GARANTINDO A CONFIDENCIALIDADE, INTEGRIDADE E DISPONIBILIDADE DOS DADOS: UM ESTUDO SOBRE A IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO APOIADO PELA LGPD

Athaide de Souza Matos[1], Nathan Correa Dias[1], Anna Patricia Zakem China [1]

[1]Faculdade de Tecnologia de Ribeirão Preto (FATEC)

Ribeirão Preto, SP – Brasil

athaide.matos@fatec.sp.gov.br,
nathan.dias2@fatec.sp.gov.br,
anna.china@fatec.sp.gov.br

Resumo. Neste artigo, discute- se a relevância da segurança de dados na era digital, em conformidade com a Lei Geral de Proteção de Dados (LGPD). Será tratado os pilares da confidencialidade, integridade e disponibilidade (CID), juntamente com estratégias de proteção e gerenciamento de riscos, a fim de compreender a complexidade do atual cenário. Diante do avanço tecnológico acelerado e do aumento das ameaças cibernéticas, é essencial adotar medidas proativas e abrangentes para atender aos requisitos da LGPD. Aspectos éticos e legais, como privacidade de dados e conformidade regulatória, ressaltam a importância de uma abordagem ampla, em conformidade com a legislação vigente. Este estudo destaca a necessidade de educação dos usuários e do comprometimento das organizações na promoção de uma cultura de segurança da informação em conformidade com a LGPD. Reconhecer os riscos e implementar as melhores práticas, desde o nível operacional até a alta gestão, é fundamental para garantir a segurança jurídica e a proteção dos dados pessoais. O objetivo é contribuir para uma análise mais aprofundada da segurança da informação, sublinhando a importância de proteger os ativos digitais e assegurar a veracidade das informações em um contexto digitalizado, dentro do arcabouço regulatório da LGPD.

Abstract. In this article, the relevance of data security in the digital era is discussed, in accordance with the General Data Protection Law (Lei Geral de Proteção de Dados - LGPD). The pillars of confidentiality, integrity, and availability (CIA) will be addressed, along with protection and risk management strategies, in order to understand the complexity of the current scenario. Given the rapid technological advancements and the increasing cyber threats, it is essential to adopt proactive and comprehensive measures to meet the requirements of the General Data Protection Law (Lei Geral de Proteção de Dados - LGPD). Ethical and legal aspects, such as data privacy and regulatory compliance highlight the importance of a broad approach, in compliance with the current legislation. This study emphasizes the need to inform users and organizational commitment, promoting a culture of information security in compliance with the General Data Protection Law (Lei Geral de Proteção de

Dados - LGPD). Recognizing risks and implementing best practices, from the operational level to senior management, it is essential to ensure legal security and protection of personal data. The goal is to contribute to a more in-depth analysis of information security, emphasizing the importance of protecting digital assets and ensuring the accuracy of information in a digitized context, within the regulatory framework of the General Data Protection Law (Lei Geral de Proteção de Dados - LGPD).

1. Introdução

A Internet transformou a forma, quantidade e velocidade em que as informações são transmitidas, processos que antigamente eram manuais se tornaram automatizados. Hoje temos facilidade de acesso em diversas áreas de nossas vidas, é possível citar diversos exemplos como a autenticação biométrica em dispositivos moveis que se tornou predominante nos Smartphones, promovendo maior segurança e facilidade para acessar os dados sensíveis. A criptografia P2P em aplicativos de mensagens introduz uma garantia que somente o remetente e o destinatário tenha acesso ao conteúdo das mensagens. No entanto, junto com essas melhorias surgiram desafios relacionados à segurança dessas informações compartilhadas, pessoas e empresas estão dia a dia nesse contexto de compartilhamento de dados e em alguns casos podendo vir a se tornar vítimas de golpes e vazamento dessas informações.

