FACULDADE DE TECNOLOGIA DE AMERICANA – MINISTRO RALPH BIASI

Curso Superior de Tecnologia em Segurança da Informação

Herik Henrique Barbosa

Juliano Parpinelli Becegato

ANÁLISE DOS REGULAMENTOS DE PROTEÇÃO DE DADOS E SUA IMPLEMENTAÇÃO EM ORGANIZAÇÕES FINANCEIRAS

Americana, SP

2023

FACULDADE DE TECNOLOGIA DE AMERICANA – MINISTRO RALPH BIASI

Curso Superior de Tecnologia em Segurança da Informação

Herik Henrique Barbosa
Juliano Parpinelli Becegato

ANÁLISE DOS REGULAMENTOS DE PROTEÇÃO DE DADOS E SUA IMPLEMENTAÇÃO EM ORGANIZAÇÕES FINANCEIRAS

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação da Prof ª Dra. Maria Cristina Aranda

Área de concentração: Segurança da Informação

Americana, SP.

2023

Herik Henrique Barbosa
Juliano Parpinelli Becegato

ANÁLISE DOS REGULAMENTOS DE PROTEÇÃO DE DADOS E SUA IMPLEMENTAÇÃO EM ORGANIZAÇÕES FINANCEIRAS

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Curso Superior de Tecnologia em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana – Ralph Biasi.
Área de concentração: Segurança da Informação

Americana, 30 de Novembro de 2023

Banca Examinadora:

Maria Cristina Aranda (Presidente)
Doutora
FATEC Americana – SP

Wagner Siqueira Cavalcante (Membro)
Mestre
FATEC Americana - SP

Mariana Godoy Vazquez Miano (Membro)
Doutora
FATEC American - SP

ANÁLISE DOS REGULAMENTOS DE PROTEÇÃO DE DADOS E SUA IMPLEMENTAÇÃO EM ORGANIZAÇÕES FINANCEIRAS

ANALYSIS OF DATA PROTECTION REGULATIONS AND THEIR IMPLEMENTATION IN FINANCIAL ORGANIZATIONS

Herik Henrique Barbosa - Fatec Americana. herik.barbosa@fatec.sp.gov.br

Juliano Parpinelli Becegato - juliano.becegato@fatec.sp.gov.br

Maria Cristina Aranda (Orientadora) - mcris.aranda@fatec.sp.gov.br

Resumo

Este artigo realiza uma análise abrangente dos regulamentos de proteção de dados e sua implementação nas organizações financeiras brasileiras. O estudo examina as leis e normas de proteção de dados em vigor no Brasil, destacando sua evolução ao longo do tempo e as implicações para as organizações. O objetivo de pesquisa é analisar as metodologias sobre como as empresas garantem a privacidade dos dados dos usuários, incluindo medidas de segurança, políticas de privacidade e treinamentos. Os resultados desse estudo apresentam as melhores práticas e recomendações para uma implementação efetiva dos regulamentos de proteção de dados em organizações do ramo financeiro podendo ser estendida para qualquer tipo de organização.

Palavras-chave: LGPD. Proteção de Dados. Segurança da Informação.

Abstract

This article conducts a comprehensive analysis of data protection regulations and their implementation in Brazilian financial organizations. The study examines the data protection laws and regulations in force in Brazil, highlighting their evolution over time and their implications for organizations. The research objective is to analyze methodologies on how companies ensure user data privacy, including security measures, privacy policies, and training. The results of this study present the best practices and recommendations for the effective implementation of data protection regulations in financial sector organizations, which can be extended to any type of organization.

Keywords: *LGPD. Data Protection. Information Security.*

1. Introdução

Este trabalho discorrerá sobre a análise dos regulamentos de proteção de dados e sua implementação em organizações financeiras brasileiras, a fim de entender como eles afetam as práticas empresariais e de que forma essas instituições podem adaptar-se às regulamentações na proteção dos dados.

A proteção de dados pessoais é um assunto de grande importância na atualidade, principalmente pelo aumento do uso da tecnologia de informação em todos os setores da sociedade. Com isso, as informações pessoais dos indivíduos estão cada vez mais expostas a riscos, como violações de privacidade e uso indevido de informações sensíveis. Por isso a implementação legal de regulamentos de proteção de dados se tornou necessária para garantir a segurança e privacidade dos dados pessoais (MENDES, 2014).

Dentre os regulamentos mais importantes está o Regulamento Geral de Proteção de Dados (GDPR) e a Lei Geral de Proteção de Dados (LGPD), os quais estabelecem diretrizes relativas à jurisdição de privacidade e proteção de dados na União Europeia e em território brasileiro, respectivamente.

A implementação adequada desses regulamentos pode ser um desafio para as organizações, pois envolve mudanças em suas práticas de coleta, uso, armazenamento e descarte de dados. No entanto, a implementação correta pode trazer benefícios significativos, como a melhoria da segurança dos dados e o aumento da confiança dos clientes que possuem conta em instituições financeiras, onde a proteção tem que ser efetiva, pois, além de todos os dados pessoais, nesse caso, inclui os dados financeiros.

A pergunta do problema de pesquisa é: quais são as principais metodologias adotadas pelas instituições financeiras e quais medidas são utilizadas para garantir a privacidade dos dados dos usuários?

Por isso, *compliance* e a análise dos regulamentos e leis de proteção de dados, sua implantação e implementação nas organizações é um assunto de grande relevância para a segurança e privacidade dos dados pessoais. Este aspecto justifica o caráter aplicado dessa pesquisa e sua importância.

