa um estágio evolutivo nas capacidades organizacionais relacionadas à gestão de privacidade em dados.

Os processos delineados são concebidos como elementos independentes entre si onde cada um, que foi estruturado e alinhado com requisitos similares, tem a flexibilidade de evoluir em sua própria trajetória de maturidade. Esta abordagem oferece uma adaptabilidade fundamental, permitindo que as organizações atendam às demandas variadas e dinâmicas da LGPD.

Cada nível de maturidade no modelo CMMPC representa um estágio evolutivo nas capacidades organizacionais relacionadas à gestão de privacidade em dados. Os processos associados a cada nível são estruturados para apoiar e atender requisitos específicos da LGPD, mas a flexibilidade inerente ao modelo reconhece que diferentes processos podem ter diferentes ritmos de evolução.

Diferentes organizações possuem naturezas distintas, equipes diversas, níveis variados de conhecimento e engajamento organizacional. Assim, essa autonomia entre os processos no contexto do modelo CMMPC permite que as organizações foquem em áreas prioritárias de melhoria, aquelas mais importantes para os objetivos da organização, atendendo às demandas específicas de conformidade da LGPD de maneira eficiente e eficaz.

Dessa forma, o modelo proporciona não apenas um meio abrangente para aprimorar a gestão de privacidade em dados, mas também a flexibilidade necessária para enfrentar os desafios únicos que cada processo pode apresentar ao buscar níveis mais elevados de maturidade.

Nesse contexto, no qual cada nível de maturidade no modelo representa um estágio evolutivo nas capacidades organizacionais relacionadas à gestão de privacidade em dados, abaixo serão apresentados os cinco níveis de maturidade. Estes níveis foram baseados em documentos e recomendações de melhores práticas segundo (PAULK et al., 1993) e (KNOKE; NWANKWO, 2022):

- **Nível 1 - Informal**: As atividades são executadas de forma assistemática, baseando-se em costumes e práticas, sem a devida documentação. Elas são implementadas de maneira informal e em resposta a pedidos isolados, sem muito envolvimento por parte dos gestores da organização ou uma coordenação efetiva entre aqueles que executam essas atividades; são atividades *ad hoc*;

- **Nível 2 - Estruturado**: Neste nível, há uma gestão mínima dos processos, realizada por pessoas com conhecimentos em proteção de dados. As ações são planejadas, e algumas práticas são estruturadas e formalizadas; há um início do monitoramento dos resultados dos processos por meio de indicadores simples, aplicados nas áreas afins da organização;

- **Nível 3 - Formalizado**: As ações neste nível são realizadas de acordo com um processo definido, padronizado, formalizado e documentado. As pessoas que executam essas ações possuem habilidades adequadas ao processo. A organização apoia o processo, fornecendo os recursos, meios e treinamento necessários para sua operação. No entanto, é crucial ressaltar que não basta apenas formalizar os processos; a fiscalização torna-se imperativa para garantir que não sejam meros documentos, mas sim práticas efetivas. Isso assegura que o processo seja bem compreendido e, igualmente, cumprido de maneira consistente, tanto pela administração quanto pelos executores.

- **Nível 4 - Gerenciado**: Neste nível, a organização estabelece metas qualitativas e quantitativas para os processos como para os produtos derivados dos processos; os processos são bem definidos, consistentes e medidos. A produtividade e a qualidade são mensurados para todas as atividades de processo em todas as áreas, como parte de um programa organizacional, resultando em uma avaliação dos processos;

- **Nível 5 - Optimizado**: Este é o último nível, e atingindo este ponto, a organização inteira está engajada em melhoramento contínuo de seus processos.

> O objetivo deste melhoramento contínuo é para identificar fraquezas e fortalecer proativamente todo o processo, visando a prevenção de defeitos. Esta melhoria ocorre tanto por avanços incrementais no próprio processo quanto por inovações em tecnologias e métodos organizacionais.

Em suma, a implementação eficaz do modelo CMMPC, com seus cinco níveis de maturidade, reflete a evolução progressiva das capacidades organizacionais na gestão de privacidade em dados. Os níveis estão correlacionados entre si de forma que não há como pular um nível, existe a necessidade de haver uma progressão sucessiva entre eles.

Algumas literaturas adotam um nível 0 (zero) considerando que a organização não possui processos. Consideramos para este modelo iniciar no nível 1 (um), o **nível informal**, por enfatizar a ideia de que, mesmo em organizações inicialmente mais precárias e atrasadas na implementação da LGPD, sempre há algum tipo de processo em funcionamento, por mais informal e simples que este seja. Esta ideia está apoiada nos conceitos mais clássicos do CMM segundo (PAULK et al., 1993).

Ao adotar esta estratégia de adequação em estágios, é crucial destacar que as organizações, no cenário atual, enfrentam a necessidade de se adequar a diversos tipos de processos, abrangendo desde a coleta até o descarte responsável de dados pessoais sensíveis, a fim de garantir uma abordagem abrangente e sustentável para a segurança da informação e conformidade com a lei.

Assim, os cinco níveis de maturidade do modelo CMM-PC serão aplicados como base para compor a maturidade dos processos que serão apresentados na sequência. Essa abordagem visa oferecer um instrumento para orientar as organizações no aprimoramento contínuo da gestão de privacidade e na garantia de conformidade com a LGPD, promovendo uma evolução consistente e sustentável.

4.3 Processos do modelo de maturidade

A LGPD abrange uma série de artigos, cuja compreensão nem sempre é uma tarefa trivial e clara para todos os membros de uma organização, especialmente ao se considerar a necessidade de garantir conformidade e segurança jurídica. Visando facilitar a compreensão e aplicação da lei, inicialmente, os artigos foram mapeados para processos organizacionais.

Para realizar o mapeamento dos processos organizacionais, primeiramente, os artigos da Lei foram analisados individualmente para identificar seu conteúdo e intenção específica. Durante essa fase, o foco foi compreender como cada artigo poderia se relacionar com as atividades e operações das organizações.

Os artigos da Lei foram organizados por temas correlatos e categorizados em seções. Após uma análise inicial, alguns artigos foram realocados para seções mais adequadas, agrupando-os de acordo com tópicos semelhantes, como "direitos dos titulares de dados", "governança e segurança da informação", "tratamento de dados sensíveis", entre outros. Esse novo agrupamento proporcionou uma visão mais clara de como os artigos podem ser aplicados a práticas operacionais específicas.

Com os artigos organizados por temas, iniciou-se a derivação dos processos organizacionais. Esse trabalho consistiu em transformar os requisitos legais em atividades e fluxos de trabalho concretos em uma organização. No total, foram identificados 28 (vinte e oito) processos distintos. Cada processo foi detalhado quanto à sua finalidade específica, garantindo que houvesse clareza sobre como cada um contribuía para a conformidade com a LGPD.

Essa metodologia não só facilitou a interpretação e aplicação da LGPD, mas também ajudou a integrar as exigências legais no cotidiano das operações organizacionais. A partir desse mapeamento, as organizações puderam adotar práticas que não só asseguram a conformidade legal, mas também fortalecem a governança e a gestão da proteção de dados pessoais.

Cada processo está associado a um conjunto de atributos, atividades e/ou ações que devem ser incorporados aos processos de negócio da organização, conforme discutido por (ARAÚJO et al., 2021). Esses elementos delineiam as áreas da Lei Geral de Proteção de Dados (LGPD) nas quais a organização precisa se adequar para garantir a conformidade, auxiliando na implementação de práticas voltadas à proteção eficaz dos dados pessoais. Nesta proposta, definimos os requisitos gerais dos processos, identificando-os e aplicando critérios de maturidade. No entanto, a definição de detalhes específicos de implementação foge ao escopo deste estudo, sendo responsabilidade de cada organização definir sua forma de implementação, dada a existência de particularidades organizacionais.

Vale salientar que grande parte desses processos são independentes entre si de forma que cada processo pode ser tratado de maneira autônoma, focando nas características específicas e nas exigências particulares de cada área da organização. Esta forma de independência proporciona uma flexibilidade valiosa, permitindo que a organização trilhe autonomamente nos desafios de conformidade em suas diferentes áreas.

Os processos descritos no modelo CMMPC estão diretamente correlacionados e agrupados conforme as áreas ou temas estabelecidos na Lei Geral de Proteção dos Dados. Para facilitar a organização e o entendimento, os processos foram distribuídos em 5 (cinco) grupos temáticos, que agrupam processos com temas e assuntos semelhantes. Esses grupos são: **Tratamento de Dados Pessoais**, na **seção 4.3.1**, **Direitos do Titular**, **seção 4.3.2**, **Transferência de Dados Internacionais**, **seção 4.3.3** , **Governança e**

Segurança da Informação, **seção 4.3.4**, e **Sanções administrativas** na **seção 4.3.5**.

Essa estrutura foi delineada para garantir que cada processo, em sua essência, aborde os princípios fundamentais e os requisitos detalhados pela legislação de proteção de dados. Da mesma forma, adotamos essa abordagem neste trabalho, que será detalhada nas próximas subseções.

4.3.1 Tratamento Dados Pessoais

O tratamento de dados pessoais é o cerne de toda a LGPD, que visa proteger os direitos fundamentais dos cidadãos em relação à sua privacidade e autonomia. Ao estabelecer as condições para o tratamento de informações pessoais, a lei busca equilibrar o desenvolvimento tecnológico e econômico com a garantia de que os dados dos indivíduos sejam utilizados de forma ética e responsável.

Antes de aprofundar-se nos detalhes de todos os processos, é crucial considerar algumas questões de natureza transversal no âmbito desta proposta do modelo CMMPC. Os processos delineados nesta seção, relativos ao tratamento de dados pessoais, devem abranger todos os tipos de meios, digitais ou não, e os destinatários para os tratamentos de dados, isto é, os titulares dos dados, podem ser pessoas físicas ou jurídicas, incluindo entidades privadas e públicas. O propósito dessas ações é regulamentar a proteção de dados pessoais, sempre levando em consideração o respeito à privacidade, à inviolabilidade da intimidade, da honra e da imagem, à livre iniciativa, à livre concorrência, bem como à defesa do consumidor, além de promover o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

A Tabela 2 aborda todos os processos relacionados ao tratamento de dados pessoais, cada um com sua respectiva explicação detalhada.

Tabela 2: Processos sobre Tratamento Dados Pessoais

Cód.	Processo	Descrição
P01	**Consentimento de Dados ao Titular**	Formalização para consentimento de uso de dados do titular
P02	**Regovação do Consentimento de Dados ao Titular**	Formalização para a revogação do consentimento de uso de dados do titular
P03	**Acesso aos Dados do Titular**	Fornecer ao titular dos dados o acesso às informações sobre o tratamento de seus dados.

Continua na próxima página

Tabela 2 – continuação da página anterior

IDProc	Titulo	Objetivos
P04	**Tratamento de Dados Sensíveis**	Tratar de forma explícita e transparente as finalidades do uso de dados pessoais sensíveis
P05	**Consentimento para Tratamento de Dados Pessoais Sensíveis**	Estabelecer processos formais para o consentimento de tratamento dos dados pessoais sensíveis por pelo menos um dos pais ou pelo responsável legal;
P06	**Publicização dos tipos de dados coletados**	Estabelecer processos formais para a publicização dos tipos de dados coletados de crianças e adolescentes.
P07	**Tratamento de Dados Pessoais pelo Poder Público**	Tratar as ações de executar as competências legais ou cumprir as atribuições legais do serviço público. Informações acerca de tratamento, compartilhamento e publiciação dos dados coletados.

Fonte: Próprio autor.

Considerando a amplitude dos temas tratados por esses processos e a diversidade de aspectos envolvidos o tratamento dos dados pessoais, optou-se por explicá-los de forma separada. Essa divisão tem o intuito de melhorar a clareza e a compreensão dos conteúdos apresentados, evitando que a leitura se torne excessivamente extensa e monótona. Desta forma, a Tabela **??** relaciona os processos **P01** a **P03** sobre tratamento de dados pessoais; a Tabela 4 apresenta o processo **P04**, tratando de tratamento de dados pessoais sensíveis; a Tabela 5, com o processos **P05** e **P06** que dispõe de dados pessoais de crianças e adolescentes e por fim, a Tabela 6 sobre tratamento de dados pessoais pelo Poder Público, representado no processo **P07**.

Iniciamos a exposição dos processos com uma abordagem preliminar abrangente do modelo de CMMPC. Estas disposições preliminares estabelecem os fundamentos essenciais a serem aplicados em todos os processos, abrangendo a totalidade da instituição.

A Lei Geral de Proteção a Dados Pessoais trata das proteções e cuidados que as organizações devem ter ao lidar com dados pessoais, incluindo todos os meios, não só os digitais, mais comum hoje em dia, mas também os meios físicos como os papeis. A LGPD é aplicada a toda pessoa, seja física ou jurídica, de direito público ou privado. O objetivo desta lei é a proteção dos direitos fundamentais de liberdade e privacidade.

O tratamento de dados pessoais, conforme o art. 7º (BRASIL, 2018), requer a observância de condições específicas. Essas incluem o consentimento explícito do titular para o uso dos dados, bem como a garantia de sua capacidade de revogação posterior.

Para atender esses requisitos, sugerimos dois processos: um para o **consentimento** (**P01**) e outro para a **revogação** (**P02**), dispostos na Tabela 3. O ato do consentimento

deve ser fornecido por escrito ou digitalmente e deve demonstrar o livre interesse do titular dos dados, bem como as finalidades do uso dos dados, conforme mencionado no art. 8º da LGPD. É importante observar que é estritamente proibida a prática denominada 'vício de consentimento'. Este consiste em pré-selecionar no sistema ou aplicativo a opção do consentimento sem as condições estarem claramente definidas e sem o usuário do sistema marcar formalmente a opção de concordância.

Tabela 3: Processos sobre Tratamento Dados Pessoais

Cód.	Processo	Descrição
P01	**Consentimento de Dados ao Titular**	Formalização para consentimento de uso de dados do titular
P02	**Regovação do Consentimento de Dados ao Titular**	Formalização para a revogação do consentimento de uso de dados do titular
P03	**Acesso aos Dados do Titular**	Fornecer ao titular dos dados o acesso às informações sobre o tratamento de seus dados.

Fonte: Próprio autor.

Outro ponto a destacar é que o titular dos dados possui o direito, a qualquer momento, de solicitar o **acesso aos seus dados pessoais** (**P03**), conforme estabelecido no artigo 9º da Lei. Com o intuito de atender a essa demanda, foi proposto um processo, que pode ser integrado ou anexado a algum processo já existente na organização, como o e-SIC [6] do governo federal, corroborando ainda com a Lei de Acesso à Informação (BRASIL, 2011). Neste processo deverá ser informado a finalidade do tratamento dos dados, o prazo e a forma em que a organização irá utilizar esses dados, a identificação e o contato do responsável pelo controle dos dados, bem como a intenção de compartilhamento dos dados e sua finalidade.

Dando continuidade, apresentamos na Tabela 4 os processos referentes aos dados pessoais sensíveis.

[6] e-SIC: <https://esic.cgu.gov.br/>

Tabela 4: Processos sobre Dados Pessoais Sensíveis

Cód.	Processo	Descrição
P04	**Tratamento de Dados Sensíveis**	Tratar de forma explícita e transparente as finalidades do uso de dados pessoais sensíveis

Fonte: Próprio autor.

Os dados sensíveis, conforme a LGPD, podem causar danos imediatos se divulgados de maneira inadequada, por isso, exigem precauções especiais e só podem ser solicitados para finalidades específicas, propósitos específicos, já que podem "implicar em riscos e vulnerabilidades potencialmente mais sérios aos direitos e liberdades fundamentais dos titulares"(SALMEN; BELLÉ, 2020). Este processo permeia os demais processos da organização, pois tratam obrigações gerais de dados pessoais sensíveis. Para aquelas organizações que lidam com pesquisa na área de saúde pública, terão autorização para acessar bases de dados pessoais, desde que sejam tratados exclusivamente dentro da instituição e estritamente para fins de estudos e pesquisas. Esses dados serão mantidos em um ambiente controlado e seguro, conforme as práticas de segurança estabelecidas em regulamento específico como uma Política de Segurança. Sempre que possível, os dados deverão ser anonimizados, e serão considerados os padrões éticos apropriados para estudos e pesquisas. Dados anonimizados são, segundo a própria LGPD, são dados relacionados ao titular e uma vez anonimizados não são capazes de identificar o titular.

Assim, ao implementar este processo para Tratamento de Dados Sensíveis **P04**, a organização deve exercer cautela e atenção meticulosas, pois além de abranger todas as áreas de sua atuação deverá aplicar técnicas para anonimização dos dados, caso haja necessidade de divulgar alguma de suas informações.

Tratamento de Dados Pessoais de Crianças e Adolescentes

A Lei Geral de Proteção de Dados (LGPD) reservou uma seção específica, seção III do segundo capítulo, para disciplinar o tratamento de dados pessoais de crianças e adolescentes. Porém, em seu artigo 14 no §1º há apenas a obrigatoriedade do consentimento por parte dos pais ou responsáveis para o tratamento de dados pessoais sensíveis para crianças, a lei não inclui para adolescentes.

Esta medida suscita uma controvérsia relevante devido à condição desses indivíduos como menores de idade. Bezerra (2020) comenta sobre o controle parental emerge como uma medida de suma importância e pertinência, considerando especialmente a vulnerabilidade e a dependência derivada das crianças. Contudo, surge um questionamento

relevante sobre a dispensa do consentimento parental para o tratamento de dados pessoais de adolescentes. Estes últimos, também enquadrados como indivíduos vulneráveis e cujo desenvolvimento psíquico-intelectual encontra-se ainda em estágio de maturação, poderia igualmente exigir a obrigatoriedade da autorização dos pais ou responsáveis legais para o tratamento de suas informações pessoais.

Analisando o Estatuto da Criança e do Adolescente, Lei Nº 8.069 de 1990 (BRASIL, 1990), que versa sobre a proteção integral para crianças e adolescentes, observamos um tratamento igualitário fundamentado em preceitos legais que reconhecem a condição peculiar desses grupos etários. Segundo o estatuto, crianças são consideradas indivíduos até doze anos incompletos, enquanto adolescentes são aqueles com idade entre doze e dezoito anos. Ambos possuem todos os direitos fundamentais inerentes à pessoa humana, garantindo-lhes proteção integral para seu desenvolvimento físico, mental, moral, espiritual e social. Além disso, a lei também se preocupa com a preservação da imagem, da inviolabilidade da integridade física, psíquica e moral, da identidade, da autonomia, dos valores, das ideias e crenças, reforçando a importância da proteção abrangente desses indivíduos.