A motivação para a elaboração deste artigo está relacionada com a curiosidade e necessidade dos docentes de entender como está o cenário de segurança da informação atualmente, especialmente no que diz respeito ao cumprimento da Lei Geral de Proteção de Dados (LGPD). Estamos imersos numa era caracterizada pela digitalização, onde a quantidade e a relevância dos dados disponíveis nas redes e sistemas digitais aumentam exponencialmente a cada dia. Esta situação exige uma abordagem crítica e proativa para enfrentar os novos desafios relacionados com a proteção e conformidade de dados. Afinal, a segurança da informação deixou de ser uma questão técnica, tornando-se uma questão estratégica que permeia todas as áreas da sociedade. Portanto, este estudo pretende contribuir com desenvolvimento de uma cultura organizacional das empresas visando garantir a segurança das informações, seguindo as recomendações existentes e buscando o melhoramento contínuo. O objetivo deste estudo é fomentar a criação de práticas mais estáveis e conscientes relacionadas à segurança da informação nas esferas profissional e social. Portanto, ao refletir sobre a intersecção entre segurança da informação, conformidade legal e ética digital, este trabalho não só visa enfrentar os desafios atuais, mas também demonstra uma gestão de dados mais eficiente e responsável na era digital. Ao promover a utilização de práticas seguras e éticas, este trabalho visa não só proteger os dados pessoais dos indivíduos, mas também promover um ambiente digital mais estável e flexível para todos os utilizadores.

Para garantir a segurança da informação, é essencial estabelecer uma cultura organizacional que tenha padrões sólidos e eficientes no quesito segurança da informação. Mas para dar segurança ao usuário é necessário fundamentar a infraestrutura de comunicação que deve estar em conformidade com os três pilares da segurança da informação: Confidencialidade, Integridade e Disponibilidade em conjunto com o não

repudio. As ferramentas de segurança como firewalls e softwares de detecção de ameaças, treinamentos regulares em práticas de segurança, e uma mentalidade de responsabilidade compartilhada em relação as organizações são primordiais para uma base consolidada de segurança. Para garantir a conformidade com a LGPD, as organizações devem adotar medidas de segurança que atendam aos requisitos legais para proteger os dados pessoais de seus clientes.

A LGPD não deve ser vista apenas como lei, ela vem para garantir segurança para ambos os lados, o seu objetivo principal é instruir a organização da maneira correta do armazenamento de dados. Grande parte das empresas tem conhecimento sobre a lei, mas ainda existe obstáculos que essas organizações enfrentam no quesito de aplicação das normas. Porém mesmo após o sancionamento e efetividade da lei, diversos processos de segurança são realizados sem padronização e os titulares dos dados ficavam dependentes da empresa ter boas práticas de S.I. Atualmente, as empresas vêm buscando entender e se enquadrar nas obrigatoriedades da LGPD, porém aparentemente será um processo complicado e vagaroso. Portanto, neste artigo é apresentado como se encontra o cenário dessas organizações e o que deve ser feito para entrar em conformidade com a LGPD garantindo os três pilares da Segurança da Informação.

O trabalho está organizado da seguinte maneira: a presente seção Introdução contém a apresentação ao tema que apresenta um panorama do cenário digital abrangido pela Segurança da Informação em conjunto com a LGPD, logo após a seção 2, apresenta o Referencial Teórico que apoia a pesquisa. A seção 3 integra os conceitos principais da Segurança da Informação integrado a políticas de segurança, posteriormente a seção 4 abrange a LGPD e seus respectivos representantes legais. Na seção 5 apresenta-se a pesquisa sobre o cenário atual da LGPD (2021) e seus desafios. Subsequente na seção 6 demonstra-se uma análise sobre os resultados obtidos. Por fim na seção 7 comenta-se sobre como foi o desenvolvimento do projeto, e as dificuldades.

2 Referencial Teórico

Atualmente, organizações enfrentam uma variedade de ameaças que colocam em risco seus sistemas de informação e redes de computadores, incluindo vazamento de dados, fraudes, invasões físicas e virtuais, além de ataques por vírus e hackers que ocorrem com frequência crescente. Para lidar com esses desafios, é essencial implementar normas e procedimentos claros, garantindo a proteção dos dados e definindo responsabilidades dentro da empresa.

> A Informação é um ativo que, como qualquer outro ativo importante para os negócios terem um valor para uma organização e consequentemente, precisa ser protegida adequadamente. A segurança de informações protege as informações contra uma ampla gama de ameaças, para assegurar a continuidade dos negócios, minimizar prejuízos e maximizar o retorno de investimentos e oportunidades comerciais. (NBR ISSO/IEC 17799:2001, p. 2).