A partir dessa proposta, objetivou-se então analisar as metodologias que essas empresas adotam para garantir a privacidade dos dados, incluindo medidas de segurança, políticas de privacidade e treinamentos de seus funcionários.

A partir de dados provenientes de diversas fontes e a realização de entrevistas não estruturadas, que é uma conversa conduzida com perguntas mais abertas sem um roteiro, com empresas do setor financeiro, nota-se a importância do tema nessas organizações. O fato de empresas não possuírem uma regulamentação na prevenção de fraudes quanto aos dados pessoais, pode impactar negativamente, tanto financeiramente quanto à credibilidade da sua imagem.

2. Referencial Teórico

De acordo com Serviço Federal de Processamento de Dados (SERPRO, 2019) do governo federal do Brasil, se uma informação permite identificar, direta ou indiretamente um indivíduo então ela é considerada dado pessoal. Entende-se de acordo com a LGPD (2020) como dado pessoal: nome, RG, CPF, gênero, data e local de nascimento, telefone, endereço residencial, localização via GPS, retrato em fotografia, prontuário de saúde, preferencias de lazer, endereço de Protocolo da Internet (IP) e *cookies*, armazenamento em seus dispositivos

entre outros. Esses dados podem conduzir à identificação de um indivíduo específico. A proteção de dados pessoais é importante para garantir a privacidade e a segurança dessas informações, evitando o seu uso indevido ou a sua divulgação não autorizada.

Dentre os dados utilizados em uma organização, existem seus dados organizacionais, bem como os dados de seus funcionários e clientes. Dentre os dados de pessoas físicas, encontra-se nome completo, filiação, CPF, RG, endereço, número de telefone, *e-mail*, entre outros. Esses dados são coletados, processados, armazenados, descartados e utilizados pelas organizações para diversas finalidades, como por exemplo, para gerenciar funcionários, fornecer serviços, realizar vendas, entre outras atividades. É importante ressaltar que esses dados pessoais são protegidos por leis e regulamentações que visam garantir a privacidade e a segurança das informações advindas deles.

2.1. Regulamentos de proteção de dados

No Brasil, o principal regulamento para proteção de dados é a LGPD, que entrou em vigor em setembro de 2020. A lei estabelece regras sobre como as empresas devem coletar, armazenar, descartar e usar os dados pessoais ou serviços no território brasileiro. Tanto os cidadãos brasileiros quanto os estrangeiros têm esse direito de acordo com LGPD (2020) – a saber:

> As empresas devem obter o consentimento expresso dos titulares dos dados para coletar e processar suas informações pessoais. O consentimento deve ser livre, informado e inequívoco, transparente, os titulares dos dados têm o direito de acessar, os dados devem ser protegidos.

Além da LGPD, outras leis e regulamentos que se aplicam à proteção de dados no Brasil, incluindo o Marco Civil da Internet, que é uma lei brasileira que entrou em vigor em junho de 2014 e estabelece princípios, direitos e deveres para o uso da Internet no país. O objetivo da lei é garantir a liberdade, a privacidade e a segurança dos usuários da Internet, bem como promover o desenvolvimento da rede no país. Alguns dos principais aspectos do Marco Civil da Internet (2014) incluem: neutralidade, responsabilidade por conteúdo, liberdade de expressão, proteção de dados pessoais e armazenamento de dados.

Juntamente com a LGPD e o Marco Civil, as organizações devem ainda seguir o Código de Defesa do Consumidor que está em vigor em solo nacional desde março de 1991 e a Lei do Cadastro Positivo. O cadastro positivo é uma legislação brasileira que entrou em vigor em julho de 2019 que reúne informações sobre histórico de crédito dos consumidores, a fim de avaliar seu perfil de risco e facilitar a concessão de crédito por instituições financeiras, conforme publicado por Maciel (2019).

2.2. Dificuldades da implementação dos regulamentos

A implementação de regulamentos de proteção de dados apresenta desafios significativos no Brasil, especialmente em relação à cultura de privacidade e segurança de dados. Além disso, muitas empresas têm dificuldades em entender e se adaptar aos requisitos dos regulamentos, o que requer investimentos em tecnologias e capacitação pessoal. A implementação de regulamentos de proteção de dados pode enfrentar várias dificuldades, assim defendidos por Garcia (2019):

- Resistência interna: Algumas organizações podem ter resistência à implementação de regulamentos de proteção de dados, seja devido a preocupações com a complexidade dos processos, custos ou por outros motivos;

• Falta de recursos: A implementação de regulamentos de proteção de dados pode exigir recursos significativos, como pessoal dedicado, tecnologia e treinamento. Algumas organizações podem não ter os recursos suficientes para implementar completamente esses regulamentos;

• Dificuldades técnicas: A implementação de regulamentos de proteção de dados pode exigir mudanças na infraestrutura de Tecnologia da Informação, o que pode ser um processo complexo e desafiador. Além disso, algumas organizações podem ter dificuldades técnicas em adotar novas tecnologias de proteção de dados;

• Conformidade com regulamentos múltiplos: As organizações podem ter dificuldades em cumprir múltiplos regulamentos de proteção de dados, especialmente se esses regulamentos têm requisitos diferentes ou conflitantes;

• Problemas de conformidade contínua: As organizações podem ter dificuldade em manter a conformidade contínua com os regulamentos de proteção de dados, especialmente se eles exigirem atualizações regulares ou mudanças na política de privacidade.

Observa-se, a partir do exposto que, a implementação de regulamentos de proteção de dados pode ser desafiadora para as organizações, devido a várias barreiras técnicas, financeiras e de conformidade.

