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

JOSÉ EDSON DE SOUTO

CONFORMIDADE DE INFRAESTRUTURA DE TI COM A LGPD NO SETOR PÚBLICO: PROPOSTA DE ARQUITETURA DE REFERÊNCIA E PROCESSO DE AVALIAÇÃO

João Pessoa – PB
2025

JOSÉ EDSON DE SOUTO

CONFORMIDADE DE INFRAESTRUTURA DE TI COM A LGPD NO SETOR PÚBLICO: PROPOSTA DE ARQUITETURA DE REFERÊNCIA E PROCESSO DE AVALIAÇÃO

Trabalho de Dissertação apresentado ao Programa de Pós-Graduação em Informática da Universidade Federal da Paraíba como requisito parcial para obtenção do título de Mestre em Informática.

Área de Concentração: Ciências da Computação
Linha de Pesquisa: Sistemas de Computação
Orientador: Prof. Dr. Gustavo Henrique Matos Bezerra Motta

João Pessoa-PB
2025

FICHA CATALOGRÁFICA

Catalogação de Publicação na Fonte. UFPB - Biblioteca Central

S728c Souto, José Edson de.
Conformidade de infraestrutura de TI com a LGPD no setor público : proposta de arquitetura de referência e processo de avaliação / José Edson de Souto. - João Pessoa, 2025.
56 f. : il.

Orientação: Gustavo Henrique Matos Bezerra Motta.
Dissertação (Mestrado) - UFPB/CI.

1. Infraestrutura de TI. 2. Empresas Públicas. 3. LGPD. I. Motta, Gustavo Henrique Matos Bezerra. II. Título.

UFPB/BC CDU 004(043)

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

Ata da Sessão Pública de Defesa de Dissertação de Mestrado de José Edson de Souto, candidato ao título de Mestre em Informática na área de Sistemas de Computação, realizada em 31 de janeiro de 2025.

Aos trinta e um dias do mês de janeiro do ano de dois mil e vinte e cinco, às dez 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 José Edson de Souto, vinculado a esta Universidade sob a matrícula nº 20221015540, candidato ao grau de Mestre em Informática, na área de *"Sistemas de Computação"*, na linha de pesquisa *"Sistemas de Computação"*, 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; Denio Mariz Timoteo de Sousa, 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 "**Conformidade de Infraestrutura de TI com a LGPD no Setor Público: Proposta de Arquitetura de Referência e Processo de Avaliação**". 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, 31 de janeiro de 2025.

gov.br Documento assinado digitalmente
GILBERTO FARIAS DE SOUSA FILHO
Data: 13/02/2025 12:56:12-0300
Verifique em https://validar.iti.gov.br

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

gov.br Documento assinado digitalmente
GUSTAVO HENRIQUE MATOS BEZERRA MOTTA
Data: 05/02/2025 12:50:56-0300
Verifique em https://validar.iti.gov.br

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

gov.br Documento assinado digitalmente
CLAUIRTON DE ALBUQUERQUE SIEBRA
Data: 05/02/2025 14:08:43-0300
Verifique em https://validar.iti.gov.br

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

gov.br Documento assinado digitalmente
DENIO MARIZ TIMOTEO DE SOUSA
Data: 12/02/2025 12:09:05-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. DENIO MARIZ TIMOTEO DE SOUSA
Examinador Externo à Instituição (IFPB)

AGRADECIMENTOS

À memória da minha mãe Maria Natércia de Souto, cuja presença iluminou minha vida e cujo apoio incondicional foi fundamental para a realização deste trabalho. Sua partida devido à COVID-19 deixou um vazio irreparável, mas sua força e dedicação continuam a me inspirar diariamente.

Ao Professor Gustavo Motta, pela orientação precisa, paciência e incentivo constante ao longo desta jornada acadêmica.

À UFPB, Ao PPGI - PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA, Ao CI - CENTRO DE INFORMÁTICA por fornecerem os recursos necessários e um ambiente propício para o desenvolvimento desta pesquisa.

RESUMO

Introdução: Lei Geral de Proteção de Dados Pessoais (LGPD), “surgiu como um mecanismo para regular o tratamento de dados pessoais em território nacional permitindo a garantia dos direitos fundamentais de liberdade e privacidade de qualquer pessoa natural cujos dados aqui sejam tratados”. **Objetivos:** Propor um modelo de referência e um processo de avaliação para a conformidade de infraestrutura em TI com a LGPD no setor público de TI. **Metodologia:** Trata-se de uma pesquisa de natureza exploratória, do tipo estudo de caso. A presente pesquisa tem como procedimentos metodológicos, análise bibliográfica do tema e implementação de um sistema de validação dos dados, com o intuito de realizar a proposta da arquitetura de referência no processo de avaliação em conformidade com os dados pessoais para não ocorrer o compartilhamento indevido, sem autorização, seguindo a legislação vigente LGPD. **Resultados:** Empresa C: Total de Respostas: 158 (SIM) + 41 (NÃO) = 199; percentual de "SIM": (158 / 199) * 100 = 79.40%; Classificação: Como 79.40% é maior ou igual a 70%, a Empresa Y é classificada como: CONFORME. Empresa D: Total de Respostas: 89 (SIM) + 53 (NÃO) = 142; percentual de "SIM": (89 / 142) * 100 = 62.68%; Classificação: Como 62.68% está entre 60% e 69.99%, a Empresa X é classificada como: PARCIALMENTE CONFORME. **Conclusão:** A proposta desse trabalho é de grande relevância para o setor público, principalmente de infraestrutura de TI, pois, algumas mudanças significativas estão alicerçadas nas ações de incremento de infraestrutura tecnológica. Cabe ressaltar que este modelo é uma base para produção de um instrumento de verificação de conformidade da LGPD em organizações públicas, devendo ser ainda validado em estudo de caso.

Palavras-chave: Empresas Públicas; Conformidade; Infraestrutura de TI;

ABSTRACT

Introduction: The General Data Protection Law (LGPD) “emerged as a mechanism to regulate the processing of personal data in the national territory, guaranteeing the fundamental rights of freedom and privacy of any natural person whose data is processed here”. Objectives: To propose a reference model and an evaluation process for IT infrastructure compliance with the LGPD in the public IT sector. Methodology: This is an exploratory research of case study type. The present research has as methodological procedures, bibliographic analysis of the topic and implementation of a data validation system, with the aim of carrying out the proposal of the reference architecture in the evaluation process in compliance with personal data to prevent improper sharing without authorization, in accordance with the current LGPD legislation. Results: Company C: Total Responses: 158 (YES) + 41 (NO) = 199; percentage of "YES": (158 / 199) * 100 = 79.40%; Classification: Since 79.40% is greater than or equal to 70%, Company Y is classified as: COMPLIANT. Company D: Total Responses: 89 (YES) + 53 (NO) = 142; percentage of "YES": (89 / 142) * 100 = 62.68%; Classification: Since 62.68% is between 60% and 69.99%, Company X is classified as: PARTIALLY COMPLIANT. Conclusion: The proposal of this work is of great relevance to the public sector, especially IT infrastructure, since some significant changes are based on actions to increase technological infrastructure. It is worth mentioning that this model is a basis for the production of an instrument to verify LGPD compliance in public organizations, and should still be validated in a case study.

Keywords: Public Companies; Compliance; IT Infrastructure;

LISTA DE FIGURAS

Figura 1 – Acontecimentos antes da LGPD 18
Figura 2 – Componentes de um sistema de informação 21
Figura 3 – A intersecção da LGPD com as ISO 27001 e a ISO 27701 29
Figura 4 – Modelo de referência 41

LISTA DE TABELAS

Tabela 1 – Mensuração utilizando os critérios de classificação 40
Tabela 2 – Modelo de referência 43
Tabela 3 – Critérios e Validação das Empresas 47
Tabela 4 – Avaliação da Conformidade com a LGPD 49

LISTA DE ABREVIATURAS E SIGLAS

LGPD	Lei Geral de Proteção de Dados Pessoais
GDPR	Regulamento Geral sobre a Proteção de Dados
TI	Tecnologia da Informação
NIST	Nuvem do Instituto Nacional de Padrões e Tecnologia
PDCA	Planejar, Executar, Controlar e Agir
SGSI	Sistema de Gestão de Segurança da Informação
DPO	Data Protection Officer
ISO	International Organization for Standardization
IOT	Internet das Coisas

SUMÁRIO

1 INTRODUÇÃO 12
2 OBJETIVOS 15
2.1 Objetivo Geral 15
2.2 Objetivos Específicos 15
3 FUNDAMENTAÇÃO TEÓRICA 16
3.1 Lei Geral de Proteção de Dados 16
3.2 Infraestrutura de TI 20
3.3 Arquitetura de referência 23
3.3.1 Exemplos de Modelos Arquiteturais 23
3.3.1.1 Arquitetura de referência de infraestrutura de TI: O RAModel 23
3.3.1.1 Arquitetura de referência de infraestrutura de TI: o NIST 25
3.3.1.2 Arquitetura de referência de infraestrutura de TI: Visão Geral 26
3.3.1.3 Arquitetura de referência de infraestrutura de TI: requisitos da LGPD 27
3.4 Normas ISO 27001/27701 30
3.4.1 Categorias de Controles ISSO 27701 32
3.5 Governança da Tecnologia da Informação 34
3.6 Segurança da Tecnologia da Informação 36
4 TRABALHOS RELACIONADOS 37
4.1 Considerações Finais 38
5 PROCEDIMENTOS METODOLÓGICOS 39
5.1 Modelo de Referência 40
5.2 Proposta de aplicação do modelo de referência em uma empresa pública 45
5.3 Validação da Proposta 45
6 ESTUDO DE CASO 47
6.1 Perfil da empresa 47
6.2 Avaliação por camadas do Modelo 48
7 CONSIDERAÇÕES FINAIS 51
REFERÊNCIAS 53
ANEXO 1 57

1 INTRODUÇÃO

A Lei 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD), “surgiu como um mecanismo para regular o tratamento de dados pessoais em território nacional permitindo a garantia dos direitos fundamentais de liberdade e privacidade de qualquer pessoa natural cujos dados aqui sejam tratados” (Morte et al., 2020).

No Art. 1º da Lei 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD) diz que esta Lei “dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (Brasil, 2018).

Segundo Sá (2019) “A LGPD criou um novo regramento para o uso de dados pessoais no Brasil, tanto online quanto off-line, nos setores privados e públicos.”. Mesmo o país tendo mais de 40 normas para a proteção à privacidade e aos dados pessoais, a LGPD vem agregar nesse setor onde a sociedade está cada vez mais movida a dados.

Segundo o autor, existindo uma Lei Geral, “o Brasil entraria nos 100 países que hoje são considerados adequados para proteger a privacidade e o uso de dados (Sá, 2019). Esses países possuem legislações que garantem um nível de proteção semelhante ou superior ao previsto pelo Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia e, as diferenças entre o Brasil e esses países incluem, principalmente, o tempo de implementação de normas rigorosas de proteção de dados.

No Art. 1º da Lei13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD) diz que esta Lei “dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (Brasil, 2018).

Como se observa, as disposições da LGPD sobre proteção de dados repercutem nas esferas públicas e privadas do direito. Considerando o número de escândalos de privacidade e a quantidade de dados pessoais que estão sendo coletados, processados e compartilhados com ou sem o conhecimento explícito do indivíduo, é razoável supor que esse compartilhamento não é totalmente atendido hoje.

Pode-se dizer que, entre a privacidade dos dados, a quantidade de dados pessoais e a tecnologia da informação, há um reconhecimento do papel crucial que a tecnologia da informação de uma organização desempenha na proteção de seus dados confidenciais, mas

muitas empresas ainda carecem de uma compreensão clara em que consiste exatamente sua infraestrutura de TI. Um equívoco comum é supor que essa infraestrutura apenas se refira à tecnologia e ao hardware usados para operar o funcionamento de uma organização.

A grande disseminação das informações mantidas em meio digital da sociedade, levou governos a proporem medidas de buscar preservação da privacidade ou de buscar regulamentar essa questão para segurança das pessoas. A lei LGPD estabelece um conjunto de requisitos e prazos para que as organizações possam implementar medidas que venham atender o que está vigente na lei.

Gerando grande impacto do ponto de vista para as organizações se prepararem e atender essa lei em vigor, que é a LGPD, tanto o que irá ser desenvolvido como o que já está estabelecido (legado). Particularmente em relação as infraestruturas que lidam com isso, existem uma série de ações que precisam ser tomadas para poder entrar em conformidade com a LGPD, com a emergência de questões complexas e desafiadoras, incluindo a questão de conformidade.

O setor público é um dos setores que mais trata de dados pessoais. Isso ocorre porque o governo coleta e armazena dados de cidadãos para diversos fins, como a prestação de serviços públicos, a fiscalização e a segurança pública. A conformidade da infraestrutura de TI com a LGPD é essencial para proteger os dados pessoais dos cidadãos, contra um conjunto diversificado de ameaças e riscos, incluindo ataques hostis, erros humanos, desastres naturais, estruturas falhas, entidades de inteligência estrangeiras e riscos de privacidade.

Isso significa que as organizações públicas devem implementar medidas para garantir que os dados pessoais sejam coletados, armazenados, tratados e eliminados de forma segura e em conformidade com a lei.