Diante da relevância do tratamento de dados pessoais de crianças e adolescentes e da controvérsia suscitada pela legislação, é crucial ressaltar a necessidade de igualdade na proteção desses grupos vulneráveis. Levando em consideração a condição de vulnerabilidade e o estágio de desenvolvimento psíquico-intelectual, seria prudente exigir autorização dos pais ou responsáveis legais para tal tratamento, em paridade com as crianças. Assim, ainda que não explicitamente recomendada pela Lei, propomos que o processo de tratamento de dados de crianças e adolescentes seja uniformemente regulado, requerendo o consentimento dos pais ou responsáveis quando necessário.

Considerando a importância do tratamento de dados pessoais de crianças e adolescentes e as discussões provocadas pela legislação de privacidade, é fundamental enfatizar a necessidade de igualdade na proteção desses grupos em fase de desenvolvimento. Levando em conta a condição peculiar e o estágio de desenvolvimento psíquico-intelectual, bem como as disposições do Estatuto da Criança e do Adolescente, sugerimos que seja exigida autorização dos pais ou responsáveis legais para tal tratamento, em igualdade de condições com as crianças. Assim, embora não explicitamente recomendada pela LGPD, propomos que o processo de tratamento de dados pessoais sensíveis de crianças e adolescentes seja uniformemente regulado, requerendo o consentimento dos pais ou responsáveis. Esta abordagem não apenas protegeria os direitos desses indivíduos, mas também promoveria um ambiente de segurança e confiança no tratamento de dados pessoais, contribuindo para o desenvolvimento saudável e a integridade desses grupos em nossa sociedade.

Sugerimos dois processos distintos, **P05** e **P06**, dispostos na Tabela 5, para tratar do consentimento sobre o tratamento de dados sensíveis e a publicização destes. A Lei

discorre que os controladores devem manter disponíveis publicamente as informações sobre os tipos de dados coletados e como são utilizados.

Tabela 5: Dados Pessoais Sensíveis de Crianças e Adolescentes

Cód.	Processo	Descrição
P05	**Consentimento para Tratamento de Dados Pessoais Sensíveis**	Estabelecer processos formais para o consentimento de tratamento dos dados pessoais sensíveis por pelo menos um dos pais ou pelo responsável legal;
P06	**Publicização dos tipos de dados coletados**	Estabelecer processos formais para a publicização dos tipos de dados coletados de crianças e adolescentes.

Fonte: Próprio autor.

Tratamento de Dados Pessoais pelo Poder Público

O tratamento de dados pessoais pelo poder público, Tabela 6, processo **P07**, é crucial devido à sensibilidade e à confidencialidade das informações que estão muitas vezes sob sua responsabilidade. A Lei Geral de Proteção de Dados (LGPD) estabelece diretrizes claras para garantir a segurança e a privacidade desses dados, visando proteger os direitos fundamentais dos cidadãos. Órgãos governamentais, como ministérios, autarquias, empresas públicas e fundações, em todas as esferas - executiva, judiciária e legislativa - estão sob a exigência da LGPD, pois lidam com uma ampla gama de informações pessoais, como dados de saúde, previdenciários, fiscais, entre outros, que devem ser tratados com o máximo de cuidado e segurança. Além disso, o tratamento adequado desses dados pelo poder público contribui para fortalecer a confiança dos cidadãos nas instituições governamentais e para garantir a transparência e a eficiência na prestação de serviços públicos.

Tabela 6: Dados Pessoais pelo Poder Público

Cód.	Processo	Descrição
P07	**Tratamento de Dados Pessoais pelo Poder Público**	Tratar as ações de executar as competências legais ou cumprir as atribuições legais do serviço público. Informações acerca de tratamento, compartilhamento e publiciação dos dados coletados.

Fonte: Próprio autor.

Até a data da escrita deste trabalho, o Governo Digital do Brasil oferece 4.407 (quatro mil, quatrocentos e sete) serviços em seu portal, dos quais, 977 (novecentos e

setenta e sete) estão de alguma forma integrados com outros órgãos públicos, como a autenticação centralizada no gov.br, por exemplo, e 3.618 serviços digitais pelo portal único do governo federal brasileiro, dos quais 1.639 foram digitalizados a partir de 2019 (BRASIL, 2024).

As Plataformas de Governo Digital representam ferramentas essenciais para a disponibilização e a prestação digital dos serviços públicos em cada esfera federativa, contribuindo para o aumento da eficiência pública, com o uso da desburocratização, da inovação, da transformação digital e da participação do cidadão. Por meio das Cartas de Serviços ao Usuário, são delineados os serviços oferecidos, os procedimentos para acesso e os compromissos e padrões de qualidade no atendimento ao público (DANTAS, 2021).

A administração pública frequentemente lida com uma variedade de bancos de dados que podem conter informações sensíveis. A coleta e o tratamento desses dados são questões cruciais para políticas públicas em grande escala (MALDONADO; BLUM, 2022).

Então, o Poder Público, como um grande detentor de informações e dados pessoais, tem a necessidade ainda mais peculiar quando lidando com essas informações, preocupando-se em não ferir a esfera da liberdade, da privacidade e do livre desenvolvimento da personalidade natural (BOTELHO; CAMARGO, 2021).

Por estar sujeito à legislação vigente, o Poder Público necessita das autorizações legais apropriadas para realizar suas atividades, o que abrange a capacidade de realizar o tratamento de dados de pessoas naturais, conforme estabelecido pela Lei Geral de Proteção de Dados (LGPD) (COTS; OLIVEIRA, 2018).

Portanto, é essencial que o Poder Público adote medidas robustas de proteção de dados, incluindo políticas claras, práticas avançadas de segurança da informação e mecanismos eficazes de prestação de contas. O tratamento de dados pessoais pelo setor público deve ser realizado visando executar competências legais e implementar políticas públicas. Ao adotar essas medidas, o Poder Público não apenas cumpre as exigências legais, mas também demonstra um compromisso sólido com o respeito aos direitos individuais, promovendo a confiança e a transparência na relação entre governo e cidadãos.

Aqui foram apresentados os processos relacionados ao tratamento de dados pessoais, abrangendo do processo P01 ao processo P07. Na próxima seção, serão detalhados os procedimentos relacionados aos Direitos do Titular dos Dados.

4.3.2 Direitos do Titular

Os processos descritos na Tabela 7 referem-se aos direitos dos titulares de dados pessoais. Esses mecanismos visam assegurar que o titular tenha pleno conhecimento e

controle sobre o tratamento de seus dados, permitindo-lhe exercer seus direitos de forma efetiva.

Tabela 7: Direitos do Titular dos Dados

Cód.	Processo	Descrição
P08	**Confirmação sobre existência de tratamento**	Confirmação de que a organização possui tratamento adequado para os dados do titular;
P09	**Acesso aos dados**	Processo para solicitar acesso aos dados do titular;
P10	**Retificação e Exclusão de Dados:**	Processo para solicitar alteração, correção ou exclusão dos dados do titular;
P11	**Portabilidade dos dados**	Solicitação de portabilidade dos dados do titular a outro fornecedor de serviço ou produto;
P12	**Informações sobre compartilhamento de dados**	Fornecer a relação das organizações que foram compartilhado os dados;

Fonte: Próprio autor.

A relação intrínseca que se estabelece entre a pessoa e seus dados exige um pouco a mais de mecanismos para garantir essa proteção. Isso porque, conforme as demandas atuais, a tradicional sequência pessoa $pessoa \rightarrow informação \rightarrow sigilo$ evoluiu para $pessoa \rightarrow informação \rightarrow circulação/controle$, onde o importante é o controle sobre os dados coletados, evitando a livre circulação. Assim, além da privacidade, a proteção de dados se baseia em princípios mais objetivos, dinâmicos e coletivos (KORKMAZ; SACRAMENTO, 2021).

A LGPD é orientada pelo princípio da autodeterminação informativa, que permite aos titulares de dados controlar suas informações pessoais. Isso inclui direitos como a confirmação da existência de tratamento de dados, acesso aos dados, correção de dados incompletos, incorretos ou desatualizados, compartilhamento de dados entre organizações e a portabilidade dos dados.

O titular dos dados possui o direito de solicitar a qualquer empresa, seja ela pública ou privada, a confirmação de que seus dados estão sendo devidamente tratados, sendo esta necessidade detalhada pelo processo **Confirmação sobre existência de tratamento** (**P08**), como também tem o direito de solicitar o **Acesso aos dados** (**P09**). Essas prerrogativas estão intimamente interligadas, pois representam a concretização do princípio da transparência, garantindo aos titulares informações claras e acessíveis sobre o tratamento

de seus dados.

O direito do titular de corrigir seus dados reflete o controle que ele tem sobre suas informações. Corrigir, complementar e atualizar dados pessoais são ações importantes para garantir que os dados representem a pessoa de forma precisa, evitando, problemas como decisões automatizadas erradas. Decisões automatizadas são aquelas tomadas por sistemas ou algoritmos sem intervenção humana direta, como a negativação de crédito, ou a exclusão de candidatos para processos seletivos, recomendações errôneas de produtos online e avaliações de risco em seguros. Manter os dados corretos e atualizados ajuda a garantir que essas decisões sejam justas e precisas, além de preservar a história pessoal do titular de forma correta e atualizada. Assim, é salutar implementar o processo de **Retificação e Exclusão de Dados** (**P10**) para assegurar a conformidade com a legislação de proteção de dados pessoais.

Outro aspecto a ser considerado é a portabilidade de dados. Esta já estava regulamentada em diversas áreas do direito brasileiro, como no mercado financeiro e na telefonia. Com a promulgação da LGPD, a abrangência da portabilidade foi ampliada e sua regulamentação simplificada, permitindo a transferência dos dados para outro provedor de serviço ou produto, respeitando os segredos comerciais e industriais, sem ônus para o titular dos dados. Diante disso, sugere-se a implementação do processo denominado **Portabilidade dos Dados** (**P11**) para viabilizar essa funcionalidade para os indivíduos.

Para finalizar, temos um último ponto nesta seção que é a respeito do compartilhamento de dados. O controlador, responsável pela coleta e tratamento dos dados pessoais, pode compartilhar essas informações com outras entidades, desde que haja uma base legal que o titular dos dados seja informado. Além disso, o controlador deve comunicar a essas entidades sobre qualquer exclusão ou correção dos dados para mantê-los sempre atualizados.

É importante distinguir entre compartilhamento e portabilidade de dados: na portabilidade, o próprio titular solicita a transferência de seus dados para outro controlador, enquanto no compartilhamento, o controlador faz a transmissão sem pedido do titular. Para garantir o cumprimento efetivo dessas diretrizes e assegurar a transparência no compartilhamento de informações, sugerimos estabelecer o processo denominado **Informações sobre compartilhamento de dados** (**P12**). Além da prerrogativa do titular de ser informado sobre o compartilhamento, é incumbência do responsável pelo tratamento de dados comunicar às entidades com as quais houve compartilhamento sobre a exclusão ou correção dos dados. Isso permite que tais entidades mantenham as informações dos titulares atualizadas.

Dessa forma, essas prerrogativas asseguram que o titular tenha acesso a informações que lhe permitem compreender as atividades da organização (SANTOS, 2021b).

Na próxima seção, será abordado o processo relacionado à transferência internacional de dados, detalhando as responsabilidades e os cuidados necessários para sua realização.

4.3.3 Transferência de Dados Internacionais

A Lei Geral de Proteção dos Dados e o Regulamentação Geral de Proteção de Dados da União Europeia (Regulamentação Geral de Proteção de Dados (RGPD)) possuem disposições quase idênticas no que tange à transferência internacional de dados pessoais. Esta última é citada um dos instrumentos mais completos e abrangentes nesta questão de proteção a dados pessoais cuja abrangência é toda União Europeia. De acordo com esses dispositivos, a transferência de dados pessoais para um país terceiro ou um organismo internacional é permitida desde que sejam observadas certas condições e garantias (NEVES, 2022).

Se uma empresa ou organização tiver sua infraestrutura alocada no exterior e realizar transferências de dados, como e-mails, entre seus membros, passando pelos servidores situados fora do Brasil, isso não é considerado uma transferência internacional, pois as informações permanecem no âmbito da empresa. No entanto, se essa empresa enviar e-mails para outras empresas mesmo sendo do grupo econômico, porém, sediadas em outros países, isso, sim, será caracterizado como transferência internacional.

Para realizar a transferência internacional de dados, a LGPD exige que os países ou organismos internacionais de destino ofereçam um nível adequado de proteção de dados pessoais. Esse nível deve ser validado e reconhecido pela ANPD com base em critérios específicos. Tal reconhecimento é essencial para assegurar a conformidade legal de qualquer transferência internacional de dados para um país terceiro ou organismo internacional. Essa transferência pode ocorrer sempre que for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, investigação e persecução, conforme os instrumentos de direito internacional.

Sugerimos, então, implementar o processo **Transferência Internacional de Dados** (**P13**), na Tabela 8, que deve incluir todos os procedimentos necessários para realizar transferências internacionais de dados com segurança e conforme a lei.

Tabela 8: Transferência Internacional de Dados

Cód.	Processo	Descrição
P13	**Transferencia internacionais de dados**	Procedimentos para transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o Brasil seja membro;

Fonte: Próprio autor.

A próxima seção tratará dos processos voltados à governança e à segurança da informação, destacando as responsabilidades envolvidas e os cuidados essenciais para sua execução.

4.3.4 Governança e Segurança da Informação

Nesta seção, foram integrados diversos processos previstos no capítulo intitulado Segurança e Boas Práticas da LGPD. Além de abranger a maioria das diretrizes contidas nesse capítulo, também foram incluídas orientações de outras seções que, por sua natureza, se alinham ou se organizam de forma mais apropriada no contexto de Governança e Segurança da Informação. Abaixo, na Tabela 9, estão listados esses processos e suas respectivas descrições.

Tabela 9: Governança e Segurança da Inforamção

Cód.	Processo	Descrição
P14	**Gestão em Segurança da Informação**	Elaborar um programa em gestão da segurança da informação que inclua a proteção os dados pessoais;
P15	**Políticas de Proteção e Privacidade de Dados**	Processo para elaborar e manter políticas de proteção e privacidade de dados;
P16	**Treinamento e Conscientização**	Realização de treinamentos e ações de conscientização periódicos para os colaboradores envolvidos no tratamento de dados pessoais
P17	**Auditorias internas**	Conduzir auditorias internas regulares para garantir a conformidade com a LGPD.
P18	**Operações de tratamento de dados pessoais**	Processo de registro atualizado das operações de tratamento de dados pessoais realizadas.

Continua na próxima página

Tabela 9 – continuação da página anterior

IDProc	Titulo	Objetivos
P19	**Plano de Resposta a Incidentes**	Desenvolver e implementar um plano de resposta a incidentes de segurança da informação
P20	**Relatório de Impacto à Proteção de Dados**	Procedimentos para a elaboração do relatório de impacto à proteção de dados pessoais (RIDP), referente a operações de tratamento de dados pessoais;
P21	**Encarregado de Dados Pessoais (DPO)**	Processo para tratar nomeação, treinamento e avaliação do encarregado de dados pessoais.
P22	**Padrões de Interoperabilidade**	Estabelecer padrões de interoperabilidade para facilitar a portabilidade, segurança e o livre acesso aos dados.

Fonte: Próprio autor.

Iniciamos pelo **Processo de Gestão em Segurança da Informação** (**P14**). Um Sistema de Gestão de Segurança da Informação (SGSI) é um conjunto estruturado de políticas, processos e controles estabelecidos por uma organização para gerenciar e proteger a informação. Este sistema visa preservar a confidencialidade, integridade e disponibilidade da informação, aplicando um processo contínuo de gestão de riscos que assegura às partes interessadas que os riscos são adequadamente gerenciados. A implementação de um SGSI é uma decisão estratégica, moldada pelas necessidades e objetivos da organização, requisitos de segurança, processos organizacionais, e a estrutura e tamanho da organização, sendo projetada para evoluir ao longo do tempo. É fundamental que o SGSI esteja integrado com os processos organizacionais e a estrutura administrativa global, considerando a segurança da informação desde o projeto dos processos e sistemas de informação até os controles implementados (Associação Brasileira de Normas Técnicas, 2013).

A LGPD, em seu artigo 46, sugere a adoção de 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 ou alteração. Apesar da LGPD não explicitar a implementação de um SGSI, pelos argumentos mencionados acima, sugere-se fortemente essa prática como uma forma eficaz de cumprir os requisitos de segurança estabelecidos pela lei. Se a organização já implementou um SGSI, deve verificar se há cobertura na área de proteção e privacidade de dados; caso não haja, deve incluí-la.

Considerando que políticas de proteção e privacidade de dados podem integrar um sistema geral de gestão de segurança da informação, decidiu-se enfatizá-las em um processo separado, devido à sua importância.

O processo **Políticas de Proteção e Privacidade de Dados** (**P15**), é essencial para garantir a proteção e a privacidade das informações pessoais. Uma política de

privacidade é um documento formal que descreve detalhadamente como uma organização coleta, utiliza, divulga e gerencia os dados pessoais dos indivíduos. Este documento informa sobre o tratamento de seus dados, incluindo quais informações são coletadas, como são armazenadas, quem tem acesso a elas e quais medidas de proteção são adotadas. Visa estabelecer transparência e confiança com os clientes ou usuários, detalhando seus direitos em relação aos dados fornecidos, como o direito de acesso, correção ou exclusão das informações. Assim, ao implementar uma política de privacidade clara e abrangente, as organizações demonstram seu compromisso com a proteção de dados e a adesão às regulamentações pertinentes.

A implementação de um programa eficaz de **Treinamento e Conscientização** (**P16**) é essencial para auxiliar na mitigação de riscos e garantir a proteção de dados pessoais em uma organização. Um aspecto central para a criação e fortalecimento de um ambiente favorável à proteção de dados é a adoção de ações que promovam a capacitação e a conscientização das equipes (PORTILHO et al., 2022).

Para combater a impunidade de delitos virtuais, é fundamental promover a conscientização sobre os riscos dos crimes cibernéticos e as formas de proteção. Isso envolve a realização de campanhas educativas, treinamentos para todos os envolvidos com a organização, sejam colaboradores ou empresas parceiras, e a disseminação de orientações ao público sobre medidas de segurança online (SILVA, 2023).

A implementação de processos de auditoria interna é uma necessidade imperativa para organizações que buscam não apenas a conformidade legal, mas também a melhoria contínua e a eficiência operacional. A LGPD, ao estabelecer diretrizes rigorosas para a proteção de dados pessoais, exige que as organizações adotem medidas robustas para garantir a segurança e a privacidade das informações. Neste contexto, a auditoria interna emerge como uma ferramenta essencial, proporcionando uma série de benefícios substanciais, tais como a detecção de fraudes, a melhoria na gestão financeira, a promoção da responsabilidade e a transparência (CHEN, 2023).