2.3. Proteção de dados nas empresas brasileiras

Para entender os principais desafios das empresas brasileiras, na adequação do novo cenário, foi analisada a "Pesquisa sobre a LGPD no mercado brasileiro", desenvolvida pela Alvares e Marsal, HLFMap, *Privacy Tools* (ALVARES, MARSAL, 2021).

A referida pesquisa sobre a LGPD no mercado brasileiro, contou com empresas em diferentes níveis de proteção em relação a LGPD, incluindo empresas de diferentes tamanhos, definições e estágios de crescimento e com variação no número de funcionários, de 100 colaboradores até mais de 10.000 colaboradores.

No ano de 2021, entre as empresas que estão mais adequadas à lei, estão aquelas que atuam nos segmentos financeiro, de seguros e serviços relacionados, segundo aponta Alvarez e Marsal (2021).

O mapa da fraude de 2022, de acordo com Confederação Nacional de Dirigentes Lojistas (CNDL), mostrou o aumento dos casos de golpes e fraudes no Brasil, que totalizam 5,8 milhões em tentativas de fraude, no período de janeiro a dezembro de 2022 (CNDL, 2023).

Segundo essa pesquisa conduzida pela CNDL, os golpes bancários estão evoluindo constantemente, demandando maior atenção por parte do consumidor. A possibilidade de acessar soluções de pagamento, transferências, compras e investimentos pelo celular torna a rotina mais conveniente, mas também impõe ao consumidor a responsabilidade de tomar precauções. De acordo com o referido estudo da CNDL, em colaboração com o Serviço de Proteção ao Crédito (SPC Brasil) e o Sebrae, cerca de 22% dos entrevistados relataram ter sido vítimas de fraudes em instituições financeiras no ano de 2022, totalizando aproximadamente 8,4 milhões de consumidores. Essa pesquisa aponta que o tipo predominante de golpe identificado foi a clonagem de cartões de crédito e débito (8%), seguido pela transferência de dinheiro para indivíduos que se faziam passar por conhecidos (4%). A pesquisa também revelou que 4% dos entrevistados tiveram experiências com transações bancárias não autorizadas, como saques, pagamentos ou transferências, enquanto outros 4% enfrentaram situações envolvendo financiamentos realizados por terceiros utilizando

documentos falsificados, roubados ou obtidos de maneira fraudulenta.

Este levantamento, conduzido pela CNDL, foi realizado entre a população que utiliza a Internet, residente nas capitais brasileiras, abrangendo homens e mulheres com 18 anos de idade ou mais. A pesquisa foi realizada *online*, com uma amostra de 800 casos e uma margem de erro de 3,0 pontos percentuais, coletando dados no período de 15 a 22 de setembro de 2022.

A adequação à LGPD continua forte neste segmento financeiro, fato este confirmado em entrevista realizada pelos autores desse trabalho, em cinco instituições financeiras do Brasil, concluindo que essas organizações se prepararam para seguir as diretrizes da LGPD.

Um estudo da Clear Sale (2022) analisou 312,2 milhões de pedidos realizados no *e-commerce* brasileiro, feitas por meio de pagamentos com cartão de crédito, que totalizou em R$5,8 bilhões em ações fraudulentas. As empresas financeiras correm para mostrar aos clientes suas medidas de segurança e privacidade, em um esforço intensificado pela competição acirrada com as *fintechs (startups* ou empresas que desenvolvem produtos financeiros totalmente digitais). A partir dessa pesquisa identificou-se que o processo de adequação à LGPD está diretamente relacionado ao tamanho da empresa, já que é preciso investir em recursos de pessoal, tecnologia e *compliance*. Empresas de pequeno porte e prestadoras de serviços não se capacitaram, para enquadrar na nova legislação de proteção de dados. Microempreendedores não criaram políticas de segurança ou sequer pensam sobre o assunto.

Embora a proteção de dados ainda não seja uma prioridade para pequenas e médias organizações, elas têm consciência de que o mau uso de dados pode resultar em multas e danos à sua reputação, colocando o negócio em risco. Por outro lado, empresas mais suscetíveis a sofrer processos judiciais e danos com a sua imagem demonstram maior preocupação em relação à proteção de dados. Por isso as instituições financeiras têm essa maior preocupação e responsabilidade com os dados de seus clientes.

No entanto, é importante ressaltar que uma adequação completa envolve diversos recursos, como treinamentos, plataformas tecnológicas, consultorias, cursos, melhorias de comunicação e transparência, além da contratação de pessoal qualificado. Tais custos são considerados investimentos, já que aprimoram a relação empresa/clientes, aumentam a reputação da organização no mercado e evitam prejuízos financeiros decorrentes de multas e sanções.

Ao estar em conformidade com a nova lei de proteção de dados, a empresa pode melhorar sua relação com as informações pessoais, trazendo benefícios muito importantes para as organizações, evitando multas e mantendo um diferencial competitivo.

De acordo com o SEBRAE (2020), um dos principais benefícios de estar em conformidade para as organizações é a melhora do relacionamento com o consumidor, pois a empresa passa a transmitir uma maior credibilidade e confiança, pois espera uma boa transparência da empresa e o respeito à sua individualidade, incluindo a privacidade e a proteção de seus dados pessoais. A empresa que zela pela privacidade e proteção de dados do cliente mostra que se preocupa com o bem-estar, direitos e liberdades do consumidor. Segundo essa pesquisa do SEBRAE, a melhoria da imagem da organização é um benefício percebido por 64,95% das empresas respondentes. A imagem da empresa é fundamental para uma conexão da empresa ao cliente.