Para garantir a eficiência da proteção desses dados, iremos abordar conceitos referentes à Segurança da Informação e a Lei Geral de Proteção de Dados.

2.1 Segurança da Informação

A segurança da informação é uma área essencial na era digital, lidando com a proteção de dados contra uma variedade de ameaças, incluindo acessos não autorizados, vazamentos de informações e ataques cibernéticos. Está área envolve não apenas a implementação de medidas técnicas, mas também a criação de políticas e procedimentos que garantam a confidencialidade, integridade e disponibilidade das informações.

A segurança da informação é um componente importante da governança de TI, assegurando que as estratégias e práticas de segurança estejam alinhadas com os objetivos e necessidades da organização (Schou & Shoemaker, 2006). Isso abrange a definição de políticas de segurança, a realização de avaliações de riscos e a implementação de medidas de controle para proteger os ativos de informação da organização.

2.2 LGPD

A Lei Geral de Proteção de Dados, oficialmente Lei nº 13.709 (Brasil, 2018), aprovada em 14 de agosto de 2018, tem o objetivo de regulamentar o uso, tratamento, armazenamento, compartilhamento e proteção de dados no Brasil, abrangendo cidadãos e organizações, sejam elas públicas ou privadas. A lei passou por um período de adequação de dois anos permitindo que as empresas se preparassem para estar em conformidade com suas regulamentações. Posterior a esse período a lei entrou em vigor, requisitando que as organizações adotassem práticas corretas visando garantir a integridade, confidencialidade e disponibilidade dos dados pessoais.

O artigo 2º da LGPD estabelece os seguintes fundamentos que orientam a aplicabilidade do tratamento de dados pessoais no Brasil: respeito à privacidade; autodeterminação informativa; liberdade de expressão, de informação, de comunicação e de opinião; inviolabilidade da intimidade, da honra e da imagem; desenvolvimento econômico e tecnológico e inovação; livre iniciativa, livre concorrência e defesa do consumidor; direitos humanos, livre desenvolvimento da personalidade, dignidade e exercício da cidadania pelas pessoas naturais.

3. Segurança da Informação

Com a adesão de um número expressivo de usuários a sistemas cada vez mais conectados, alimentados pelo fornecimento de dados, torna-se necessária a adoção de medidas para gestão e manutenção da proteção de informações privadas. Nesse sentido, para as organizações, a informação se tornou um bem de valor inestimável, e a implementação de sistemas que abordem as vulnerabilidades emergentes é crucial para o seu bom funcionamento (Coutinho, 2017). A ISO/IEC 27001 é o padrão internacional para o gerenciamento da segurança da informação, fornecendo diretrizes para a introdução, implementação e manutenção do Sistema de Gestão de Segurança da Informação (SGSI) em organizações. O SGSI é projetado para assegurar a seleção de controles de segurança adequados e proporcionados para proteger os ativos de informação e propiciar confiança às partes interessadas (ABNT, 2006). No Brasil, a norma ABNT NBR ISO/IEC

27002:2006 estabelece como objetivo da segurança da informação a preservação da confidencialidade, integridade e disponibilidade da informação (ABNT, 2006). Além disso, Hintzbergen (2018) destacam estes outros aspectos importantes para a segurança da informação: a autenticidade, a confiabilidade e o não repúdio. A autenticidade baseia-se na garantia de uma entidade ser o que é, ou seja, que a integridade da entidade seja preservada. A confiabilidade está associada à consistência operacional de um sistema de acordo com os requisitos desejados. Por fim, o não repúdio é a capacidade de provar a ocorrência de um evento realizado pela entidade de origem.

A segurança da informação assegura a confidencialidade, integridade e disponibilidade das informações, descrevendo como elas devem ser manuseadas, controladas, protegidas e descartadas. Em uma era onde a informação é considerada o ativo mais valioso de uma organização, a segurança da informação é crucial para sua sobrevivência. Portanto, é fundamental implementar um Programa de Segurança abrangente que reduza as vulnerabilidades dos sistemas e melhore suas capacidades de detecção, resposta e adaptação às ameaças em constante evolução.