O desafio de alinhar uma infraestrutura de TI com a conformidade das regulamentações da LGPD é complexo. Esse alinhamento, muitas vezes, gera uma alta expectativa e muitas organizações não satisfazem, mas não compreendem os motivos dessa lacuna que ocorre por uma série de razões. Particularmente no que diz a respeito as infraestruturas de TI há um desafio de saber se elas estão ou não em conformidade para atender os requisitos legais dessa proteção de dados.

Alcançar conformidade com a LGPD não é algo trivial. As organizações devem implantar mecanismos que rastreiem e gerenciem seus dados. No entanto, adaptar sistemas e processos já em uso há bastante tempo requer esforços e investimentos para associar noções jurídicas de alto nível com noções técnicas de baixo nível, incorporando as leis na prática à realidade operacional

dos negócios no mais, muitas organizações não têm ideia de quais informações pessoais elas possuem e como elas estão sendo combinadas (Ujcich; Bates; Sanders, 2018).

Um caminho nesse sentido está em entender profundamente os requisitos da LGPD e possuir conhecimento técnico em infraestrutura de TI. Para verificar a conformidade, é necessário avaliar os processos de coleta, armazenamento e tratamento de dados pessoais, identificar riscos de segurança, implementar medidas como criptografia e definir políticas de privacidade.

Considerando a legislação, pauta-se, seguindo as normas vigentes, para desenvolver uma melhor infraestrutura de TI que esteja em conformidade com a utilização de dados no setor público, de uma forma segura e cautelosa para proteger os dados pessoais nos órgãos públicos.

A ausência de um esquema de dados em uma infraestrutura de TI pode levar a um cenário complexo e inacessível, tornando difícil identificar os dados pessoais coletados e tratados pela organização. Isso dificulta o cumprimento dos requisitos da LGPD, como a identificação dos titulares dos dados, o fornecimento de informações sobre o tratamento de dados e a adoção de medidas de segurança adequadas.

A ideia é propor uma modelo de referência de infraestrutura de TI que contemple seus principais elementos os controles de segurança baseada na norma ISO de modo que se possa realizar verificação da conformidade com a LGPD, de forma sistemática, que pessoas capacitadas possam um fazer o diagnóstico e obter resultados identificando possíveis falhas na aplicação e ou implementação dos requisitos da LGPD em órgãos públicos.

A pergunta norteadora deste trabalho foi: Como os órgãos públicos podem garantir a conformidade de sua infraestrutura de TI com as exigências da Lei Geral de Proteção de Dados (LGPD) e garantir a segurança das informações dos cidadãos? Além disso, diversos órgãos públicos enfrentam desafios como a utilização de sistemas legados desatualizados, que não atendem aos requisitos de segurança e privacidade exigidos pela LGPD, além da falta de integração entre os sistemas, dificultando o controle centralizado dos dados pessoais.

2 OBJETIVOS

2.1 OBJETIVO GERAL

Propor um modelo de referência e um processo de avaliação para a conformidade de infraestrutura em TI com a LGPD no setor público de TI

2.2 OBJETIVOS ESPECÍFICOS

- Apontar os elementos que devem ser abordados no programa de compliance de infraestrutura de TI no setor público;
- Identificar os requisitos necessários para a definição de criticidade da Infraestrutura de TI
- Elaborar a proposta de gestão e conformidade baseada em evidências.

3 FUNDAMENTAÇÃO TEÓRICA

3.1 Lei Geral de Proteção de Dados

A grande disseminação das informações mantidas em meio digital, levou governos a proporem medidas e preservação da privacidade, regulamentar essa questão para segurança das pessoas. A lei LGPD estabelece um conjunto de requisitos e prazos para que as organizações possam programar medidas que atenda o que está vigente na Lei (Lima, 2020).

Entende-se que a LGPD é uma resposta ao crescente volume de informações digitais e à necessidade de proteger a privacidade dos cidadãos em um ambiente de dados cada vez mais interconectado e suscetível publicamente, além de impor uma série de obrigações para empresas e órgãos públicos que processam dados pessoais, exigindo que implementem medidas adequadas para garantir a segurança e a confidencialidade das informações coletadas e armazenadas, incluindo o tratamento de dados sensíveis, que exige proteção adicional, considerando o potencial de impacto negativo na vida dos indivíduos caso haja falhas de segurança ou uso indevido (D'Oliveira et al., 2024).

Para as organizações, a conformidade com a LGPD representa uma mudança estrutural, pois implica na adoção de tecnologias avançadas de segurança, revisões nos processos de coleta e armazenamento de dados, alterando o respeito à privacidade como um valor central. Em muitas empresas, isso exige uma reestruturação de sistemas de software e uma implementação de infraestrutura de Tecnologia da Informação (TI) que suporte o armazenamento seguro e o tratamento ético dos dados.

Considerando que a LGPD entrou em vigor recentemente, empresas de diferentes setores e órgãos públicos ainda estão enfrentando desafios para adequarem seus sistemas de software e infraestrutura de TI em conformidade com a legislação vigente.

No setor público, a implementação da LGPD traz desafios específicos, especialmente no que se refere à complexidade e ao volume de dados que o governo lida em suas interações com os cidadãos. Muitos sistemas de órgãos governamentais foram desenvolvidos antes da vigência da LGPD e, por isso, não foram elaborados com requisitos de proteção de dados em mente e, com isso, adaptar esses sistemas envolve não apenas atualizações tecnológicas, mas também a capacitação de funcionários para que compreendam a importância da segurança dos dados e estejam preparados para adotar práticas que minimizem os riscos de vazamento (Voigt; Bussche, 2017).

A LGPD impõe o princípio de transparência, que exige que as empresas e entidades públicas informem claramente aos titulares dos dados sobre como suas informações estão sendo coletadas, utilizadas e armazenadas (Hoofnagle et al., 2019).

Para garantir essa transparência, é necessário implementar políticas de privacidade compreensíveis e acessíveis, o que muitas vezes implica na tradução de termos técnicos para uma linguagem mais clara e próxima do usuário comum. A lei também garante direitos aos titulares dos dados, como o direito de acesso, retificação e exclusão dos dados, ou que requer a criação de canais de atendimento eficientes para lidar com essas transações (Díaz, 2016).

Para as infraestruturas que lidam com isso, existem ações que precisam ser tomadas para entrarem em conformidade com a LGPD. Um aspecto importante em relação à implementação da LGPD diz respeito à segurança da infraestrutura em que opera os sistemas de informação de uma determinada organização (Laudon e Laudon, 2007).

De acordo com a LGPD devem ser adotadas medidas de segurança que envolve uma abordagem multidisciplinar, que engloba aspectos técnicos, organizacionais e jurídicos para proteger dados pessoais de acesso não autorizados (Brasil, 2018).

A Lei 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), surgiu como um mecanismo para regular o tratamento de dados pessoais em território nacional permitindo a garantia dos direitos fundamentais de liberdade e privacidade de qualquer pessoa natural cujos dados aqui sejam tratados (Morte, 2020).

Segundo a LPGD, dados pessoais são todos e qualquer informação relacionadas a pessoa natural identificada ou identificável (Brasil, 2018). Essa iniciativa adéqua a legislação brasileira aos regulamentos já aplicados em outros países, como é o caso da *General Data Protection Regulation (*GDPR), lei sancionada na União Europeia e na qual a LGPD se baseia.

A LGPD define como tratamento de dados qualquer operação realizada com dados pessoais, tais como: Coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, modificação, comunicação, transferência, difusão ou extração (Brasil, 2018).

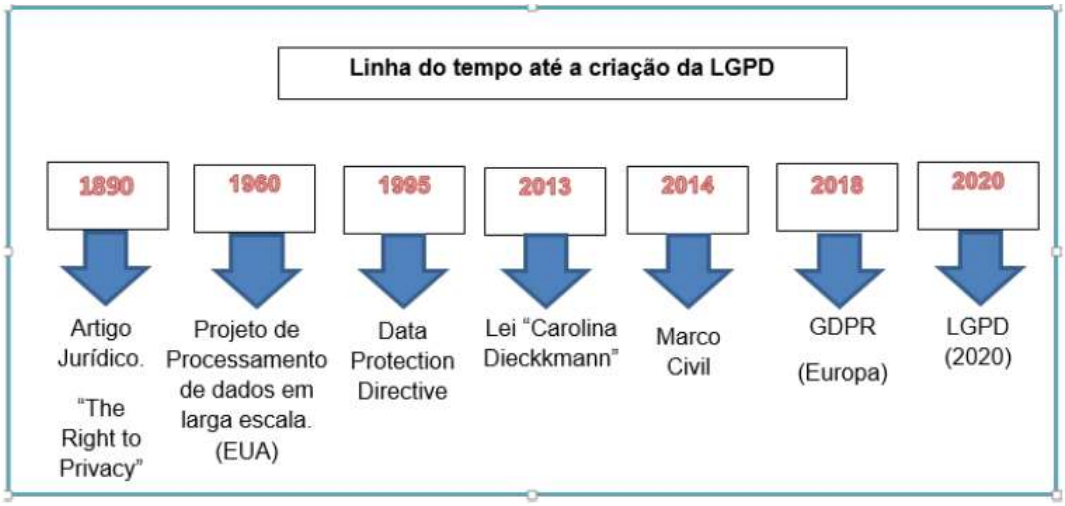
A Lei Geral de Proteção de Dados (LGPD), composta por 65 artigos divididos em 10 capítulos, é uma legislação brasileira que estabelece regras e diretrizes para o tratamento de dados pessoais no país. A LGPD define princípios fundamentais, direitos dos titulares dos dados, obrigações das organizações e penalidades por não conformidade.

Samuel Warren e Louis Brandeis publicaram o artigo jurídico The Right to Privacy na revista Harvard Law Review. Esta obra é reconhecida no meio jurídico como uma das mais

influentes na história dos Estados Unidos como a primeira publicação do país sobre a defesa do direito à privacidade, inaugurando o conceito “direito de ser deixado só” (right to be let alone) (Warren; Brandeis, 1890).

A Figura 1, sem o intuito de esgotar o tema, traz uma linha do tempo na qual é possível vislumbrar importantes marcos que contribuíram para o panorama atual no que concerne à proteção de dados pessoais. Outrossim, o primeiro artigo científico publicado com a finalidade da defesa do direito à privacidade é datado do ano de 1890, intitulado “The Right to Privacy”, são também destacados outros relevantes momentos, como a edição da Lei Carolina Dieckman, até a publicação da LGPD (Cruz, 2021).

Figura 1 – Acontecimentos antes da LGPD.



Fonte: Cruz (2021).

Em 2016, entrou em vigor na União Europeia (UE) o Regulamento Geral de Proteção de Dados (GDPR), com regras direcionadas à proteção de dados pessoais e à sua livre circulação. Devido ao pioneirismo e à relevância da proteção desses dados, o GDPR influenciou outros países a desenvolverem legislações voltadas para a proteção de dados pessoais (Brasil, 2018).

Conforme Sharma (2020), Diretiva de Proteção de Dados de 1995, a GDPR tem um duplo objetivo: por um lado, procura facilitar a livre circulação de dados pessoais entre os vários Estados-Membros da UE, e, por outro lado, estabelece um quadro de proteção dos direitos fundamentais, baseado no direito à proteção de dados no Artigo 8 da Carta dos Direitos Fundamentais da União Europeia (Weingartner, 2019).

O GDPR possui definição semelhante, de forma que um tratamento em conformidade com a GDPR também estará em conformidade com a LGPD. No Brasil, a primeira iniciativa mais geral relacionada a proteção de dados digitais se deu com a criação do chamado Marco Civil da Internet, a Lei 12.965, sancionada no ano de 2014, que estabelece diretrizes para o uso da internet no Brasil — princípios, garantias, direitos e deveres das partes no que tange ao uso da internet no Brasil (Brasil, 2014).

Pouco tempo depois, em 14 de agosto de 2018, já influenciada pela iniciativa europeia da GDPR, foi promulgada no Brasil a Lei nº. 13.709, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), iniciativa com foco na proteção de dados pessoais, que altera artigos relacionado ao tema do Marco Civil da Internet aprofunda a regulamentação da questão em uma lei específica (Brasil, 2018). Adotou os mesmos fundamentos da GDPR e, conforme Maciel (2019), "[...] busca um equilíbrio entre os novos modelos de negócio baseados no uso de dados pessoais e a proteção à privacidade".

A LGPD previa a entrada em vigor dos dispositivos legais em agosto de 2020, ou seja, deu-se um prazo de dois anos para as entidades envolvidas se adaptarem aos novos requisitos legais. A lei passa então a assegurar, em numerosos aspectos, a proteção de dados pessoais da pessoa natural, ao explicitar no cerne do seu texto, os princípios a serem adotados por quem realiza qualquer tipo de tratamento destes dados. Tal regulamentação no Brasil ocorreu, de certa forma, tardiamente em relação a países vizinhos, pois já havia à época legislação protetiva desta natureza na Argentina, pioneira no aspecto de proteção de dados, Chile, Colômbia, Peru e México (Bezerra, 2019).

A LGPD é um novo paradigma, pois envolve mudanças e alterações da maneira como as empresas vem utilizando os dados pessoais de pessoas físicas nos meios online e off-line e tem a função de proteger os direitos fundamentais de liberdade e privacidade em qualquer relacionamento que envolva dados pessoais (SÁ, 2019).

