FUNDAÇÃO OSWALDO ARANHA
CENTRO UNIVERSITÁRIO DE VOLTA REDONDA
CURSO DE GRADUAÇÃO EM ADMINITRAÇÃO
TRABALHO DE CONCLUSÃO DE CURSO

MÁRIO VÍTOR LAZARONE FREITAS
PEDRO DE OLIVEIRA CARREIRO

RESPONSABILIDADE NO TRATAMENTO DE DADOS: CAMINHOS PARA A CONFORMIDADE COM A LGPD NO CONTEXTO EMPRESARIAL

VOLTA REDONDA
2024

FUNDAÇÃO OSWALDO ARANHA
CENTRO UNIVERSITÁRIO DE VOLTA REDONDA
CURSO DE GRADUAÇÃO EM ADMINITRAÇÃO
TRABALHO DE CONCLUSÃO DE CURSO

RESPONSABILIDADE NO TRATAMENTO DE DADOS: CAMINHOS PARA A CONFORMIDADE COM A LGPD NO CONTEXTO EMPRESARIAL

Trabalho de conclusão de curso apresentado ao curso de administração do UniFOA como requisito parcial à obtenção do título de Bacharel em Administração.

Alunos:
Mário Vítor Lazarone Freitas.
Pedro de Oliveira Carreiro.

Orientadora:
Profª Dra. Lucimeire Cordeiro da Silva

VOLTA REDONDA
2024

FOA UniFOA Centro Universitário de Volta Redonda

FOLHA DE APROVAÇÃO

Trabalho de Conclusão de Curso intitulado TRANSPARÊNCIA E RESPONSABILIDADE NO TRATAMENTO DE DADOS: CAMINHOS PARA A CONFORMIDADE COM A LGPD, elaborado por MARIO VÍTOR LAZARONE FREITAS e PEDRO DE OLIVEIRA CARRERO, apresentado publicamente perante a Banca Avaliadora, como parte dos requisitos para conclusão do curso de Bacharelado em Administração.

Aprovada em 05 dezembro de 2024

Banca Avaliadora:

Professor Orientador
Lucineia Pereira Ribeiro da Silva (Doutora, UNIFOA)

Professor Avaliador
Salete Leone Ferreira (Doutora, UNIFOA)

Professor Avaliador
Ariadne Yurkin Scandiuzzi (Doutora, UNIFOA)

RESUMO

O artigo objetiva examinar o impacto da Lei Geral de Proteção de Dados (LGPD) no contexto empresarial, com foco nas implicações para as práticas de coleta, armazenamento, processamento e compartilhamento de dados pessoais por empresas. A LGPD, promulgada no Brasil, tem como objetivo proteger a privacidade dos indivíduos e estabelecer diretrizes claras para as empresas lidarem com dados pessoais. Aborda-se a importância crescente da proteção de dados pessoais na era digital, destacando preocupações com a privacidade e segurança. São discutidos os principais aspectos da LGPD, incluindo seus princípios fundamentais, como finalidade, adequação, necessidade, transparência e segurança, e as responsabilidades que impõe às empresas. Explorou-se o impacto direto da LGPD no âmbito empresarial, incluindo a necessidade de adaptação às novas obrigações legais, tais como a nomeação de um encarregado de proteção de dados, a realização de avaliações de impacto de privacidade e a implementação de medidas técnicas e organizacionais para garantir a segurança dos dados pessoais. Em suma, a LGPD representa um marco importante na proteção de dados pessoais no âmbito empresarial. Sua implementação requer uma mudança de cultura, investimentos em recursos e uma abordagem proativa para garantir a conformidade e a segurança dos dados. As empresas que adotarem uma postura responsável em relação à proteção de dados estarão não apenas cumprindo a lei, mas também fortalecendo a confiança dos clientes e se destacando em um mercado cada vez mais preocupado com a privacidade e segurança das informações pessoais.

Palavra-chave: Lei Geral de Proteção de Dados. LGPD. Empresarial. Dados. Segurança

ABSTRACT

The article examines the impact of the General Data Protection Law (LGPD) in the business context, focusing on the implications for the collection, storage, processing, and sharing of personal data by companies. The LGPD, enacted in Brazil, aims to protect individuals' privacy and establish clear guidelines for companies to handle personal data. The article addresses the growing importance of personal data protection in the digital age, highlighting concerns regarding privacy and security. It discusses the key aspects of the LGPD, including its fundamental principles such as purpose, adequacy, necessity, transparency, and security, as well as the responsibilities it imposes on companies. The direct impact of the LGPD on the business realm is explored, including the need for adaptation to new legal obligations, such as appointing a data protection officer, conducting privacy impact assessments, and implementing technical and organizational measures to ensure data security. In short, the LGPD represents an important milestone in the protection of personal data at the corporate level. Its implementation requires a culture change, investment in resources and a proactive approach to ensuring compliance and data security. Companies that adopt a responsible stance towards data protection will not only comply with the law, but will also strengthen customer trust and stand out in a market increasingly concerned about the privacy and security of personal information.

Keywords: LGPD, business, data, security.

1 INTRODUÇÃO

As informações são de grande valia para o desenvolvimento do capital humano sendo utilizada de forma adequada, com a grande massa de dados se tornando informações de importância no mercado, as organizações querem que suas pesquisas e seu capital sejam preservados.

A procura por métodos de segurança de dados é de um crescente absoluto, o mercado cresce e as informações são adquiridas a todo instante, com essas informações é possível gerar produtos de grande valor no mercado e possivelmente chegar ao tão esperado sucesso de mercado.

Com a segurança dos dados em crescente, empresas apostam em software de segurança e de bons profissionais para manuseá-los com capacidade técnica impecável, grandes investimentos em back-up, dados em nuvem, servidores e muito planejamento e treinamento intensivo de seus usuários.