Na era digital a segurança da informação está em ascensão, com o aumento do número de dados armazenados se torna necessário manter uma padronização de metodologias para desenvolver uma gestão inteligente e eficaz. Abordar os princípios é fundamental para entender o que fazer para um melhoramento contínuo dos processos existentes.

3.1 Confidencialidade

Uma das bases fundamentais da segurança da informação que tem como visão a garantia das informações contra acessos não autorizados. Portanto, tem como parâmetros o acesso aos dados e processos somente pelos indivíduos devidamente autorizados. Esse princípio é essencial para a proteção das informações e evitar violações de sistemas que podem vir a causar danos, perdas financeiras e outros prejuízos. Esse princípio é fundamental em diversos ambientes como ramo empresarial, governamental e pessoal, justamente porque todos os âmbitos são diariamente bombardeados de novas informações e que necessitam do tratamento correto.

> A implementação de controles de acesso robustos é crucial para a manutenção da confidencialidade, garantindo que apenas usuários devidamente autorizados possam acessar e manipular informações sensíveis (Whitman & Mattord, 2018, p. 94).

3.1.2 Política de Segurança da informação (PSI)

A política de segurança da informação é imprescindível quando o assunto é confidencialidade pois define controles de acesso e outras medidas de segurança que, em conjunto de outras políticas, gera um sistema robusto e eficaz de proteção. Sua finalidade é possibilitar o gerenciamento da segurança em uma organização, estabelecendo regras e padrões para proteção da informação. A PSI possibilita manter a confidencialidade, garantir que a informação não seja alterada ou perdida e permitir que a informação esteja disponível quando for necessário.

3.3 Integridade

A integridade no conceito de segurança da informação está referenciada a garantia de que as informações sejam mantidas a sua forma original ou a forma desejada após as alterações autorizadas. Portanto, é estritamente necessário promover a confiabilidade e a exatidão dos dados por intermédio das políticas de segurança que possuem o objetivo de evitar detrimentos para a organização. Conforme afirmado por Whitman e Mattord (2018), "A integridade assegura que a informação não foi alterada de maneira não autorizada, garantindo a confiabilidade dos dados" (p. 112). Além disso, Stallings (2017) ressalta a importância de mecanismos como assinaturas digitais e check-ups para verificar a integridade dos dados e prevenir alterações maliciosas ou acidentais (p. 85).

3.3.1 Política de Backup

A política de backup estabelece metodologias padronizadas para proteger as informações de uma organização. Ao implementar rotinas de backup regulares e eficientes, conectado a outras medidas de segurança é possível implementar um sistema confiável para o armazenamento dos dados. O objetivo principal é a garantia total das informações, prevenindo perdas ou corrupções, além de possibilitar a rápida recuperação no caso de falhas e incidentes. Portanto, ela assegura que os dados estejam disponíveis quando necessários, minimizando os danos gerados pela perca dos dados e garantindo a continuidade das operações da organização.

3.3 Disponibilidade

O conceito de disponibilidade está relacionado a capacidade que um sistema, serviço ou recurso possui de estar acessível e utilizável quando necessário, independentemente do local e horário solicitados. A disponibilidade promove aos usuários acesso aos dados e recursos de forma contínua, independentemente do tempo de inatividade. Segundo Stallings e Brown (2015), "Disponibilidade refere-se ao fato de que os serviços e dados de um sistema estejam acessíveis quando necessário" (STALLINGS; BROWN, 2015, p. 8).

3.3.1 Política de Controle de Acesso e Autenticação

Garante que apenas pessoas autorizadas tenham acesso a sistemas e dados sensíveis, através de processos de autenticação, registros de auditoria, criptografia e controles de alteração. Todos os usuários devem seguir as diretrizes de segurança estabelecidas. Violações serão tratadas conforme os procedimentos de segurança da informação.

A integração dos princípios de S.I - Segurança da Informação com as políticas de segurança promove maior resguardo para as empresas que visam atender as conformidades da LGPD e consequentemente ter maior controle de suas informações.