Assim, sugerimos o processo **P17**, de **Auditorias Internas** que além de promover um exame minucioso nos processos internos e verificar a adesão às políticas de proteção de dados, a auditoria interna desempenha um papel crucial na detecção e prevenção de fraudes. Esse exame detalhado permite a identificação de vulnerabilidades e inconsistências que poderiam ser exploradas para atividades fraudulentas. A função da auditoria interna é, portanto, vital para manter a integridade dos dados e a confiança de todos os envolvidos nas organizações.

Registrar transações que envolvem dados pessoais é essencial para garantir a conformidade e proteger os direitos dos titulares. Para tal, sugere-se o processo **P18** – **Operações de Tratamento de Dados Pessoais** que permite rastrear e documentar

essas operações, assegurando transparência e mitigando riscos relacionados à privacidade e à segurança da informação.

Este processo permite que as empresas monitorem e analisem a movimentação de dados, assegurando que seu processamento seja legal e ético. Ao registrar transações, as organizações demonstram seu compromisso em proteger os direitos de privacidade dos indivíduos e em cumprir suas obrigações legais (FERREIRA et al., 2022).

Além disso, documentar transações com dados pessoais facilita a identificação de riscos e vulnerabilidades nas operações de processamento de dados, permitindo a implementação oportuna de estratégias de mitigação. Manter um registro organizado das transações auxilia o Diretor de Proteção de Dados (DPO) a supervisionar as atividades de processamento e a garantir a conformidade contínua com as leis de proteção de dados. O monitoramento e a revisão constantes das transações registradas são vitais para se adaptar às práticas de processamento de dados em evolução e manter a conformidade com as exigências legais (LORENZON, 2021)

Um Plano de Resposta a Incidentes, também mencionado na Lei, e sugerido no processo **P19** deve contemplar, além das medidas usuais de proteção à segurança da informação, a comunicação com a Autoridade Nacional de Proteção de Dados (ANPD) sempre que necessário. Em casos de vazamento de dados ou incidentes que comprometam a privacidade dos titulares dos dados, a organização deve informar a ANPD com detalhes sobre o incidente, as medidas tomadas para contê-lo e os esforços de mitigação realizados. A comunicação com a ANPD deve ser clara e detalhada, fornecendo todas as informações relevantes sobre incidentes e medidas corretivas adotadas. É fundamental estabelecer canais de comunicação eficientes para garantir que qualquer necessidade de interação com a ANPD seja realizada de forma ágil e precisa.

Comunicar com a ANPD é necessário para garantir a transparência e a conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD). Em cenários de vazamento de dados, incidentes de segurança significativos ou violações de privacidade, a ANPD deve ser informada para que possam ser tomadas as medidas apropriadas para proteger os direitos dos titulares dos dados e para que a organização possa demonstrar sua diligência em cumprir as obrigações legais.

O relatório de impacto à proteção de dados pessoais, indicado no processo **P20**, é o resultado de uma avaliação geral da organização cujo objetivo é analisar, mapear, planejar, implementar e monitorar a conformidade de uma organização com as leis de proteção de dados. Em termos simples, pode ser comparado a um diagnóstico das atividades de tratamento de dados de uma empresa.

Um dos papéis mais importantes do relatório de impacto é servir como documentação de conformidade. Ele é frequentemente visto como o produto final de um processo

de adequação à LGPD, documentando o mapeamento realizado, identificando os riscos associados ao tratamento de dados e descrevendo as medidas que a organização adotará para mitigar esses riscos. Isso é vital para demonstrar conformidade e responsabilidade perante a Autoridade Nacional de Proteção de Dados (ANPD).

Portanto, o relatório de impacto é fundamental não apenas para atender às exigências legais da LGPD, mas também como uma prática de boa governança que garante a proteção contínua dos dados pessoais. Ele auxilia as organizações a identificar e mitigar riscos, demonstrar responsabilidade e promover a transparência no tratamento de dados. (GOMES, 2019)

O papel do Oficial de Proteção de Dados (DPO - do inglês *Data Protection Officer*) ou **Encarregado de Dados Pessoais** (processo **P21**) é multifacetado, abrangendo diversas responsabilidades voltadas para a proteção de dados e a conformidade com a legislação vigente. Este profissional é encarregado de auditar internamente os processos da organização para assegurar a proteção dos dados e garantir que todas as atividades estejam consoante com a lei. Ele também deve fiscalizar o cumprimento das normas pelos colaboradores e revisar manuais, políticas e contratos para alinhá-los às exigências legais (FARIAS; BARROS, 2022).

Além dessas atividades, o DPO tem um papel ativo na implementação de medidas de proteção de dados, auxiliando a organização a adotar práticas seguras e eficazes. Ele é o ponto de contato para reclamações e comunicações dos titulares de dados, prestando esclarecimentos e adotando providências para resolver as questões apresentadas. A identidade e as informações de contato do encarregado devem ser divulgadas publicamente de maneira clara e objetiva, preferencialmente no site do controlador. O DPO também responde às solicitações dos titulares e da Autoridade Nacional de Proteção de Dados (ANPD), garantindo uma comunicação clara e eficiente.

Outra função que vale a pena destacar, é a de receber e agir sobre as comunicações da autoridade nacional, adotando as medidas necessárias para atender às exigências regulatórias. Ele orienta funcionários e contratados sobre as melhores práticas de proteção de dados pessoais, promovendo uma cultura de privacidade e segurança dentro da organização. Além disso, o DPO auxilia na criação de normas e padrões internos para o cumprimento das obrigações legais e executa outras atribuições determinadas pelo controlador ou estabelecidas em normas complementares (BARCELOS et al., 2021).

Dessa forma, o DPO não apenas garante a conformidade legal, mas também contribui para a construção de uma organização mais segura e transparente, fortalecendo a confiança das partes interessadas e promovendo a proteção eficaz dos dados pessoais. Assim, sugere-se a criação de um processo que auxilie o DPO em suas atividades, elencando etapas claras e estruturadas para suas funções.

Com um processo organizacional bem estruturado, o DPO poderá desempenhar suas funções de maneira mais eficiente e eficaz, garantindo não só a conformidade legal, mas contribuindo para a segurança e a confiança na organização.

O titular pode solicitar ao controlador a portabilidade de seus dados para outro serviço, conforme discutido na seção "Direitos do Titular". Porém, a organização deverá dispor ao controlador de dados mecanismos para prover esta portabilidade. Um desses mecanismos, recomendando pela ANPD, é a interoperabilidade dos dados, indicado pelo preocsso **P22**. Entende-se por interoperabilidade como a capacidade de dois ou mais sistemas funcionarem juntos, independentemente de interfaces, plataformas ou escolhas tecnológicas onde busca permitir que organizações interajam de forma mutuamente benéfica, compartilhando dados, informações e conhecimentos entre si e seus sistemas garantindo ao mesmo tempo, a segurança dessas interações (WEGNER, 1996) e (NEGRO-CALDUCH et al., 2021).

A interoperabilidade de informações entre instituições levanta preocupações importantes, especialmente em relação à proteção de dados pessoais e à propriedade intelectual. Isso ocorre porque essas informações podem incluir dados sensíveis, como segredos comerciais ou industriais, dados financeiros ou dados de saúde, como prontuários médicos. Quando o titular dos dados pessoais deseja que essas informações sejam acessadas por diferentes instituições, é crucial que o acesso se limite a dados não tratados — ou seja, dados brutos que não foram submetidos a cruzamentos, agregações ou qualquer tratamento pelos sistemas de inteligência artificial das instituições. Essa medida visa proteger tais os segredos, garantindo a segurança, sigilo e a privacidade das informações compartilhadas (SILVA et al., 2021).

Assim, considerou-se um processo dedicado para esta finalidade diante da relevância do assunto, denominado "Padrões de Interoperabilidade", **P22**, cujos padrões são definidos pela ANPD.

Na próxima seção, serão detalhados os processos abordados pela LGPD relacionados às sanções administrativas.

4.3.5 Sanções Administrativas

Nesta seção, são apresentados os mecanismos pelos quais os agentes de tratamento de dados podem ser responsabilizados em razão das infrações cometidas. O conteúdo foi estruturado em cinco processos organizacionais, identificados como P23 a P27, conforme descrito na Tabela 10. Esses processos detalham de forma abrangente as ações relacionadas às infrações eventualmente ocorridas, proporcionando uma visão clara e sistemática sobre as medidas aplicáveis e os procedimentos correspondentes..

Tabela 10: Sanções Administrativas

Cód.	Processo	Descrição
P23	**Comunicação de Não Conformidade**	Identificar, documentar e notificar as infrações cometidas pelos agentes de tratamento de dados;
P24	**Notificação e Aplicação de Sanções**	Este processo envolve a avaliação e cálculo de multas simples e diárias, com base no faturamento da organização e na gravidade da infração
P25	**Publicidade e Transparência de Infrações**	Divulga infrações confirmadas para garantir transparência; Define e publica metodologias para cálculo de multas
P26	**Bloqueio, Eliminação e Suspensão de Dados**	Bloqueia e elimina dados pessoais em caso de infração; Suspende temporariamente o tratamento de dados pessoais
P27	**Proibição de Tratamento de Dados**	Proíbe atividades de tratamento de dados em casos graves

Fonte: Próprio autor.

Iniciando pelo processo **P23**, **Comunicação de Não Conformidade**, este visa identificar, documentar e notificar as infrações, devidamente apuradas e confirmadas a sua ocorrência, pelos agentes de tratamento de dados, indicando um prazo para a adoção de medidas corretivas. Inclui a elaboração de relatórios detalhados e a comunicação formal das não conformidades identificadas. Esses relatórios procuram manter os padrões de proteção de dados, defender os direitos de privacidade e assegurar a responsabilidade nas práticas de processamento de dados (TOLFO; KAPPES; GOULART, 2023)

Processo sobre **Notificação e Aplicação de Sanções**, **P24**, este processo envolve a avaliação e cálculo de multas simples e diárias, com base no faturamento da organização e na gravidade da infração. Inclui etapas para a comunicação formal da multa, bem como o acompanhamento do cumprimento das obrigações impostas.

Espera-se que a ANPD, ao aplicar as sanções administrativas, observe a proporcionalidade e a razoabilidade das punições. O objetivo é penalizar o infrator sem levá-lo à falência ou à interrupção de suas atividades econômicas, a menos que estas violem a LGPD de maneira intolerável para a sociedade em geral (OLIVEIRA, 2021)

A **Publicidade e Transparência de Infrações - P25** foca na comunicação pública das infrações devidamente apuradas e confirmadas, garantindo transparência e responsabilidade. Inclui a preparação de comunicados oficiais e a divulgação das informações necessárias ao público.

A transparência na denúncia de infrações contribui para estabelecer confiança entre organizações e indivíduos, promovendo uma cultura de responsabilidade e conformidade com os regulamentos de proteção de dados (TOLFO; KAPPES; GOULART, 2023)

O processo **P26**, **Bloqueio, Eliminação e Suspensão de Dados**, estabelece os procedimentos para o bloqueio e a eliminação de dados pessoais em caso de infração. Define critérios e métodos para assegurar que os dados sejam bloqueados ou eliminados de forma segura e conforme a legislação.

A princípio, o bloqueio ou eliminação de dados relacionados a uma infração pode parecer uma penalidade simples. No entanto, quando aplicada em larga escala, essa medida pode inviabilizar a atividade fim da organização. Atualmente, vivemos em uma realidade onde a venda de bancos de dados é uma prática comum, com empresas de setores diversos, como farmacêuticas e drogarias, obtendo uma parte significativa de seu faturamento através dessa atividade. Os dados se tornaram um ativo extremamente valioso, e qualquer legislação deve considerar essa dimensão. Assim, o bloqueio ou eliminação de dados em abundância pode desvalorizar consideravelmente o banco de dados de uma empresa. Isso, por sua vez, pode levar a uma recuperação judicial ou até mesmo à falência (MARTIN, 2020).

Por fim, o processo **P27**, **Proibição de Tratamento de Dados Pessoais** procura administrar a imposição de uma proibição a uma pessoa ou entidade, impedindo-a de realizar atividades relacionadas ao tratamento de dados, como sanção decorrente do descumprimento das normas estabelecidas.

Alguns dos processos mencionados acima podem já estar incorporados aos procedimentos administrativos internos de empresas públicas ou privadas. No entanto, separar e destacar esses processos dos demais procedimentos administrativos é fundamental. Isso se deve à necessidade de enfatizar a importância específica dessas etapas no contexto da conformidade com a LGPD.

Adicionalmente, criar um processo organizacional específico para lidar com sanções administrativas é de grande importância, pois isso assegura que as entidades estejam preparadas para enfrentar possíveis violações e cumprir os regulamentos de proteção de dados. Tal abordagem ajuda a estabelecer responsabilidade dentro da organização, promovendo uma cultura de transparência e comprometimento em relação às práticas de tratamento de dados. Dessa forma, a organização não apenas se alinha aos requisitos legais, mas também fortalece sua governança interna e a confiança de seus públicos.

A seguir, na próxima seção, serão correlacionados os processos com os níveis de maturidade apresentados em detalhe na seção 4.4.

4.4 Avaliando processos e níveis de maturidade

Nas seções anteriores, foram apresentados os processos organizacionais associados ao CMMPC (*Capability Maturity Model for Privacy Concern*), elaborados com base nas exigências estabelecidas pela Lei Geral de Proteção dos Dados. Além disso, na seção 4.2, foi discutida a classificação dos processos em diferentes níveis de maturidade. A seguir, combinam-se essas duas perspectivas do modelo, resultando na Tabela 11:

Tabela 11: Matriz de Maturidade

Processos	Níveis de Maturidade				
	Nível 1	Nível 2	Nível 3	Nível 4	Nível 5
Processo 1					
Processo 2					
...					
Processo n					

Fonte: Próprio autor.

A tabela ilustra que os processos previamente definidos podem ser aplicados a diferentes níveis de maturidade, sendo cada um específico para um determinado processo. Importante destacar que cada processo é independente dos demais, não havendo correlação com os processos que o precedem ou sucedem. Dessa forma, cada processo opera de maneira autônoma, permitindo flexibilidade e adaptação conforme o nível de maturidade correspondente.

Além disso, cada tabela corresponde a um grupo de processos de uma área específica, facilitando a organização e gestão das atividades dentro de cada setor. Isso permite uma abordagem mais estruturada e focada, garantindo que os processos, embora não relacionados entre si, sejam adequadamente alinhados com os objetivos e necessidades de cada área.

A Tabela 12 apresenta, por meio de valores hipotéticos, a relação entre os processos e seus respectivos níveis de maturidade.

Tabela 12: Matriz de Maturidade – Exemplo

Processos	Níveis de Maturidade				
	Nível 1	Nível 2	Nível 3	Nível 4	Nível 5
P01	X				
P02			X		
P03		X			

Fonte: Próprio autor.

No exemplo acima, observa-se que o processo **P01** de **Consentimento de Dados ao Titular** está em seu estágio inicial de maturidade, classificado no nível 1. Já o processo **P02** de **Revogação do Consentimento de Dados ao Titular** encontra-se em um estágio mais avançado, no nível 3. Por fim, o processo **P03** de **Acesso aos Dados do Titular** está em um nível intermediário, classificado no nível 2.

Aplicando os critérios estabelecidos para cada nível, obtém-se uma matriz de maturidade. A partir dessa matriz, é possível derivar diversas perspectivas, incluindo uma visão de valor unitário, condensada em um índice de maturidade, e uma visão espacial, representada por um gráfico que serão apresentados a seguir.

4.4.1 Indicador de Conformidade

A fim de trazer mais clareza e uma visão mais objetiva, pensou-se em aplicar uma forma de quantificar toda a aplicação do CMM-PC. A quantificação permite uma avaliação objetiva dos processos organizacionais, fornecendo métricas claras e dados concretos. Isso facilita a identificação de pontos fortes e fracos, possibilitando um diagnóstico preciso do estado atual dos processos. Além disso, a quantificação permite estabelecer padrões de desempenho e benchmarks. Esses padrões servem como referência para comparações internas e externas, ajudando a organização a entender sua posição relativa no mercado e identificar oportunidades de melhoria.

Cálculo do Indicador

Para quantificar a avaliação geral de uma organização, foi desenvolvido um método quantitativo. Os processos descritos nas seções anteriores resultaram de uma análise detalhada da legislação, da qual foram extraídos os itens que exigiam ações específicas. Esses itens foram então mapeados em processos organizacionais. Após o mapeamento, os processos foram agrupados em temas correlatos, resultando em cinco grupos principais. Como mencionado na seção Níveis de maturidade do modelo (4.2), cada processo organizacional pode alcançar até cinco níveis de maturidade, sendo que, quanto maior o nível de

maturidade, mais a organização demonstra maturidade em seus processos organizacionais. Todos os processos são igualmente importantes.

Para avaliar todo o modelo do CMMPC, foi adotada uma abordagem baseada em pontuação. O modelo é composto por cinco grupos de processos organizacionais, cada um com igual importância. Assim, a pontuação total é distribuída igualmente entre esses grupos.

Cada processo dentro desses grupos pode alcançar até o 5º nível de maturidade. Portanto, as pontuações variam de 1 (menos maduro) a 5 (mais maduro), refletindo o grau de maturidade do processo.

A pontuação de cada grupo é a soma das pontuações dos processos dentro desse grupo. Se um grupo possui n processos, e cada processo p_i está em um nível de maturidade m_i, então a pontuação do grupo G é dada por:

$$\text{Grupo} = \sum_{i=1}^{n} m_i$$

Semelhante à pontuação por grupo, a pontuação total da organização seria a soma das pontuações dos 5 grupos:

$$\text{Pontuação Total} = \sum_{j=1}^{5} G_j$$

onde G_j é a pontuação do grupo j.

Por fim, a maturidade total em valores percentuais ou indicador de maturidade é calculado da seguinte forma:

$$\text{Maturidade Percentual} = \left(\frac{\text{Pontuação Total}}{\text{Pontuação Máxima}} \right) \times 100$$

A pontuação máxima é o somatório de todos os processos aplicáveis na avaliação da organização, multiplicado pelo valor máximo de maturidade, que é 5 (cinco). Em algumas organizações, determinados tipos de tratamento de dados podem não ser considerados. Nesses casos, esses grupos de processos não serão incluídos no cálculo da pontuação máxima. Por exemplo, em uma organização que não possui relação com empresas ou instituições internacionais, o grupo referente ao tratamento de dados internacionais não será considerado no cálculo do total máximo.

Exemplo do Indicador de Maturidade

O processo completo será detalhado na seção 5, no entanto, para elucidar melhor

o cálculo do indicador e, com base nos dados mencionados anteriormente, a Tabela 13 ilustra como se pode obter os seguintes valores como resultado de uma análise para um grupo específico, como o de Tratamento de Dados Pessoais, que possui três processos:

Tabela 13: Exemplo de pontuação em grupo de processos

Processo	Nível de Maturidade
P01	3
P02	4
P03	2
Total	9

Fonte: Próprio autor.