O treinamento de seus funcionários é uma das maneiras mais eficazes do mercado pois os dados de alguma forma passa por um humano, sendo assim o treinamento de boas práticas e prevenções é de grande valor para gerar segurança para dados valiosos no qual somos capazes manejá-los de forma correta quando assim capacitado e evitando que falhas humanas aconteçam melhorando a segurança das informações.

A tecnologia dos bancos de dados é de crescimento em grande escala e uma abundância de informação é adquirida todos os dias. Logo a busca por atualizações é constante para corresponder com a evolução do cenário. Com o crescimento e a importância do assunto, o conhecimento precisa ser adquirido para lidar melhor com a segurança das informações, sendo assim, evoluir junto ao crescimento da tecnologia. Com a grande demanda de armazenar informações com segurança e evitar quaisquer tipos de dano aos interessados, como forma de armazenar dados evitando e diminuindo o risco de invasões e ataques aos bancos de dados.

Assim, a LGPD – Lei Geral de Proteção de Dados, tem a sua devida importância, pois o seu objetivo é gerar proteção e normatização utilização dos dados tratados que geram informações.

Cada vez mais eminente são caso de exposição de dados pessoais na internet. A exemplo o vazamento de dados do Banco Pan que foi investigado pelo Ministério Público no Distrito Federal após noticiado pelo site (***The Hack***) em 22 julho de 2019,

supostamente teria sido exposto cerca de 245 gigabytes de dados, o equivalente a 1.235.151 arquivos de clientes ligado a instituição financeira.

1.1 Objetivo Geral

Examinar o impacto da Lei Geral de Proteção de Dados (LGPD) no contexto empresarial, com foco nas implicações para as práticas de coleta, armazenamento, processamento e compartilhamento de dados pessoais por empresas.

1.2 Objetivos Específicos

- Examinar as Tecnologias de Armazenamento Seguro;
- Avaliar as estratégias de Implementação de Segurança;
- Analisar Riscos de Vazamentos de Dados;

1.3 Justificativa

O presente estudo traz a recente Lei Geral de proteção de dados, que atualmente é de extrema importância visto que toda pessoa jurídica e física que trate de dados deve estar em conformidade com a mesma. Desta forma é esperado contribuir com esse tema no sentido de explicar de forma clara o que consta e como pode ser feita seu impacto no âmbito das instituições empresariais.

2 REFERENCIAL TEÓRICO

2.1. LGPD

A Lei nº 13.709 publicada em 14 de agosto de 2018 Lei Geral de Proteção de Dados Pessoais (LGDP) que entrou em vigência em 1º de agosto de 2020, tem por objetivo, proteger os direitos fundamentais de liberdade e privacidade e o tratamento de dados pessoais, inclusive em meios digitais. Ou seja, a LGDP obrigará as instituições financeira a regulamentar os modelos/métodos de proteção dos dados sigilosos que possuem acesso, informações estas que não devem ser públicas.

Aprovada no Brasil a Lei n. 13.709 de 14 agosto de 2018 que estabelece como primordialmente o disposto:

> 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)

Principalmente a (LGPD) possui em seus princípios a segurança, os entes obrigados a essa lei deverão utilizar-se de medição de técnicas e administrativas com a aptidão de favorecer a proteção dos dados pessoais. Saliente-se ainda que outros princípios são observados tais como: finalidade, adequação, necessidade, livre acesso, quantidade de dados, transparência, prevenção, não discriminação e responsabilização e prestação de conta (Lei n. 13.709, 2018).

Dessa forma, a segurança de modo geral é importante, o profissional que recebe acesso a dados restrito é responsável por sua segurança, devendo verificar e identificar brechas que apontam falhas e erros de segurança e todo acesso deverá ser registrado para controle de verificação (Alves, 2006)

Machado (2004) afirma que, para o dado ficar protegido do uso indevido de qualquer usuário, a linguagem SQL permite a definição dos privilégios que cada um pode ter em relação às tabelas criadas no banco de dados. Dessa forma, os privilégios garantem a segurança e a integridade dos dados, bem como a responsabilidade de cada usuário sobre seus dados específicos.

Como visto anteriormente que um acesso restrito usado de maneira maliciosa pode trazer um grande risco, segundo Sêmola (2003p. 67) “risco é a probabilidade de ameaças explorarem vulnerabilidades, provocando perdas de confidencialidade, integridade e/ou disponibilidade, causando, possivelmente, impactos nos negócios”.

Com um banco vulnerável exposto a riscos continuo o Alves (2006) aponta, que o tratamento contínuo do risco é de fundamental importância para que as empresas obtenham informações mais precisas quanto aos pontos fracos dos seus sistemas, pessoas, ambiente e outros.

Tratando-se de auditoria em segurança nos bancos de dados Lemos (2001) avalia que a função do auditor de sistemas é zelar para que as providências planejadas estejam sendo desempenhadas conforme o previsto e planejado, analisando-se aspectos como o de atendimento aos recursos orçados, sigilo das informações a dados processados pelos sistemas de informações empresariais,

manutenção do processo de produção de software em bons termos, conforme planos empresariais, cuidando para que sua função seja desempenhada no máximo sigilo, discrição, responsabilidade, compreensão dos envolvidos e atualizada nos termos técnicos que dizem respeito à produção de software.

Portanto após a utilização de ferramentas para auditoria e avaliação de acessos a ao banco de dados junto a utilização de acordo a Norma ABNT NBR 27002: 2005 para controle de acessos e boas práticas de manuseio será possível evitar falhas e diminuir os riscos exposto ao dia-a-dia de utilização dos dados (Brasil, 2005). Para buscar segurança é necessário conquistar boas práticas e para isso buscando capacitação para o profissional responsável, com o uso de normas e fiscalizações podemos reduzir o risco de se expor e não tornando vulnerável.