Segundo Lima (2020, p. 15),

> O Brasil possui diversas leis e diretrizes que tratam a proteção e privacidade dos dados, como o Marco Civil da Internet, Código do Consumidor, criando um cenário com diversas legislações e uma estrutura legal complexa. A LGPD substitui esse cenário complexo com muitas diretrizes, leis, e traz uma regulamentação específica para o uso, proteção e transferência de dados pessoais no Brasil.

A lei dispõe que as atividades de processamento de dados pessoais sigam aos seguintes princípios: objetivo, suficiência, necessidade, acesso livre, qualidade dos dados como:

transparência, segurança, prevenção, não discriminação, responsabilidade e contribuição, Art. 6º da Lei n°. 13.709 de 14 de agosto de 2018 (Brasil, 2018).

Os principais fatores que motivaram a criação de uma lei de proteção de dados foram (Sá, 2019): Uso cada vez maior de dados pessoais; O recurso mais valioso do mundo não é mais petróleo, mas dados. (The Economist); Era digital, redes sociais, “analytics”; Possibilidade de impactos nas vidas das pessoas, negócios e até eleições; Ausência de um marco regulatório nacional quanto à proteção de dados; Acontecimentos recentes e outros fatores; Cambridge Analytic; GDPR (General Data Protection Regulation - União Europeia); OCDE (Organização para a Cooperação e Desenvolvimento Econômico); Lei do Cadastro Positivo; Ano Eleitoral

A subseção a seguir corresponde sobre a infraestrutura de TI, onde será explanado desde a sua definição até os seus controles.

3.2 Infraestrutura de TI

Laudon e Laudon (2007) definem o conceito de infraestrutura de tecnologia da informação (TI) como a plataforma que sustenta todos os sistemas de informação da empresa composta por cinco elementos principais: hardware, software, tecnologias de gestão de dados, tecnologias de rede e telecomunicações e serviços.

As organizações públicas devem delinear medidas para garantir que os dados pessoais sejam coletados, armazenados, tratados e eliminados de forma segura e em conformidade com a lei bem como, implantar mecanismos que rastreiem e gerenciem seus dados. Costa (2022) afirma que os setores de Tecnologia da Informação (TI), tem por objetivo “implementar ações para que problemas como vazamento de dados, ou como informações de terceiros não prosperem”.

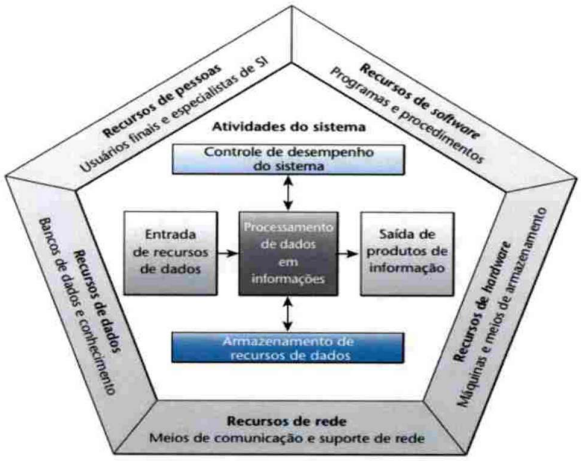
A conformidade com a legislação exige que as organizações desenvolvam uma infraestrutura segura e capaz de atender aos direitos e deveres previstos na LGPD, também enfatiza a importância de uma cultura organizacional que valorize a privacidade e a proteção de dados, envolvendo todos os colaboradores na conscientização e adesão às práticas adequadas de tratamento de dados (Costa, 2022).

Assim, as organizações públicas devem delinear medidas para garantir que os dados pessoais sejam coletados, armazenados, tratados e eliminados de forma segura e em conformidade com a lei bem como, implantar mecanismos que rastreiem e gerenciem seus dados. No entanto, adaptar sistemas e processos já em uso requer esforços e investimentos. O desafio de alinhar uma infraestrutura de TI com a conformidade das regulamentações da LGPD

é complexo, sendo preciso saber se elas estão ou não em conformidade para atender os requisitos legais dessa proteção de dados (Costa, 2022).

Esse alinhamento, muitas vezes, gera uma expectativa e a maioria das organizações públicas não se satisfazem ou compreendem os motivos dessa lacuna que, ocorre por uma série de razões, uma delas é compreender como os dados são coletados, armazenados e processados. Na Figura 2, se observa um modelo conceitual que demonstra os elementos necessários para que um sistema de informação receba recursos (dados) como entrada e os transforme em produtos (informações).

Figura 2 – Componentes de um sistema de informação.



Fonte: O´Brien (2004).

Para O'Brien (2004), um sistema de informação depende de recursos de pessoas (usuários finais e especialistas de TI), hardware (máquinas e meios de armazenamento de dados), software (programas e procedimentos), dados (bases de dados e conhecimento) e redes (meios de comunicação e suporte de rede) para realizar a entrada, processamento, saída, armazenamento e para controlar as atividades que convertem os recursos de dados em produtos de informação.

Um aspecto importante em relação à implementação da LGPD diz respeito a segurança da infraestrutura em que opera os sistemas de informação de uma determinada organização. De acordo com a LGPD devem ser adotadas medidas de segurança que envolve uma abordagem multidisciplinar, que engloba aspectos técnicos, organizacionais e jurídicos para proteger dados pessoais de acesso não autorizados. A conformidade com a legislação exige que as organizações

desenvolvam uma infraestrutura robusta, segura e capaz de atender aos direitos e deveres previstos na LGPD.

Os requisitos da LGPD que estabelecem que a infraestrutura deve ter os meios necessários para proteger os dados é o princípio da segurança (Art. 46). Esse princípio é um dos fundamentos da LGPD e visa garantir que os dados pessoais sejam tratados de forma segura, evitando acessos não autorizados, perdas, alterações, divulgações ou destruições acidentais ou ilícitas.

De acordo com o Artigo 46 da LGPD, o controlador dos dados pessoais (a organização ou pessoa responsável pelo tratamento dos dados) deve adotar medidas de segurança, técnicas e administrativas, que sejam adequadas ao estado da técnica e ao custo de implementação, para proteger os dados pessoais contra esses incidentes. Essas medidas devem ser proporcionais ao nível de risco que o tratamento dos dados apresenta para os direitos e liberdades dos titulares das informações.

Segundo Fernandes e Abreu (2014), é possível observar a infraestrutura de TI como uma espécie de "prédio". Em um prédio, a parte de cima se apoia na parte de baixo, construída anteriormente; assim, para que a parte de cima possa manter-se erguida, é necessário que a parte de baixo subsista, sendo ela a base necessária para que todo o resto do prédio se mantenha firme.

Trazendo a afirmação de Fernandes e Abreu (2014) e fazendo uma analogia para uma infraestrutura de TI, afirmam que o (1) primeiro nível seria o nível de infraestrutura física, que abrange todos os componentes físicos, químicos e elétricos responsáveis pela composição infraestrutura; sobre o componente físico, ergue-se o segundo nível (2), os componentes de *hardware*; embora o *hardware* seja algo eminentemente físico, ele diferencia-se por possuir diferentes tipos e arranjos elétricos, cumprindo diferentes papeis, nesta categoria inserem-se o processador, o HD, a memória, dentre outros componentes; subindo mais um nível (3) , chega-se aos softwares básicos que formam a base imaterial do sistema, estes softwares envolvem tanto o sistema operacional que será utilizado quanto "*sub-softwares*" que serão utilizados para desempenhar tarefas específicas do sistema, neste interim, têm-se a próxima camada (4), que é a camada de rede, esta camada contém os *switches*, roteadores, *firewalls* e *gateways* de segurança, responsável por interligar todos os elementos da infraestrutura; acima da camada de rede, têm se a camada de (5) serviços e (5.1) armazenamento, o nível de serviços abrange as ferramentas de monitoramento de desempenho, sistemas de gerenciamento de configuração, dentre outras coisas; o nível de armazenamento, por sua vez, abrange servidores físicos e

virtuais, que irão conter os bancos de dados e arquivos; (6) acima deste nível, têm-se o nível de aplicações, neste nível, incluem-se todas as aplicações que são relativas ao ofício ao qual aquela arquitetura se destina (por exemplo, se é uma arquitetura destinada a um sistema de saúde, ou a um sistema de trânsito, *etc.*); por fim, na última camada (7), têm se a interface, onde o usuário final tem acesso ao sistema.

3.3 Arquitetura de referência

Antes de se abordar o que é a arquitetura de referência, é necessário se oferecer alguns conceitos e parâmetros importantes para que a explicação acerca da arquitetura de referência se torne mais clara. De acordo com Bass et al. (2003), a palavra "arquitetura" serve para designar o ato de projetar algum elemento ou objeto cuja composição depende da interação de vários elementos e de subelementos que devem funcionar harmonicamente entre si para que o objeto cumpra a sua finalidade. Portanto, a arquitetura é um modo de se observar o sistema a partir de uma abstração de alto nível, fazendo com que haja uma diminuição entre a implementação do *software* e os seus consequentes requisitos (Bass et al., 2003).

Coadunando com o que foi afirmado por Bass et al. (2003), Clements e Northrop (2002) apontam que a arquitetura nada mais é do que uma espécie de instrumento cujo propósito é auxiliar o programador durante o desenvolvimento de um sistema, já que a arquitetura tem como princípio a representação e a organização gráfica dos elementos que envolvem as facetas importantes que devem ser levadas em consideração durante a implementação de um sistema. Ademais, a arquitetura também é um importante indicador da qualidade do sistema, já que quanto mais enxuta for a arquitetura, melhor tende a ser o desempenho do sistema.

3.3.1 Exemplos de Modelos Arquiteturais

3.3.1.1 Arquitetura de referência de infraestrutura de TI: O RAModel

Mesmo dentro da área da tecnologia, a arquitetura pode ser aplicada em diferentes níveis e *layers*. Por exemplo: em Nagakawa et al. (2012) é realizado um estudo acerca do RAModel: um modelo arquitetural que é utilizado como referência para a montagem de outros modelos de arquitetura que podem ser utilizados nos mais diversos sistemas. Destarte, o RAModel pode fornecer informações sobre os elementos e suas relações que podem estar contidos em arquiteturas de referência, não importando o domínio da aplicação ou a finalidade para qual aquela determinada arquitetura se dirige.

A etapa 1, segundo Nagakawa et al. (2012), é a identificação de fontes de informação. Os arquitetos responsáveis pelo projeto devem ter de maneira clara quais são as definições que eles buscam em arquitetura de referência, já que e acordo com os autores, o resultado final que será alcançado por eles irá depender das referências que eles possuem de arquitetura.

É com base em tais definições que, através da pesquisa em arquitetura de referência, o arquiteto irá ter o conhecimento sobre como projetar arquiteturas concretas de sistemas em um determinado domínio de aplicação; portanto, ela deve abordar as regras de negócios, estilos arquitetônicos (que lidam com atributos de qualidade na arquitetura de referência), melhores práticas de desenvolvimento de software (por exemplo, decisões arquitetônicas, restrições de domínio, legislação, regulamentos e padrões) e os elementos de software que apoiam o desenvolvimento de sistemas para aquele domínio.

Todos esses aspectos devem ser abrangidos por uma terminologia de domínio unificada, inequívoca e amplamente compreendida. Portanto, os elementos contidos nessas definições devem ser abordados pelo modelo de referência para arquiteturas de referência que é alvo da presente pesquisa: a LGPD.

Em outras palavras, uma arquitetura de referência é um modelo que define os componentes, padrões e melhores práticas recomendadas para a construção de sistemas ou infraestruturas que atendam a determinados requisitos. No contexto da LGPD, uma arquitetura de referência delineia a estrutura técnica e organizacional necessária para garantir a conformidade com os princípios e requisitos da legislação.

Arquitetura de referência é um modelo que fornece uma estrutura para o desenvolvimento e implementação de sistemas de TI. Ela pode ser usada para garantir que os sistemas sejam projetados e implementados de forma consistente e eficiente. Um modelo ou arquitetura de referência também pode fornecer uma linguagem comum e compartilhada entre os diferentes stakeholders envolvidos no desenvolvimento e implementação de sistemas, facilitando a comunicação e compreensão mútua (Rocco, 2001).

Segundo Rocco, (2001, p. 12),

> Porém, uma das maiores dificuldades da engenharia de requisitos reside na complexidade da própria atividade. Almeja-se uma compreensão completa e correta das necessidades, em atividades que participam os stakeholders.

De acordo com Rocco (2001), pode-se perceber que o desenvolvimento de software é caracterizado de acordo com as necessidades do usuário, isso é justamente o que acontece na

infraestrutura de TI e na arquitetura de referência, pois tem que se adequar a instituição e suas necessidades. Pode-se perceber que o domínio é uma infraestrutura de TI, que usa uma padronização de dados em setores. E como podemos padronizar o domínio dessa infraestrutura de dados em bases legais. Através do estudo podemos realizar e aprimorar a padronização de referência, ou seja, a arquitetura de referência.