Embora as sanções previstas na LGPD passaram a valer desde agosto de 2021, muitas empresas parecem ainda não ter incluído ações de proteção de dados e privacidade de seus clientes, parceiros e fornecedores em sua rotina (ALVAREZ; MARSAL, 2021).

Da mesma forma, a política de privacidade, considerada um dos passos iniciais para uma relação com os clientes respeitando a proteção de dados, é cada vez mais buscada pelos clientes e, por isso, deve estar acessível e ser apresentado de forma clara e compreensível (BRASIL, 2021).

A transparência exigida pela LGPD pode ser alcançada de forma mais simples por meio da política de privacidade, a qual é elaborada por profissionais especializados da própria empresa, consultores ou com o uso de plataformas que geram modelos personalizáveis.

2.4. Auxílio à implementação da LGPD pela FEBRABAN às instituições financeiras

A Federação Brasileira de Bancos (FEBRABAN 2019), em outubro de 2019, lançou um guia personalizado voltado para o setor bancário que visava auxiliar na implementação da LGPD que entrou em vigor em 2022. O propósito fundamental deste material da FEBRABAN foi esclarecer os conceitos e diretrizes necessários para a efetivação da LGPD, com um enfoque direcionado aos impactos que essa legislação tem no mercado financeiro, especialmente nas instituições bancárias. Esse guia denominado "Guia de Boas Práticas", contendo 62 páginas, foi subdividido em duas seções distintas. Os primeiros capítulos discorrem sobre os aspectos cruciais da LGPD, incluindo tópicos como governança, privacidade e as bases legais que fundamentam o tratamento de informações pessoais. A segunda parte do guia aprofunda-se nos aspectos relacionados aos modelos de tratamento de dados a serem adotados pelos bancos, na documentação padrão necessária e no esforço de conscientização que as instituições devem realizar junto aos seus colaboradores.

De acordo com Ulisses Gomes Guimarães, diretor da comissão executiva de tratamento de dados da FEBRABAN e *Chief Data Officer* (CDO) e encarregado (DPO) do banco Santander, o setor bancário em 2019 estava em uma posição vantajosa para absorver a LGPD de maneira mais natural, em comparação a outros segmentos da economia, devido à já existente regulamentação rigorosa no setor (FEBRABAN 2019). Ulisses destacou que os bancos estão acostumados a lidar com a segurança de dados e a proteção do sigilo bancário, mas salienta que a LGPD traz consigo uma mudança cultural considerável, principalmente devido à necessidade de lidar com terceiros. Por esse motivo, os bancos se concentraram em um intenso processo de adaptação à nova legislação, envolvendo o comprometimento de todas as instituições financeiras.

A comissão executiva de tratamento de dados da FEBRABAN é composta por representantes de quinze bancos que abrangem mais de 90% do mercado bancário. Essa comissão se reuniu mensalmente para tratar da implementação da LGPD, abordando, desde questões tecnológicas e de governança de dados, até aspectos jurídicos, sendo que esses últimos foram analisados por meio da subcomissão de assuntos jurídicos e *compliance* de dados, uma subdivisão criada especificamente para essa finalidade, com a participação de trinta e quatro instituições financeiras. O empenho dessa comissão executiva explica o feito dos bancos terem se adequado com mais facilidade

2.5. Prevenção contra ataques

A prevenção contra ataques cibernéticos envolve uma série de estratégias e práticas que visam prevenir, detectar e responder a ameaças virtuais. A proteção da rede desempenha um papel fundamental, pois ajuda a controlar o acesso a sistemas, monitorar o tráfego de dados e identificar possíveis atividades maliciosas. Juntamente com a proteção de rede, a proteção *web* é importante, pois muitos ataques têm como alvo as aplicações e serviços *online* utilizados pelas empresas.

No que diz respeito às medidas técnicas adotadas pelas organizações para evitar o vazamento de dados pessoais, após análise aprofundada do referencial bibliográfico sugere-se implementar as seguintes medidas de proteção de rede de acordo com Hintzbergen, Smulders e Barrs (2018):

- NAC (*Network Access Control* - Controle de Acesso à Rede). É crucial estabelecer procedimentos e atribuir responsabilidades para a gestão de equipamentos de rede quando se trata da interconexão de sistemas dentro de uma mesma empresa. Esses procedimentos devem ser desenvolvidos e implementados com antecedência, com o objetivo de mitigar os riscos de segurança evitáveis. Mesmo que as aplicações individuais possam ser protegidas eficazmente, é importante reconhecer que vulnerabilidades podem surgir quando essas aplicações estão interligadas. Isso é evidenciado em cenários como sistemas de administração e contabilidade, nos quais informações são compartilhadas entre diferentes setores da organização.
- Uma rede privada virtual (VPN) faz uso de uma rede já existente, normalmente a Internet, a fim de permitir a troca de informações entre redes geograficamente separadas como se estivessem na própria rede da empresa. Os dados são efetivamente protegidos – garantindo assim a sua integridade, autorização e autenticidade – enquanto são enviados. Muitos protocolos técnicos foram desenvolvidos para assegurar a disponibilidade desse serviço, destacando assim a importância da utilização de uma VPN para garantir a segurança dos dados.