A segurança do banco de dados envolve a proteção do banco de dados contra acesso, modificação ou destruição não autorizada. Como o banco de dados representa um recurso corporativo essencial, a segurança do banco de dados é um subcomponente importante do plano geral de segurança dos sistemas de informação de qualquer organização (Lemos ,2001)

Além da necessidade de preservar e proteger os dados para o bom funcionamento da organização, os projetistas de bancos de dados têm a responsabilidade de proteger a privacidade das pessoas sobre as quais os dados são mantidos. Privacidade é o direito das pessoas de ter algum controle sobre as informações sobre si mesmas (Sêmola, 2003)

Muitos países têm leis projetadas para proteger a privacidade, e toda organização que coleta e armazena informações sobre indivíduos é legalmente obrigada a adotar políticas que estejam em conformidade com a legislação de privacidade local.

Segundo os Elmasri e Navathe (2011), nos Estados Unidos, o design do banco de dados deve refletir o compromisso da organização com a proteção dos direitos de privacidade individuais, incluindo apenas os itens que a organização tem o direito de conhecer e mantê-los seguros. A segurança das informações geralmente segue o modelo da CIA, onde a CIA representa confidencialidade, integridade e disponibilidade.

A confidencialidade exige que apenas usuários autorizados tenham acesso a informações para preservar a privacidade de indivíduos, propriedade intelectual comercial e esforços de segurança nacional. Com o crescimento das mídias sociais e

dos negócios on-line devido à Internet, manter a confidencialidade envolve o uso de técnicas de criptografia apropriadas, bem como procedimentos de autorização, identificação e autenticação do usuário (Lemos ,2001)

A integridade exige que apenas usuários autorizados possam modificar dados, mantendo assim a consistência e a confiabilidade dos dados. Se os dados estiverem incorretos, não serão mais úteis. Dados incorretos também podem ser prejudiciais para indivíduos (como dados incorretos em um relatório de crédito) e organizações (como relatórios financeiros inválidos) (Sêmola, 2003)

De acordo o Sêmola (2003) a disponibilidade exige que as informações sejam acessíveis por usuários autorizados, quando necessário. E os ataques de segurança contra uma organização podem fazer com que os serviços de negócios fiquem indisponíveis, levando a violações dos acordos de nível de serviço que são críticos para as operações de negócios. Para tanto se fazer necessário o surgimento de preceitos que visem assegurar a segurança das informações ao que se refere as informações.

São apresentadas várias propostas de modelos de segurança discricionários e obrigatórios para a proteção de bancos de dados convencionais e sistemas de banco de dados orientados a objetos. Ainda assim, não há um padrão para projetar esses modelos de segurança.

Existem vários tipos de ataques e ameaças contra os quais um banco de dados deve ser protegido. Neste trabalho, serão demonstradas soluções da maioria das ameaças mencionadas, embora algumas sejam boas, enquanto outras são apenas temporárias. Diferentes tipos de ameaças são discutidos neste documento (REGINA, 2021)

De acordo Alves (2006) ressalta que, a armazenagem de dados podem ser consideradas como a espinha dorsal de muitos aplicativos atualmente. Eles são a principal forma de armazenamento para muitas organizações. Portanto, os ataques aos bancos de dados também estão aumentando, pois são formas muito perigosas de ataque. Eles revelam dados importantes ou importantes para o invasor.

Para o Elmasri e Navathe (2011) há dois tipos de criptografia em relação ao uso de chaves. A sua utilização é para primar pela segurança das informações, que são de extrema necessidade para uma empresa. E o seu método é cifrar ou decifrar uma mensagem usando a mesma chave tanto para o ciframento quanto para o

decifrамento, este pode ser considerado como sistema de criptografia por chave simétrica ou chave secreta.

Aprovada no Brasil a Lei n. 13.709 de 14 agosto de 2018 que estabelece como primordialmente o disposto. Esclarece o Art. 1º da Lei 13.709 de 14 de 2018. (Brasil, 2018).

A Lei n. 13.709 não será aplicada no tratamento de dados pessoais, em virtude de pessoa natural para fins exclusivamente particulares e não econômicos, jornalístico e artísticos ou acadêmicos, no entanto torna-se efetiva para fins de segurança pública, defesa nacional, segurando do Estado ou atividades de investigação e repressão de infrações penais (Lei n. 13.709, 2018).

No que diz respeito ao tratamento de dados pessoais, poderão ser realizados desde que, haja consentimento do titular e esta manifestação deve ser por escrito ou outro meio que evidencie a vontade do titular.

Também serão realizados, para o cumprimento de obrigações legal ou regulatória pelo controlador; para o exercício regular de direito em processo judicial, administrativo ou arbitral; para proteção da vida ou incolumidade física da titular ou de terceiros; para a proteção de crédito, inclusive quanto ao disposto na legislação pertinente (Lei n. 13.709, 2018).

A toda pessoa natural é assegurada a titularidade de seus dados pessoais, garantido seus direitos fundamentais e assegurando a confirmação da existência de tratamento; acesso aos dados; correção de dados incompletos, inexistentes ou desatualizados, anonimização, bloqueio ou eliminação de dados desnecessários (Lei n. 13.709, 2018).

2.2 Agentes da Lei

A Lei passou a obrigar os agentes de tratamento, pessoas físicas ou jurídicas de direito público ou privado a indicar um encarregado pelo tratamento de dados pessoais e adoção de medidas de segurança, técnica e administrativa aptas a proteger os dados pessoais de acessos não autorizados ou qualquer outra forma de tratamento inadequado ou ilícito.

Aos controladores e operadores cabem o exercício das boas práticas de governança dos dados pessoais, desde que, atenda os princípios indicados na Lei n.

13.709 em observância a estrutura, escala e volume de suas operações. A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado.