Considerando que os processos do grupo de Tratamento de Dados Pessoais obtenham as pontuações de 3, 4 e 2, o valor total deste grupo será a soma dos níveis de maturidade, resultando em um total de 9 pontos. Semelhante à pontuação por grupo, a pontuação geral da organização seria a soma das pontuações dos 5 grupos:

$$\text{Total} = \sum_{j=1}^{5} G_j$$

onde G_j é a pontuação do grupo j.

Após calcular a pontuação de cada processo e cada grupo, somam-se os valores de todos os grupos de nosso exemplo fictício, conforme a Tabela 14:

Tabela 14: Exemplo de pontuação em todos os grupos

Grupos	Processos	Níveis	Valor
Grupo 1	7 Processos	1, 3, 4, 2, 5, 2, 1	18
Grupo 2	5 Processos	2, 4, 3	9
Grupo 3	1 Processos	3, 4, 2, 5	14
Grupo 4	9 Processos	1, 2, 1, 2, 3, 2, 1, 2, 2	16
Grupo 5	5 Processos	2, 2, 3, 2,1	14
Total			71

Fonte: Próprio autor.

No exemplo acima, a instituição avaliada atingiu uma pontuação de 71. Para calcular o indicador de maturidade geral, é necessário calcular qual seria o máximo de

pontos possíveis. A fórmula para calcular a pontuação máxima possível é:

$$\text{Pontuação Máxima} = 5 \times \left(\sum_{i=1}^{G} n_i \right)$$

onde:

- 5 representa o nível máximo de maturidade
- G é o número total de grupos (neste caso, 5),
- n_i é o número de processos no grupo i.

Por fim, a maturidade total em valores percentuais é calculado da seguinte forma:

$$\text{Maturidade Percentual} = \left(\frac{\text{Pontuação Total}}{\text{Pontuação Máxima}} \right) \times 100$$

Em nosso exemplo, temos

$$\text{Maturidade Percentual} = \left(\frac{71}{140} \right) \times 100$$

logo:

$$\text{Maturidade Percentual} = 51,70\%$$

Assim, por essa avaliação fictícia, a organização obteve um índice de pouco mais de 50% de conformidade com a LGPD. Será apresentada a seguir, uma representação gráfica da avaliação dos processos e de seus níveis.

A seguir, será apresentada uma representação gráfica que ilustra a avaliação dos processos e seus respectivos níveis.

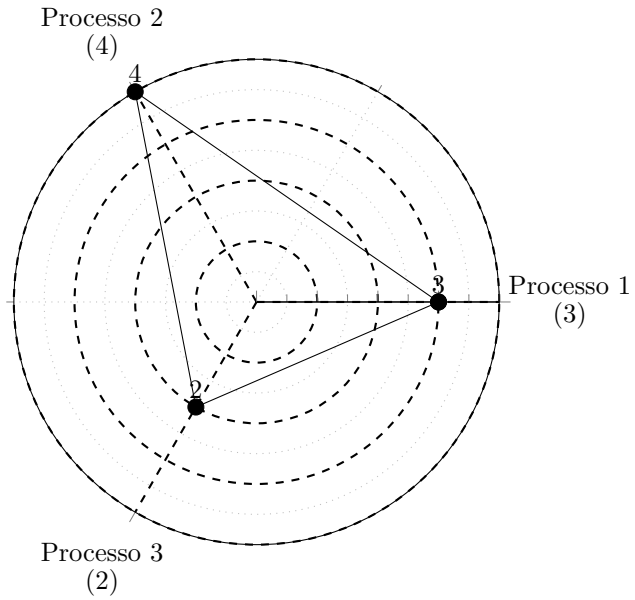
4.4.2 Análise Gráfica do Grupo de Processos

Além da análise numérica, é possível obter uma visão geral, gráfica, da maturidade da organização ou mais específica, por grupo de processos, por meio de gráfico de radar. Um gráfico de radar, também conhecido como gráfico de aranha ou gráfico de teia, é uma ferramenta visual que permite a representação de múltiplas variáveis em um único gráfico.

Neste tipo de gráfico, cada variável é representada por um eixo que se estende a partir de um ponto central, formando um formato de estrela ou teia. A pontuação de cada variável é então plotada ao longo desses eixos e conectada, formando uma área poligonal.

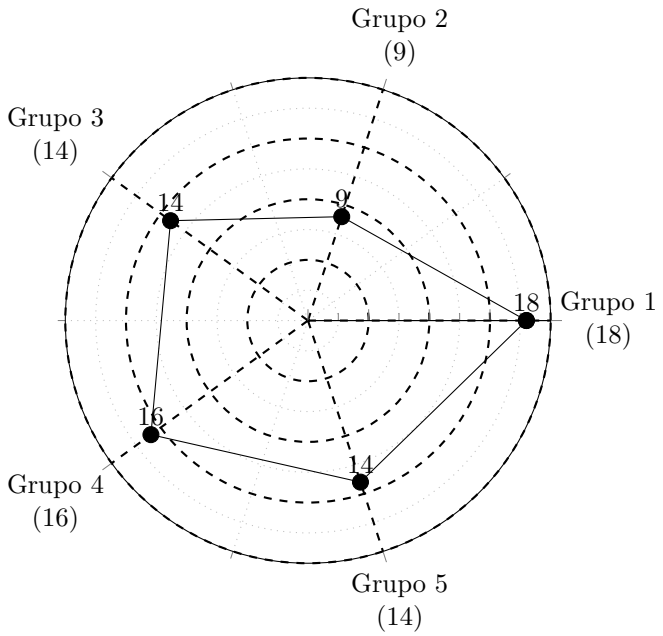
Neste contexto do CMMPC, quanto mais próximo o valor estiver do centro do gráfico, menor será a maturidade da organização ou do grupo de processos. Por outro lado, valores mais afastados do centro indicam uma maior maturidade. Esse formato facilita a comparação visual de diferentes áreas e a identificação rápida de pontos fortes e áreas que necessitam de melhoria. Aplicando ao modelo, tanto pode-se ter uma representação por processo como na figura 2 como também pode-se ter uma visão geral, contendo todos os grupos de processo, como exemplificado na figura 3.

Figura 2: Representação por grupo de processos



Fonte: Próprio autor, 2024.

Figura 3: Representação com todos os grupos



Fonte: Próprio autor, 2024.

4.5 Exemplo de aplicação do modelo CMMPC

Nesta seção será apresentada uma aplicação do modelo CMMPC com dados fictícios. Inicialmente, será caracterizada a organização, na seção de modo a contextualizar a avaliação, descrevendo seu porte, setor de atuação e principais atividades.

Em seguida, serão detalhadas os grupos de processos a serem aplicados modelo CMMPC. Para cada um desses grupos de processos, será realizada a avaliação conforme os critérios definidos em cada nível de maturidade. Por fim, serão discutidos os resultados obtidos, com a apresentação do nível de maturidade diagnosticado para cada processo, indicador e gráfico, como também o nível geral para a organização na totalidade. Espera-se que este exemplo ilustre de forma prática a utilização do modelo proposto, demonstrando como poderá auxiliar as organizações no amadurecimento dos processos em busca da adequação à LGPD.

4.5.1 A Organização

A organização avaliada será uma plataforma de e-commerce especializada produtos esportivos. A empresa atua em todo território nacional e vende produtos e acessórios para os mais diversos esportes.

Para efetuar as compras, a empresa solicita que os usuários realizem um cadastro, fornecendo informações como nome completo, endereço, data de nascimento e, de forma

opcional, dados de cartão de crédito caso o usuário deseje utilizar este meio como forma de pagamento. A empresa também oferece outras opções de pagamento, como boleto bancário, transferência e carteiras digitais.

4.5.2 Processos avaliados

Serão avaliados os grupos de processos de Tratamento de Dados Pessoais, detalhados na seção 4.3.1, bem como os processos de Governança e Segurança da informação, retratado na seção 4.3.4

Porém, antes de aplicar os processos, será explicado na seção 4.5.3 o método para se avaliar a maturidade.

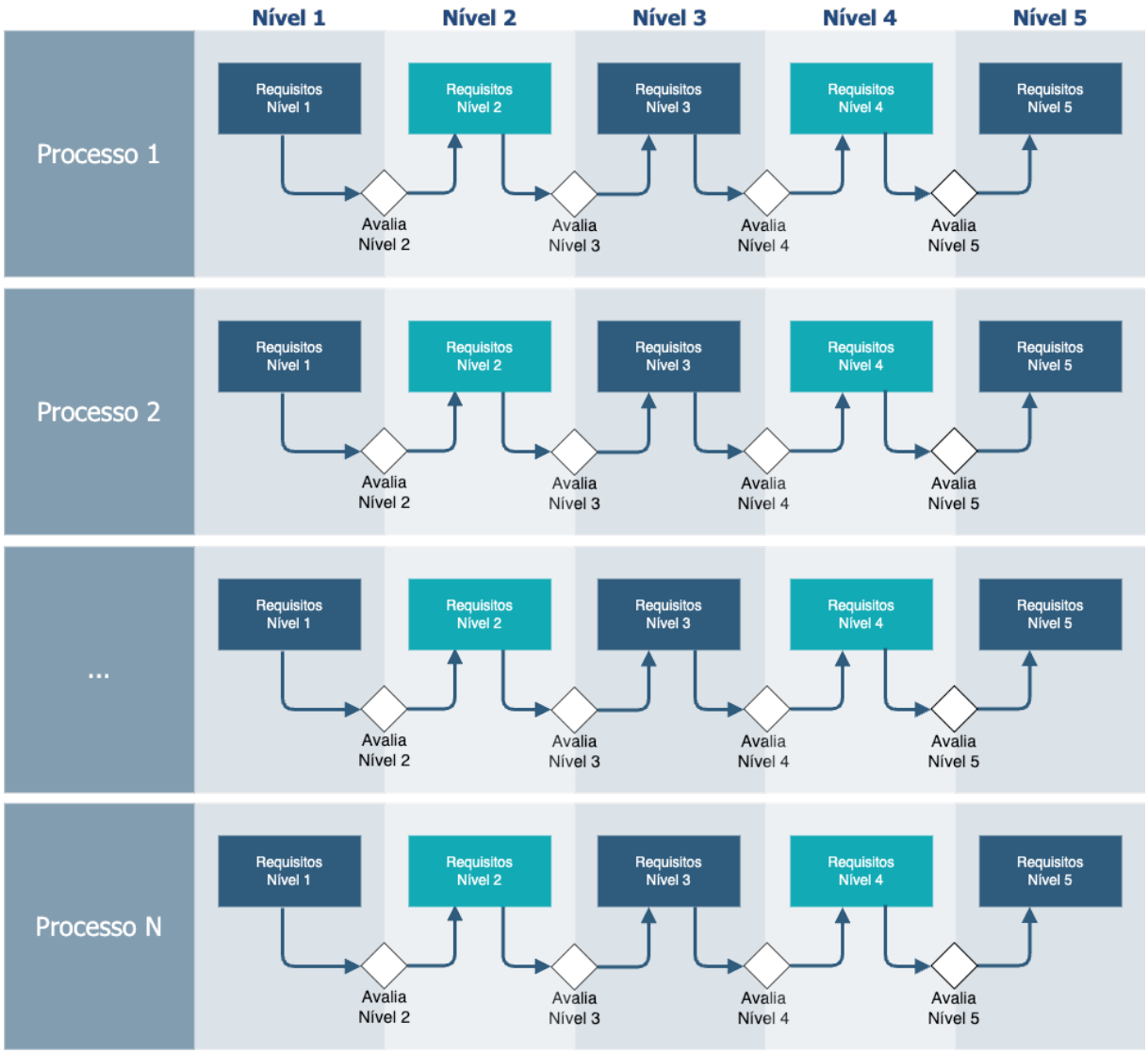
4.5.3 Método para Aplicação dos Níveis de Maturidade

Para determinar o nível de maturidade de um processo qualquer, o método de avaliação segue as seguintes etapas: considerando um processo n, inicia-se a análise pelos requisitos necessários para atender ao nível 1, conforme descrito na Seção 4.2. Caso os requisitos desse nível sejam cumpridos, procede-se com a avaliação do nível seguinte. Se o processo também atender aos requisitos do próximo nível, avança-se para o nível subsequente.

No entanto, se o processo não atender aos requisitos do nível 1, ele será automaticamente classificado como fora dos padrões de maturidade e a avaliação para esse processo é encerrada. Nesse caso, passa-se à análise do próximo processo. Esse procedimento deve ser repetido para todos os grupos de processos ou para um processo específico que se deseje avaliar.

A figura 4, resume a aplicação dos processos com os níveis de maturidade.

Figura 4: Aplicação dos níveis de maturidade



Fonte: Próprio autor, 2024.

A seguir será dado um exemplo de como aplicar este método em um processo.

4.5.4 Exemplificando a aplicação

Nesta seção, será detalhado o processo de aplicação dos níveis de maturidade em diferentes processos. Para ilustrar, serão avaliados os processos de tratamento de dados, abrangendo do **P01** ao **P07**, visando validar a conformidade da organização nesses aspectos.

Para cada processo deste grupo, foi analisado o nível de maturidade correspondente. Tomemos como exemplo o primeiro processo, P01 – Consentimento de Dados ao Titular. O objetivo deste processo é formalizar o consentimento de uso de dados pessoais

do titular dos dados.

Para determinar o nível em que o processo se encontra, é necessário iniciar a avaliação a partir do primeiro nível. A primeira verificação a ser realizada é: a organização executa esta atividade? Ela solicita o consentimento do titular para o uso de seus dados?

As opções de resposta são as seguintes:

1. Não se aplica. Esta atividade não faz parte das atividades da empresa;
2. Não, a empresa não realiza esta atividade, mas deveria;
3. Sim, a empresa realiza esta atividade;

Se o processo em questão não estiver inserido nas atividades operacionais da empresa, ele será desconsiderado e não será incluído no cálculo geral do índice de conformidade, o qual será detalhado posteriormente. Nesse caso, a análise seguirá para o próximo processo relevante, a qual é o caso da primeira opção das respostas acima. Um exemplo desse tipo de situação é o processo de transferência internacional de dados. Caso a empresa não realize transações internacionais, esse processo torna-se irrelevante e, portanto, não será aplicado.

Caso a resposta seja negativa, o processo é desconsiderado e recebe pontuação 0 (zero), uma vez que não se enquadra em nenhum nível de maturidade.

Se a resposta for positiva, indicando que a empresa realiza essa atividade, a análise avança para identificar o nível de maturidade em que o processo se encontra. Inicialmente, é necessário verificar se os requisitos do primeiro nível são atendidos, tais como: como essa atividade é conduzida? As práticas são executadas de maneira assistemática, sem uma estrutura formal definida, sendo sustentadas apenas por procedimentos informais? Caso essas condições sejam atendidas, conclui-se que o processo se encontra no primeiro nível de maturidade. No entanto, é necessário prosseguir com a avaliação para verificar se o processo atende aos critérios do próximo nível, a fim de determinar se ele pode ser classificado em um nível superior.

Assim, após verificar os requisitos do nível 2 (dois), denominado nível estruturado, questiona-se: há uma gestão mínima dos processos? As ações são devidamente planejadas? Algumas práticas foram formalizadas e documentadas? Se essas condições forem atendidas, o processo será classificado nesse nível, refletindo uma maior maturidade e organização. Entretanto, é fundamental avançar para a análise do próximo nível, o nível 3 (três), a fim de avaliar se o processo pode ser elevado a um nível superior, levando a uma avaliação mais precisa de sua maturidade. Caso o processo não atenda aos critérios do nível seguinte, ele permanecerá classificado no nível anterior, encerrando-se a análise

desse processo. Em seguida, o próximo processo será avaliado, repetindo-se a mesma metodologia.

Após a avaliação de todos os processos do grupo de tratamento de dados pessoais, pode-se construir a Tabela 15, que também é denominada de matriz de maturidade, pois relaciona os processos juntamente com os níveis de maturidade.

Tabela 15: Matriz de Maturidade

Processos	Níveis de Maturidade				
	Nível 1	Nível 2	Nível 3	Nível 4	Nível 5
P01		X			
P02	X				
P03			X		
P04					X
P05		X			
P06	X				
P07				X	

Fonte: Próprio autor.

Ao final da avaliação, tem-se como resultado a tabela ilustrada, onde demonstra a relação entre os processos avaliados e seus respectivos níveis de maturidade, compondo uma matriz de maturidade que poderá proporcionar uma melhor visualização da análise do desempenho organizacional. Ressalta-se que os valores apresentados foram preenchidos de maneira aleatória, com o propósito exclusivo de exemplificar o processo, não refletindo nenhuma avaliação real.

4.6 Considerações Finais

Apresentamos neste capítulo a proposta do modelo de maturidade de processo adequado para avaliar a conformidade de organizações com a Lei Geral de Proteção dos Dados (LGPD). Inspirados pelos fundamentos do Modelo de Maturidade de Capacidade (CMMI), criou-se o CMMPC - Modelo de Maturidade e Capacidade para Privacidade, voltado especificamente para abordar os desafios relacionados à proteção de dados nas organizações.

O principal objetivo do CMMPC é de fornecer um instrumento sistemático e estruturado que possibilite às organizações avaliar e aprimorar continuamente suas práticas de proteção de dados. A estrutura do modelo baseou-se em níveis de maturidade que refletiam a evolução das capacidades de privacidade da organização, desde a conformidade inicial até sua excelência em proteção de dados.

Com a avaliação dos processos, chega-se a uma matriz de maturidade, que relaciona cada processo com seu respectivo nível de conformidade avaliado. Além disso, propusemos uma representação quantitativa dessa avaliação mediante um índice, proporcionando um valor único e uniforme que reflete a situação global de conformidade da organização. Este índice de conformidade sintetiza de forma clara e objetiva a análise dos processos, facilitando a compreensão e o monitoramento contínuo da situação de conformidade com a LGPD.

Para complementar essa análise, também foi proposta a utilização do gráfico radar, oferecendo outra visão da organização na totalidade. Este gráfico permite visualizar de maneira intuitiva e comparativa o desempenho de cada processo, destacando pontos fortes e áreas que necessitam de melhorias. Assim, a combinação da matriz de maturidade, o índice de conformidade e o gráfico radar fornecem uma visão abrangente e detalhada do estado de conformidade da organização.

É importante que todos dentro da organização entendam os processos e procedimentos em caso de ocorrência de infrações. A LGPD prevê uma série de medidas que podem ser tomadas, como advertências, multas simples ou diárias, publicização da infração, bloqueio dos dados pessoais a que se refere a infração até a sua regularização, eliminação dos dados pessoais a que se refere a infração, suspensão parcial do funcionamento do banco de dados e até mesmo a proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados

Na próxima seção, será apresentado o estudo de caso conduzido em três organizações de naturezas distintas. Foram selecionados dois grupos de processos relevantes e diferentes para possibilitar a comparação da versatilidade e aplicabilidade do modelo de processo.