- EDR (*Endpoint Detection and Response* - Detecção e Resposta a *Endpoint*) representa uma estratégia integrada e em camadas para a proteção de *endpoints*, que envolve o monitoramento contínuo em tempo real e a análise de dados dos dispositivos de *endpoint*, aliados a respostas automatizadas baseadas em regras. Com o aumento da prática do trabalho remoto, a segurança sólida de *endpoints* se torna um elemento cada vez mais crucial na estratégia de segurança cibernética de qualquer organização. A implementação de uma solução eficaz de EDR desempenha um papel fundamental na proteção tanto da empresa quanto dos trabalhadores remotos contra ameaças cibernéticas.
- ATP (*Advanced Threat Prevention* - Prevenção de Ameaças Avançadas) é uma categoria de soluções de segurança projetadas para se defender contra ameaças de *malware* sofisticado e ataques direcionados por *hackers* visando dados confidenciais. Essas soluções avançadas podem estar disponíveis tanto na forma de *software* quanto como serviços gerenciados. Embora as abordagens e os componentes das soluções de ATP possam variar, a maioria delas inclui uma combinação de agentes de *endpoint*, dispositivos de rede, *gateways* de *e-mail*, sistemas de proteção contra *malware* e um console de gerenciamento centralizado para correlacionar alertas e administrar as defesas.
- WAF (*Web Application Firewall* - Firewall de Aplicação *Web*) o funcionamento dos f*irewalls* e WAFs varia de acordo com a instalação e as camadas de atuação de cada tipo. Quando comparados no contexto do Modelo OSI, os *firewalls* tendem a operar nas camadas mais externas, mais distantes do usuário final, enquanto os WAFs atuam em camadas mais próximas do usuário, oferecendo uma proteção mais específica para aplicativos *web.*
- DLP (*Data Loss Prevention* - Prevenção de Perda de Dados) é uma solução projetada para evitar a perda de dados, abrangendo a descoberta de dados em repouso, o monitoramento de dados em trânsito e o bloqueio desses dados para evitar acessos não autorizados. A análise é conduzida com base em políticas compostas por regras que determinam as ações a serem tomadas após a identificação de correspondências, incluindo o bloqueio, a quarentena, a notificação ao ponto focal da política ou até mesmo o envio de um *e-mail* personalizado solicitando treinamento em Segurança da Informação para o usuário responsável pela infração.
- IDM ou IAM (*Identity and Access Management* - Gerenciamento de Identidade e Acesso) assegura que somente pessoas autorizadas tenham acesso aos recursos tecnológicos necessários para desempenhar suas funções de trabalho.
- MFA (*Multi-Factor Authentication* - Autenticação de Múltiplos Fatores) Esse processo acrescenta uma segunda ou mais camadas de segurança ao acesso de uma conta. Ele requer que o usuário, além de inserir a senha correta, valide o acesso por meio de um segundo código verificador temporário.
- IPS *(Intrusion Prevention System* - Prevenção de Intrusão de Rede) é uma abordagem preventiva de segurança de rede que tem como objetivo detectar possíveis ameaças e responder rapidamente a ataques cibernéticos. O funcionamento do IPS envolve a coleta de dados dos usuários, a análise de padrões comportamentais, o monitoramento do fluxo de dados, entre outros elementos. Com base nessas informações e no conhecimento prévio de padrões de ataques, é possível identificar se uma atividade em curso é maliciosa ou não.

- IDS (*Intrusion Detection System* - Detecção de Intrusão de Rede) é um sistema que monitora ativamente uma rede em busca de eventos que possam violar as regras de segurança estabelecidas para essa rede. Esses eventos incluem atividades anômalas de programas, detecção de *malwares* e invasões de nós na rede. O funcionamento do IDS envolve a coleta de dados dos usuários, que são posteriormente analisados quanto a padrões comportamentais, fluxo de dados, horários e outros parâmetros relevantes. A combinação dessas informações com o conhecimento prévio de padrões de ataques conhecidos permite ao IDS discernir se um evento em curso é malicioso ou não.
- CASB (*Cloud Access Security Broker* - Rompedor de Segurança de Acesso à Nuvem) são *softwares* que podem ser implantados na nuvem ou localmente, e atuam como intermediários entre os consumidores de serviços em nuvem e os provedores desses serviços. Sua função principal é impor políticas de segurança, conformidade e governança para aplicativos em nuvem. Essas soluções auxiliam as organizações a estenderem os controles de segurança de sua infraestrutura local para ambientes de nuvem.

A segurança do uso de dados é muito importante para as empresas. Para proteger as informações sensíveis, é necessário usar um *software* especializado que identifica ameaças, previne ataques e mantém os dados seguros.

De acordo com Santos e Silva (2021, p. 9), a Gestão da Segurança da Informação é baseada na interação entre processos, procedimentos, controles, melhores práticas e tecnologias, orientando os modelos utilizados.

Já Marcondes (2020), identifica quatro funções da gestão de segurança da informação que podem ser adotadas pelas organizações: planejamento, organização, direção e controle. O planejamento envolve a implementação de processos administrativos, com ações e medidas preventivas para reduzir vulnerabilidades e possíveis invasões. A organização abrange os procedimentos internos relacionados aos recursos humanos, *hardwares*, procedimentos, políticas e outros aspectos. A direção refere-se à capacidade dos gestores de liderar as equipes, motivando-os, por meio de uma boa comunicação, para alcançar os objetivos estabelecidos, coordenando e orientando as equipes. Além disso, o controle desempenha o papel de identificar falhas e corrigi-las.