Segundo Souza (2022, p. 20),

> A governança de dados (GD), se refere a todos os processos utilizados em uma organização para assegurar o controle e a transformação dos dados em informações. Um tema que vem sendo colocado com grande importância nas organizações, principalmente pelo fato de auxiliar o processo de conformidade, por exemplo, à Lei Geral de Proteção de Dados Pessoais (LGPD) e o reforço na importância do domínio, controle e uso dos dados, de forma segura e eficiente.

Ainda segundo o autor Souza, (2022, p. 22),

> No processo da Governança de Dados os frameworks facilitam a criação das diretrizes para a governança alinhada às boas práticas de gestão, sendo esse umas das principais vantagens de uso. Além de orientar e facilitar a implementação da GD, o uso de um framework auxilia na identificação de possíveis falhas e oportunidades na trajetória, possibilita a instalação gradual evitando ruídos, facilitando a divisão de tarefas e tudo com mais clareza. Como resultado ao final do processo, a empresa terá à disposição dados mais sólidos, mitigação de riscos e custos, satisfação do cliente, tomada de decisão assertiva e maior eficiência operacional.

3.3.1.2 Arquitetura de referência de infraestrutura de TI: O NIST

Arquitetura de referência de infraestrutura de TI com base nas Recomendações do Nacional Instituto de Padrões e Tecnologia o NIST (NIST, 2011). O Modelo de Referência Conceitual apresentado pelo NIST que apresenta um modelo de serviço chamado infraestrutura de nuvem como serviço (IaaS).

A arquitetura NIST é dividida em cinco domínios: Arquitetura de negócios: define os objetivos e processos de negócios da organização. Arquitetura de dados: define os dados utilizados pela organização e como eles são armazenados e gerenciados. Arquitetura de aplicativos: define os aplicativos utilizados pela organização e como eles são integrados. Arquitetura de infraestrutura: define o hardware, software e redes utilizados pela organização. Arquitetura de segurança: define as políticas e controles de segurança utilizados para proteger os sistemas de TI da organização.

Dentre os 5 domínios no qual focaremos no único domínio da Arquitetura de infraestrutura de infraestrutura de TI. E especificamente a Arquitetura de Referência de

Computação em Nuvem do Instituto Nacional de Padrões e Tecnologia (NIST, 2011) que é uma estrutura desenvolvida que fornece uma visão geral de alto nível dos principais componentes e relacionamentos em ambientes de computação em nuvem. Ele oferece uma abordagem estruturada para compreender e implementar serviços em nuvem. A arquitetura inclui vários componentes essenciais, como consumidores, provedores, serviço de nuvem, corretor de nuvem e operadora de nuvem. A arquitetura de referência do NIST visa padronizar e promover a interoperabilidade na computação em nuvem, permitindo que as organizações tomem decisões informadas e aproveitem efetivamente os serviços em nuvem, ao mesmo tempo em que enfatizam a segurança, a escalabilidade e a flexibilidade.

3.3.1.3 Arquitetura de referência de infraestrutura de TI: Visão Geral

Os ‘frameworks’, ou melhor a ‘estrutura’ oferece facilidade na criação das diretrizes para a governança dos dados e na infraestrutura de TI. E auxilia na identificação possíveis falhas, evita ruídos e facilita a divisão de tarefas. As empresas públicas e privadas dispõem sobre esta estrutura de governança de dados. A gestão dos dados com a infraestrutura de TI pode classificar atividades principais como planejamento e controle e isso propicia o entendimento da função estratégica dos dados da empresa ou instituições públicas, como no setor público.

Os elementos que devem ser abordados no programa de conformidade de infraestrutura de TI no setor público, é justamente o código de ética e conduta da instituição de acordo com a legislação aplicada no país, e na devida instituição ou setor público. Esta proposta de arquitetura de referência visa fornecer um guia para a verificação da conformidade de uma infraestrutura de TI com a LGPD no setor público.

As arquiteturas de referência podem ser uma ferramenta útil para o desenvolvimento e implementação de infraestruturas de TI que atendam aos requisitos da LGPD. No entanto, é importante ressaltar que as arquiteturas de referência não cobrem todos os requisitos da LGPD e identificá-las é muito importante.

Por exemplo, as arquiteturas de referência geralmente não abordam questões específicas de privacidade, como a anonimização de dados pessoais ou a criação de mecanismos de consentimento. Além disso, as arquiteturas de referência podem ser limitadas em termos de flexibilidade e adaptabilidade, o que pode dificultar o seu uso para atender às necessidades específicas de cada organização.

Para garantir a conformidade com a LGPD, as organizações devem considerar fatores adicionais além da arquitetura de referência, como: Os objetivos e processos de negócios da

organização. Os riscos de privacidade associados aos dados pessoais coletados, armazenados ou tratados pela organização. As necessidades específicas da organização em termos de flexibilidade e adaptabilidade.

A combinação de uma arquitetura de referência com uma abordagem personalizada é a melhor maneira de garantir que a infraestrutura de TI de uma organização esteja em conformidade com a LGPD.

3.3.1.4 Arquitetura de referência de infraestrutura de TI: requisitos da LGPD

A conclusão de quais artigos são relevantes para a infraestrutura de TI depende do contexto específico da organização, do tipo de dados que são processados e das práticas de tratamento de dados. Para determinar quais artigos se aplicam, é aconselhável realizar uma análise detalhada da infraestrutura de TI em conjunto com um advogado especializado em privacidade e proteção de dados. Além disso, é importante estar sempre atualizado sobre as regulamentações e diretrizes da ANPD, que podem fornecer orientações adicionais sobre a conformidade com a LGPD.

Os artigos da LGPD que compõe uma infraestrutura de TI são justificados pelo princípio da proteção de dados pessoais, que está previsto no artigo 2º da lei. Esse princípio estabelece que os dados pessoais devem ser tratados de forma lícita, justa e transparente, com o objetivo de proteger os direitos fundamentais dos titulares dos dados.

Os artigos da LGPD também são justificados pela necessidade de garantir a segurança e a privacidade dos dados pessoais. Os dados pessoais são informações sensíveis que podem ser usadas para identificar, rastrear ou prejudicar indivíduos. É importante proteger esses dados contra acessos não autorizados, uso indevido e divulgação.

Conclui-se que os artigos listados abaixo da LGPD, foram os mais relevantes para a proteção dos dados pessoais em uma infraestrutura de TI, foram baseados nos seguintes critérios:

Abordagem holística: os artigos devem abordar todos os componentes da infraestrutura de TI, incluindo hardware, software, redes e dados.

Relevância: os artigos devem ser relevantes para a proteção dos dados pessoais.

Conclui-se que os artigos da LGPD que compõe uma infraestrutura de TI são os seguintes artigos:

Artigo 3º: define os conceitos básicos da LGPD, incluindo os conceitos de infraestrutura de TI. O artigo define infraestrutura de TI como "o conjunto de componentes físicos, lógicos e organizacionais que suportam as operações de uma organização".

Artigo 5º, inciso I: estabelece que os dados pessoais devem ser tratados de forma lícita, justa e transparente. Esse artigo exige que as organizações coletem e tratem dados pessoais de forma legal e ética.

Artigo 6º: estabelece os princípios gerais de tratamento de dados pessoais, incluindo o princípio da segurança. O princípio da segurança exige que as organizações implementem medidas técnicas e organizacionais para proteger os dados pessoais contra acessos não autorizados, uso indevido e divulgação.

Artigo 7º: estabelece os direitos dos titulares dos dados, incluindo o direito de acesso aos dados pessoais. Esse direito exige que as organizações forneçam aos titulares dos dados acesso aos seus dados pessoais.

Artigo 18º: estabelece que o controlador deve adotar medidas técnicas e organizacionais para proteger os dados pessoais. Esse artigo exige que as organizações implementem medidas técnicas e organizacionais para proteger os dados pessoais contra acessos não autorizados, uso indevido e divulgação.

Artigo 38º: estabelece que o controlador deve informar os titulares dos dados sobre o tratamento de seus dados pessoais. Esse artigo exige que as organizações forneçam aos titulares dos dados informações sobre o tratamento de seus dados pessoais.

Artigo 39º: estabelece que o controlador deve manter registros de todas as operações de tratamento de dados pessoais. Esse artigo exige que as organizações mantenham registros de todas as operações de tratamento de dados pessoais.

Artigo 41º: estabelece que o controlador deve designar um encarregado de dados (DPO). O DPO é responsável por auxiliar o controlador no cumprimento da LGPD.

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

Art. 50: Os controladores e operadores poderão formular regras de boas práticas e de governança.

§ 1º Ao estabelecer regras de boas práticas

§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:

I - Implementar programa de governança em privacidade

II - Demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e promover o cumprimento desta Lei.

§ 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

Abrangência: os artigos devem ser abrangentes, cobrindo todos os aspectos relevantes da proteção dos dados pessoais.

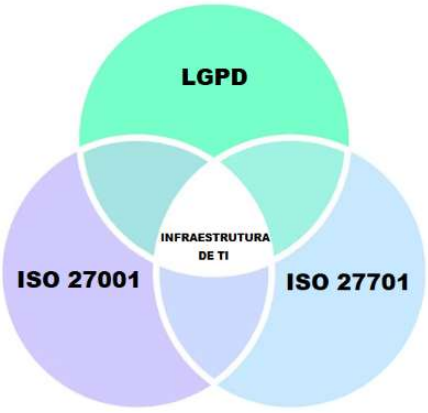
A LGPD e as ISO se configuram em características semelhantes, por isso, trouxemos essa figura 3 como ilustração, pois elas têm requisitos semelhantes e proporcionais em suas proposições. Na Figura 3, se tem as interseções da LGPD com as ISO 27001 e a ISO 27701.

A interseção entre os três elementos (LGPD, ISO 27001 e ISO 27701) representa a área em que a legislação e as normas se encontram para garantir a proteção de dados pessoais dentro da infraestrutura de TI.

Em outras palavras, a figura demonstra que a conformidade com a LGPD e a implementação das normas ISO 27001 e ISO 27701 são essenciais para garantir a segurança e a privacidade dos dados pessoais na infraestrutura de TI de uma organização.

Essa figura é uma representação visual clara e eficaz da interconexão entre os conceitos e da importância de uma abordagem integrada para a proteção de dados na infraestrutura de TI.

Figura 3 – A intersecção da LGPD com as ISO 27001 e a ISO 27701.



Fonte: Elaborado pelo autor (2024).

Ao combinar os requisitos da LGPD com os controles de segurança da ISO 27001, você terá um roteiro claro para verificar a conformidade da infraestrutura de TI de maneira sistemática e eficaz.

3.4 NORMAS ISO 27001 / 27701

Atualmente, existe uma tecnologia avançada, normas e códigos de boas práticas internacionais (ISO, por exemplo) relativas à infraestrutura necessária para a segurança e proteção da informação em casos de incidentes críticos e não críticos, assim como para a continuidade e recuperação do negócio. A infraestrutura mínima envolve terminais (clientes), servidores, *gateways*, rede física ou sem fio, *firewalls*, *switches*, etc., compondo um domínio técnico, trabalhoso de implantar e operar, principalmente em se tratando do setor público.

A norma ISO 27701 é uma extensão da ISO 27001, que é uma norma internacional de segurança da informação. A ISO 27701 se concentra na extensão de sistemas de gestão de segurança da informação para incluir requisitos de privacidade, fornecendo orientações sobre o gerenciamento de informações pessoais e o cumprimento de regulamentos de privacidade, como a LGPD.

A norma ISO 27701, é um código de controle de segurança que vem dando suporte as empresas e instituições a utilizarem a LGPD, na proteção dos dados e na gestão de privacidade da informação.

Segundo a norma ISO 27001,

> A norma ISO 27001 – Sistema de Gestão de Segurança da Informação é uma norma que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente o sistema de gestão em segurança da informação, enquanto a norma ISO 27701 – Sistema de Gestão da Privacidade da Informação é uma extensão da norma ISO 27001 - Código de prática para controles de segurança da informação, tem como objetivo adicionar novos controles ao sistema de gestão da informação para auxiliar as empresas na gestão de riscos de privacidade relacionados com dado pessoal (ABNT, 2006).

Segundo a Norma ISO 27001, [...] é importante destacar que é necessário implementar a ISO 27001 para que possa atender também a ISO 27701, porém não é possível implementar somente a ISO 27701 sem a ISO 27001. As duas normas podem ser implementadas simultaneamente possuem um único sistema de gestão (ABNT, 2006).