O controlado que causar qualquer tipo de dano (patrimonial, moral, individual ou coletivo) no exercício do tratamento dos dados pessoais é obrigado a repará-lo. Os agentes de tratamento de dados que descumprirem os dispostos neste Lei em relação às normas dos dados pessoais estarão sujeitas as sanções, tendo como principais: advertência, com prazo pré-estipulado para correção; multa simples de até 2% (dois por cento) do faturamento da pessoa de direito privado limitado ao valor de R$ 50.000.000,00 (cinquenta milhões de reais) por infração; bloqueio dos dados pessoas até sua regularização e proibição total ou parcial de suas atividades. Para análise aplicação e direito à defesa dos controladores e operadores com relação as infrações será levado em consideração algumas premissas da (LGPD), tais como, gravidade e natureza da infração; a boa-fé do infrator, grau de dado; a cooperação do infrator; condição econômica; pronta adoção de medidas corretivas; procedimentos internos capazes de minimizar os dados e boas práticas de governança (Brasil, 2018).

2.3 Dados Pessoais, de Acordo a LGPD

Através do advento da tecnologia, nos últimos tempos, a sociedade passou por mudanças consideráveis em diversos âmbitos. O advento da tecnologia trouxe consigo a necessidade de se reinventar e consequentemente passou a surgir novas formações de relações interpessoais.

Neste sentido, a preocupação com a transmissão dos dados, também deve ser algo determinante das mídias sociais. Um fator importante neste aspecto foi a origem desta lei, que foi através da repercussão com a divulgação dos dados gerados pela rede social facebook (Regina, 2021)

Pode-se compreender que, este preceito legal se destina aos tratamentos de dados pessoais, inclusive na esfera digital, por pessoa natural ou pessoa jurídica, objetivando a proteção dos direitos fundamentais, sendo estes: da liberdade, dignidade da pessoa humana, privacidade e do livre desenvolvimento da personalidade natural, estes princípios são estabelecidos pela Constituição Federal de 1988. Assim, será apresentado os princípios e fundamentos da LGPD.

2.4 Princípios da LGPD

Estão definidos pela lei, no Capítulo II, Seção I, os requisitos para o tratamento de dados pessoais, mas antes vamos voltar ao artigo 6o do Capítulo I para compreender os princípios que serão utilizados com as hipóteses que lhe fornecerão a base legal para poder tratar os dados pessoais**.**

No artigo 6º da lei, é demonstrado os princípios de boa-fé que devem levar em consideração no tratamento de dados pessoais: Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

A boa fé é um dos princípios estampados no artigo 4º acima demonstrado no inciso III e constitui um dos preceitos que norteiam a conduta da sociedade, tendo sido normatizada pelo legislador. Ela ainda aprece em outros momentos no CDC, a exemplo do artigo 51, que trata das cláusulas abusivas do inciso IV, que seriam aqueles que estabelecem "[...] obrigações consideradas iniquas, abusivas, que coloquem o consumidor em desvantagem exagerada, ou sejam incompatíveis com a boa-fé ou a equidade" (Brasil, 1990)

Desta forma, nota-se que o espirito da legislação é positivar uma conduta de lealdade entre agente das relações de consumo, valorizando o equilíbrio e a boa fé independentemente de uma verificação da existência da má fé subjetiva, ou seja, a regra é a boa-fé.

O princípio da boa-fé contratual é também balizador das relações de consumo eletrônicos. Tal princípio propugna aos contratantes a missão de buscarem a verdadeira intenção das partes no momento da contratação e não o sentido literal da linguagem, conforme dispõe o art. 85 do Código Civil de 2002. Em toda relação contratual a boa-fé é presumida, devendo indicar a harmonia, a transparência e o equilíbrio na relação jurídica formalizada.

O contrato de consumo virtual é considerado móvel e dinâmico, pois os meios eletrônicos se canalizam cada vez mais para sistemas móveis de comunicação. Assim, a comunicação não mais se restringe a computadores localizados em espaços territoriais fixos e delimitados, apresentando-se altamente dinâmica, como por meio de aparelho celular ou televisão por exemplo. Como ressalta Ronaldo Alves de Andrade (2004**).**

São contratos à distância aqueles celebrados sem a presença física simultânea do comprador e do vendedor, de maneira tal que a oferta é lançada e a aceitação é confirmada por um meio de comunicação à distância de qualquer natureza, que permita a formalização do negócio jurídico.

3. IMPACTOS DA LEI NO ÂMBITO EMPRESARIAL

3.1 Responsabilidade das empresas

O relatório de impacto à proteção de dados pessoais (RIPD) também conhecido como *Data Protection Impact Assessment* (DPIA) pode ser considerado como um documento de valor legal que deve trazer detalhes de todos os processos de tratamento pelos quais, as informações pessoais passam durante o seu ciclo de vida (Regina, 2021)

Assim, deve contemplar os riscos da aplicação da segurança. Ou seja, é um documento que possui a exibição de um panorama do tratamento de dados na organização, e a criação desse documento pode favorecer ao auxilio na identificação ajudar de pontos de importantes no processo de conformidade. Assim, deve ser dado o início na criação desse relatório, enquanto o processo de conformidade deve ter a sua aplicação é uma forma de contribuir para que todos os requisitos legais estejam em conformidade. Esse relatório pode ser considerado obrigação legal, mesmo que não se tenha o requisitado. (Maia, 2020)

A tarefa de mapeamento dos dados sensíveis deve ser realizada para favorecer auxilio para contribuir com a identificação dos controles de segurança que devem ser adotados na proteção dessas informações

Após o mapeamento dos dados, é necessário favorecer a sua aplicação com medidas de segurança e proteção para favorecer a confiabilidade e garantia de que o tratamento de dados tenha a sua execução com o mais alto nível de proteção. (REGINA, 2021)

O Relatório de impacto à proteção de dados pessoais é uma exigência legal. Encontramos a referência ao relatório de impacto à proteção de dados pessoais no artigo 5º: Art. 5º Para os fins desta Lei, considera-se:

> [...] XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos

> fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

Esse documento deverá ser criado pelo controlador (empresa controladora), e nele deverão constar todos os detalhes sobre os dados e como é feito o seu tratamento desde a coleta, o que inclui especificar a base legal usada até o fim do ciclo de vida, informação em que devem constar ainda todas as medidas utilizadas na proteção e na garantia da privacidade. (Regina, 2021).