A pesquisa de Alvarez e Marsal (2021) mostrou que a maioria das empresas reconhece a importância de investir em soluções de proteção de dados. Muitas delas já têm um *software* especializado ou planejam adquirir um em breve. A utilização desse tipo de *software* traz vários benefícios para as empresas. Ele permite gerenciar os dados de forma mais eficiente, com recursos avançados de criptografia, autenticação, controle de acesso e detecção de ameaças. Além disso, essas soluções são projetadas para cumprir as leis de privacidade de dados, como a LGPD no Brasil, o que garante conformidade legal e proteção extra para a empresa e seus clientes.

No contexto das instituições financeiras, é evidente que a implementação de medidas de segurança cibernética desempenha um papel essencial na salvaguarda de dados pessoais e na garantia da integridade de suas operações. A escolha e configuração dessas medidas variam substancialmente de acordo com diversos fatores, incluindo o tamanho da instituição, a abrangência de suas operações, os tipos de dados que ela lida e as políticas de segurança adotadas.

Uma prática comum entre as instituições financeiras de acordo com a pesquisa realizada pelos autores, é a utilização de uma combinação de medidas de segurança para reforçar a proteção dos dados sensíveis de seus clientes. Dentre essas medidas, pode-se citar o controle de acesso à rede (NAC), que desempenha um papel vital na gestão dos dispositivos de rede e na mitigação de riscos de segurança. Além disso, as redes privadas virtuais (VPNs) são amplamente empregadas para garantir a integridade e segurança dos dados durante a sua transmissão, especialmente em cenários de interconexão de sistemas geograficamente separados entre agências e matriz.

Outras medidas, como a *endpoint detection and response advanced threat prevention*, desempenham um papel crucial na proteção contra ameaças cibernéticas sofisticadas. O WAF é empregado para proteger especificamente os aplicativos da *web*, enquanto a *data loss prevention* é fundamental para evitar a divulgação não autorizada de informações confidenciais.

O *identity and access management* e a *multi-factor authentication* são adotados para controlar o acesso a recursos tecnológicos e garantir que apenas pessoal autorizado tenha permissão de acesso. Além disso, a IPS e a IDS são estratégias preventivas e reativas que monitoram e protegem contra atividades maliciosas na rede.

Cada instituição financeira ajusta sua estratégia de segurança com base em requisitos específicos e na evolução das ameaças cibernéticas. Consequentemente, a combinação de medidas de segurança adotadas pode variar de uma instituição para outra e se adaptar ao dinamismo das tecnologias e ameaças emergentes.

3. Resultados e Discussões

O presente estudo analisou a realidade de cinco agências bancárias levando em conta as maiores instituições financeiras do Brasil. Com base em entrevistas não estruturada com perguntas abertas sem um roteiro pré-definido, realizadas pelos autores em cinco das maiores agências da cidade de Americana – SP, sendo aqui preservados seus nomes em função do acordo de confidencialidade com estas agências. As resposta dessas cinco instituições foram efetivamente comparadas com os resultados da pesquisa que foi feita por Alvarez e Marsal (2021) e correlacionadas à realidade das práticas empresariais no contexto da LGPD no Brasil.

Os resultados obtidos pelas entrevistas nas agências bancárias, demonstraram uma clara validação dos dados apresentados neste artigo, evidenciando que as implicações da LGPD são mais do que meramente teóricas, impactando diretamente nas operações e estratégias adotadas pelas organizações.

No estudo, identificou-se que realmente, as organizações financeiras nacionais se prepararam mais para a implementação de proteção dos dados, enquanto empresas de outros setores e de menor porte não dispenderam de grandes investimentos nessa área.

Os resultados da pesquisa em campo por meio das entrevistas, amplamente reforçaram a relevância da LGPD como um marco regulatório de impacto significativo nas práticas empresariais brasileiras. Os casos discutidos e verificados na prática ilustram a complexidade da adaptação e a diversidade de abordagens.

No contexto da implementação da LGPD, foi crucial entender como as instituições financeiras se prepararam para garantir a conformidade com as disposições da lei. Isso envolve uma série de aspectos, desde a coleta, processamento e armazenamento de dados pessoais dos clientes até a proteção desses dados por meio de medidas de segurança e políticas de privacidade.

Para saber sobre essa preparação, foram pensadas algumas perguntas-chave, sendo elas embutidas na entrevista aberta. Por exemplo, como a instituição financeira se preparou para lidar com solicitações de acesso, correção ou exclusão de dados pessoais dos clientes, como exigido pela LGPD? Além disso, foi questionado quais foram as principais medidas de segurança e políticas de privacidade que a instituição financeira implementou como parte de sua preparação para proteger os dados pessoais dos clientes em conformidade com a LGPD?

Outra questão relevante é se a instituição financeira realizou preparações específicas, como auditorias ou avaliações regulares, para garantir a conformidade contínua com a LGPD, e, em caso afirmativo, como essas preparações foram conduzidas e quais medidas corretivas foram implementadas quando necessárias. Essas informações são essenciais para avaliar a eficácia das práticas de conformidade da instituição financeira em relação à LGPD e sua preparação para cumprir as regulamentações de proteção de dados.

As respostas obtidas destacaram a importância de manter a confidencialidade das políticas internas e procedimentos de auditoria. Por exemplo, quando questionadas sobre a preparação em relação à coleta, processamento e armazenamento de dados pessoais de clientes, as agências enfatizaram sua atenção ao detalhe de medidas de segurança, mas também afirmaram que os detalhes das políticas internas são sigilosos.

Entre algumas das respostas obtidas, a agência 1 citou: "Nossas políticas internas e procedimentos de auditoria são confidenciais, mas posso garantir que realizamos uma revisão completa de nossos processos e implementamos medidas de segurança de dados para cumprir a LGPD. E todos os funcionários foram capacitados se preparados para quando lei entrou em vigor". A agência 2 respondeu: "Nossa instituição financeira se preparou com muito cuidado para cumprir a LGPD, como políticas e treinamento interno, mas mais detalhes das políticas internas são confidenciais."