A ISO 27001 pode ajudar a atender às demandas do LGPD das seguintes maneiras. 1) Segurança: A LGPD propõe o uso adicional de sistemas de acreditação como ISO 27001 como uma garantia para garantir que a organização gerencie seus riscos de segurança de dados com eficiência. 2) Não apenas informações privadas: a ISO 27001 emprega estratégias globais que ajudariam empresas na criação de procedimentos que protegem não apenas os dados do cliente, mas todos os dados recursos, como dados mantidos digitalmente e no modo de formato impresso. 3) A estrutura e controles de segurança: A LGPD especifica que as organizações devem utilizar controles tecnológicos e operacionais para amenizar as ameaças reconhecidas, que a ISO 27001 também recomenda. 4) Pessoas, Processos e Tecnologia: As empresas podem salvaguardar sua organização não apenas contra ameaças baseadas em computador, mas também contra ameaças mais comuns desafios, incluindo funcionários mal treinados ou processos ineficientes. 5) Responsável: ISO 27.001 exige que a estrutura de segurança das empresas seja endossada pela alta gestão e integrados no estilo de vida e política da empresa. Também envolve a seleção de uma pessoa-chave responsável pelo sistema de gerenciamento de informações (ISMS). A LGPD define claramente a responsabilidade de segurança e privacidade em toda a empresa. 6) Risco de avaliação: A conformidade com a ISO 27001 implica avaliações periódicas de risco para definir desafios e fraquezas que podem influenciar os recursos de dados das organizações e estabelecer medidas para proteger tais informações. Explicitamente, uma avaliação de risco é necessária na LGPD para garantir que uma organização reconheça as fraquezas que podem afetar informação confidencial. 7) Melhorar continuamente: O ISMS implementado através da ISO 27001 exige que os negócios sejam continuamente acompanhados, revisados e avaliados, evoluindo à medida que a empresa progride através de uma abordagem de melhoria contínua. É assim implica que o ISMS deve evoluir à medida que as empresas reconhecem e diminuem continuamente ameaças. 8) Testes e inspeções: A conformidade com o LGPD implica que uma organização deve realizar testes e inspeções periódicas para demonstrar que sua estrutura de segurança funciona de forma eficiente. Um SGSI em conformidade com a ISO 27001 deve ser avaliado com frequência o que é consistente com as regras de auditoria interna estabelecidas na especificação. 9) Certificação: A LGPD exige que as empresas adotem as medidas necessárias para garantir que as medidas de proteção funcionem como pretendido. Obtendo a certificação ISO 27001 fornece uma avaliação independente e especializada sobre se a organização adotou políticas de proteção de dados apropriadas. (Lopes, Guarda & Oliveira, 2019).

De acordo com a ISO 27001, pode-se realizar os passos do ciclo PDCA (Planejar, Executar, Controlar e Agir), com isso, pode ser utilizada outras metodologias mais específicas, como sistemas de informação, infraestrutura de TI e modelos de referência para fins de avaliação de conformidade em organizações públicas.

Pode-se salientar que as organizações têm de estar em conformidade com a ISO 27001, pincipalmente com as cláusulas obrigatórias da norma, pois essa tem que ser seguida pelas instituições públicas.

Subseção a seguir refere-se as categorias e os controles.

3.4.1 Categorias de Controles ISO 27701

A norma ISO 27701 é específica e possui requisitos relacionados a sistemas e gestão da informação, proporcionando diretrizes a partir de controladores e operadores pessoais, a partir de seus requisitos. A norma ISO 27701 de 2020, propõe especificidades em seus requisitos,

> A norma ISO 27701 especifica requisitos relacionados ao SGPI (Sistema de Gestão da Privacidade da Informação) e diretrizes para os controladores e operadores de dados pessoais, atores com grandes responsabilidades no tratamento de dados. A ISO 27701 é uma extensão dos requisitos da ISO 27001 e de diretrizes da 27002, todos focados em privacidade da informação e complementando as demais normas de segurança da informação com seus requisitos específicos na ISO 27701, de 2020 (ABNT, 2020).

Os controles da ISO 27701 propõem diretrizes que são essenciais para a implementar um sistema de gestão de privacidade e proteção de dados em conformidade com a LGPD. Segundo Carvalho (2021) o conceito de segurança está ligado à identificação de vulnerabilidades em sistemas de computadores. Os usuários réprobos costumam explorar as vulnerabilidades desenvolvendo formas de ataques, com diferentes possíveis danos avaliados pelos riscos dos ataques.

A segurança se encarrega pela avaliação das vulnerabilidades e as possibilidades de ataques, considerando seus riscos, alcances e potenciais de dano encontrando medidas para aplicar modelos sólidos e definir propriedades de segurança satisfatório, colocando em prática formas de defesas e monitoramento dos sistemas para que se possa validar a estabilidade dos ambientes e eventuais correções necessárias.

De acordo com Nonato (2022), a ação em segurança tem a intenção de evitar a perda dos princípios da segurança da informação, ou seja, a confidencialidade, integridade,

disponibilidade e autenticidade. Nessa perspectiva, a proteção dos dados deve corresponder ao valor das informações e dos prejuízos que possa decorrer com o uso impróprio das informações.

Assim, segundo Goodrich e Tamassia, (2013, apud Carvalho, 2021) com o intuito de garantir a autenticidade de determinadas transações, os sistemas vinculam uma propriedade ou característica do indivíduo ao mundo real, garantindo que o usuário "logado" corresponda a determinado indivíduo. Entretanto, essa solução gera nos sistemas uma relação envolvendo as identidades dos indivíduos, estas relações intercambiáveis entre os inúmeros sistemas acabam inter-relacionando as plataformas, permitindo a criação de um perfil invasivo obtido pela coleta de dados desenfreada.

Podemos perceber que os controles das normas ISO 27001 (Sistema de Gestão de Segurança da Informação - SGSI) e ISO 27701 (Sistema de Gestão de Privacidade da Informação - SGPI), normas internacionais que tratam de segurança da informação e privacidade de dados, propõem elementos essenciais em consonância com a LGPD sendo assim, possível fazer um comparativo entre eles (Carvalho, 2021).

A ISO 27701 foi criada para complementar a ISO 27001, oferecendo controles mais detalhados e específicos voltados para questões de privacidade, no qual se verifica que a ISO 27001 tem um catálogo de 93 controles de gerenciamento de riscos e a ISO 27701 tem 114 controles de segurança, porém, nem todos são obrigatórios para alcançar a conformidade.

O foco da conformidade com a ISO 27001 e 27701 reside em compreender o nível de risco específico da organização e selecionar os controles mais adequados dentre os disponíveis, visando mitigar os riscos associados aos ativos de informação, dos quais seguem relacionados: A.11- Segurança de Operações, A.16.1.5- Gerenciamento de Incidentes de Segurança da Informação, A.12.3.1- Tratamento dos Direitos dos Titulares de Dados, A.12.1.2- Tratamento Justo e Lícito de Dados Pessoais, A.16.1.1- Processo de Melhoria, A.12.1.2- Política de Privacidade, A.7.2.2- Treinamento e Conscientização de Segurança da Informação, A.14.1.1 - Processamento de acordo com a Lei.

Dentro desse contexto podemos verificar e definir as camadas específicas de uma infraestrutura de TI em uma conformidade com a LGPD.

A camada de **Infraestrutura Física** diz respeito às medidas de segurança para proteger fisicamente locais que armazenam dados, como data centers e salas cofre. Isso inclui controle de acesso para impedir entrada não autorizada (vigilância e controle de entrada) e mecanismos para prevenir sinistros como incêndio e inundação.

Na camada de **Hardware** refere-se a utilização dos hardwares seguros e atualizados, adotando boas práticas como criptografia de dados **(**segurança do hardware), gerenciamento do ciclo de vida dos hardwares, incluindo uma verificação do ciclo de vida do hardware.

Na camada dos ***Softwares*** **Básicos** tem relação direta com sistemas operacionais (SO), software antivírus e anti-malware e registro de atividades que devem ser atualizados regularmente para corrigir vulnerabilidades de segurança e garantir a integridade e disponibilidade dos dados pessoais.

Na camada de **Rede** refere-se a parte da arquitetura de tecnologia da informação responsável pela interconexão de dispositivos, sistemas e serviços dentro de uma rede de computadores, responsável pela segurança de rede, segmentação de rede e criptografia de rede.

Na camada de **Aplicações** referem-se aos sistemas, softwares e aplicativos utilizados para processar, armazenar e gerenciar dados pessoais dentro da organização. Analisando fatores como gestão de consentimento, criptografia de dados, acesso baseado em funções, auditoria e rastreabilidade, políticas de retenção de dados etc.

Na camada de **Internet** refere-se à parte da arquitetura de tecnologia da informação que lida com a exposição de serviços, aplicativos e dados pessoais por meio da Internet ou de redes corporativas. Essa camada engloba todos os aspectos relacionados à disponibilização e interação com recursos online, como sites, portais, aplicativos e APIs.

Na camada de **Usuários** refere-se aos indivíduos que interagem com os sistemas e dados pessoais dentro da organização. Essa camada abrange todos os usuários autorizados que acessam, manipulam ou processam dados pessoais como parte de suas atividades diárias.

A de **Segurança da Informação** abrange uma série de medidas, controles e práticas de segurança destinadas a proteger os dados pessoais em todas as etapas do seu ciclo de vida.

Os usuários, segurança da informação e a governança de TI são elementos integrados e atuam transversalmente em todas as camadas para garantir a conformidade eficaz e a proteção dos dados pessoais à infraestrutura de TI (Vieira; Barreto, 2019).

3.5 Governança da Tecnologia da Informação

O termo “governança” vem da palavra grega *kubernan*, que significa navegação ou processo de continuamente orientar e ajustar, sendo o termo utilizado por muitas disciplinas, como Direito, Políticas Públicas, Medicina e, em especial, Administração. É um termo amplo usado em diferentes contextos de diversas óticas entre as áreas de estudo.

Governança refere-se a todos os processos de governar, sejam realizados por um governo, mercado ou rede; seja sobre uma família, tribo, corporação ou território; e seja por leis, normas, poder ou linguagem. Governança é um termo mais amplo do que governo porque se enfoca não apenas no estado e suas instituições, mas também na criação de regras e ordem nas práticas sociais (Carvalho, 2021). Ou seja, é um termo que, à primeira vista, refere-se somente a governos locais ou de países, porém, é algo maior e, para esta pesquisa, nos concentraremos no conceito de governança no âmbito das organizações.

De acordo com Roth *et al* (2012, p. 112), governança é uma definição

"[...] de regras, critérios para a tomada de decisão, responsabilidades e limites de autonomia e ação dos participantes. É criada pelas organizações envolvidas e ao mesmo tempo as afeta, pois implica a definição de regras que elas próprias devem cumprir [...]". Ou seja, refere-se a um modelo de prática que possui um conjunto de elementos que se fazem necessários ao sucesso das instituições.

Sendo assim, pode haver uma confusão com relação a diferença entre gestão e governança, no entanto "[...] o papel da governança não é gerir, mas delimitar a gestão [...]" (ROTH et al., 2012). Há vários tipos de governanças dentro da literatura e, para esta pesquisa, abordaremos a governança de tecnologia da informação e a de dados. A Governança de Tecnologia da Informação (TI), que surgiu com a intenção de governar estrategicamente os ativos de informação e tecnologia de informação de uma organização, sendo, portanto, conforme alguns autores, um desdobramento da Governança Corporativa (Weill; Ross, 2006).

Segundo Feely (2007), a governança de TI é algo complexo, não envolve apenas controle, gerenciamento de riscos e conformidade, mas também deve fortalecer o desempenho e a inovação. Portanto, encontrar o modelo de governança de TI é um alvo em movimento. A questão crítica é quem deve tomar decisões, posto que a governança de TI precisa ser um mecanismo para promover o diálogo entre a TI e a empresa, não um substituto para essa mediação, os órgãos de governança devem desempenhar quatro funções principais: auditoria, supervisão, treinamento e direção.

Na Governança de TI existe uma relação com o conjunto de políticas, processos e práticas estabelecidos para garantir que a gestão de TI esteja alinhada, tendo como objetivo principal assegurar que a organização esteja em conformidade com as normas e regulamentações de proteção de dados, promovendo uma cultura de responsabilidade, transparência e eficácia na gestão dos dados pessoais.

3.6 Segurança da Informação

Segundo Goodrich e Tamassia (Goodrich, 2013) o conceito de segurança está intimamente ligado à identificação de vulnerabilidades em sistemas de computadores. Os usuários mal intencionados costumam explorar essas vulnerabilidades permitindo desenvolver diversas formas de ataque, com diferentes potenciais de danos avaliados pelos riscos dos ataques.

A segurança então se posiciona como a guardiã que, avaliando as vulnerabilidades, as possibilidades de ataques, seus riscos, alcances, potenciais de dano e contramedidas, propõe modelos sólidos e define propriedades de segurança desejáveis, implementando e testando defesas efetivas e monitorando sistemas a fim de validar continuamente a estabilidade dos ambientes e eventuais correções, caso necessárias.

Ainda no capítulo introdutório de seu livro, Goodrich e Tamassia (Goodrich, 2013) apresentaram o anonimato como um conceito da segurança. Para os autores, a fim de garantir a autenticidade de determinadas transações (podemos acrescentar aqui o contexto de prevenção à fraude, onde essa característica é bastante explorada), os sistemas geralmente vinculam uma propriedade ou característica do indivíduo no mundo real (tal como a biometria), garantindo que, por exemplo, o usuário logado de fato corresponde a determinado indivíduo.

Entretanto, essa solução tem um efeito colateral, pois gera nos sistemas uma relação envolvendo as identidades dos indivíduos no mundo real. E estas relações intercambiáveis entre os inúmeros sistemas que utilizam nossos DP para tal acabam nos inter-relacionando entre as plataformas, permitindo a criação de um perfil invasivo obtido pela coleta de dados desenfreada (Goodrich, 2013).

A Segurança da Informação abrange uma série de medidas, controles e práticas de segurança destinadas a proteger os dados pessoais em todas as etapas do seu ciclo de vida.