5 ESTUDO DE CASO

Nesta seção, apresenta-se os resultados da aplicação de uma avaliação inicial do modelo CMMPC em três organizações distintas: uma instituição federal de ensino médio e superior, um hospital privado de médio porte e uma organização vinculada ao Poder Judiciário.

O objetivo deste estudo é avaliar a aplicabilidade do modelo CMMPC, apresentado anteriormente no capítulo 4, em diferentes organizações. A diversidade das organizações selecionadas visa demonstrar a eficácia e versatilidade do modelo, bem como a facilidade de sua aplicação.

Foram selecionados os grupos, dentro do modelo, com maior quantidade de processos, visando produzir uma maior quantidade de conteúdo para o estudo de caso e a análise do modelo CMMPC. Dessa forma, optou-se pelos grupos que tratam de dados pessoais, governança e segurança da informação.

A análise deste estudo de caso foi realizada com base em documentos públicos da instituição. Como a Lei de Acesso à Informação determina que os órgãos e entidades públicas devem, independentemente de solicitações, divulgar em seus sites da internet informações de interesse coletivo ou geral, como estrutura organizacional, legislações pertinentes, dados sobre programas, ações, projetos e obras, entre outras (BRASIL, 2011). Além da própria LGPD que destaca o princípio da transparência e publicização em vários pontos da lei, exigindo que os agentes de tratamento de dados forneçam informações claras, precisas e facilmente acessíveis sobre o tratamento de dados pessoais, garantindo que os titulares compreendam como seus dados estão sendo utilizados (BRASIL, 2018). Entende-se que a ausência de informações públicas pode indicar que tais processos não existem, não foram formalizados ou não estão sendo gerenciados.

Uma vez escolhidas as organizações e os processos, iniciou-se a etapa de coleta de informações. Em todas as organizações, o método utilizado foi o mesmo: inicialmente, analisou-se a página principal dos respectivos sites para verificar a existência de seções dedicadas à proteção de dados, segurança e privacidade. Caso não houvesse uma seção específica para a LGPD, pesquisou-se no site com o Google[7]. Para isso, foram utilizadas palavras-chave específicas como: LGPD, segurança, proteção de dados, privacidade, política, POSIN [8], POSIC [9], política de privacidade, política de segurança, DPO e encarregado de dados.

O resultado da análise e compilação das informações foi a criação de uma matriz de maturidade. A partir dessa matriz, derivaram-se duas outras representações: um

[7]https://google.com
[8]Política de Segurança da Informação
[9]Política de Segurança da Informação e Comunicação

indicador de maturidade e um gráfico radar, que oferece uma visão espacial do grupo de processos. Para cada processo na matriz, foi indicado o nível de maturidade em que se encontra ou sua ausência, bem como uma indicação caso aquele processo não seja aplicável na organização, conforme a legenda a seguir:

- "**X**": Possui o nível indicado;
- " **-** ": Não possui o nível indicado;
- "**N.A.**": Não aplicável;

Em seguida, serão apresentadas as análises das três organizações na seguinte ordem: primeiro, a instituição de ensino; depois, o hospital; e, por fim, a organização vinculada ao Poder Judiciário.

5.1 Instituição de Ensino

A organização escolhida para esta seção do estudo de caso foi uma instituição de ensino federal que oferece uma ampla variedade de cursos nos níveis médio, superior e além de cursos de pós-graduação.

A instituição analisada possui diversos sites em sua estrutura, incluindo um dedicado ao repositório de produção acadêmica, como os Trabalhos de Conclusão de Curso (TCC), artigos científicos e etc. Além disso, há um site específico para ensino à distância, outro voltado para processos seletivos de alunos e mais um para processos seletivos de servidores. Então, análise foi focada no site principal da instituição, aquele que possui as informações gerais da organização.

A organização possui três eixos de atuação: ensino, pesquisa e extensão, com projetos voltados para a comunidade. Dado o amplo escopo dessas atividades, este estudo de caso se concentrou especificamente no eixo de ensino.

5.1.1 Tratamento de Dados de Pessoais

Este é o maior grupo de processos do modelo CMMPC, sendo constituído por 7 (sete) processos organizados em alguns subgrupos: Tratamento de Dados Pessoais, Tratamento de Dados Pessoais Sensíveis, Tratamento de Dados Pessoais de Crianças e Adolescentes e Tratamento de Dados Pessoais pelo Poder Público.

Os processos analisados aqui se concentraram nos meios digitais. Para uma análise mais abrangente e detalhada, seria necessário adotar uma abordagem diferente, utilizando questionários nos setores-chave de atendimento ao público, a fim de averiguar todo o

trâmite de dados provenientes de meios físicos. Supõe-se que algumas informações de pessoas físicas ou jurídicas externas à organização, que não possuem acesso aos sistemas internos, utilizem meios físicos para interagir com a organização.

São procedimentos de caráter transversal em toda a organização, um processo maior onde se faça claro para os usuários em questão todos os procedimentos disponíveis da organização no tangente à proteção de dados pessoais. Seria uma formalização, uma declaração que ali naquela organização há um pensamento e uma preocupação com os dados por eles mantidos.

As informações sobre o tratamento de dados pessoais foram extraídas da Política de Privacidade e da Política de Proteção de Dados Pessoais, ambas disponíveis publicamente no site da organização. Esses documentos são políticas, e não normas ou procedimentos específicos, resultando em informações mais gerais que não fornecem detalhes sobre a execução dos procedimentos. Além disso, não há informações sobre planejamento, gestão ou mensuração dos processos, o que impede a inferência de um nível mais elevado de maturidade dos processos.

Processos	Níveis de Maturidade				
	Nível 1	Nível 2	Nível 3	Nível 4	Nível 5
P01	X				
P02	X				
P03	X				

Tabela 16: Instituição de Ensino – Tratamento de Dados Pessoais

Na Política de Proteção de Dados Pessoais foram encontradas referências ao tratamento de dados pessoais do titular, abrangendo os processos **P01** (Consentimento de Dados ao Titular), **P02** (Revogação do Consentimento de Dados ao Titular) e **P03** (Acesso aos Dados do Titular). Em relação aos procedimentos específicos para consentimento, revogação ou acesso dos dados do titular, a política apenas menciona que essas solicitações devem ser direcionadas ao encarregado de dados, sem fornecer detalhes adicionais.

Tratamento de Dados Pessoais Sensíveis

Tabela 17: Instituição de Ensino – Tratamento de Dados Pessoais Sensíveis

Processos	Níveis de Maturidade				
	Nível 1	Nível 2	Nível 3	Nível 4	Nível 5
P04	X				

Fonte: Próprio autor.

Foram identificadas evidências apenas em estágio inicial. Nos documentos analisados, há um reconhecimento de que o tratamento de dados sensíveis representa um maior risco ao titular. Por esse motivo, a organização assume o compromisso de adotar medidas de resguardo e cuidados especiais nas operações que envolvem esse procedimento.

Tratamento de Dados de Crianças e Adolescentes

Devido à condição de vulnerabilidade e necessidade de proteção especial para crianças e adolescentes, a Lei Geral de Proteção de Dados (LGPD) estabelece normas específicas para o tratamento de seus dados pessoais. A legislação reconhece que menores de idade estão em uma posição particularmente sensível, exigindo medidas de segurança mais rigorosas para salvaguardar suas informações. Nesse contexto, os dados de crianças e adolescentes são classificados como dados especiais, o que demanda uma proteção aprimorada e uma atenção redobrada por parte de todas as entidades envolvidas no seu tratamento (PINHEIRO, 2020).

A organização atende alunos menores de idade e oferece, além do ensino, serviços de atendimento médico a esses alunos. Esses dados, por si só, já demandam maior atenção, cuidado e sigilo. A instituição afirma que os dados pessoais de crianças e adolescentes serão tratados com o mesmo nível de cuidado exigido para dados pessoais sensíveis, seguindo as disposições do Art. 14 da LGPD e outras normas específicas aplicáveis. Ressalta também a imprescindibilidade de obter consentimento específico e destacado de pelo menos um dos pais ou do responsável.

Contudo, a conformidade com as regulamentações de proteção de dados revelou-se deficiente, especialmente no que diz respeito aos alunos menores de idade. A ausência de informações detalhadas sobre como os dados desse grupo serão tratados demonstra que os processos ainda se encontram em estágios iniciais de maturidade. A Tabela 18 abaixo apresenta o resultado da avaliação:

Tabela 18: Instituição de Ensino – Tratamento de Dados Pessoais

Processos	Níveis de Maturidade				
	Nível 1	Nível 2	Nível 3	Nível 4	Nível 5
P05	X				
P06	–				

Fonte: Próprio autor.

Foi encontrada evidência apenas no processo **P05** (Consentimento para Tratamento de Dados Pessoais Sensíveis), que abrange o consentimento de uso de dados de

crianças e adolescentes. No entanto, não foram encontradas maiores menções quanto ao tratamento específico e aos tipos de dados coletados.

Tratamento de Dados Pessoais pelo Poder Público

O tratamento de dados pessoais pelo Poder Público envolve ações de natureza transversal à organização pública, objetivando assegurar a celeridade e a eficiência necessárias para a implementação de políticas e a prestação de serviços públicos. Esse processo deve respeitar os direitos à proteção de dados pessoais e à privacidade, garantindo um equilíbrio entre a eficácia das ações e a proteção dos direitos dos cidadãos. A Tabela 19 demonstra o resultado desta análise:

Tabela 19: Instituição de Ensino – Tratamento de Dados Pessoais pelo Poder Público

Processos	Níveis de Maturidade				
	Nível 1	Nível 2	Nível 3	Nível 4	Nível 5
P07		X			

Fonte: Próprio autor.

Foram encontradas evidências da existência de um Comitê Gestor de Dados Pessoais, que tem entre suas atribuições a avaliação dos procedimentos de tratamento e proteção de dados pessoais. Além disso, o comitê é responsável por propor estratégias e metas conforme a LGPD, assegurando que as práticas da organização estejam alinhadas com os requisitos legais de proteção de dados. Assim, considera-se que haja um mínimo de gerência dos processos, alcançando um nível 2 (dois) de maturidade.

5.1.2 Tratamento Governança e Segurança da Informação

Na segunda avaliação, focada no grupo de governança e segurança da informação, observou-se um nível bem baixo de maturidade dos processos, com alguns inexistentes ainda. A Tabela 20 demonstra este cenário:

Tabela 20: Instituição de Ensino – Governança e Segurança da Informação

Processos	Níveis de Maturidade				
	Nível 1	Nível 2	Nível 3	Nível 4	Nível 5
P14		X			
P15	X				
P16	–				
P17	–				
P18	–				
P19	–				
P20	–				
P21	–				
P22	–				

Fonte: Próprio autor.

Durante a avaliação, foram identificados elementos específicos de conformidade nos processos **P14** e **P15**. No processo **P14**, destacou-se a atuação eficaz de um comitê de segurança da informação. Já no processo **P15**, constatou-se que documentos, como normas e procedimentos, foram disponibilizados no portal institucional. A Política de Segurança da Informação também apresentou informações sobre vigência e revisão, sugerindo a existência de um gerenciamento ativo desse processo. Com base nesses achados, foi recomendada a classificação no nível 2 para este processo. Nos demais processos, **P16**, **P17**, **P18**, **P19** e **P20**, não foram observados indícios de implementação ou existência. O treinamento e conscientização (**P16**) é um dos principais agentes para promover a mudança cultural interna nas organizações, conforme (CRESPO, 2021), e sua ausência poderá causar atraso no processo de conformidade com a lei. As auditorias internas (**P17**) auxiliam a demonstrar a efetividade do programa de segurança e privacidade. A falta de procedimentos para registro de ações sobre o tratamento de dados (**P18**) e plano de resposta a incidentes (**P19**), por exemplo, compromete a capacidade da instituição de registrar e notificar incidentes a órgãos reguladores e monitoradores, como a Autoridade Nacional de Proteção de Dados (ANPD). Ainda, o relatório de impacto à proteção de dados pessoais (**P20**) é um documento relevante, pois contém a descrição dos processos que podem representar riscos às liberdades civis e aos direitos fundamentais, podendo ser solicitado pela ANPD a qualquer momento. A ausência desses processos pode comprometer a capacidade da organização de alcançar e manter a conformidade com a legislação, aumentando o risco de violações e sanções regulatórias.

5.1.3 Indicador de Maturidade

Nas seções anteriores, foram analisados dois grupos distintos: tratamento de dados pessoais e governança e segurança da informação. A seguir, apresentaremos o indicador de maturidade, que avalia o estágio de desenvolvimento e a eficácia dos processos. Nas Tabelas 21 e 22 relembram os valores dos processos para demonstrar o cálculo do indicador de maturidade.

Para os processos do grupo de tratamento de dados pessoais, teremos:

Tabela 21: Instituição de Ensino - Pontuação Processos Tratamento Dados Pessoais

Processo	Nível
P01	1
P02	1
P03	1
P04	1
P05	1
P06	0
P07	2
Total	7

Fonte: Próprio autor.

Para o segundo grupo de processos avaliados, governança e segurança, teremos:

Tabela 22: Instituição de Ensino - Pontuação Processos Governança e Segurança

Processo	Nível
P14	2
P15	1
P16	0
P17	0
P18	0
P19	0
P20	0
P21	0
P22	0
Total	3

Fonte: Próprio autor.

Os processos P06 e P16 a P22 não receberam pontuação e, por essa razão, foram considerados como zero. Para cálculo do indicador iremos considerar apenas os processos avaliados, pois a multiplicação por zero resultará em zero. Assim, conforme a fórmula abaixo teremos:

$$\text{Total} = \sum_{j=1}^{2} G_j$$

logo

$$\text{Total} = 10$$

Considerando que foram avaliados 16 processos (7 processos do grupo de Tratamento de Dados e 9 processos do grupo de governança e segurança da informação), a pontuação máxima desta estudo de caso é:

$$\text{Pontuação Máxima} = (7 + 9) \times 5$$

então,

$$\text{Pontuação Máxima} = 80$$

Calculando o indicador de maturidade em valores percentuais teremos:

$$\text{Indicador} = \left(\frac{\text{Pontuação Total}}{\text{Pontuação Máxima}} \right) \times 100$$

$$\text{Indicador} = \left(\frac{10}{80} \right) \times 100$$

logo,

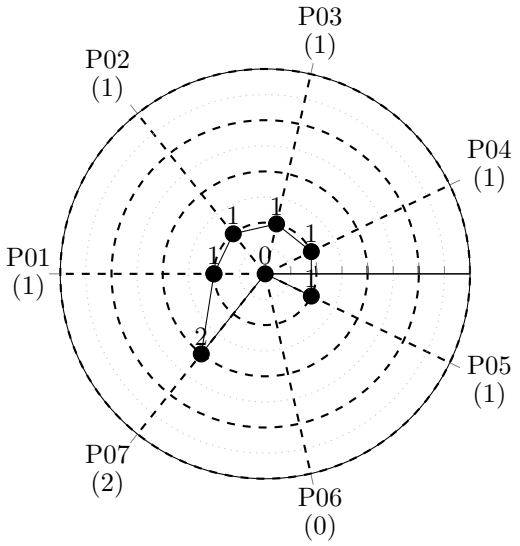
$$\text{Indicador} = 12{,}5\%$$

Com base nos processos avaliados, a organização alcançou um indicador de maturidade de 12,5%. É importante ressaltar que esta é uma avaliação parcial, pois ainda há processos que não foram avaliados. Somente após a avaliação completa, será possível obter uma visão mais abrangente.

Gráfico Radar de Maturidade

Aqui estão as representações visuais correspondentes aos indicadores discutidos na seção anterior.

Figura 5: Avaliação instituição de ensino – Tratamento de Dados Pessoais

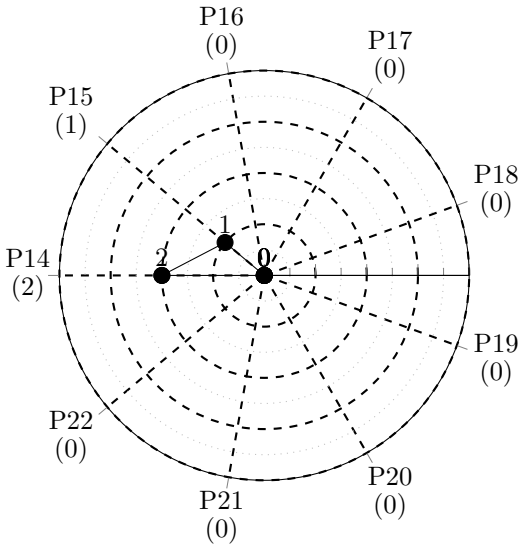


Fonte: Próprio autor, 2024.

O gráfico apresentando na figura 5 demonstra quem quanto mais próximo da área interna do círculo, mais demonstra uma imaturidade da organização quanto aos seus processos.

Abaixo, na figura 6, está a representação visual do grupo de Governança e Segurança da Informação

Figura 6: Avaliação instituição de ensino – Governança e Segurança da Informação



Fonte: Próprio autor, 2024.

O gráfico pode causar uma impressão incomum, pois apresenta apenas três pontos. Contudo, ao analisarmos a tabela de valores de avaliação, notamos que apenas 2 (dois) dos 9 (nove) processos foram avaliados. Os outros 7 (sete) processos receberam a avaliação 0 (zero), o que explica a ausência de pontos no gráfico para esses casos.

5.2 Hospital Privado

Este estudo de caso analisou um hospital privado de médio porte onde, semelhante ao estudo de caso anterior, examinou o portal institucional em busca de informações e evidências sobre as ações voltadas para a privacidade e proteção dos dados pessoais de seus usuários.

Em sua página principal, não há informações sobre a LGPD ou sobre privacidade. Embora não seja uma exigência, disponibilizar essas informações facilitaria para que os usuários do hospital compreendam os procedimentos e tratamentos aplicados aos seus dados.

Utilizando o *Google* como ferramenta de pesquisa e realizando buscas por palavras-chave no site da organização, foi identificada a existência de uma política de segurança da informação integrada a uma política de privacidade. Essa integração resultou na apresentação de informações combinadas e, por vezes, indistintas entre as duas políticas. Desse modo, o referido documento foi estudado visando averiguar quais informações nele contidas indicariam ou poderiam indicar características dos processos do modelo CMMPC.

A seguir, serão elencadas as informações sobre o tratamento de dados pessoais, bem como os aspectos de governança e segurança da informação identificados.

5.2.1 Tratamento de Dados Pessoais

Nesta seção, será avaliado todo o tratamento de dados pessoais. Ao todo, são sete processos, subdivididos em quatro subgrupos, sendo eles: Tratamento de Dados Pessoais, Tratamento de Dados Pessoais Sensíveis, Tratamento de Dados Pessoais de Crianças e Adolescentes e Tratamento de Dados Pessoais pelo Poder Público.