Semelhantemente à preparação para lidar com solicitações de acesso, correção ou exclusão de dados pessoais dos clientes, bem como a notificação de clientes em caso de incidentes de segurança de dados ou violações de privacidade, foram mencionadas como parte de suas práticas, mas com a observação de que as políticas internas são confidenciais. A agência 3 respondeu: "Nossas políticas internas e processos nos orientam sobre como responder a essas solicitações de maneira oportuna e em conformidade com a LGPD, " e a agência 4: "Lidar com solicitações de acesso e outras solicitações dos clientes está de acordo com nossos procedimentos internos, buscando sempre a confidencialidade dos dados e passados".

Além disso, as agências reconheceram a importância de auditorias e avaliações regulares, mas mantiveram a confidencialidade sobre os detalhes específicos dessas práticas. Tendo como resposta dada pela agência 5: "Conduzimos auditorias internas para manter a conformidade, averiguando os processos para que sempre sejam seguidas as normas de proteção e considera-se importante que se tenha auditoria interna e sejam implementas medidas corretivas conforme necessário." E agência 2: "Nossas auditorias são realizadas internamente e fazem parte de nossos esforços contínuos para cumprir a LGPD.

Todas as medidas corretivas necessárias são implementadas, mas não se pode divulgar detalhes específicos. Essas informações são essenciais para avaliar a eficácia das práticas de conformidade da instituição financeira em relação à LGPD e sua preparação contínua para cumprir as regulamentações de proteção de dados. Através da

FEBRABAN, todos os bancos, por lidarem com informações sigilosas, internalizaram a importância da proteção de dados e se prepararam com antecedência em relação à entrada em vigor da LGPD, o que os diferencia de outras áreas econômicas. Vale ressaltar que algumas dessas instituições são de cunho internacional, fato este que as conduziu anteriormente a se adequarem às práticas da GDPR.

A LGPD não apenas impõe responsabilidades legais, mas também fomenta uma cultura de respeito à privacidade que progressivamente se consolida em diversos setores econômicos, promovendo assim um ambiente mais seguro e confiável para a interação entre empresas e seus *stakeholders*.

A LGPD não é apenas uma regulamentação legal; ela representa um marco na conscientização sobre a importância da privacidade e da segurança dos dados. No entanto, a implementação eficaz da LGPD, conforme apresentado neste artigo, pode ser desafiadora para muitas empresas, mas no caso das instituições financeiras se tornou parte do processo.

A LGPD transcende o mero cumprimento legal; ela representa uma oportunidade significativa para aprimorar a segurança de dados e fomentar uma cultura de privacidade nas empresas nacionais. Nesse contexto, os bancos desempenham um papel crucial ao implementar medidas proativas para garantir a conformidade com a LGPD e proteger os dados pessoais de seus clientes.

Uma abordagem fundamental adotada por muitas instituições financeiras foi a preparação e conscientização de seus funcionários para as novas exigências legais. Isso envolveu a disponibilização de orientações e cursos internos durante o horário de trabalho. Como um exemplo, uma das instituições entrevistadas revelou que incorporou o treinamento em proteção de dados à sua lista de cursos obrigatórios oferecidos aos colaboradores.

O treinamento e a instrução dos funcionários desempenham um papel crítico nesse contexto. Conforme discutido na seção 2.5 deste artigo, as instituições financeiras frequentemente utilizam *software* e equipamentos especializados para controlar o acesso a dados e detectar tentativas de invasão. No entanto, um dos pontos mais vulneráveis nesse sistema é o fator humano. Funcionários mal-informados, mal-intencionados ou despreparados podem, acidentalmente ou intencionalmente, compartilhar informações confidenciais ou permitir acesso não autorizado a alguma conta. Conclui-se então que o fator humano se tornou um elo fraco na segurança dos dados.

Portanto, a conscientização e o treinamento adequado dos funcionários não são apenas uma medida de conformidade, mas uma defesa essencial contra ameaças internas, desempenhando um papel crucial na construção de uma cultura organizacional focada na proteção de dados e na promoção da segurança cibernética, contribuindo assim para o cumprimento eficaz da LGPD e a preservação da confiança dos clientes.

4. Considerações finais

O presente estudo permitiu captar, processar e entender a relação entre a LGPD e as instituições financeiras e como essas se adequaram às normas de proteção de dados. Umas das mais importantes observações junto a essas instituições é o fato delas darem grande importância ao ciclo de vida dos dados que são utilizados nas prestações de serviço. Os resultados ressaltam a importância e o impacto significativo que a LGPD trouxe para as operações e estratégias das organizações.

Outra conclusão vivenciada com a implementação da pesquisa é que empresas de maior porte demonstraram um comprometimento mais sólido com a adoção de medidas de proteção de dados, enquanto empresas de menor porte enfrentam desafios na aquisição de recursos para essa finalidade.

As instituições financeiras tem tido uma postura proativa, incluindo treinamento intensivo de seus colaboradores, em resposta à conscientização sobre as severas penalidades associadas a vazamentos de dados por meio de fator humano.

Constatou-se que a LGPD, além de sua natureza regulatória, configura-se como um propulsor para uma mudança significativa na percepção da importância da privacidade e segurança dos dados. Destaca-se o êxito das instituições financeiras que efetivamente implementaram e adotaram as diretrizes da LGPD em suas práticas, consolidando assim uma postura proativa na gestão e proteção das informações.