3.2 Principais desafios das empresas na adequação à Lei.

Com a LGPD, tem-se mais um grande motivo para treinar os usuários da empresa a se conscientizarem de que agora existe uma regulamentação que envolve o tratamento de dados pessoais e que cada pessoa na empresa deve entender e saber o seu papel diante dessa regulamentação. As chances de uma empresa em que os funcionários foram treinados e conscientizados sobre as regulamentações da LGPD sofrer com multas e advertências serão muito menores (MAIA, 2020)

O treinamento é importante pois os dados pessoais podem ser tratados muitas vezes, direta ou indiretamente. E sem o conhecimento ao menos básico da LGPD, os usuários podem iniciar um novo processo de tratamento para agilizar uma tarefa, o que certamente é feito com a melhor das intenções, porém ferindo a política de segurança da corporação e as leis.

3 METODOLOGIA

Trata-se de um artigo científico de natureza qualitativa e explicativa. A pesquisa qualitativa analisa os casos de maneira aprofundada e interpretativa das práticas adotadas pelas empresas em conformidade com LGPD. Para ocasionar o cumprimento dessa lei, garantindo a proteção de dados pessoais de seus clientes.

Quantos aos fins a pesquisa é descritiva e quanto aos meios bibliográfica e documental.

> As pesquisas descritivas têm como objetivo primordial a descrição das características de determinada população ou fenômeno ou, então, o estabelecimento de relações entre variáveis. São inúmeros os estudos que podem ser classificados sob este título e uma de suas características mais significativas está na utilização de técnicas padronizadas de coleta de dados, tais como o questionário e a observação sistemática. (GiL, 2010, p. 42)

> A pesquisa bibliográfica é um apanhado geral sobre os principais trabalhos já realizados, revestidos de importância, por serem capazes de fornecer dados atuais e relevantes relacionados com o tema. O estudo da literatura pertinente pode ajudar a planificação do trabalho, evitar publicações e certos erros, e representa uma fonte indispensável de informações podendo até orientar as indagações. (Lakatos; Marconi, 2003, p. 158).

> A característica da pesquisa documental é que a fonte de coleta de dados está restrita a documentos, escritos ou não, constituindo o que se denomina de fontes primárias.

.

Com isso, a pesquisa é descritiva**,** bibliográfica e documental**,** porque busca caracterizar as práticas de conformidade com a LGPD de maneira detalhada, utilizando fontes bibliográficas e documentais para embasar as análises e conclusões.

4 RESULTADOS E DISCUSSÕES

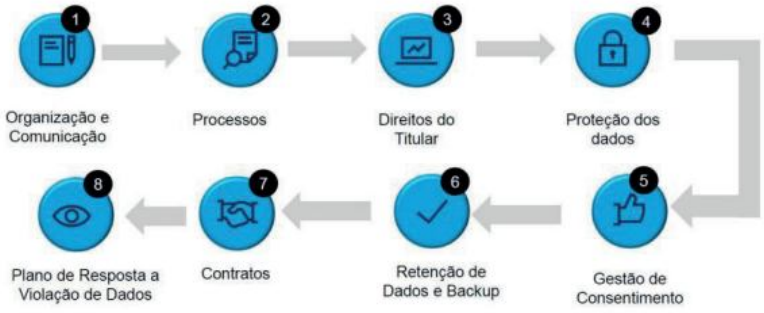
5.1 Implicações para as práticas de coleta, armazenamento, processamento e compartilhamento de dados pessoais por empresas.

A LGPD cria regras expressas sobre os processos de coleta, armazenamento e compartilhamento dessas informações, ajuda a promover o desenvolvimento tecnológico na sociedade e a própria defesa do consumidor, estabelecendo uma série de obrigações para a empresa que lida com dados pessoais.

A Lei nº 13.709/18 que estabelece as organizações deve adotar procedimentos internos de proteção de dados coletados, além da clara indicação de autorização do titular, que essa coleta de dados (nome, endereço, CPF, entre outros) tenha proteção e garantia de privacidade (Brasil, 2018).

As empresas devem garantir a **privacidade** e a **proteção** dessas informações por meio de políticas e práticas claras; utilizando apenas os dados essenciais para a utilização de serviço, a coleta de dados deve ter uma finalidade específica e não deve ser utilizada para outras finalidades sem o consentimento do usuário, ter transparência de como seus dados serão tratados, por quem, por quanto tempo, armazenados e compartilhados por terceiros, as empresas devem adotar medidas de segurança para proteger os dados contra vazamentos e devem ser responsáveis pelo comprimento da LGPD. A seguir a figura demostra os passos de forma mais clara:

Figura 1- Processo de tratamento de dados



Fonte: Brasil,2021.

5.2 Tecnologias de armazenamento seguras

As conexões VPN são criadas por roteadores, mas, os clientes devem entender que diferentes roteadores estabelecem essas conexões e saber qual é a melhor para eles. Há um roteador de consumo que suporta conexões VPN e um roteador empresarial que é mais dinâmico e oferece todas as medidas de segurança difíceis para os intrusos penetrarem e violarem os dados (Ezra et al., 2021).

De acordo com Ezra *et al* (2021), as VPNs são empregadas em diversos ramos, desde microempresas até grandes multinacionais, em colégios, universidade e governos. É graças a esse sistema que os dados e as informações podem manter-se seguras com seus proprietários, o uso dessa tecnologia vai conforme o esforço global em manter os dados e informações pessoais seguras, um dos exemplos dessa cooperação nacional e mundial é a sanção da Lei Geral de Proteção de Dados (13.709/2018).

Surge a necessidade de as organizações utilizarem uma tecnologia conhecida como VPN (do inglês, Virtual Private Network), o qual foi criado para permitir que as empresas tivessem conexões de rede seguras e protegidas.