Tratamento de Dados Pessoais

As informações compiladas sobre o tratamento de dados pessoais foram extraídas da política de privacidade, que está disponível publicamente na área do site da organização. A Tabela demonstra o resultado desta avaliação.

Tabela 23: Hospital Privado – Tratamento de Dados Pessoais

Processos	Níveis de Maturidade				
	Nível 1	Nível 2	Nível 3	Nível 4	Nível 5
P01	X				
P02	X				
P03	X				

Fonte: Próprio autor.

Embora não existam procedimentos claramente definidos e específicos para os processos P01 (Consentimento de Dados ao Titular), P02 (Revogação do Consentimento de Dados ao Titular) e P03 (Acesso aos Dados do Titular), há apenas instruções estabelecidas na política, indicando um nível inicial de maturidade.

Tratamento de Dados Pessoais Sensíveis

Nenhuma informação foi registrada neste segmento P04, sendo assim, a Tabela 24 encontra-se totalmente vazia.

Tabela 24: Hospital Privado – Tratamento de Dados Pessoais Sensíveis

Processos	Níveis de Maturidade				
	Nível 1	Nível 2	Nível 3	Nível 4	Nível 5
P04					

Fonte: Próprio autor.

Tratamento de Dados Pessoais de Crianças e Adolescentes

Os processos da Tabela 25, P05 sobre Consentimento para Tratamento de Dados Pessoais Sensíveis e P06 sobre Publicização dos Tipos de Dados Coletados, abordam diretamente dados sensíveis de crianças e adolescentes. O hospital declara que necessitará de autorização de pai ou responsável para o tratamento desses dados. No entanto, não há uma definição clara e específica dos processos, que se enquadram em procedimentos genéricos da organização. Em relação à publicização, a declaração foi bastante genérica, sem especificar quais dados são coletados.

Tabela 25: Hospital Privado – Tratamento de Dados Pessoais de Crianças e Adolescentes

Processos	Níveis de Maturidade				
	Nível 1	Nível 2	Nível 3	Nível 4	Nível 5
P05	X				
P06	X				

Fonte: Próprio autor.

Tratamento de Dados Pessoais pelo Poder Público

Por se tratar de uma organização privada, esta seção não é aplicável. Assim, a Tabela 26 apresenta apenas o valor "N.A."(Não Aplicável).

Tabela 26: Hospital Privado – Tratamento de Dados Pessoais pelo Poder Público

Processos	Níveis de Maturidade				
	Nível 1	Nível 2	Nível 3	Nível 4	Nível 5
P07	N.A.				

Fonte: Próprio autor.

5.2.2 Tratamento Governança e Segurança da Informação

Nesta seção será apresentada, na Tabela 27, a avaliação realizada no grupo de processos sobre governança e segurança da informação.

Tabela 27: Hospital Privado – Avaliação sobre Governança e Segurança da Informação

Processos	Níveis de Maturidade				
	Nível 1	Nível 2	Nível 3	Nível 4	Nível 5
P14	–				
P15	X				
P16	–				
P17	–				
P18	X				
P19	–				
P20	–				
P21	X				
P22	–				

Fonte: Próprio autor.

Pouco foi encontrado sobre governança e segurança da informação. Apenas os processos **P15** (Políticas de Proteção e Privacidade de Dados), **P18** (Operações de tratamento de dados pessoais) e **P21** (Encarregado de Dados Pessoais - DPO) foram identificados. A política foi localizada por meio da pesquisa, mas não há um *link* direto na página inicial do portal institucional. Todas as informações relevantes foram encontradas nesta política.

A política fornece detalhes sobre o tratamento de dados pessoais, incluindo com quem podem ser compartilhados, ressaltando que o consentimento do titular é necessário. Informações de contato do encarregado de dados estão disponíveis, embora a lei exija que tanto o nome quanto a forma de contato sejam publicizados. A política menciona que para alteração, exclusão ou qualquer outra forma de exercício dos direitos do titular, deve-se entrar em contato através do *e-mail* do encarregado de dados.

5.2.3 Indicador de Maturidade

Apresentaremos, nesta seção, o indicador de maturidade para o estudo de caso do hospital privado, que avalia o estágio de desenvolvimento e a eficácia dos processos nesta organização.

No hospital privado, a proteção de dados pessoais é crítica, dado o volume e a sensibilidade das informações dos pacientes. A governança e segurança da informação também desempenham um papel essencial na garantia da confidencialidade, integridade e disponibilidade desses dados. A análise do indicador de maturidade nos permitirá compreender melhor o estágio atual de desenvolvimento desses processos no hospital privado e identificar áreas para melhorias contínuas.

Na Tabela 28, são descritos os processos que compõem o primeiro grupo avaliado, conforme exposto a seguir:

Tabela 28: Hospital Privado - Pontuação Processos Tratamento Dados Pessoais

Processo	Nível
P01	1
P02	1
P03	1
P04	1
P05	1
P06	0
Total	6

Fonte: Próprio autor.

Para o segundo grupo, apresentamos na Tabela 29,os processos avaliados do governança e segurança da informação, teremos:

Tabela 29: Hospital Privado - Pontuação Processos Governança e Segurança

Processo	Nível
P14	0
P15	1
P16	0
P17	0
P18	1
P19	0
P20	0
P21	1
P22	0
Total	3

Fonte: Próprio autor.

O processo P07 não se aplica, pois trata de informações referentes a órgãos públicos, enquanto o estudo de caso analisado envolve um hospital privado. Para o cálculo do indicador, serão considerados apenas os processos avaliados. Assim, o resultado será obtido pelo somatório dos pontos dos dois processos avaliados, conforme demonstrado a seguir:

$$\text{Total} = \sum_{j=1}^{2} G_j$$

logo

$$\text{Total} = 9$$

Considerando que foram avaliados 15 processos (6 processos do grupo de Tratamento de Dados e 9 processos do grupo de governança e segurança da informação), a pontuação máxima deste estudo de caso é:

$$\text{Pontuação Máxima} = (6 + 9) \times 5$$

então,

$$\text{Pontuação Máxima} = 75$$

Calculando o indicador de maturidade em valores percentuais, teremos:

$$\text{Indicador} = \left(\frac{\text{Pontuação Total}}{\text{Pontuação Máxima}} \right) \times 100$$

$$\text{Indicador} = \left(\frac{9}{75} \right) \times 100$$

portanto,

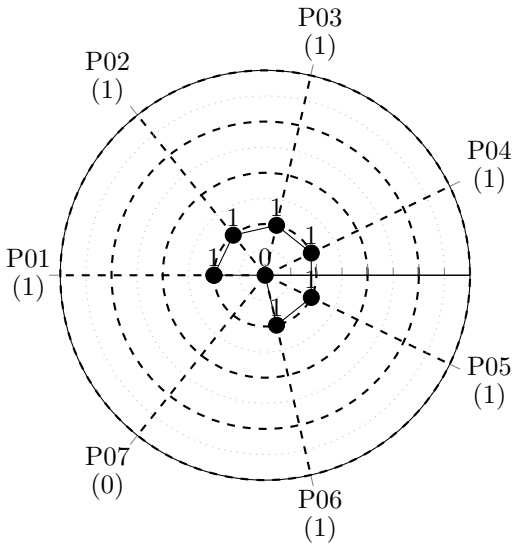
$$\text{Indicador} = 12{,}0\%$$

A avaliação é bastante similar à anterior, com uma diferença de apenas meio ponto percentual, indicando que ambas as organizações estão em níveis de maturidade praticamente iguais. A seguir, serão apresentadas as representações visuais dos indicadores dos grupos avaliados.

Gráfico de Maturidade

Observa-se, pelo gráfico na figura 7, uma concentração dos pontos na região central, indicando um baixo nível de maturidade. A escala deste gráfico varia do centro para a periferia, onde o centro representa menor maturidade e a extremidade, maior maturidade.

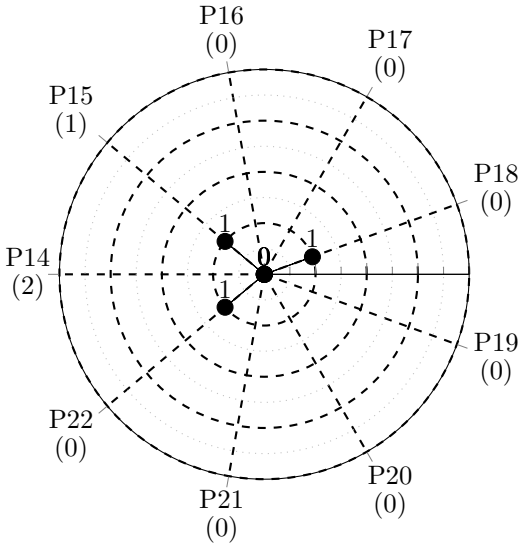
Figura 7: Avaliação Hospital Privado – Tratamento de Dados Pessoais



Fonte: Próprio autor, 2024.

Segue, no gráfico da figura 8, a representação visual do grupo de Governança e Segurança da Informação:

Figura 8: Avaliação Hospital Privado – Governança e Segurança da Informação



Fonte: Próprio autor, 2024.

Nesta avaliação de Governança e Segurança da informação, apresentada na figura 8 observa-se a ausência de uma forma no gráfico, mas devido à quantidade de processos sem atingir o primeiro nível de maturidade. De forma geral este grupo de processos está em um estágio bastante inicial maturidade.

5.3 Órgão ligado ao Poder Judiciário

Nesta seção, foi analisado um órgão ligado ao Poder Judiciário. Semelhante aos estudos de caso anteriores, o portal institucional foi examinado em busca de informações e evidências sobre as ações voltadas para a privacidade e proteção dos dados pessoais dos usuários. Na página inicial do site, não há uma referência direta a documentos e procedimentos relacionados à LGPD; porém, uma seção específica foi localizada como um subitem de um menu.

Seguindo a mesma sequência e estrutura das seções anteriores, apresentaremos a análise sobre o tratamento de dados pessoais, seguida pela análise sobre governança e segurança da informação.

5.3.1 Tratamento de Dados Pessoais

Nesta seção, será avaliado todo o tratamento de dados pessoais. Ao todo, foram identificados sete processos, organizados em quatro subgrupos. Os processos com seus

níveis de maturidade serão apresentados nas Tabelas 30 a 33.

As informações sobre o tratamento de dados pessoais foram compiladas a partir de diversos documentos, incluindo a política de privacidade e um projeto de implementação da LGPD, todos disponíveis publicamente na área do site da organização.

Tabela 30: Órgão Poder Judiciário – Tratamento de Dados Pessoais

Processos	Níveis de Maturidade				
	Nível 1	Nível 2	Nível 3	Nível 4	Nível 5
P01		X			
P02		X			
P03		X			

Fonte: Próprio autor.

Para todos os processos de tratamento de dados pessoais (P01, P02 e P03), foram encontradas evidências de procedimentos para sua execução. No entanto, não foram identificados níveis adicionais de gerenciamento desses processos, permanecendo no nível 2.

Tratamento de Dados Pessoais Sensíveis

Há informações sobre o tratamento de dados sensíveis, mas estas são básicas e não indicam um formalismo ou estrutura robusta que permitisse elevar o processo ao próximo nível de maturidade. Assim, o nível avaliado foi o nível 1.

Tabela 31: Órgão Poder Judiciário – Tratamento de Dados Pessoais de Crianças e Adolescentes

Processos	Níveis de Maturidade				
	Nível 1	Nível 2	Nível 3	Nível 4	Nível 5
P04	X				

Fonte: Próprio autor.

Tratamento de Dados Pessoais de Crianças e Adolescentes

Há uma declaração na política de privacidade informando que os dados de crianças e adolescentes não são coletados. Assim, entende-se que esse grupo não faz parte do leque de usuários da organização, sendo, portanto, considerado como **N.A.** – não aplicável.

Processos	Níveis de Maturidade				
	Nível 1	Nível 2	Nível 3	Nível 4	Nível 5
P05	N.A.				
P06	N.A.				

Tabela 32: Órgão Poder Judiciário – Tratamento de Dados Pessoais de Crianças e Adolescentes

Tratamento de Dados Pessoais pelo Poder Público

As informações sobre o tratamento de dados pelo poder público, que se enquadram neste estudo de caso, apenas declaram que serão observadas as finalidades específicas de execução de políticas públicas. Não há registro de processos ou qualquer outra informação que indique um nível mais avançado de maturidade. A Tabela 33 contém apenas este único processo.

Tabela 33: Órgão Poder Judiciário – Tratamento de Dados Pessoais pelo Poder Público

Processos	Níveis de Maturidade				
	Nível 1	Nível 2	Nível 3	Nível 4	Nível 5
P07	1				

Fonte: Próprio autor.

5.3.2 Tratamento Governança e Segurança da Informação

A Tabela 34 apresenta uma análise dos processos de governança e segurança da informação. Para sua elaboração, foram realizadas pesquisas no *site* institucional, visando identificar evidências que subsidiem a avaliação descrita nesta seção.

Tabela 34: Órgão Poder Judiciário – Avaliação sobre Governança e Segurança da Informação

Processos	Níveis de Maturidade				
	Nível 1	Nível 2	Nível 3	Nível 4	Nível 5
P14		X			
P15	–	X			
P16	–	X			
P17	X				
P18	–				
P19	–		X		
P20	–				
P21	–				
P22	–				

Fonte: Próprio autor.

Há diversas evidências que indicam a existência de uma gestão de segurança da informação processos P14 e P15. No entanto, devido à natureza intrínseca ou mais sigilosa dessa área, não foi possível determinar com clareza um nível mais elevado de maturidade. Por conseguinte, será considerado o nível 2 para esses processos.

Em relação à conscientização (P16), foram identificadas postagens no site que mencionam treinamentos e capacitações destinados às equipes responsáveis pela implementação das diretrizes da LGPD. Contudo, não há indícios de que esses treinamentos sejam contínuos ou de que haja um gerenciamento eficaz desses processos de capacitação.

No que tange à auditoria interna (P17), foram encontradas notícias que confirmam sua presença. No entanto, não há registros ou informações detalhadas sobre os processos de auditoria, ou evidências que comprovem a regularidade dessas atividades.

Por fim, no elemento analisado (P19), foram encontradas evidências que apontam para um nível de maturidade avançado, possivelmente nível 4. No entanto, tais evidências não foram conclusivas. O nível 3 revelou-se mais preciso, uma vez que há referências a indicadores quantitativos, mas não a indicadores qualitativos, justificando assim a classificação no nível indicado.

Processos P14 e P15, há bastante evidencias que demonstram haver gestão de segurança da informação, porém, por se tratar de algo mais intrínseco não foi possível observar se há uma maturidade maior, portanto será considerado o nível 2.

Acerca do processo de Conscientização, P16, há publicações no site sobre treinamentos e capacitações para as equipes responsáveis pela implantação das diretrizes da LGPD. No entanto, não há indícios de continuidade ou de gerenciamento desses treina-

mentos.

Semelhante ao processo anterior, o processo P17, referente à auditoria interna, apresenta informações sobre sua existência, mas não oferece detalhes sobre os procedimentos envolvidos, nem evidências que indiquem a regularidade dessas auditorias.

Foram identificadas evidências que indicam um nível de maturidade avançado para o processo P19, sugerindo um possível nível 4. No entanto, essas evidências não foram suficientemente conclusivas. Por outro lado, o nível 3 se mostrou mais consistente, respaldado por referências a indicadores quantitativos, mas sem a presença de indicadores qualitativos. Isso justifica a decisão de manter o nível de maturidade no estágio indicado.

5.3.3 Indicador de Maturidade

Além dos casos anteriores, examinamos uma instituição vinculada ao Poder Judiciário. Este estudo visa avaliar a implementação e a eficácia dos processos de tratamento de dados pessoais e governança e segurança da informação em uma organização governamental.

Espera-se que esta instituição apresente um desempenho superior em relação às anteriores, devido ao rigor e às exigências específicas associadas à segurança da informação no contexto jurídico. A análise do indicador de maturidade nesta organização permitirá uma compreensão detalhada de como os processos estão estruturados e operacionais, bem como a identificação de boas práticas e áreas que necessitam de aprimoramento.

A Tabela 35 apresenta os processos do primeiro grupo avaliado, assim, temos:

Tabela 35: Órgão Poder Judiciário - Pontuação Processos Tratamento Dados Pessoais

Processo	Nível
P01	2
P02	2
P03	2
P04	1
P07	1
Total	8

Fonte: Próprio autor.

Os processos P05 e P06 não foram considerados na avaliação, uma vez que foi estabelecido que a organização não realiza o tratamento de dados de crianças e adolescentes.

Para o segundo grupo de processos avaliados, apresentados na Tabela 36, são os processos de governança e segurança, teremos:

Tabela 36: Órgão Poder Judiciário - Pontuação Processos Governança e Segurança

Processo	Nível
P14	2
P15	2
P16	2
P17	1
P18	0
P19	3
P20	0
P21	0
P22	0
Total	10

Fonte: Próprio autor.

O processo P07 não se aplica, pois trata de informações referentes a órgãos públicos, enquanto o estudo de caso analisado envolve um hospital privado. Para o cálculo do indicador, serão considerados apenas os processos avaliados.

$$\text{Total} = \sum_{j=1}^{2} G_j$$

logo

$$\text{Total} = 18$$

Considerando que foram avaliados 13 processos (4 processos do grupo de Tratamento de Dados e 9 processos do grupo de governança e segurança da informação), a pontuação máxima desta estudo de caso é:

$$\text{Pontuação Máxima} = (4 + 9) \times 5$$

então,

$$\text{Pontuação Máxima} = 65$$

Calculando o indicador de maturidade em valores percentuais teremos:

$$\text{Indicador} = \left(\frac{\text{Pontuação Total}}{\text{Pontuação Máxima}} \right) \times 100$$

$$\text{Indicador} = \left(\frac{18}{65} \right) \times 100$$

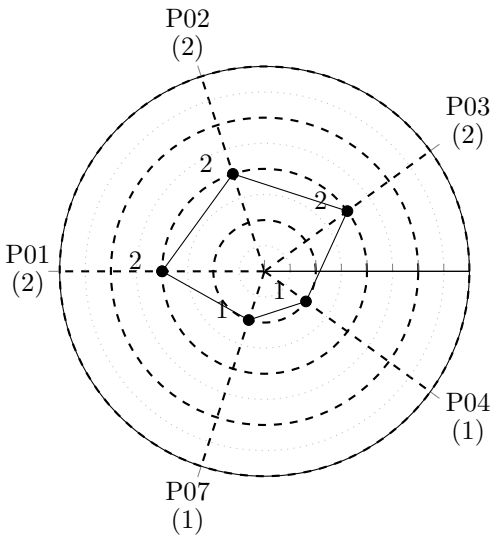
logo,

$$\text{Indicador} = 27{,}69{,}0\%$$

A avaliação foi bastante positiva, superando as avaliações das demais organizações, como era esperado. No entanto, ainda há carências significativas em diversos processos na área de governança e segurança da informação. A seguir serão apresentadas as representações visuais dos indicadores dos grupos avaliados.