A conformidade com a LGPD nas instituições públicas utiliza uma abordagem bem planejada para a infraestrutura de TI. Esta proposta de arquitetura de referência fornece os principais componentes que devem ser considerados para avaliar a conformidade de uma infraestrutura de TI com a LGPD e com os controles da ISO 27001 e ISO 27701.

A LGPD pode impactar a infraestrutura de TI de diversas maneiras, incluindo: A necessidade de implementar controles de segurança mais rigorosos para proteger os dados pessoais. A necessidade de implementar processos de governança de dados para garantir o cumprimento da LGPD. A necessidade de realizar auditorias de conformidade para verificar se a organização está em conformidade com a LGPD.

4 TRABALHOS RELACIONADOS

Neste Capítulo, iremos apresentar os trabalhos que mais se assemelham a proposta dessa dissertação. Os artigos citados fornecem informações relevantes para a implementação de um modelo de referência de infraestrutura de TI em conformidade com a LGPD. A combinação dessas informações pode ajudar, dentro de uma infraestrutura de TI, as organizações a proteger os dados pessoais.

Neste sentido, alguns esforços foram direcionados para representar o regulamento por meio de modelos conceituais visando a utilização deles para o desenvolvimento de soluções que estejam em conformidade com os requisitos regulatórios. A seguir, serão discutidos alguns trabalhos sobre o projeto em questão no contexto da conformidade da LGPD que influenciaram na construção da proposta dessa dissertação.

ISO/IEC 27001 de 2022 - É uma norma internacional que fornece uma estrutura para o gerenciamento de segurança da informação e estabelece os requisitos para um sistema de gestão de segurança da informação (SGSI). A nova versão que os novos cenários que as empresas devem enfrentar ela pode ser usado para avaliar a segurança de uma infraestrutura de TI, ajudado as organizações a atender aos requisitos da norma e identificar áreas onde melhorias podem ser feitas.

NIST *Cloud Computing Reference Architecture* - Esta publicação do *National Institute of Standards and Technology* (NIST, 2011) dos Estados Unidos que fornece diretrizes para controles de segurança para sistemas de informação. No qual também preconiza a implementação de controles de segurança para garantir a confidencialidade, integridade e disponibilidade dos dados. A sinergia com os princípios do NIST (2011) é evidente, com foco na segurança, privacidade e conformidade.

A Lei Geral de Proteção de Dados Pessoais Aplicada à Internet das Coisas: uma revisão sistemática. Renato Brito Costa, 2022. O artigo apresenta um uma revisão sistemática da literatura sobre a LGPD e a Internet das Coisas (IoT), e identifica os desafios e oportunidades para a proteção de dados pessoais na IoT, revelando pontos cruciais na interseção entre a conformidade com a LGPD/GDPR e a infraestrutura de TI, com destaque para a crescente relevância da Internet das Coisas (IoT). Convergindo na centralidade da segurança da informação como pilar fundamental da privacidade, essencial para a proteção de dados pessoais.

Lei Geral de Proteção de Dados e poder público, por Daniela Copetti Cravo; Daniela Zago Gonçalves da Cunda; Rafael Ramos, livro publicado em 2021. Este livro revela pontos cruciais na interseção entre a conformidade com a LGPD e a infraestrutura de TI, com foco no

setor público e destaca que o setor público lida com grande volume de dados pessoais, o que exige atenção redobrada na implementação da LGPD. E aborda a importância da infraestrutura de TI como base para a aplicação da LGPD no setor público, incluindo a necessidade de políticas de segurança e privacidade.

GDPR *compliance through standard security controls: An automated approach*, artigo publicado em 2024 por Granata D, Mastroianni M, Rak M, Cantiello P, Salzillo G. GDPR compliance through standard security controls: An automated approach. Que apresenta uma metodologia e ferramenta para auxiliar na seleção de controles de segurança para garantir a conformidade com o GDPR, utilizando controles de segurança padrão da NIST. Concomitantemente com o trabalho proposto no que diz a necessidade de medidas técnicas e organizacionais, importância da segurança da informação e foco na proteção de dados pessoais.

A compliant and secure IT infrastructure for the National Library of Greece in consideration of internet security and GDPR, artigo publicado por VAVOUSIS, Konstantinos et al. O artigo oferece *insights* valiosos sobre o tema, destacando a importância da segurança da informação e da privacidade dos dados pessoais.

É fundamental que empresas e órgãos públicos invistam em soluções de segurança cibernética e em treinamentos para seus funcionários, a fim de garantir a conformidade com a LGPD/GDPR e proteger os dados pessoais dos cidadãos.

4.1 CONSIDERAÇÕES FINAIS

Neste capítulo foram apresentados alguns modelos voltados às referências da infraestrutura de TI na conformidade com a LGPD.

Os modelos que abordam os conceitos principais do regulamento foram propostos com o intuito de servir como ponto de partida para o desenvolvimento de soluções automatizadas que verificam a conformidade com a lei, mas não abordam características diretas sobre a infraestrutura de TI. É válido ressaltar que os modelos possuem caráter genérico e não focam na resolução de questões de conformidade com a lei e a infraestrutura de TI.

Além disso, também não foram encontrados modelos de referência direcionado à infraestrutura de TI. Sendo assim, é nítida a necessidade de um modelo que guie a coleta de metadados essencialmente sobre os conjuntos de dados armazenados em uma infraestrutura de TI, os tratamentos aplicados sobre eles e adicionalmente, represente os conceitos básicos da lei brasileira.

5 PROCEDIMENTOS METODOLÓGICOS

Trata-se de uma pesquisa de natureza exploratória, do tipo estudo de caso. A presente pesquisa tem como procedimentos metodológicos, análise bibliográfica do tema e implementação de um sistema de validação dos dados, com o intuito de realizar a proposta da arquitetura de referência no processo de avaliação em conformidade com os dados pessoais para não ocorrer o compartilhamento indevido, sem autorização, seguindo a legislação vigente LGPD.

O estudo de caso constitui um método de pesquisa de um fenómeno social, através da análise de um contexto específico dessa realidade. No enquadramento da definição apresentada, é possível agregar uma diversidade de asserções, devido à grande variedade tipológica de estudos de caso e respetivos contextos de aplicação

Segundo Gil

(2008, p. 153), "[...] tratamento dos dados, a inferência e a interpretação, por fim, objetivam tornar os dados válidos e significativos."

Para realizar a validação deste Modelo, foi desenvolvido um estudo de caso com o objetivo de mensurar quais benefícios práticos podem ser obtidos ao aplicar as atividades propostas no Modelo, utilizando um questionário em anexo. O método usado para mensurar estes benefícios hipotéticos foi aplicado medidas de qualidade de dados na coleta de ingestão de dados, a fim de mensurar os resultados e validar o modelo de referência proposto.

Utilizando dados produtivos relacionados com o modelo de referência, foi realizada a ingestão de dados (através de um questionário em anexo a partir da extração dos dados de desse questionário). Resultantes dessa carga, foram tomadas medidas de qualidade de dados, que, segundo o exposto no referencial teórico deste trabalho, pode ser considerado um método de quantificar a utilidade do dado para mensurar e qualificar os órgãos de acordo com os critérios a seguir.

Critérios de Classificação

Conforme:

O órgão público atende integralmente aos requisitos da LGPD.

Existem evidências documentais e práticas que comprovam a conformidade.

Os controles de segurança e privacidade são eficazes e abrangentes.

Parcialmente Conforme:

O órgão público atende a alguns requisitos da LGPD, mas existem lacunas e áreas de melhoria.

Existem evidências parciais da conformidade.

Não Conforme:

O órgão público não atende aos requisitos da LGPD.

Não existem evidências da conformidade ou as evidências são insuficientes.

Os controles de segurança e privacidade são inexistentes ou inadequados.

No qual de acordo com os resultados obtidos das perguntas respondidas os critérios serão analisados e qualificados dando um somatório de forma que esses resultados implicarão, de acordo com os resultados, em uma nota que definirão em que patamar o órgão se classificará. Onde será identificado o problema e sua ação recomendada.

Tabela 1 - Mensuração utilizando os critérios de classificação.

Critérios	**Conforme**	**Parcialmente Conforme**	**Não Conforme**
Percentual de “SIM”	**70%**	**60%**	**50%**

Fonte: Elaborado pelo autor (2024).

No qual ao aplica-se o questionário e coletados os dados os resultados serão analisados e mensurados tomando como base os percentuais de “SIM” e “Não”, descartando “Não tenho conhecimento suficiente para responder.". Com isso o cálculo será da seguinte forma:

Somatório dos Critérios = Totais de “SIM” + Totais de “NÃO” = 100%

Percentual de "SIM" = (Totais de “SIM” dividido por Somatório dos Critérios) multiplicado por 100

Esse resultado indicará o percentual à ser utilizado para definir a classificação dos Critérios conforme tabela 1.

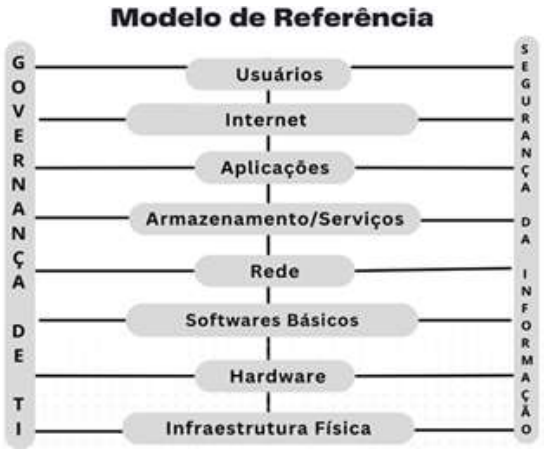
5.1 MODELO DE REFERÊNCIA

Nesta seção, apresenta-se, inicialmente, o esquema de um Modelo de Referência, que abrange as diferentes camadas da infraestrutura de TI, e logo após o mapeamento de requisitos da LGPD relacionadas com as normas ISO 27001/27701 dentro de uma infraestrutura de TI.

Podemos considerar que os requisitos da LGPD podem ser alinhados com as práticas recomendadas pelas normas de segurança da informação, auxiliando na efetivação de um programa abrangente de segurança e preservação de privacidade em dados. A afirmação de Fernandes e Abreu (2014) de que permite formular o modelo de referência proposto pode estar relacionada à ideia de que “uma infraestrutura de TI robusta e bem estruturada é fundamental

para garantir a conformidade com as normas de segurança e privacidade de dados, podemos formular o seguinte esquema (Figura 4):

Figura 4 – Modelo de referência.



Fonte: Elaborado pelo autor (2024).

O modelo de referência proposto abrange as diferentes camadas da infraestrutura de TI, correlacionando cada uma delas com os princípios e requisitos da LGPD. A camada de **Infraestrutura Física** deve atender aos requisitos mínimos necessários para garantir a execução eficiente e segura das operações. Em conformidade com as Subseções ISO 27001 / 27701 - A.11 - Segurança de Operações e sua relação com o Art. 46, inciso II, é necessário estabelecer controles específicos que assegurem a Segurança Física e do Ambiente, alinhando as práticas às normas exigidas.

Na camada de **Hardware** devem ser atendidos os requisitos e controles relacionados à segurança física e lógica dos dispositivos, incluindo a implementação de mecanismos para proteção contra falhas, acessos não autorizados e vulnerabilidades. Conforme descrito nas Subseções ISO 27001 / 27701 - A.16.1.5 - Gerenciamento de Incidentes de Segurança da Informação e no Art. 48 - Gestão de Incidentes e Violações, assegurando uma abordagem eficaz para o tratamento de incidentes relacionados aos dispositivos físicos.

Na camada dos **Softwares Básicos** devem ser atendidos os seguintes requisitos e controles para assegurar conformidade com a subseção A.12.3.1 - Tratamento dos Direitos dos Titulares de Dados da ISO 27001/27701 e os Artigos 18 a 21 da LGPD (Direitos dos Titulares).

Na camada de **Rede** devem ser atendidos os seguintes requisitos e controles para garantir conformidade com a subseção A.12.1.2 - Tratamento Justo e Lícito de Dados Pessoais da ISO 27001/27701 e os Artigos 2, 4, 6 e 46 da LGPD. Essas medidas visam assegurar a confidencialidade, integridade e a conformidade com os requisitos de segurança e proteção de dados pessoais.

Na camada de **Aplicações** devem ser atendidos controles que assegurem a conformidade com a subseção A.12.1.2 - Política de Privacidade da ISO 27001/27701 e os Artigos 3, 5, 10 e 52 da LGPD, que tratam da transparência, consentimento e segurança dos dados. Isso inclui a implementação de funcionalidades que garantam que o tratamento de dados pessoais seja realizado de forma transparente, com o devido consentimento dos titulares, além de assegurar a segurança das informações processadas pelas aplicações.

Na camada de **Internet** devem ser atendidos controles relacionados à subseção A.7.2.2 - Treinamento e Conscientização de Segurança da Informação da ISO 27001/27701 e ao Art. 39 da LGPD, que tratam da importância do treinamento e conscientização sobre segurança. Isso inclui a implementação de programas contínuos de capacitação para todos os usuários e funcionários, visando aumentar a conscientização sobre práticas seguras de navegação, proteção de dados pessoais e mitigação de riscos cibernéticos.