O investimento em *firewalls*, sistemas de antivírus e outras tecnologias de segurança fornecem proteção, mas não impedem, de per si, que vazamentos de dados e brechas de segurança ocorram. É importante reconhecer que investir apenas na tecnologia, sem o necessário aporte em treinamento humano, simplesmente não é efetivo quando se trata de segurança.

5.3 Estratégias de Implementação de Segurança

Para dar conta do desafio da segurança da informação, especialmente de dados pessoais, é preciso que se desenvolvam práticas comprometidas com essa governança, o que envolve tarefas simples cotidianas, tais como: uso adequado da internet, com acesso aos sites seguros; não abrir links que acompanham e-mail suspeitos; adotar procedimentos e cuidados com os equipamentos e locais de trabalho; não acessar sites suspeitos no trabalho e com os equipamentos destinados e este fim; reportar ao setor competente a detecção de atividades que fogem ao padrão usual; ter cuidados com o descarte de papéis, relatórios e informações, especialmente aquelas relacionadas à tecnologia da informação; eleger senhas de acesso mais complexas e não as partilhar com terceiros; manter a tela do computador e as mesas de trabalho limpas, sem informações que configurem dados pessoais, dentre outras orientações simples, mas que precisam ser adotadas por todos os segmentos da empresa. (Noticebored, 2022).

Adotando essas práticas no seu dia a dia o individuo estará amparado em questões de segurança de seus dados pessoais, além de nunca compartilhar os dados pessoais e senhas de aplicativos com desconhecidos na internet. Em resumo, trata-se de ficar alerta no ambiente digital, para evitar riscos e proteger seus dados.

Os treinamentos e capacitações devem fazer parte da rotina da organização em todos os seus níveis, desde aquele que recebe os dados cadastrais dos titulares até quem responde pela tomada de decisão. Quanto a esses, vale lembrar que um gerente deve ser responsável por garantir que informações adequadas, conhecimento e treinamento cheguem a todos os setores. Sem um suporte de gerenciamento é possível que não existam recursos suficientes para a facilitação, compreensão e treinamento de todos (Government Communications Security Bureau, 2017).

A importância de uma boa gerência é uma reciclagem anual de capacitação na área que o trabalhador atua, fazendo com que todos da empresa que lidam com os dados pessoais de seus clientes estejam bem informados e capacitados para atende-lós da melhor maneira possível e com uma maior segurança.

O esforço para promover a segurança dos dados deve ser contínuo, o que exige a incorporação de boas práticas, pois estudos apontam que, sem treinamentos constantes, a atenção, consciência e o conhecimento dos trabalhadores degradam-se com o passar do tempo, ampliando as chances de incidentes de segurança.

Garantir de forma contínua que a segurança da informação seja de conhecimento de todos manterá os trabalhadores conscientes de eventuais problemas, contribuindo para que assumam suas responsabilidades (Government Communications Security Bureau, 2017).

Ao oferecer um serviço continuo, transmite ainda mais segurança para os clientes da empresa e mantém todos os trabalhadores alertas a respeito de alguma anomalia do sistema de segurança da empresa, além de ser fundamental para garantir que todos sabiam como agir no momento e como se resguardar desse empecilho do sistema**.**

5.4 Minimizar os riscos de vazamentos de dados

Um vazamento de dados é o pior pesadelo de uma organização. Seja por negligência do funcionário, uma ameaça interna ou resultado de um hack, um vazamento de dados pode resultar em problemas financeiros, de reputação e legais. Quando os arquivos confidenciais de uma organização são expostos, dados, como, números de CPF, números de cartão de crédito, telefone, informações financeiras e de saúde estão em risco.

> No Brasil, a realidade do vazamento de dados se torna cada vez mais preocupante. Em 2023, o país registrou **mais de 50 milhões de casos**. Essa estatística alarmante reforça a necessidade de as empresas tomarem medidas proativas para minimizar os danos causados por um incidente dessa natureza.

A popularização da internet junto aos mais diversos artefatos e meios tecnológicos facilitou os processos de comunicação e uso da informação. Conforme ressaltam Martins *et al* (2019, p. 711**),** “o advento da Sociedade da Informação, principalmente a partir das últimas duas décadas, acabou por mitigar, em certos aspectos, o que se concebe por vida privada”.

Ainda de acordo com Martins *et al* (2019),

> [...] a fase de geração de dados consiste naquela em que o usuário está no controle e pode alimentar o sistema de duas maneiras: ativa ou passiva. Para estes autores, na maneira ativa, o fornecimento dos dados pelo indivíduo ocorre de modo consciente a um terceiro; já na forma passiva, ao contrário, isso ocorre inconscientemente, como é o caso de um rastreio do comportamento do usuário em determinado site, por exemplo. Buscando garantir certa segurança e viabilizar autonomia ao usuário quanto ao uso dos seus dados pessoais, é que leis vêm sendo sancionadas para regulamentar e evitar violações à privacidade.

Essa citação em questão fornece informações de duas maneiras: ativa e passiva. Na geração ativa, o usuário tem controle sobre o que fornece, pois o usuário está ciente do fornecimento dos dados. Por outro lado, na geração passiva os dados são coletados sem o consentimento explicado do usuário. Um exemplo disso, é o rastreamento do comportamento online do usuário, como o monitoramento de suas ações em um site. Para garantir a segurança e a privacidade dos dados pessoais dos usuários, legislações vêm sendo criadas e implementadas para regulamentar o uso dessas informações e evitar abusos. A Lei Geral de Proteção de Dados (LGPD) no Brasil por exemplo, é a legislação que busca assegurar que as empresas tratem de dados pessoais de maneira ética e transparência.