4. LGPD

A criação da Lei Geral de Proteção de Dados – LGPD se deu a necessidade do controle e tratamento dos dados dos Brasileiros, estes que antes desta lei estavam à mercê das organizações sobre a forma em que suas informações eram tratadas e compartilhadas A lei foi sancionada em agosto de 2018 e teve inspiração na *GDPR (General Data Protection Regulation)* que é utilizada em alguns países da Europa, essa lei é um conjunto de normas sobre como as empresas, pessoas e órgãos públicos devem guardar, proteger e usar as informações pessoais coletadas dos usuários. A LGPD tem como objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, através do controle sobre o tratamento das informações armazenadas dos indivíduos, parametrizando os processos e fiscalizando organizações.

A lei estabelece diretrizes acerca de coleta e processamento de dados pessoais das organizações. Portanto, temos a necessidade de consentimento explicito do titular dos dados, transparência com a finalidade e usabilidade dos dados. São direitos regidos pela LGPD como o direito de correção de informações imprecisas, exclusão de dados desnecessários ou inadequados perante a política vigente e a portabilidade para outros serviços ou plataformas. Esses direitos têm um impacto significativo das práticas de segurança da informação das empresas, pois exigem a implementação de medidas para garantir que o titular dos dados possa exercer seus direitos de modo válido e seguro.

4.1 Princípios da LGPD

A LGPD contém dez princípios (finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação; responsabilização e prestação de contas) que servem como base para a compreensão e exercício de boas condutas por parte dos seus envolvidos.

4.2 Papéis e Responsabilidades

A LGPD determina que é necessário haver um encarregado pelo tratamento dos dados pessoais, denominado *DPO – Data Protection Officer,* esse indivíduo será responsável por garantir que a corporação esteja em conformidade com a lei, seguindo padrões pré-estabelecidos e que serão avaliados pela ANPD - Agência Nacional de Proteção de Dados. Além disso, existem outros dois papeis cruciais para a aplicabilidade da lei: O Controlador responsável por definir como e por que os dados pessoais são processados; e o Operador que realiza o tratamento de dados pessoais em nome do controlador, seguindo suas instruções.

5. Pesquisa

A implementação da Lei Geral de Proteção de Dados trouxe diversos desafios para as empresas, especialmente para os Microempreendedores Individuais (MEI), que representam o total de 73,4% de empresas formais do Brasil (SEBRAE). Embora muitas dessas organizações afirmem possuir conhecimento sobre a nova regulamentação e seus objetivos, a implementação e adequação têm sido processos difíceis. Através da Pesquisa (Empresas e LGPD: Cenários, desafios e caminhos) feita pela RD STATION com apoio

do Instituto Manar e a banca Eduardo Dorfmann Aranovich & Cia., é possível ter conhecimento sobre como está o processo de adequação das empresas em relação a LGPD. A pesquisa quantitativa foi realizada com 997 empresas de diversas localidades como São Paulo, Santa Catarina, Rio Grande do Sul, Minas Gerais, Paraná e outros, com duração de 3 pesquisa meses (janeiro-abril, 2021) e tem uma porcentagem de erro amostral de 3,1% para resultado gerais com intervalo de confiança é de 95%.

Figura 1. Gráfico da pesquisa referente a explanação
Fonte: (RESULTADOS DIGITAIS, 2021)

Foi constatado que cerca de 93% das organizações entrevistadas afirmam conhecer ou já ter ouvido falar acerca da LGPD, sua maior parte está localizada no estado de São Paulo com cerca de 41% do público total entrevistado. Alguns dados são extremamente importantes, como o tamanho dessas corporações, em média 60% dessas empresas são denominadas Microempresas - até 19 funcionários, grande parte dessas empresas sequer tem conhecimento básico sobre os procedimentos necessários para se adequar à Lei Geral de Proteção de Dados. No âmbito geral da pesquisa apenas 26% adotam providencias e consideram sua base de dados segura, a partir dessas informações podemos constatar que não existe um problema central em relação a LGPD, é perceptível a existência de um conjunto de complexidades impostas pela Lei, principalmente por não existir uma definição clara e objetiva do que deve ser feito para realizar a adequação e a ausência de profissionais capacitados em conjunto da carência de conhecimento necessário sobre o assunto.