Com base nas conclusões destacadas, este estudo não apenas fornece *insights* valiosos sobre a interação entre a LGPD e as instituições financeiras, mas também oferece contribuições significativas para o mercado e outros tipos de instituições. A compreensão aprofundada da postura proativa das instituições financeiras, sua ênfase no ciclo de vida dos dados, e o comprometimento demonstrado por empresas de maior porte, fornecem um conjunto de melhores práticas que podem ser utilizadas para beneficiar o mercado em geral.

As observações sobre os desafios enfrentados por empresas de menor porte na implementação de medidas de proteção de dados oferecem *insights* (*insights* são percepções ou compreensões profundas sobre um assunto específico) úteis para desenvolver estratégias e políticas adaptáveis, considerando as limitações de recursos dessas organizações. A postura proativa das instituições financeiras, incluindo o treinamento intensivo de colaboradores, pode servir como um modelo inspirador para outras empresas que buscam elevar seus padrões de segurança de dados.

Ao destacar o êxito das instituições financeiras na efetiva implementação das diretrizes da LGPD, este estudo ressalta a necessidade de enxergar essa regulamentação, não apenas como um requisito legal, mas como uma oportunidade estratégica. Essa perspectiva pode servir como um catalisador para inspirar outras empresas a refinarem suas práticas de proteção de dados. Essas iniciativas não apenas as prepariam para os desafios da era digital, mas também fomentariam um ambiente empresarial mais seguro e ético. A LGPD, percebida como um marco regulatório, está redefinindo a abordagem das empresas brasileiras em relação à proteção de dados, impactando diversos setores. Sua implementação transcende a mera conformidade legal, oferecendo uma via para aprimorar práticas e enfrentar os desafios emergentes com responsabilidade e confiança.

Referências

ALVAREZ & MARSAL, **LGPD no mercado brasileiro**. 2021. Disponível em: https://www.alvarezandmarsal.com/sites/default/files/2021-11/E-book%20LGPD%20no%20Mercado%20Brasileiro.pdf Acesso em: 15 mar. 2023

BRASIL. Ministério da Economia. Secretaria Especial de Desburocratização, Gestão e Governo Digital. Departamento de Governança de Dados e Informações. Coordenação-Geral de Segurança da Informação. **Guia de elaboração de Termo de Uso e Política**

de Privacidade para serviços públicos. Brasília, setembro de 2021. Disponível em: Microsoft Word - guia_tupp.docx (ifes.edu.br). Acesso em: 14 out. 2023.

CNDL. Confederação Nacional de Dirigentes Lojistas. **8 milhões de consumidores sofreram golpes financeiros nos últimos 12 meses, aponta CNDL / SPC Brasil**. 2023. Disponível em: https://site.cndl.org.br/8-milhoes-de-consumidores-sofreram-golpes-financeiros-nos-ultimos-12-meses-aponta-cndl-spc-brasil. Acesso em: 29 out. 2023.

Clear Sale. Mapa da fraude da Clear Sale registra R$ 58 bilhões em tentativas de fraudes no Brasil em 2022. **E-commerce Brasil**. Disponível em: https://www.ecommercebrasil.com.br/noticias/mapa-da-fraude-clearsale-brasil-2022. Acesso em: 23 ago. de 2023.

FEBRABAN, **FEBRABAN lança guia de orientação aos bancos para a implementação da LGPD.** São Paulo. 2019. Disponível em: https://portal.febraban.org.br/noticia/3384/pt-br. Acesso em 01 nov. 2023

GARCIA, F. **Lei geral de proteção de dados pessoais:** manual de implementação. Salvador/BA: Ed. JusPodivm, 2019.

Hintzbergen, Jule; Baars, Hans; Smulders, André; Hintzbergen, Kees. **Fundamentos de segurança da informação com base na ISO 27001 e 27002**. Rio de Janeiro: Brasport Livros e Multimídia Ltda, 2018.

LGPD**. Lei geral de proteção de dados**. Brasília 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 03 mar. 2023

MACIEL, Rafael Fernandes. **Manual prático sobre a lei geral de proteção de dados pessoais:** atualizado com a medida provisória nº 869/18. Goiânia: RM Digital Education, 2019.

MARCONDES, J. S. **Gestão de segurança da informação:** o que é, o que faz, processos. 2020. Disponível em: https://gestaodesegurancaprivada.com.br/gestao-de-seguranca-da-informacao-conceitos-processos/.Acesso em: 13 maio 2023.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

SANTOS, R. B.; SILVA, T. B. Gestão da segurança da informação e comunicações: análise ergonômica para avaliação de comportamentos inseguros. **RDBCI: Rev. Dig. Bibliotec e Ci. Inf.** Campinas, São Paulo, v. 19, p. 1-31, 2021. Disponível em: https://periodicos.sbu.unicamp.br/ojs/index.php/rdbci/article/download/8665529/27400/109334. Acesso em: 13 maio 2023.

SEBRAE. **LGPD exige adequações de empresas a dados de clientes.** São Paulo: SEBRAE, 2020 Disponível em: https://sebrae.com.br/sites/PortalSebrae/artigos/lgpd-exige-adequacoes-de-empresas-a-dados-de-clientes-veja-o-que muda,fe51f2520da54710VgnVCM1000004c00210aRCRD. Acesso em: 20 jul. 2023

SERPRO. **Proteção de dados pessoais**. [S.l.]: SERPRO, 2019. Disponível em: https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-pessoais-lgpd. Acesso em: 30 maio 2023.