Gráfico de Maturidade

Figura 9: Avaliação Órgão do Poder Judiciário – Tratamento de Dados Pessoais

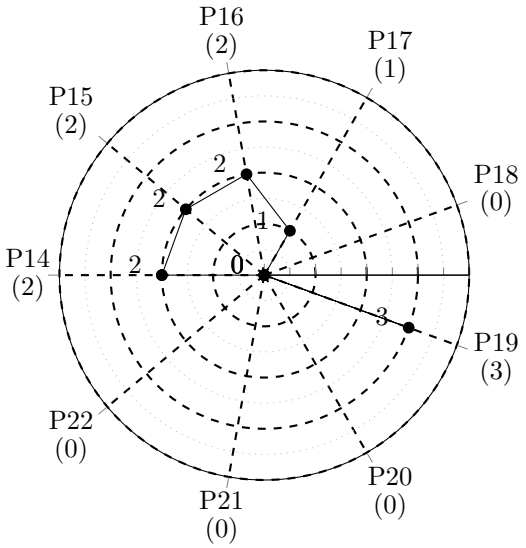


Fonte: Próprio autor, 2024.

Nesta análise, na figura 9 acima, observa-se um leve deslocamento em relação ao ponto central do gráfico, sugerindo um nível de maturidade dos processos um pouco mais elevado. Os processos relacionados ao tratamento de dados de crianças e adolescentes, identificados como P05 e P06, foram excluídos da avaliação, por haver evidências claras de que não pertencem ao perfil de usuários atendidos.

A seguir, está a representação visual do grupo de Governança e Segurança da Informação:

Figura 10: Avaliação Órgão do Poder Judiciário – Governança e Segurança da Informação



Fonte: Próprio autor, 2024.

No grupo de governança e segurança da informação, a legibilidade do gráfico, representando na figura 10 acima, foi comprometida devido à presença significativa de processos com avaliação zero (0). Essa concentração de avaliações mínimas causou uma distorção na visualização geral do gráfico. A partir do processo P14, é possível observar uma tendência de formação de um contorno. No entanto, os processos P18, P20, P21 e P22, com avaliações muito baixas, impediram a formação de uma estrutura coesa, resultando em uma representação visual desorganizada.

5.4 Considerações Finais

Durante o estudo de caso, perceberam-se algumas limitações como de processos podem existir, porém, não estão disponíveis ao público por se tratarem de rotinas ou procedimentos internos, ou ainda de níveis do sistema acessíveis apenas a usuários específicos. Um exemplo disso é o processo de Consentimento para Tratamento de Dados Pessoais Sensíveis de Crianças e Adolescentes avaliado no primeiro estudo de caso, da instituição de Ensino. Pode haver definições sobre esse tratamento que estejam evidenciadas apenas em áreas restritas de cadastro ou alteração de dados pessoais dos usuários. Embora a LGPD e outras legislações exijam a publicização de informações sobre tratamento de dados, a gestão detalhada desse processo, incluindo avaliações qualitativas e quantitativas, geralmente não é divulgada publicamente. A menos que a instituição possua um portal de transparência, onde sejam publicadas notas, métricas e indicadores de seus processos – o

que não foi observado durante este estudo – essas informações permanecem inacessíveis ao público geral.

A Lei Geral de Proteção de Dados Pessoais (LGPD) prevê certas dispensas e flexibilizações quando o tratamento de dados pessoais é realizado por organizações governamentais no exercício de suas funções de interesse público. Em particular, a LGPD dispensa a necessidade de consentimento do titular dos dados quando o tratamento é efetuado para a execução de políticas públicas previstas em leis, regulamentos ou respaldadas por contratos, convênios ou instrumentos congêneres.

Embora os direitos dos titulares, como acesso, correção e exclusão de dados, sejam garantidos, o tratamento deve respeitar os princípios da finalidade e transparência, utilizando os dados exclusivamente para os fins que justificaram sua coleta.

O compartilhamento de dados pessoais entre órgãos governamentais é permitido, desde que sejam observadas as finalidades específicas e as normas de segurança e sigilo estabelecidas. No entanto, essa permissão não exime a necessidade de mecanismos robustos para garantir o controle sobre o tratamento de dados, promovendo a transparência das atividades e o cumprimento rigoroso das normas de proteção de dados.

Um ponto de preocupação é a falta de publicação de informações por parte de órgãos governamentais sobre a coleta e o tratamento de dados, justificando-se por estarem executando políticas públicas. Embora a LGPD permita certas flexibilizações, a ausência de transparência pode gerar desconfiança e dificultar a fiscalização das práticas de tratamento de dados. A lei 13.709 reforça a importância da transparência, exigindo que o tratamento de dados respeite os princípios da finalidade e da publicidade, garantindo que os titulares tenham conhecimento sobre como seus dados são utilizados, mesmo no contexto de políticas públicas. Portanto, é fundamental que os órgãos governamentais equilibrem a execução de suas funções com a necessidade de informar e proteger os direitos dos cidadãos.

No estudo de caso do hospital privado, a situação é preocupante devido à escassez de informações sobre o tratamento de dados pessoais, bem como a inadequação dos processos de governança e segurança pública. Essa preocupação se acentua diante da falta de processos claros e bem definidos, além da transparência nas medidas de proteção das informações sigilosas de saúde dos cidadãos atendidos pelo hospital. A ausência desses processos coloca em risco a privacidade e a segurança dos pacientes, comprometendo a confiança no sistema de saúde e violando os princípios estabelecidos pela lei.

No estudo de caso de um órgão ligado ao Poder Judiciário, os resultados foram os mais positivos entre todos os analisados. Este órgão demonstrou boas práticas no tratamento de dados pessoais, com a implementação de várias orientações da Lei Geral de Proteção de Dados (LGPD). Destaca-se a disponibilidade de um formulário no site para

solicitações, ainda que de forma genérica, a divulgação do nome e contato do Encarregado de Proteção de Dados (DPO) e uma quantidade significativa de informações conforme as diretrizes da LGPD. Essas medidas indicam um compromisso sólido com a proteção de dados pessoais e a transparência no tratamento dessas informações.

Além disso, há indícios de que o órgão possui comitês de privacidade, o que sugere uma gestão mais estruturada e preocupações bem definidas em comparação com as outras organizações avaliadas. A existência desses comitês pode significar uma maior supervisão e um enfoque mais rigoroso na conformidade com as normas de proteção de dados. Esse desempenho superior não apenas reforça a confiança dos cidadãos na proteção de seus dados pessoais, mas também serve como um modelo de boas práticas para outras entidades públicas.

No entanto, é importante reconhecer uma limitação na avaliação das práticas de proteção de dados do órgão analisado: a dificuldade de averiguar maiores níveis de maturidade em razão da ausência de documentos publicados sobre os processos, como, por exemplo, o Plano de Resposta a Incidentes (processo P19). A natureza confidencial e sigilosa desses procedimentos internos pode impedir a divulgação de informações mais específicas, o que limita a capacidade de uma avaliação completa. Enquanto o órgão pode ter um plano robusto para responder a incidentes, detalhes como a frequência de revisões ou a quantificação de incidentes não são necessariamente divulgados. Essa falta de transparência sobre aspectos críticos pode deixar uma lacuna na compreensão real da eficácia do plano de resposta a incidentes. Para obter uma visão mais detalhada e precisa, seria necessária uma abordagem de pesquisa mais aprofundada, envolvendo possivelmente entrevistas e formulários direcionados aos responsáveis pelos processos internos. Essa abordagem permitiria uma análise mais detalhada e um entendimento mais completo das práticas implementadas, contribuindo para uma avaliação mais precisa da maturidade da proteção de dados.

Outra ressalva diz respeito ao cálculo do índice de maturidade, que atualmente é realizado de forma igualitária, atribuindo o mesmo peso a todos os processos. No entanto, acredita-se que, com uma análise mais aprofundada dos estudos de caso, será possível desenvolver uma fórmula que reflita de maneira mais precisa a realidade das organizações. Essa análise permitirá obter uma visão mais detalhada e acurada da situação específica de cada organização, resultando em um indicador de maturidade mais justo e representativo.

Os processos do CMM-PC foram concebidos para serem independentes entre si, permitindo que cada um seja tratado de maneira autônoma, com foco nas características específicas e nas demandas particulares de cada área da organização. No entanto, durante a aplicação prática do modelo, verificou-se que, apesar de ser possível abordar os processos separadamente, em determinados contextos organizacionais podem surgir inter-relações e dependências entre eles. Por exemplo, alguns processos podem depender dos resultados de

outros para serem implementados de maneira eficaz, como ocorre com os processos **P01** (Consentimento de Dados ao Titular) e **P02** (Revogação do Consentimento de Dados ao Titular). Em uma avaliação inicial, poderia ocorrer um equívoco ao classificar o processo P01 com nível de maturidade 0 e o processo P02 com nível 3. Tal resultado seria incoerente, já que o processo P02 depende, em certa medida, do P01 para seu funcionamento adequado.

Contudo, dado o escopo desta dissertação, o foco se manteve na avaliação individual e detalhada de cada um dos 27 processos, visando sua análise e caracterização isolada. A investigação das interdependências entre eles requereria uma ampliação do estudo, o que ultrapassaria os limites temporais e metodológicos estabelecidos para este trabalho.

6 CONCLUSÃO

A criação do modelo CMMPC, desenvolvido para avaliar a conformidade com a Lei Geral de Proteção de Dados (LGPD), envolveu várias fases de análise e refinamento. Inicialmente, foi feita uma análise da LGPD para identificar e interpretar os princípios e exigências legais relevantes. Esta etapa foi visou garantir a identificação de todos os requisitos estabelecidos pela legislação para assegurar a conformidade. Em seguida, estes requisitos foram mapeados em processos organizacionais e organizados em categorias que contemplavam assuntos semelhantes e correlatos, tais como tratamento de dados pessoais, direitos do titular, transferência internacional de dados, governança e segurança da informação e sanções administrativas. Este processo foi repetido e reanalisado para refinar e validar os processos e suas categorias. Por fim os processos mapeados foram aplicados escalas de maturidade que variam do 1 (um), sendo o menos maduro, ao 5 (cinco) o mais maduro.

Como resultado, o modelo CMMPC foi estabelecido para fornecer uma avaliação de conformidade com a LGPD, oferecendo um instrumento para as organizações na implementação e monitoramento de seus processos relacionados a práticas de proteção de dados.

A proposta de um modelo de processo com maturidade para adequação aos requisitos da Lei Geral de Proteção de Dados (LGPD), o CMMPC, representa uma contribuição singular para a área de privacidade proteção de dados, uma vez que nos trabalhos pesquisados não foram encontradas propostas similares. O trabalho de (ARAÚJO et al., 2021) aborda a conformidade de processos de negócio com a LGPD, utilizando notações BPMN. (OKANO et al., 2022) conduz uma pesquisa acerca da implementação da LGPD no Brasil e avalia a utilização de um método visual para auxiliar organizações com os requisitos da LGPD. Os trabalhos de (NASCIMENTO, 2023) e (MARQUES, 2020) referenciam a utilização *Data Maturity Model* (DMM) para gestão dos dados e como pode ser utilizado para adequação e conformidade com a LGPD, seja na implementação dos processos sugeridos, seja na adequação dos processos existentes.

O CMMPC foi elaborado abrangendo os pontos específicos definidos e exigidos pela LGPD, contemplando todos os aspectos do tratamento de dados pessoais, desde dados sensíveis até informações de crianças e adolescentes, além dos dados gerenciados pelo setor público. Ademais, incluíram-se considerações sobre segurança da informação, governança e práticas recomendadas. Para cada uma dessas áreas, estabeleceram-se objetivos gerais, aos quais foram aplicados os respectivos níveis de maturidade. Assim, o foco neste modelo é na gestão dos processos que foram mapeados a partir dos requisitos da Lei.

Além dos benefícios diretos da conformidade com a LGPD, o modelo oferece outras vantagens adicionais para as organizações. Ele estimula a melhoria contínua ao permitir a

evolução gradual e individual dos processos, assegurando uma abordagem sustentável. A aplicação do modelo pode auxiliar na mitigação de riscos e ameaças associadas à privacidade e proteção de dados e diminuindo a probabilidade de incidentes e suas consequências. Ademais, pode fortalecer a confiança e reputação das organizações, ao demonstrar a capacidade de proteger os dados pessoais e melhorar a percepção da organização no pela sociedade.

Por fim, a padronização dos processos voltados à proteção e privacidade de dados poderá promover a eficiência operacional. A busca por níveis mais elevados de maturidade dentro da organização ajudará a alinhar suas práticas com os requisitos da Lei, contribuindo para a conformidade. Como resultado, o país demonstra um compromisso sólido com a segurança e privacidade das informações, o que é essencial para ingressar em blocos econômicos e organismos internacionais. A conformidade consistente e a adoção de práticas de segurança e privacidade reforçam a confiança internacional, facilitando acordos comerciais e cooperação em níveis mais amplos, e posicionando o país como um parceiro confiável no mercado global.

6.1 Limitações e Trabalhos Futuros

O estudo de caso poderia ter sido mais aprofundado, considerando especialmente a escassez de evidências de conformidade com a LGPD nas organizações avaliadas. A inclusão de entrevistas *in loco* com profissionais de áreas específicas poderia ter enriquecido a análise. Contudo, o objetivo principal do estudo foi examinar os documentos públicos disponíveis nos portais institucionais e empresariais, conforme preconiza a LAI. A falta de publicização de informações acerca de requisitos de conformidade com a LGPD levanta uma questão preocupante sobre como as organizações estão lidando com as exigências desta Lei.Estariam as organizações conforme a LGPD, mas negligenciando a divulgação de suas ações? Ou, de fato, não estão em conformidade e estão desrespeitando a Lei em vigor?

Outra limitação é que a aplicação do modelo ainda é realizada de forma manual, sem automação. Seria interessante estabelecer padrões na pesquisa para possibilitar a automação parcial ou total do processo, o que poderia aumentar a eficiência e a consistência dos resultados.

Conforme discutido na seção 5.4 - Considerações Finais, verificou-se a possibilidade de existência de dependências entre os processos, um aspecto identificado somente após a aplicação do estudo de caso. Reconhecemos, portanto, essa limitação, que não foi abordada no presente trabalho.

O tema analisado por este trabalho apresenta ainda diversas oportunidades para estudo e pesquisa. A área em questão é rica em possibilidades para novas investigações

acadêmicas e estudos de caso. Assim, propõem-se alguns caminhos promissores que podem ser seguidos em futuros trabalhos, utilizando como base os artefatos e conceitos discutidos ao longo deste estudo:

- Nova metodologia de coleta de dados, incluindo a análise documental e entrevistas com pessoas-chave da organização;
- Aplicação de um novo método para cálculo do índice de maturidade que inclua a revisão dos processos e a avaliação da possibilidade de atribuir pontuações diferenciadas a cada processo;
- Apresentação de novas visualizações do nível de maturidade da organização, oferecendo uma representação mais clara e detalhada do seu estado atual;
- Investigação acerca das ações de conformidade com a LGPD e a publicização destas em portais oficiais;
- Verificação das possíveis dependências entre os processos, de modo a evitar incoerências nos resultados de sua aplicação.

REFERÊNCIAS

AGUIRRE, E. et al. Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of Retailing*, v. 91, n. 1, p. 34–49, 2015. ISSN 0022-4359. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0022435914000669>. 19

ALIYU, A. et al. A holistic cybersecurity maturity assessment framework for higher education institutions in the united kingdom. *NATO Adv. Sci. Inst. Ser. E Appl. Sci.*, Multidisciplinary Digital Publishing Institute, v. 10, n. 10, p. 3660, maio 2020. Disponível em: <https://www.mdpi.com/2076-3417/10/10/3660>. 46

ALVES, C.; NEVES, M. Especificação de requisitos de privacidade em conformidade com a lgpd: Resultados de um estudo de caso. In: *WER*. [S.l.: s.n.], 2021. 33

ARAÚJO, E. et al. Are my business process models compliant with LGPD? the LGPD4BP method to evaluate and to model LGPD aware business processes. In: *XVII Brazilian Symposium on Information Systems*. New York, NY, USA: ACM, 2021. p. 1–9. 41, 50, 107

Assessoria Especial de Imprensa Ministério Público Distrito Federal. *MPDFT e Netshoes firmam acordo para pagamento de danos morais após vazamento de dados*. 2024. https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2019/10570-mpdft-e-netshoes-firmam-acordo-para-pagamento-de-danos-morais-coletivos-apos-vazamento-de-dados. Acesso em: 2 set. 2024. 24

Associação Brasileira de Normas Técnicas. *ABNT NBR ISO/IEC 27001:2013 Tecnologia da Informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos*. 2013. 62

AUGUSTO, P.; FRANCISCO, P.; VENTURINI, J. *Privacidade, Vigilância e Inteligência no Brasil: O marco legal e suas lacunas*. 2017. 33

Banco Central do Brasil. *Lei Geral de Proteção de Dados (LGPD) - Registro de Incidentes com Dados Pessoais*. 2024. Acesso em: 2 set. 2024. Disponível em: <https://www.bcb.gov.br/acessoinformacao/lgpd?modalAberto=registro_de_incidentes_com_dados_pessoais>. 24

BARBOSA, L. F. O conceito de 'agentes de tratamento'na lgpd: um olhar sobre sua interpretação inicial no brasil. *Revista Semestral de Direito Empresarial*, n. 25, p. 189–232, 2019. 34

BARBOSA, S. C. T. Capacidade de gestão: coordenação interorganizacional na implementação de programas públicos federais no brasil. Instituto de Pesquisa Econômica Aplicada (Ipea), 2016. 22

BARBOSA, T. S. et al. A lei geral de proteção de dados (lgpd) nas instituições públicas de ensino: Possíveis impactos e desafios. In: *VII ENPI-Encontro Nacional de Propriedade Intelectual*. api.org.br, 2021. Disponível em: <https://repositorio.ifsc.edu.br/bitstream/handle/123456789/1433/Artigo-MarcoAntonioTorrezRojas-vf.pdf?sequence=1&isAllowed=y>. Acesso em: 16 abril 2023. 22

BARCELOS, A. K. et al. A lei geral de proteção de dados e o papel do dpo. *Revista Projetos Extensionistas*, periodicos.fapam.edu.br, v. 1, n. 2, p. 87–92, 2021. 65

BATE, R. et al. *A Systems Engineering Capability Maturity Model, Version 1.1*. [S.l.]: Carnegie Mellon University, Software Engineering Institute, 1995. 36