Alguns dos problemas são:

a) A Complexidade de medidas e volume de trabalho necessário para estar em conformidade da Lei;

b) A Inexistência de uma área dedicada a informação e tratamento de dados na companhia é uma das principais dificuldades pois as MEI sequer tiveram essa preocupação com a segurança de suas informações no ato de fundamento da empresa;

c) Indisponibilidade de metodologia adequada;

d) A falta de verba para a contratação de consultoria especializada;

e) O desconhecimento sobre os impactos pelo descumprimento da LGPD.

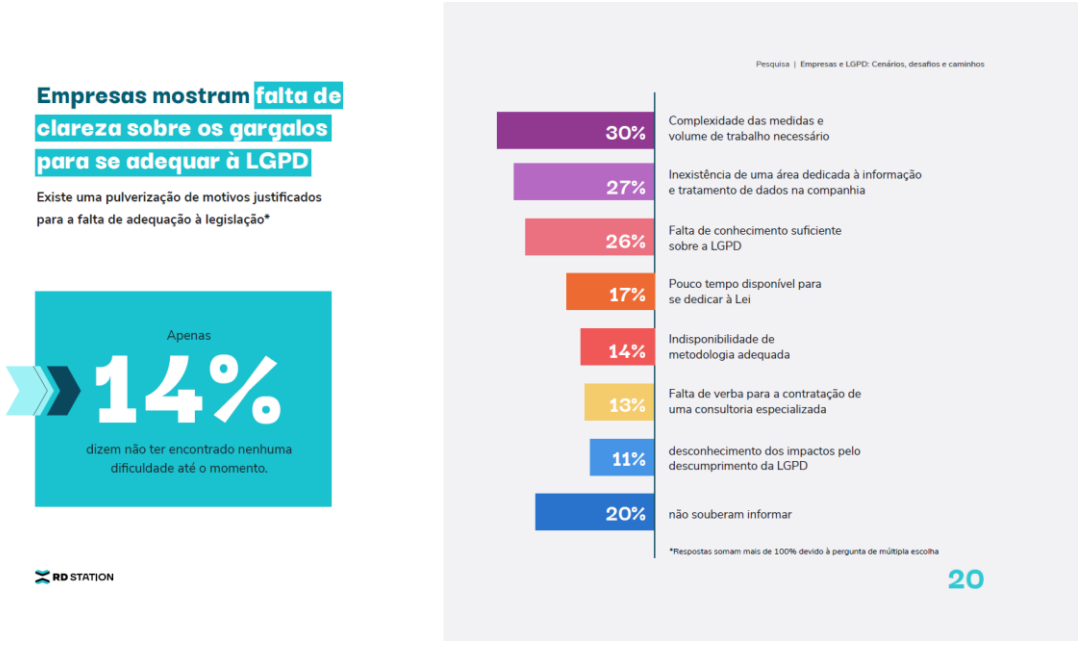

Figura 2. Gráfico da pesquisa referente a explanação
Fonte: (RESULTADOS DIGITAIS, 2021)

6 Análise

Um dos principais obstáculos ao realizar a implementação da LGPD é a falta de uma área interna dedicada exclusivamente ao tratamento de dados. Sem uma base estabelecida, muitas empresas precisam começar praticamente do zero, o que pode ser um grande desafio. Para as pequenas empresas, essa tarefa torna-se ainda mais inacessível devido aos custos associados, como a contratação de consultorias, aquisição de ferramentas e formação de pessoal. No entanto, outra dificuldade que impede a implementação da LGPD envolve a cultura do Brasil, juntamente com as questões de aplicações das sanções pela ANPD. As empresas podem até dizer que tem conhecimento sobre a lei, porém falta conhecimento e conscientização sobre a relevância da proteção e preocupação com os dados pessoais. A partir desses fatores expostos é possível constatar que a maioria das empresas não demonstram interesse em realizar um projeto de adequação. Portanto, existe uma porção de atividades que, se planejadas e executadas da maneira correta e bem direcionada, podem acelerar esse processo.