Na camada de **Usuários** devem ser atendidos controles que garantam o processamento de dados em conformidade com a Lei, conforme a subseção A.14.1.1 da ISO 27001/27701 e os Artigos 6 e 18 da LGPD, que tratam da autonomia informativa e consentimento. Isso inclui garantir que os usuários tenham o controle sobre seus dados pessoais, com a devida transparência sobre como suas informações são coletadas e utilizadas, e assegurando que o consentimento para o tratamento de dados seja obtido de forma clara, livre e explícita, respeitando a autonomia do titular dos dados.

No contexto da LGPD, um Modelo de Referência delineia a estrutura técnica e organizacional necessária para garantir a conformidade com os princípios e requisitos da legislação. Trazendo esse mapeamento entre controles e requisitos gerando um modelo de referência proposto que podemos observar na Tabela 2.

Tabela 2 – Modelo de referência.

Subseções ISO 27001 / 27701	Modelo de Referência	Artigos da LGPD
A.11 - Segurança de Operações.	Infraestrutura Física	Art. 46, inciso II. Segurança Física e do Ambiente.
A.16.1.5 - Gerenciamento de Incidentes de Segurança da Informação.	Hardware	Art. 48 - Gestão de Incidentes e Violações.
A.12.3.1 - Tratamento dos Direitos dos Titulares de Dados.	Softwares Básicos	Art. 18 a 21 - Direitos dos Titulares.
A.12.1.2 - Tratamento Justo e Lícito de Dados Pessoais.	Rede	Art. 2, 4, 6 e 46 – Segurança e compatibilidade do tratamento.
A.16.1.1 - Processo de Melhoria.	Armazenamento e Serviços	Art. 5, XVII - Avaliação de Riscos, auditorias Internas.
A.12.1.2 - Política de Privacidade.	Aplicações	Art. 3, 5, 10 e 52 - Transparência e Consentimento e segurança dos dados.
A.7.2.2 - Treinamento e Conscientização de Segurança da Informação.	Internet	Art. 39 Treinamento e Conscientização.
A.14.1.1 - Processamento de acordo com a Lei.	Usuários	Art. 6, 18, 39 - Autonomia informativa, consentimento.

Fonte: Elaborado pelo autor (2024).

A Tabela 2 faz um comparativo de requisitos da LGPD relacionada com as normas ISO 27001/27701 dentro de uma infraestrutura de TI. Observa-se que os requisitos da LGPD foram refinados em conjunto com os controles ISO/IEC 27001/27701 e requisitos da norma.

Uma análise comparativa identificou semelhanças e redundâncias entre os requisitos da LGPD mais relevantes para a proteção de dados pessoais em uma infraestrutura de TI. Esses requisitos foram categorizados para eliminar duplicidades, mantendo uma versão adequada. A seleção foi baseada em uma abordagem holística, relevância e abrangência, resultando na escolha dos requisitos mais importantes para proteger dados pessoais em conformidade com a LGPD.

A tabela 2 é o resultado de uma abordagem estruturada para mapear os requisitos da LGPD (Lei Geral de Proteção de Dados) nas camadas de uma infraestrutura de TI típica, considerando também os controles e as melhores práticas das normas ISO 27001 e ISO 27701.

Identificação das Camadas da Infraestrutura de TI:

O texto define camadas distintas dentro de uma infraestrutura de TI: Infraestrutura Física, Hardware, Softwares Básicos, Rede, Aplicações, Internet, Usuários.

Essas camadas representam uma visão abrangente de um ambiente de TI, desde a segurança física dos data centers até a interação dos usuários com os sistemas.

Seleção dos Artigos Relevantes da LGPD:

Os artigos da LGPD mais pertinentes à proteção de dados pessoais dentro de cada camada da infraestrutura de TI.

Essa seleção foi orientada por dois critérios principais:

Abordagem holística: Garantir que os artigos abordem todos os componentes da infraestrutura de TI (hardware, software, redes etc.).

Relevância: Priorizar os artigos que tratam diretamente da proteção dos dados pessoais.

Por exemplo, o Art. 46, que determina medidas de segurança, é vinculado às camadas de "Infraestrutura Física" e "Rede" porque essas camadas são cruciais para a implementação de controles de segurança.

Mapeamento das Subseções das Normas ISO 27001/27701:

Reconhecendo o alinhamento entre os requisitos da LGPD e as normas ISO, o(s) autor(es) mapearam as subseções relevantes das normas ISO 27001 e ISO 27701 para as camadas correspondentes da infraestrutura de TI.

A ISO 27001 fornece uma estrutura para o gerenciamento da segurança da informação, enquanto a ISO 27701 a estende para o gerenciamento de informações de privacidade.

Esse mapeamento aproveita os controles e as melhores práticas estabelecidas pelas normas ISO para fornecer orientação prática para a conformidade com a LGPD.

Por exemplo, "A.11 - Segurança de Operações" da ISO 27001, que trata da segurança operacional, é mapeada para a camada de "Infraestrutura Física", pois a segurança física é um aspecto fundamental das operações.

A tabela 2 também é um resultado desse processo de mapeamento. Ela organiza sistematicamente as relações entre: Camadas da Infraestrutura de TI (Modelo de Referência); Artigos Relevantes da LGPD: Subseções Correspondentes das Normas ISO 27001/27701.

Essa estrutura fornece uma visão clara e concisa de como os requisitos da LGPD se traduzem em ações e controles específicos em diferentes partes de uma infraestrutura de TI, e como as normas ISO podem apoiar sua implementação.

Sendo uma ferramenta que preenche a lacuna entre os requisitos legais (LGPD) e a implementação prática (infraestrutura de TI), utilizando normas estabelecidas (ISO 27001/27701) como um arcabouço para ação. Ela simplifica a complexa tarefa de alcançar a conformidade com a LGPD, fornecendo uma abordagem estruturada e organizada.

5.2 PROPOSTA DE APLICAÇÃO DO MODELO DE REFERÊNCIA EM UMA EMPRESA PÚBLICA

Foi apresentado um modelo de referência, que fornece uma visão integrada de alto nível da organização, sua tecnologia e seus dados, utilizado como referência para a construção da proposta como solução ao problema de pesquisa abordado nesse trabalho oferecendo uma base estruturada à conformidade com a LGPD.

Este modelo de referência proposto abrange as diferentes camadas da infraestrutura de TI, correlacionando cada uma delas com os princípios e requisitos da LGPD. A segurança da informação e a governança de TI são elementos integrados em todas as camadas para garantir a conformidade eficaz e a proteção dos dados pessoais. A implementação de uma arquitetura de infraestrutura de TI eficaz é essencial para o setor público. A proposta apresentada nesta seção fornece um modelo de referência que pode ser usado para melhorar a eficiência, confiabilidade e segurança da infraestrutura de TI do setor público.

5.3 VALIDAÇÃO DA PROPOSTA

A etapa de validação da proposta apresentada nesta pesquisa tem como objetivo principal verificar sua aplicabilidade, relevância e aderência às necessidades identificadas no contexto estudado. Para isso, foram adotados métodos qualitativos e quantitativos que permitiram avaliar a conformidade da infraestrutura de TI com os requisitos estabelecidos pela Lei Geral de Proteção de Dados (LGPD).

Aplicação Prática no Setor Público: O modelo de arquitetura de referência proposto foi implementado em uma organização pública piloto, selecionada com base na disponibilidade de dados e interesse em adequação às normas da LGPD. Durante a implementação, foi possível identificar pontos fortes e limitações da proposta, além de avaliar o alinhamento com os elementos-chave de conformidade. O estudo foi realizado em três etapas:

1. **Coleta de Dados**: Análise documental: políticas, procedimentos e registros da empresa. Entrevistas com gestores de TI, segurança da informação e DPO (Encarregado de Proteção de Dados). Auditoria nos sistemas e processos relacionados ao tratamento de dados pessoais.
2. **Avaliação Baseada no Modelo de Referência**: Utilização de um checklist (ANEXO 1) para verificar o atendimento a cada camada. Classificação dos itens em: Conforme, Parcialmente Conforme e Não Conforme.
3. **Análise Crítica e Propostas de Melhoria**: Consolidação dos resultados. Elaboração de um plano de ação para suprir as lacunas.

6 ESTUDO DE CASO

6.1 Perfil da empresa

As empresas públicas avaliadas atuam no setor de serviços essenciais e possui uma infraestrutura de TI robusta, com servidores internos e uso de nuvem para armazenamento de dados, além de apresentar uma base significativa de dados pessoais, incluindo dados sensíveis, como informações pessoais e dados financeiros. Ainda, a empresa C possui um DPO designado, mas com recursos limitados para atuação de forma ampla.

Fazendo a análise com os dados (removendo a categoria "Não tenho conhecimento suficiente para responder"), teremos os seguintes resultados:

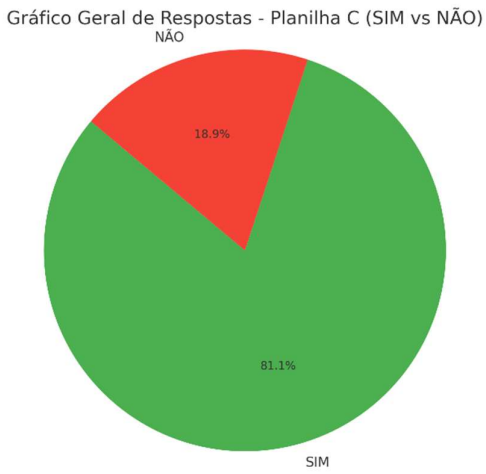
Tabela 3 - Critérios e Validação das Empresas

Empresa	Total SIM	Total NÃO	Total Respostas	% SIM	Classificação
Empresa C	158	41	199	79.40%	Conforme
Empresa D	89	53	142	62.68%	Parcialmente Conforme

Fonte: Elaborado pelo autor (2024).

Cálculos Detalhados:

Empresa C:

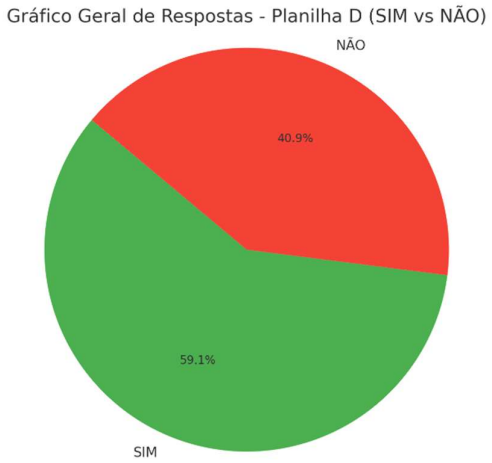


Total de Respostas: 158 (SIM) + 41 (NÃO) = 199

Percentual de "SIM": (158 / 199) * 100 = **79.40%**

Classificação: Como 79.40% é maior ou igual a 70%, a Empresa Y é classificada como: **CONFORME**

Empresa D:



Total de Respostas: 89 (SIM) + 53 (NÃO) = 142

Percentual de "SIM": (89 / 142) * 100 = **62.68%**

Classificação: Como 62.68% está entre 60% e 69.99%, a Empresa X é classificada como: **PARCIALMENTE CONFORME.**

Conclusão:

De acordo com a sua metodologia revisada, baseada no percentual de respostas "SIM" (desconsiderando "Não tenho conhecimento suficiente para responder"):

A Empresa D apresenta um percentual de "SIM" de 62.68%, o que a classifica como **Parcialmente Conforme** em relação aos resultados da aplicação Modelo de referência, indicando que atende a alguns requisitos, mas existem lacunas e áreas de melhoria nos controles de segurança e privacidade.

A Empresa C apresenta um percentual de "SIM" de 79.40%, o que a classifica como **Conforme** em relação aos resultados da aplicação Modelo de referência, sugerindo que atende integralmente aos requisitos, com evidências documentais e práticas de conformidade e controles de segurança e privacidade eficazes e abrangentes.

6.2 Avaliação por camadas do Modelo

Na Tabela 4, observa-se os resultados obtidos no estudo de caso, que, embora algumas áreas demonstraram um nível satisfatório de conformidade, outras necessitam de atenção e ações corretivas.

Tabela 4 – Resultados do Estudo de Caso: Avaliação da Conformidade com a LGPD.

Camada	Status	Problema identificado	Ação recomendada
Usuários	Parcialmente conforme	Falta de treinamentos regulares para colaboradores sobre a LGPD	Implementar um programa de capacitação periódica para todos os níveis
Internet	Conforme	-	-
Aplicações	Parcialmente conforme	Algumas aplicações internas não possuem registros de auditoria adequados	Atualizar os sistemas para incluir funcionalidades de log.
Armazenamento/Serviços	Não conforme	Dados pessoais armazenados sem criptografia adequada	Implementar criptografia ponta a ponta para os dados armazenados
Rede	Parcialmente conforme	Segmentação insuficiente da rede interna	Revisar a arquitetura de rede para isolar dados sensíveis
Softwares Básicos	Conforme	-	-
Hardware	Parcialmente conforme	Falta de controle rigoroso no descarte de equipamentos antigos	Implementar um processo de descarte seguro de hardware
Infraestrutura Física	Conforme	-	-

Fonte: Própria (2024), com base no estudo de caso nas empresas públicas.