5.5 Como proteger os dados dos clientes.

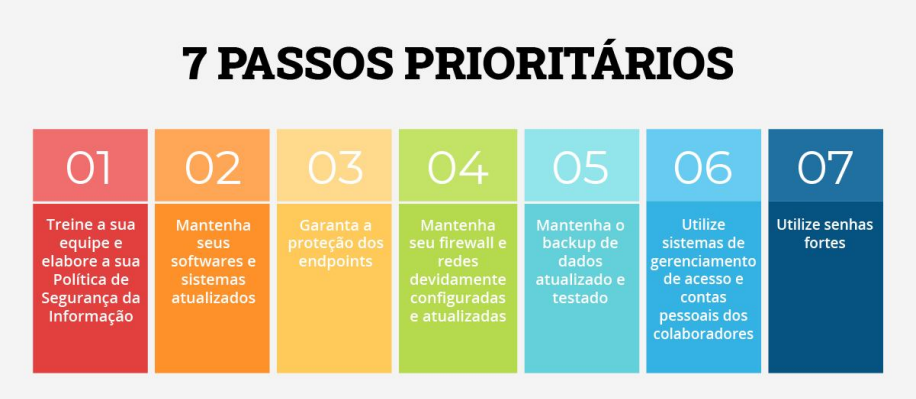
Investimento em segurança é a melhor maneira de evitar ser vitima de um vazamento de dados. As principais causas dos vazamentos de dados podem sem mitigadas com medidas de Segurança e Informação, incluindo treinamento de trabalhadores. Além disso, investir em segurança também é um requisito para esta em conformidade coma lei LGPD.

Conforme destaca ALMEIDA (et al., 2020, p. 2490), a “conformidade com as leis gerais de proteção de dados, portanto, requer tecnologia, infraestrutura e pessoal especializado para que os dados sejam tratados de forma lícita, justa e responsável em relação aos titulares”.

A proteção de dados pessoas devem ser de responsabilidade conjunta entre tecnologia, infraestrutura e recursos humanos qualificados. Não é possível assegurar que dados dos titulares serão tratados de maneira lícita, justa e responsável, conforme exigido pela legislação. Porém, a conformidade com as leis de proteção de dados não é apenas uma questão legal, mas também operacional e estratégica, exigindo a integração das diversas áreas dentro da organização.

Os passos mencionados abaixo são fundamentais para proteger os dados pessoais dos clientes e prevenir vazamentos de informações:

Figura 2 - Passos que integram ambiente de segurança.



Fonte: Rotta (disponível no site gepcompliance)

Esses passos integram um ambiente de segurança robusto, com várias camadas de proteção, defendendo de ameaças externas até a conscientização dos funcionários. Ajudando a garantir a conformidade com as leis de proteção de dados.

6. CONSIDERAÇÕES FINAIS

Com base em tudo o que foi mencionado, o objetivo dessa pesquisa é evidenciar as implicações de práticas de coleta de dados, armazenamento, processamento e compartilhamento de dados pessoais por empresas e destacar que a Lei Geral de Proteção de Dados (LGPD) tem um impacto significativo no contexto empresarial. A legislação visa proteger a privacidade dos indivíduos e estabelecer diretrizes claras para o tratamento de dados pessoais pelas empresas. No entanto, sua implementação e conformidade apresentam desafios para as organizações, especialmente as de menor porte, que possuem recursos limitados.

Um dos principais desafios é a criação de uma cultura de proteção de dados, tanto dentro das empresas quanto na sociedade em geral. É necessário sensibilizar os trabalhadores e as partes interessadas sobre a importância da privacidade e segurança dos dados pessoais, promovendo uma mudança de mentalidade e comportamento em relação ao tratamento dessas informações.

Além disso, as empresas enfrentam a necessidade de se adequarem às novas obrigações legais, como a nomeação de um encarregado de proteção de dados, a realização de avaliações de impacto de privacidade e a implementação de medidas técnicas e organizacionais para garantir a segurança dos dados pessoais. Essas

adaptações exigem investimentos em recursos humanos, tecnológicos e processuais, o que pode ser um desafio para empresas com recursos limitados.

No entanto, a conformidade com a LGPD não é apenas uma questão de cumprir as obrigações legais, mas também de proteger a reputação e a confiança dos clientes. Violações da lei podem resultar em sanções administrativas, multas e danos à imagem da empresa. Portanto, é fundamental que as organizações compreendam a importância da proteção de dados como um diferencial competitivo e adotem medidas proativas para garantir a conformidade e a segurança das informações pessoais dos usuários.

REFERENCIAS

ALMEIDA, Bethania de Araujo et al. Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global. Ciência & Saúde Coletiva, v. 25, p. 2487-2492, 2020.

ANDRADE, Ronaldo Alves de. Contrato eletrônico no novo código civil e no código do consumidor. Barueri: Manole, 2004.

ANDRION, Roseli; YUGE, Claudio. História da segurança virtual: a origem do antivírus de computador. 2021. Disponível em: https://canaltech.com.br/seguranca/historia-da-seguranca-virtual-a-origem-do-antivirus-de-computador-197745/. Acesso em: 05.2023.

BEZERRA, Juliana; Revolução Industrial. 2013. Disponível: https://www.todamateria.com.br/revolucao-industrial/. Acesso em: 05.2023.

BRANCO, Dácio Castelo; YUGE, Claudio. História da segurança virtual: a origem do vírus de computador. 2021. Disponível em: https://canaltech.com.br/seguranca/origem-do-virus-de-computador-197667/. Acesso em: 05.2023.

BRASIL. Constituição da República Federativa do Brasil. Brasília: Senado Federal, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

BRASIL. Decreto-Lei nº 2.848, de 07 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, 31 de dezembro de 1940.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Diário Oficial da União, Brasília, 3 de dezembro de 2012.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, 24 de abril de 2014.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Tribunal de Justiça de São Paulo. Disponível em: https://www.tjsp.jus.br/LGPD/LGPD/ALGPD#:~:text=A%20Lei%2013.709%2F18%20dispõe,livre%20desenvolvimento%20da%20personalidade%20natural. Acesso em: 3 nov. 2024.