BEZERRA, L. A. M. LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) E O USO DA INTERNET POR CRIANÇAS E ADOLESCENTES NO BRASIL: POR QUE O TRATAMENTO DE DADOS PESSOAIS DE ADOLESCENTES DISPENSA O CONSENTIMENTO PARENTAL? *Revista FIDES*, revistafides.ufrn.br, v. 11, n. 2, p. 335–351, 2020. Disponível em: <http://www.revistafides.ufrn.br/index.php/br/article/view/511>. 54

BIONI, B. R. *Proteção de Dados Pessoais - A Função e os Limites do Consentimento*. [S.l.]: Editora Forense, 2018. 33

BITTAR, C. A. *Os direitos da personalidade*. [S.l.]: Saraiva Educação SA, 2017. 32

BOTELHO, M. C.; CAMARGO, E. P. do A. O TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO NA LGPD. *RDSPP*, portal.unifafibe.com.br, v. 9, n. 3, p. 549–580, 2021. Disponível em: <https://portal.unifafibe.com.br/revista/index.php/direitos-sociais-politicas-pub/article/view/1034>. 57

BRASIL. Estatuto da criança e do adolescente. Brasília, DF, 1990. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l8069.htm>. Acesso em: 13 mai. 2024. 55

BRASIL. Lei de acesso à informação. *Diário Oficial [da] República Federativa do Brasil*, Brasília, DF, 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 29 julho 2022. 53, 81

BRASIL. Marco civil da internet. *Diário Oficial [da] República Federativa do Brasil*, Brasília, DF, 2014. Disponível em: <https://www.in.gov.br/web/dou/-/lei-n-12-965-de-23-de-abril-de-2014-30054600>. Acesso em: 21 jul. 2022. 32

BRASIL. Lei geral de proteção dos dados. *Diário Oficial [da] República Federativa do Brasil*, Brasília, DF, 2018. Disponível em: <https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/36849373/do1-2018-08-15-lei-no-13-709-de-14-de-agosto-de-2018-36849337>. Acesso em: 21 jul. 2022. 52, 81

BRASIL. Decreto no 10.222, de 5 de fevereiro de 2020. *Diário Oficial [da] República Federativa do Brasil*, Brasília, DF, 2020. Disponível em: <https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419>. Acesso em: 27 julho 2022. 19

BRASIL. *Governo Digital*. 2024. Disponível em: <https://www.gov.br/governodigital/pt-br>. Acesso em: 05 mai. 2024. 57

BRASIL, C.-G. d. U. *Acesso à informação pública: uma introdução à Lei nº 12.527, de 18 de novembro de 2011*. [S.l.]: Ministério Público do Estado da Bahia, 2011. 28

CHEN, Y. Study on the role of internal audit in university governance. *SHS Web of Conferences*, EDP Sciences, v. 169, p. 01033, 2023. Disponível em: <https://www.shs-conferences.org/10.1051/shsconf/202316901033>. 63

COTS, M.; OLIVEIRA, R. *Lei geral de proteção de dados pessoais: comentada*. 2. ed. São Paulo: Thomson Reuters Brasil, 2018. 33, 57

CRESPO, M. Proteção de dados pessoais e o poder público: noções essenciais. In: *Lei Geral de Proteção de Dados e o Poder Público*. [s.n.], 2021. p. 16. Disponível em: <https://www.academia.edu/download/71210708/TCE_ESDM.pdf#page=17>. 21, 86

CUNDA, D. Z. G. et al. A proteção e a transparência de dados sob a perspectiva dos controles externo e social e a governança digital. *LEI GERAL DE PROTEÇÃO DE DADOS E O PODER PÚBLICO*, Escola Superior de Gestão e Controle Francisco Juruena, p. 223, 2021. 21

CURTIS, B.; HEFLEY, W. E.; MILLER, S. A. *The People Capability Model: Guidelines for Improving the Workforce*. [S.l.]: Boston: Addison-Wesley, 2001. 36

DANIEL, M. A. *A evolução e aplicação da segurança da informação por meio da lei geral de proteção de dados pessoais (lgpd): um estudo de caso em uma instituição financeira*. [S.l.]: Araranguá, SC, 2022. 31, 33

DANTAS, C. F. *Governo digital: oferta de serviços digitais do Governo Federal disponibilizados no portal Gov. BR*. 2021. <https://repositorio.ufrn.br/handle/123456789/46727>. Accessed: 2024-5-15. Disponível em: <https://repositorio.ufrn.br/handle/123456789/46727>. 57

DENER, C. et al. *GovTech Maturity Index: The State of Public Sector Digital Transformation*. [S.l.]: World Bank Publications, 2021. 20

FARIAS, F. P.; BARROS, R. LGPD – from theory to practice. In: *2022 17th Iberian Conference on Information Systems and Technologies (CISTI)*. IEEE, 2022. p. 1–6. Disponível em: <https://ieeexplore.ieee.org/abstract/document/9820267/>. 65

FAYAYOLA, O. A.; OLORUNFEMI, O. L.; SHOETAN, P. O. Data privacy and security in it: A review of techniques and challenges. *Comput. sci. IT res. j.*, Fair East Publishers, v. 5, n. 3, p. 606–615, mar. 2024. 19

FERNANDES, M. E.; NUZZI, A. P. E. Fundamentos da lei geral de proteção de dados (lgpd): uma revisão narrativa. *Research, Society and Development*, v. 11, n. 12, p. e310111234247–e310111234247, 2022. 34

FERREIRA, L.; OKANO, M. T. Um panorama da implementação da LGPD no brasil: uma pesquisa exploratória com 216 profissionais. In: *XVI Simpósio dos Programas de Mestrado Profissional*. [S.l.]: unknown, 2021. 40

FERREIRA, L. et al. A panorama of the implementation of the general law for the protection of personal data (lgpd) in brazil: an exploratory survey. In: *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*. [S.l.: s.n.], 2022. p. 0723–0729. 64

FINKELSTEIN, M. E.; FINKELSTEIN, C. Privacidade e lei geral de proteção de dados pessoais. *Rev. Direito Bras.*, Conselho Nacional de Pesquisa e Pos-Graduacao em Direito - CONPEDI, v. 23, n. 9, p. 284, fev. 2020. 31

GARCIA, M. *Big Data: O que é, conceito e definição*. 2022. Disponível em: <https://cetax.com.br/big-data/>. Acesso em: 05 set. 2022. 30

GIL, A. C. *Como Elaborar Projetos de Pesquisa*. 5a. ed. São Paulo: Atlas, 2010. 1–184 p. 45

GOMES, L. F. A. M.; GOMES, C. F. S. *Tomada de decisão gerencial: enfoque multicritério*. [S.l.]: Editora Atlas SA, 2014. 35

GOMES, M. C. O. Relatório de impacto à proteção de dados. *Uma breve análise da sua definição e papel na LGPD. Publicado na Revista do Advogado*, n. 144, p. 9–11, 2019. 65

GONÇALVES, T. C. N. M. Gestão de dados pessoais e sensíveis pela administração pública federal: desafios, modelos e possíveis impactos com a nova lei. UniCEUB, nov. 2020. 21, 31

KERZNER, H. *Gestão de Projetos-: As Melhores Práticas*. [S.l.]: Bookman editora, 2010. 42

KNOKE, F.; NWANKWO, I. Practitioner's corner managing data protection compliance through maturity models: A primer. *Eur. Data Prot. Law Rev.*, Lexxion Verlag, v. 8, n. 4, p. 536–543, 2022. Disponível em: <https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/edpl8&section=77>. 48

KORKMAZ, M. R. R.; SACRAMENTO, M. Direitos do titular de dados:: potencialidades e limites na lei geral de proteção de dados pessoais. *Revista Eletrônica da PGE-RJ*, revistaeletronica.pge.rj.gov.br, v. 4, n. 2, 2021. Disponível em: <https://revistaeletronica.pge.rj.gov.br/index.php/pge/article/view/234>. 58

LABADIE, C.; LEGNER, C. *Understanding data protection regulations from a data management perspective: A capability-based approach to EU-GDPR*. serval.unil.ch, 2019. <https://serval.unil.ch/resource/serval:BIB_65AAB323C49C.P001/REF.pdf>. Accessed: 2024-1-16. Disponível em: <https://serval.unil.ch/resource/serval:BIB_65AAB323C49C.P001/REF.pdf>. 41

LORENZON, L. N. Análise comparada entre regulamentações de dados pessoais no brasil e na união europeia (LGPD e GDPR) e seus respectivos instrumentos de enforcement. *Revista do Programa de Direito da União Europeia*, v. 1, p. 39–52, 2021. Disponível em: <http://periodicos.fgv.br/rpdue/article/view/83423>. 64

MAGALHÃES, R. A.; OLIVEIRA, E. C. R. N. O direito à privacidade na era digital. *Revista Jurídica da FA7*, v. 18, n. 1, p. 55–70, 2021. 28

MALDONADO, V. N.; BLUM, R. O. *Lgpd - Lei Geral de Proteção de Dados Pessoais Comentada*. 4. ed. [S.l.]: 22 abril, 2022. 32, 57

MARCONI, M. d. A.; LAKATOS, E. M. *Fundamentos de metodologia científica*. [S.l.]: Atlas, 2006. 44, 45

MARQUES, L. N. O mapeamento do modelo data management maturity (DMM) à lei geral de proteção de dados (LGPD). Pontifícia Universidade Católica de Goiás, dez. 2020. Accessed: 2024-1-16. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/handle/123456789/1289>. 42, 107

MARTIN, B. Aplicação das penalidades da lei geral de proteção de dados. *Conhecimento Interativo*, v. 14, n. 2, 2020. 68

MAXIMIANO, I. V. Lei geral de proteção de dados: dificuldades da efetivação frente a administração pública e seus reflexos no setor privado. Fundação de Ensino e Pesquisa do Sul de Minas, dez. 2022. 21

NASCIMENTO, B. A. V. d. *Um estudo da maturidade em gestão de dados em um órgão público de trânsito*. 2023. Accessed: 2024-03-15. Disponível em: <https://repositorio.ufpe.br/handle/123456789/50455>. 38, 39, 40, 41, 107

NEGRO-CALDUCH, E. et al. Technological progress in electronic health record system optimization: Systematic review of systematic literature reviews. *Int. J. Med. Inform.*, Elsevier BV, v. 152, n. 104507, p. 104507, ago. 2021. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1386505621001337>. 66

NEVES, R. d. A. P. Lgpd e gdpr: Transferências internacionais de dados pessoais. In: *IV CONGRESSO INTERNACIONAL DE DIREITOS HUMANOS DE COIMBRA: UMA VISÃO TRANSDISCIPLINAR*. [S.l.: s.n.], 2022. p. 65. 60

OKANO, M. T. et al. Lgpd model canvas: proposta de um framework para diagnosticar as empresas para a lgpd. *Humanidades & Inovação*, v. 9, n. 20, p. 188–193, 2022. 34, 107

OLIVEIRA, A. C. S. et al. Manual de normalização bibliográfica para elaboração de monografia. *Natal: Universidade Potiguar*, v. 46, 2006. 44, 45

OLIVEIRA, D. M. A (IN) CONSTITUCIONALIDADE DAS prisões POR RECONHECIMENTO FACIAL VIA CÂMERAS DE VÍDEO: conflito entre o direito à privacidade eo direito à segurança pública? 2020. 32

OLIVEIRA, R. Lgpd: Como evitar as sanções administrativas. *São Paulo: Expressa*, 2021. 67

OSTERWALDER, A.; PIGNEUR, Y.; CLARK, T. *Modelo de Negócio EU*. [S.l.]: Leya, 2013. 41

PARAGUAI, C. E. N.; DELAZERI; RIBEIRO, N. S. A utilizaÇÃo do sistema de informaÇÃo gerencial na tomada de decisÃo. In: *Anais Colóquio Estadual de Pesquisa Multidisciplinar (ISSN-2527-2500) & Congresso Nacional de Pesquisa Multidisciplinar*. publicacoes.unifimes.edu.br, 2023. Disponível em: <http://publicacoes.unifimes.edu.br/index.php/coloquio/article/view/2739>. Acesso em: 22 março 2024. 36

PAULK, M. C. et al. Capability maturity model, version 1.1. *IEEE Softw.*, v. 10, n. 4, p. 18–27, jul. 1993. Disponível em: <http://dx.doi.org/10.1109/52.219617>. 36, 48, 49

PINHEIRO, P. P. *Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018 -LGPD*. [S.l.]: Saraiva Educação S.A., 2020. 30, 32, 34, 84

PLOTKIN, D. *Data stewardship: An actionable guide to effective data management and data governance*. [S.l.]: Academic press, 2020. 37

POMPEU, A. M. et al. Contribuições do Ciclo PDCA e do Sistema de Informações Gerenciais em Processos Decisórios de Gestão Organizacional. *Revista Augustus*, revistas.unisuam.edu.br, v. 30, n. 57, p. 190–208, out. 2022. Disponível em: <https://revistas.unisuam.edu.br/index.php/revistaaugustus/article/view/926>. Acesso em: 20 março 2024. 35

PORTILHO, L. et al. Privacidade e Proteção de Dados em Organizações Públicas e Privadas do Brasil: Avanços e Desafios. *Comunication Policy Research Latin America*, cprlatam.org, v. 15, 2022. Disponível em: <https://www.cprlatam.org/s/Proceedings-CPR-LATAM-2022.pdf#page=92>. 63

PRESSMAN, R. S.; MAXIM, B. R. *Software Engineering: A Practitioner's Approach, Ninth Edition*. [S.l.]: McGraw-Hill Education, 2021. 37

PROENÇA, D.; BORBINHA, J. Maturity models for data and information management: a state of the art. In: SPRINGER. *Digital Libraries for Open Knowledge: 22nd International Conference on Theory and Practice of Digital Libraries, TPDL 2018, Porto, Portugal, September 10–13, 2018, Proceedings 22*. [S.l.], 2018. p. 81–93. 37, 38

RAINIE, L.; ANDERSON, J. The Internet of Things Connectivity Binge: What are the Implications? Pew Research Center, 2017. 19

RNP. *Adeque-se à LGPD*. 2022. <https://www.rnp.br/sistema-rnp/adeque-se-a-lgpd>. Accessed: 2023-6-9. Disponível em: <https://www.rnp.br/sistema-rnp/adeque-se-a-lgpd>. Acesso em: 09 jun. 2023. 22

RODOTÀ, S. A Vida na Sociedade da Vigilância: a Privacidade Hoje. In: *A Vida na Sociedade da Vigilância: a Privacidade Hoje*. [S.l.: s.n.], 2015. p. 381–381. 29

RUA, M. das G. Análise de Políticas Públicas: Conceitos Básicos. *Manuscrito elaborado para o curso de formação para a carreira de Especialista em Políticas Públicas e Gestão Governamental.*, 1997. 22

SALMEN, C. S.; BELLÉ, C. M. B. A Proteção de Dados Sensíveis e as Inovações da Área da Saúde. In: WACHOWICZ, M. o. (Ed.). *Proteção de dados pessoais em perspectiva: LGPD e RGPD na ótica do direito comparado*. [S.l.]: GEDAI, 2020. p. 242–270. 54

SANDOVAL-ALMAZÁN, R. Open government and transparency: building a conceptual framework. *Convergencia*, scielo.org.mx, 2015. 20

SANTOS, C. F. P. GDPR, CCPA e LGPD como instrumentos legislativos para proteção de dados pessoais. 002, dez. 2021. 31

SANTOS, I. M. R. *LGPD: Quais são os direitos do titular dos dados?* LAPIN, 2021. Disponível em: <https://lapin.org.br/2021/05/31/lgpd-quais-sao-os-direitos-do-titular-dos-dados/>. Acesso em: 20 mai. 2024. 59

SANTOS, R. G. T. dos. *A Lei Geral de Proteção de Dados Brasileira: Uma política pública regulatória*. Tese (Doutorado) — Instituto Serzedello Corrêa,, 2020. 22

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. *RDFD*, v. 27, n. 3, p. 217–253, dec 2022. Disponível em: <https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2285>. 35

SILVA, A. B. da et al. Open Banking sob a Perspectiva da Proteção de Dados: Interoperabilidade, Compartilhamento de Dados e Concorrência. *Open Banking: Direito da Concorrência, Proteção de Dados Pessoais e Interfaces Consumeristas*, academia.edu, p. 23, 2021. Disponível em: <https://www.academia.edu/download/86129485/Nuced_2021_Open_Banking_Direito_da_concorrencia_protecao_de_dados_pessoais_e_interfaces_consumeristas.pdf#page=24>. 66

SILVA, C. V. S. Crimes cibernéticos e impunidade: os desafios ao direito ante verificação de autoria e materialidade nos delitos informáticos. Universidade do Estado da Bahia, 2023. Disponível em: <https://saberaberto.uneb.br/handle/20.500.11896/4947>. 63

TCU. *Diagnóstico do grau de implementação da Lei Geral De Proteção De Dados na Administração Pública Federal*. [S.l.], 2022. Disponível em: <https://portal.tcu.gov.br/imprensa/noticias/tcu-verifica-risco-alto-a-privacidade-de-dados-pessoais-coletados-pelo-governo.htm>. Acesso em: 16 abril 2023. 26

TEAM, I. G. P. *EU general data protection regulation (gdpr) an implementation and compliance guide*. [S.l.]: IT Governance Ltd, 2020. 20, 29, 30

TOLFO, D. E. M.; KAPPES, F. C.; GOULART, G. D. A autoridade nacional de proteção de dados (ANPD) e a expressão da proporcionalidade imposta na análise das sanções administrativas aplicáveis consoante os dispositivos da lei geral de proteção de dados (LGPD) - n° 13.709/2018. ojs.cesuca.edu.br, n. 17, p. 107–115, 2023. Disponível em: <https://ojs.cesuca.edu.br/index.php/mostrac/article/view/2500>. 67, 68

VALESI RAQUEL; AOKI, M. Y. O direito à privacidade e à proteção de dados pessoais nas relações de consumo. *Rev. Dent.*, Revista de Estudos Jurídicos UNA, 2021. 32

VASCONCELOS, M. L. L. S. C. R. *LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: Desafios e impactos para o Poder Público*. 2021. 33

WARREN, S.; BRANDEIS, L. *The Right to Privacy Harvard Law Review (1890) 193-220*. 1890. 29

WEGNER, P. Interoperability. *ACM Comput. Surv.*, Association for Computing Machinery (ACM), v. 28, n. 1, p. 285–287, mar. 1996. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/234313.234424>. 66

WEISS, E. How to convince customers to share data after gdpr. *Harvard Business Review*, 2018. 19

ZITOUN, C. et al. Dmmm: Data management maturity model. In: . [S.l.: s.n.], 2021. p. 33–39. 42

ANEXOS

Sem anexos

APÊNDICE

Sem apêndice