Os resultados demonstram que a empresa pública D possui uma base sólida em algumas áreas, mas precisa investir em melhorias em outras para atingir a conformidade total com a LGPD. As não conformidades identificadas, especialmente a falta de criptografia no

armazenamento de dados e a segmentação insuficiente da rede, representam riscos significativos para a privacidade dos dados pessoais (Alessi et al., 2021).

Com base nos resultados obtidos, algumas propostas de melhorias podem ser realizadas, como por exemplo, treinamento contínuo, criando programas de capacitação em proteção de dados para os colaboradores, reforço na segurança de dados, implementando criptografia ponta a ponta e segmentação de rede, atualização de aplicações, garantindo que todos os sistemas internos tenham funcionalidades de registro de auditoria e, gestão de Hardware, adotando boas práticas para o descarte seguro de dispositivos (Danezis et al., 2015; Voigt; Von Dem Bussche, 2017).

A implementação das ações recomendadas é necessária para mitigar esses riscos e garantir o cumprimento da LGPD. Além disso, é importante que a empresa adote uma abordagem contínua para a conformidade com a LGPD, com revisões e atualizações periódicas de suas políticas, procedimentos e controles de segurança. A alocação de recursos adequados para o DPO é fundamental para que ele possa desempenhar seu papel de forma eficaz na promoção da cultura de privacidade e no monitoramento da conformidade com a LGPD (Machado, 2024).

7 CONSIDERAÇÕES FINAIS

A segurança da informação é de suma importância para as instituições públicas e não importa o tamanho da qual está inserida, manter a segurança dos dados e protegê-los através da infraestrutura de TI das organizações e estar em conformidade com a ISO 27001, principalmente com as cláusulas obrigatórias da norma, é uma obrigação que tem de ser seguidas pelas instituições públicas.

A proposta desse trabalho é de grande relevância para o setor público, principalmente de infraestrutura de TI, pois, algumas mudanças significativas estão alicerçadas nas ações de incremento de infraestrutura tecnológica. Cabe ressaltar que este modelo é uma base para produção de um instrumento de verificação de conformidade da LGPD em organizações públicas, devendo ser ainda validado em estudo de caso.

Um aspecto relevante sobre as ações de incremento de infraestrutura tecnológica é que elas devem atender às necessidades dos usuários internos e externos, em conformidade com a LGPD, pois, a insuficiência de um esquema de dados em uma infraestrutura de TI pode gerar dificuldades na identificação de dados pessoais coletados e tratados pela organização, levando ao descumprimento dos requisitos da LGPD.

A partir dessas discussões, infere a importância de um modelo de referência de uma infraestrutura de TI que contemple seus principais elementos, situando os controles de segurança baseada na norma ISO de modo que, se possa realizar verificação da conformidade de uma forma sistemática, onde qualquer pessoa capacitada possa obter resultados semelhantes quando repetido por diferentes órgãos públicos.

Nesse sentido, há necessidades dos órgãos públicos se aprofundem sua compreensão sobre a infraestrutura de TI para otimizar seus recursos e serviços, pois podem se deparar com alguns equívocos, um deles é supor que essa infraestrutura apenas se refira à tecnologia e ao hardware, usados para operar o funcionamento de uma organização.

Um caminho possível para solucionar tal problema está em entender profundamente os requisitos da LGPD e possuir conhecimento técnico em infraestrutura de TI. O resultado desse trabalho sugere que este modelo sirva como um guia para outros órgãos e que este estudo seja mais aprofundado, pois servirá como base para trabalhos futuros e aprimoramento das melhorias da conformidade com a LGPD e um processo de avaliação dentro de um órgão público em uma infraestrutura de TI.

A avaliação da conformidade com a LGPD na empresa pública revelou um cenário misto, com pontos fortes na infraestrutura física, softwares básicos e internet, mas com lacunas críticas

em usuários (falta de treinamento), aplicações (ausência de logs de auditoria), armazenamento/serviços (falta de criptografia) e rede (segmentação insuficiente). As implementações prioritárias do plano de ação, com foco nessas áreas deficientes, juntamente com a conscientização dos usuários, o fortalecimento da governança em privacidade e o suporte ao DPO, são cruciais para mitigar os riscos à privacidade dos dados pessoais e garantir a conformidade contínua com a LGPD.

Espera-se que com aplicação do proposto as instituições públicas melhores suas análises com relação ao atendimento da conformidade com a LGPD. E quais benefícios práticos poderão ser obtidos ao aplicar as atividades propostas.

REFERÊNCIAS

ABNT NBR ISO/IEC 27001:2022 - Tecnologia da informação - Técnicas de Segurança - Sistema de gestão de segurança da informação - Requisitos.

ABNT NBR ISO/IEC 27701:2019. Técnicas de segurança — Extensão da ABNT NBR ISO/ IEC 27001 - Gestão da privacidade da informação.

ALESSI, A.; CICCARELLI, G.; CIPOLLI, L.; GUIDOTTI, L.; MARSANO, A.; HANGANU, A. **Privacy by design and by default in software development in order to prevent unlawful processing of personal data**. Privacy certifications impact on software development and liabilities. 2021.

BEZERRA, M. R. B. Autoridade Nacional de Proteção de Dados Pessoais: A importância do modelo institucional independente para a efetividade da lei. **Caderno Virtual**, v. 2, n. 44, 2019.

BRASIL **Lei n. 13.709, de 14 de agosto de 2018**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em fevereiro 2024.

CARVALHO, A. P. **Proposta de um Framework de Compliance à Lei Geral de Proteção a Dados Pessoais (LGPD): Um estudo de caso para prevenção a fraude no contexto de Big Data.** Dissertação de Mestrado Profissional Universidade de Brasília, Faculdade de Tecnologia. Departamento de Engenharia Elétrica Brasília, 2021.

COSTA, R. B. **A Lei Geral de Proteção de Dados Pessoais Aplicada à Internet das Coisas:** uma revisão sistemática. 2022. Trabalho de Conclusão de Curso. Monografia, (Bacharelado em Engenharia de Computação) - Universidade Federal do Ceará, 2022.

CRAVO, D. C.; CUNDA, D. Z. G.; RAMOS, R. **Lei Geral de Proteção de Dados e poder público.** Porto Alegre: Escola Superior de Gestão e Controle Francisco Juruena; Centro de Estudos de Direito Municipal, 2021.

CRUZ, D. C. S. **A lei geral de proteção de dados pessoais (LGPD): contribuições sobre o uso e proteção de dados para as instituições de ensino.** 2021.

FERNANDES, A. A.; ABREU, V. F. **Implantando a governança de TI:** da estratégia à gestão dos processos e serviços. Rio de Janeiro: Brasport, 2014.

GIL, A. C. **Como Elaborar Projetos de Pesquisa.** 4.ed. Ed. Atlas, 2008.

GRANATA D, MASTROIANNI M, RAK M, CANTIELLO P, SALZILLO G. GDPR compliance through standard security controls: An automated approach. Journal of High Speed Networks. 2024;30(2):147-174. doi:10.3233/JHS-230080.

ISO CENTRAL SECRETARY. **Information technology — security techniques — information security management systems — requirements**. Standard ISO/IEC TR 27001:2022, International Organization for Standardization, Geneva, CH.

LAUDON, K. C.; LAUDON, J. P. **Sistemas de Informação Gerenciais. Tradução Telma Guimarães. Revisão técnica: Belmiro**. N. João 7, 2007. Ed. São Paulo.

LIMA, V. H. P. **LGPD Análise dos Impactos da Implementação em ambientes corporativos: estudo de caso**. 2020. Monografia (Trabalho de Conclusão de Curso à Escola de Ciências Exatas e da Computação) - Pontificia Universidade Católica de Góias. Goiânia, 2020.

MORTE, A. B.; MEIRA, A.; COSTA, R.; MARIZ, D. **Uma análise sobre o uso de dlts no tratamento de dados pessoais: Aderência aos princípios e direitos elencados na lgpd.** In: Anais do III Workshop em Blockchain: Teoria, Tecnologia e Aplicações. Porto Alegre, RS, Brasil: SBC, 2020. p. 74–87.

NIST Cloud Computing Reference Architecture Recommendations of the National Institute of Standards and Technology Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Badger and Dawn Leaf, (NIST, 2011).

NONATO, R. S. **Gestão da Informação e Sistemas de Gestão de Segurança da Informação: Modelo para a garantia de disponibilidade em processos de contratação**. UFMG. Belo Horizonte, 2022.

OLIVEIRA, M. A. L. **Formação de uma infraestrutura de informação para telerradiologia:** uma série de estudos de caso baseados na teoria de projeto para complexidade dinâmica. 2015. Dissertação (Sistemas de Computação) - Centro de Informática da Universidade Federal da Paraíba. João Pessoa, 2015.

ROCCO, G. E. **Um Modelo de Estruturação de Requisitos para o Método Fusion. Dissertação de Mestrado**. 2001. Universidade federal do Rio Grande do sul. Programa de Pós-Graduação em Computação. Porto Alegre.

SÁ, M. D. **Análise do Impacto da Nova Lei de Proteção de Dados Pessoais nas aplicações de Internet das coisas: Aplicações mobile do governo.** 2019 UFMG. Brasília.

SHARMA, S. **Data Privacy and GDPR Handbook**. Hoboken: John Wiley & Sons, 2020.

SOUZA, N. V. D. **Governança de dados em organização pública:** um estudo de caso sobre a cultura de orientação a dados. 2022. Monografia (Trabalho de Conclusão de Curso) - Universidade Federal de Pernambuco. Recife, 2022.

VIEIRA, J. B. B.; SOUZA, R. T. **Governança, gestão de riscos e integridade.** 2019. Brasília.

VAVOUSIS, Konstantinos et al. A compliant and secure IT infrastructure for the National Library of Greece in consideration of internet security and GDPR. Qualitative and Quantitative Methods in Libraries, [S.l.], v. 9, n. 2, p. 219-236, july 2020. ISSN 2241-1925.

VOIGT, P.; VON DEM BUSSCHE, A. The eu general data protection regulation (gdpr). **A Practical Guide, 1st Ed., Cham: Springer International Publishing**, v. 10, n. 3152676, p. 10-5555, 2017.

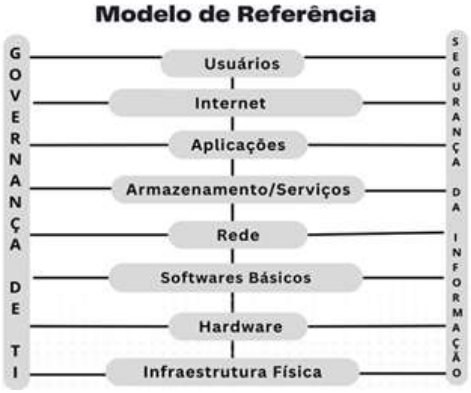
WEINGARTNER, I. **Os impactos da Aplicação (Extra) territorial do Regulamento Geral de proteção de Dados da União Europeia para as Empresas de Tecnologia da Informação de Florianópolis - SC**. 2021. Trabalho de Conclusão de Curso (Bacharel do Curso de Graduação em Direito) - Universidade Federal de Santa Catarina, 2021.

ANEXO 1 - QUESTIONÁRIO

"Olá! Este questionário faz parte de um estudo de caso da dissertação intitulada *'Conformidade de Infraestrutura de TI com a LGPD no Setor Público: Proposta de Arquitetura de Referência e Processo de Avaliação'*

Obs: Sua participação é voluntária, e as respostas serão tratadas de forma confidencial, sendo utilizadas apenas para fins acadêmicos. Agradecemos sua participação nesta pesquisa! Suas respostas serão de grande valor para a construção de uma proposta de arquitetura de referência e um processo de avaliação mais eficiente.

Checklist de Perguntas para Avaliação



Usuários

1) Todos os colaboradores têm conhecimento básico sobre a LGPD?
2) Existem treinamentos regulares sobre proteção de dados?
3) Os usuários são informados sobre suas responsabilidades na proteção de dados pessoais (senhas, acesso a sistemas etc.)?

Internet

4) As conexões utilizam protocolos seguros (como HTTPS)?
5) Existem mecanismos de monitoramento de acessos?
6) Políticas de segurança estão configuradas para acesso remoto?

Aplicações

7) As aplicações internas possuem mecanismos de registro de auditoria?

8) Há controle de acesso baseado em funções para os sistemas?
9) Os sistemas são atualizados regularmente para corrigir vulnerabilidades?

Armazenamento/Serviços

10) Os dados pessoais são armazenados com criptografia?
11) Existem ferramentas de monitoramento de desempenho e disponibilidade dos serviços com alertas proativos?
12) Há controle de acesso físico aos servidores?

Rede

13) A rede é segmentada em zonas de segurança com base no risco e tipos dos dados?
14) Ferramentas de detecção de intrusão estão implementadas?
15) Há um firewall configurado e ativo?

Softwares Básicos

16) Os softwares estão licenciados corretamente?
17) Os logs de acesso aos softwares básicos são monitorados e auditados?

Hardware

18) Os equipamentos de hardware são inventariados e rastreados?
19) Existe um processo definido para o descarte seguro de hardware antigo?

Infraestrutura Física

20) Existem controles de acesso físico (biometria, crachás) para data centers e salas de servidores?
21) Existem sistemas de monitoramento ambiental (temperatura, umidade, detecção de incêndio) com alertas em tempo real?
22) Existem nobreaks e geradores para garantir a continuidade do fornecimento de energia?