BRASIL. Medida Provisória nº 869, de 27 de dezembro de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869.htm#:~:text=MPV%20869&text=Altera%20a%20Lei%20nº%2013.709,que%20lhe%20confere%20o%20art. Acesso em: 3 nov. 2024.

BRASIL. Supremo Tribunal de Justiça. Recurso especial Nº 1117633/RO, Relator: Ministro Herman Benjamin. Brasília, 09 de março de 2010. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/8569044/recurso-especial-resp-1117633-ro-2009-0026654-2/inteiro-teor-13668131. Acessado em: 17/07/2022.

BROOKSHEAR, J. Glenn. Ciência da Computação: Uma visão abrangente. 11ª. ed. – Porto Alegre: Bookman, 2013.

COTS, Márcio. Desafios na adequação das empresas à LGPD. In: CONGRESSO DE DIREITO DIGITAL, 10, 2019, São Paulo. Anais do 10º Congresso de Direito Digital. São Paulo: Editora ABCD, 2019. p. 123-138.

EZRA, P., MISRA, S., AGRAWAL, A., OLURANTI, J., MASKELIUNAS, R., & DAMASEVICIUS, R. (2021). Secured Communication Using Virtual Private Network (VPN). Lecture Notes On Data Engineering And Communications Technologies, 309-319. Disponível em: https://link.springer.com/chapter/10.1007/978-981-16-3961-6_27

FERREIRA, Ivette Senise. A criminalidade informática. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Co-ord.). Direito & internet: aspectos jurídicos relevantes. São Paulo: Quartier Latin, 2008, v.2. p. 213.

FERREIRA, Ivette Senise. Direito & Internet: Aspectos Jurídicos Relevantes. 2 ed. São Paulo: Quartier Latin, 2005, p. 261.

FONSECA, J. J. S. Metodologia da pesquisa científica. Fortaleza: UEC, 2002. Apostila.

GCSB, New Zealand Information Security Manual. Disponível em: https://nzism.gcsb.govt.nz/ism-document/. Acesso em: 14 fev. 2023.

GIL, Antônio Carlos. Como elaborar projetos de pesquisa. 4ª. ed. São Paulo: Atlas, 2002. Disponível em: https://files.cercomp.ufg.br/weby/up/150/o/Anexo_C1_como_elaborar_projeto_de_pesquisa_-_antonio_carlos_gil.pdf

GOVERNMENT COMMUNICATIONS SECURITY BUREAU (GCSB). Legislation. The Intelligence and Security Act 2017. Disponível em: https://www.gcsb.govt.nz/about-us/legislation. Acesso: 2 dez 2024.

JESUS, D. E. Direito penal – Parte Geral. Vol. 1. São Paulo: Saraiva: 2003.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. Fundamentos de metodologia científica. 5. ed. São Paulo: Atlas, 2003. Disponível em: https://docente.ifrn.edu.br/olivianeta/disciplinas/copy_of_historia-i/historia-ii/china-e-india/view

LEMOS, Aline Moraes. Política de Segurança da Informação. 2001, Monografia (Curso de Administração) – UNESA – Universidade Estácio de Sá, Rio de Janeiro – RJ.

MACHADO, F. N. R. Banco de Dados: projeto e implementação. São Paulo: Erica. 2004.

MAIA, Rafael. Lei Geral de Proteção de Dados Comentada. 2ª ed. São Paulo: Revista dos Tribunais, 2020.

MARTINS, Marcelo Guerra; JORGETTO, Leonardo Felipe de Melo Ribeiro Gomes; SUTTI, Alessandra Cristina Arantes. Big data e a proteção do direito à privacidade no contexto da sociedade da informação. Revista Jurídica Cesumar, Maringá, v. 19, n. 3, p. 705-725, set. /dez. 2019. Disponível em: https://10.17765/2176-9184.2019v19n3p705-725 Acesso em: 18 maio 2022.

NOTICEBORED. Information Security 101: back to basics. 2022. Disponível em: https://www.noticebored.com/html/infosec_101.html. Acesso em: 9 fev. 2023.

RAMOS, Pedro H.A. Regulação de proteção de dados e seu impacto para a publicidade online: um guia para a LGPD. Disponível em: https://www.udop.com.br/download/noticias/2020/03_03_20_arquivo_oab_pe.pdf#page=3. Acesso em: 03.2023.

REALE, Miguel. Teoria Tridimensional do Direito. 5ª ed., Editora Saraiva São Paulo, 2003.

REGINA, Luiza. Impactos da Lei Geral de Proteção de Dados (LGPD) no contexto empresarial. Revista de Direito Digital, v. 3, n. 2, p. 45-62, jul./dez. 2021.

ROQUE, André. A tutela coletiva dos dados pessoais na lei geral de proteção de dados pessoais (LGPD). Revista Eletrônica de Direito Processual – REDP, Rio de Janeiro. Ano 13. Volume 20. Número 2 Maio a Agosto de 2019. Disponível em: https://www.epublicacoes.uerj.br/index.php/redp/article/view/42138/30270. Acesso em: 22 Abr. 2022.

ROTA, Maurício. Multas da LGPD: saiba como evita-las. Blog GEP – Soluções em Compliance. Disponível em: https://www.gepcompliance.com.br/blog/multas-lgpd/. Acesso: 25 nov 2024.

SÊMOLA, Marcos. Gestão da segurança da informação: Uma visão executiva. Rio de Janeiro: Campus, 2003.

SÊMOLA, Marcos. Gestão da segurança da informação: Uma visão executiva. Rio de Janeiro: Campus, 2003.

SILVA, Rosane Leal da; SILVA, Raonny Canabarro Costa da; REHBEIN, Katiele Daiana Da Silva. A Proteção de Dados Pessoais por Agentes de Pequeno Porte a Governança e as boas práticas como estratégias de implementação da LGPD. Meritum, Revista de Direito da Universidade FUMEC, v;18, n.1. janeiro/abril, 2023. Disponível em: https://doi.org/10.46560/meritum.v18i1.9249. Acesso: 2 dez 2024.