Sendo assim, o desenvolvimento de modelos simplificados de políticas de privacidade e governança de dados, adaptados às necessidades das pequenas empresas, pode facilitar a implementação e o gerenciamento dessas práticas. Além disso, programas governamentais de capacitação gratuitos para empresários podem ajudar a entender e implementar as novas regulamentações de forma eficaz. Oferecer consultorias mais acessíveis para pequenas e microempresas permitirá que elas obtenham o suporte necessário sem comprometer suas finanças. Ferramentas simplificadas e adaptadas ao nível de conhecimento dessas empresas também são essenciais para facilitar a gestão e

proteção dos dados. A ANPD em conjuntos dos responsáveis pela LGPD poderia fazer um tratamento diferenciado no quesito das penalidades em relação as microempresas visando flexibilidade para empresas de menor porte financeiro que estão buscando entrar em conformidade. Finalmente, proporcionar incentivos governamentais para empresas que investirem na conformidade com a LGPD, como benefícios fiscais ou subsídios, pode aliviar o peso financeiro e incentivar a adesão.

Com essas medidas, as pequenas empresas terão mais condições de se adequar à LGPD, garantindo a proteção dos dados pessoais e fortalecendo a confiança dos clientes.

7. Considerações Finais

Este estudo aborda a importância da segurança da informação em conformidade com a LGPD, destacando os pilares de confidencialidade, integridade e disponibilidade.

A implementação eficaz da LGPD requer não apenas medidas proativas, mas também uma mudança cultural nas organizações. No entanto, micro e pequenas empresas enfrentam desafios significativos devido a restrições financeiras e de recursos. Para superar essas dificuldades, sugerem-se soluções como políticas de segurança simplificadas e programas de capacitação.

Portanto, é fundamental que as empresas, o governo e os órgãos reguladores trabalhem de forma integrada e colaborativa para garantir a conformidade com a lei.

As dificuldades enfrentadas durante a realização deste estudo estiveram inicialmente relacionadas à compreensão da Lei Geral de Proteção de Dados (LGPD), dada a sua abrangência e complexidade, bem como os requisitos da Norma ISO relacionada ao tema em estudo.

Referências

Abe, N. (2017). Estudo de caso: Principais pilares da segurança da informação nas organizações.

ABNT. (2006). NBR ISO/IEC 27001:2006, Tecnologia da Informação –Técnicas de segurança –Sistema de gestão de segurança da informação – Requisitos – Rio de Janeiro: Associação Brasileira de Normas Técnicas (ABNT), 2006, 34p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. L. Norma ISSO/ IEC 17799: Código de prática para a segurança da informação nas empresas. Curitiba, 2003.

Brasil. (2018). Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)

Coutinho, M. M., Santos, R. N. dos, Custodio, V. H. da S., Amaral, E. C., Sabino, E., & ISO/IEC 27005:2008 Gestão de Riscos de Segurança da Informação.

Schou, C. D., & Shoemaker, D. (2006). Information Assurance for the Enterprise: A Roadmap to Information Security. McGraw-Hill.

SEBRAE. Brasil tem quase 15 milhões de Microempreendedores Individuais. Disponível em: <https://sebrae.com.br/sites/PortalSebrae/artigos/brasil-tem-quase-15-milhoes-de-microempreendedores-individuais,e538151eea156810VgnVCM1000001b00320aRCRD>. Acesso em: 09 de junho de 2024.

RESULTADOS DIGITAIS (2021). Pesquisa Empresas e LGPD: resultados apontam cenários, desafios e caminhos. Disponível em <Pesquisa Empresas e LGPD: veja o cenário brasileiro (rdstation.com)> Acesso em: 12 de junho de 2024.

STALLINGS, W.; BROWN, L. **Computer Security: Principles and Practice**. 3rd ed. Upper Saddle River, NJ: Pearson, 2015.

Whitman, M. E., & Mattord, H. J. (2018). *Principles of Information Security*. Cengage Learning.

As referências devem ser listadas em ordem alfabética usando tamanho de fonte de 12 pontos, com 6 pontos de espaço antes de cada referência, alinhada à esquerda. A primeira linha de cada referência não deve ser recuada, enquanto as subsequentes deve ser recuada em 0,5 cm.