CENTRO UNIVERSITÁRIO DOUTOR LEÃO SAMPAIO
PÓS-GRADUAÇÃO EM REDES DE COMPUTADORES COM ÊNFASE EM SEGURANÇA DA INFORMAÇÃO

EDSON RODRIGUES DO NASCIMENTO
ALAN DA SILVA CAVALCANTE

OBRIGATORIEDADE DA IMPLEMENTAÇÃO DA LGPD-LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NO AMBIENTE CORPORATIVO

JUAZEIRO DO NORTE-CE
2022

A OBRIGATORIEDADE DA IMPLEMENTAÇÃO DA LGPD-LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NO AMBIENTE CORPORATIVO

EDSON RODRIGUES DO NASCIMENTO
ALAN DA SILVA CAVALCANTE

Trabalho de Conclusão de Curso de pós-graduação, apresentado ao curso de Redes de Computadores com Ênfase em Segurança da Informação do Centro Universitário Doutor Leão Sampaio, como requisito para obtenção do título de especialista.
Orientador: Esp. Cláudio Joel Brito Lóssio

JUAZEIRO DO NORTE-CE
2022

RESUMO

Este trabalho foi realizado no intuito de conhecer de maneira prática, em um ambiente corporativo, a aplicabilidade e cumprimento da Lei da LGPD - Lei Geral de Proteção de Dados Pessoais. Sabe-se que muitas empresas estão se adaptando ao novo sistema da Lei em manter os dados pessoais protegidos de coletas ilegais. De fato, será difícil adaptar-se, imediatamente, por falta de estrutura e treinamentos qualificados em segurança de proteção de dados ao pessoal do estabelecimento comercial. Muitas empresas estão sendo vitimadas de ataques de hacking por falta de investimento em proteção e treinamentos; bem como, em equipamentos e estar em conformidade com a LGPD.

Palavras-Chave: LGPD. Obrigatoriedade. Privacidade. Governança. Conhecimento. Segurança da Informação.

ABSTRACT

This work was carried out in order to know in practice, in the corporate environment, if the LGPD Law - General Law for the Protection of Personal Data is being applied and complied with by the company's employees. It is known that many companies are adapting to the new system of the Law in keeping personal data protected from illegal collections. In fact, it will be difficult to adapt immediately, due to the lack of structure and qualified training in data protection security for the commercial establishment's personnel. Many companies are being victimized by hacking attacks due to lack of investment in protection and training; as well as in equipment and comply with the LGPD.

Keywords: LGPD. Obligatoriness. Privacy. governance. Knowledge. Information security.

1. INTRODUÇÃO

Com o advento da Lei Geral de Proteção de Dados - LGPD, Lei 13.709/2018, sancionada em agosto de 2021, diz que às instituições públicas e privadas devem manter os dados de seus clientes protegidos de terceiros, tem como princípio, proteger os direitos fundamentais de liberdade e privacidade dos cidadãos brasileiros.

No mercado de trabalho onde há cadastro de clientes, como por exemplo, uma empresa de Provedores de Serviços de Internet, percebe-se a importância da aplicabilidade de uma Política de Segurança e a contratação de um Oficial de Proteção de Dados – DPO, onde irá orientar os colaboradores da empresa a seguirem os regulamentos estabelecidos pela Lei Geral de Proteção de Dados - LGPD, assuntos relevantes que servem de base para o ambiente coorporativo da empresa. A LGPD favorecerá à organização do estabelecimento comercial e a obediência dos colaboradores com mais rigor em proteger os dados de todos aqueles que fazem parte da empresa, como: diretores, funcionários e clientes.

Muitos profissionais que trabalham com Tecnologia da Informação - TI, ainda não têm maturidade de segurança suficiente para trabalhar com as ferramentas de trabalho onde armazenam os dados, fazem a utilização de maneira ingênua possibilitando riscos ou danos aos dados sigilosos do estabelecimento corporativo, levando a empresa a ser multada caso haja alguma denúncia por parte do titular que foi prejudicado. É de fundamental importância a implementação de uma Política de Segurança de dados para que todos os integrantes da empresa possam seguir as regras conforme a Lei da LGPD (BRASIL, 2018).

Quando se diz ser um bom profissional de TI, não é somente saber manusear uma ferramenta computacional física, porém ter a responsabilidade e o conhecimento necessário em segurança de dados para não deixar vulnerabilidades causando riscos aos dados. Portanto, seguindo às regras da empresa em conformidade com a LGPD, garantirá que os dados estejam seguros de coleta ilegal e o profissional manterá segura a imagem da instituição, bem como, preservará seu emprego, evitando assim, uma demissão por justa causa ou responder judicialmente por não obediência aos princípios da segurança da informação assegurada pelos regulamentos que rege a LGPD – Lei Geral de Proteção de Dados.

2. JUSTIFICATIVA

A pesquisa realizada sobre a LGPD foi de fundamental importância, porque proporcionou conhecimentos relevantes que as empresas são obrigadas a implantar a Lei Geral de Proteção de Dados Pessoais no Ambiente Corporativo e aquelas que não aderirem os regulamentos estabelecidos poderão ser multadas por desobediência. Não é tão difícil de ser planejada e projetada a LGPD para uma instituição corporativa. O problema é convencer os colaboradores estarem em conformidades com a Lei e seguir o que o projeto de políticas da empresa determina. Por ser uma Lei nova, colaboradores ainda não tem maturidade de como proceder com suas atividades de maneira que os dados sejam compartilhados com segurança, mas através de um bom projeto e de pessoas qualificadas, facilitará a aplicabilidade da Lei da LGPD na instituição corporativa, seja pública ou privada. Somente depende da colaboração de todos os integrantes da empresa para que o projeto saia do papel e que esteja em execução.

2.1 CENÁRIO MUNDIAL DE CIBERATAQUES

Com o surgimento da tecnologia, o cenário mundial vive outra realidade em relação a segurança dos dados pessoais. A maioria dos dados que existe em um estabelecimento comercial são arquivados e armazenados no banco de dados em discos rígidos ou em nuvens com o objetivo de uma melhor segurança, mas mesmo assim estas informações não estão totalmente protegidas, devido a falhas de segurança que os usuários finais proporcionam na rede interna da empresa, muitas vezes por falta de conhecimento em segurança da informação, ocasionando vulnerabilidades, onde o invasor se aproveita destas brechas e coleta ilegalmente os dados que estão armazenados nos computadores. De acordo com o Art. 46 da LGPD, deve-se adotar técnicas de medida de segurança para que os dados estejam íntegros e protegidos de acessos não autorizados (BRASIL, 2018).

> Art. 46. Os agentes de tratamentos devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou lícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (BRASIL, 2018).

Conforme à citação do Art.46, é de fundamental importância que as empresas busquem por segurança para manter protegidos os dados dos seus clientes evitando que ocorra vazamento de informações, pelos funcionários ou por outras pessoas não autorizadas, porque a Lei está bem clara, que os dados devem ser mantidos em segurança, longe de tratamento inadequado ou ilícito, ou seja, manter a informação com total segurança de ocorrências acidental, perda ou destruição.

Sgundo Donda (2020), sempre que se fala em ataques, é comum virem à mente os hacking, e essa denominação ficou associada a algo sempre malicioso e ilegal. No entanto, um hacker vai além disso: este é um indivíduo que se dedica a conhecer os mecanismos e a entendê-los profundamente, a fim de solucionar problemas, principalmente no meio cibernético.

O hacker, como mencionado por Donda (2020), é o White Hat por ser um tipo de hacker ético e por estudar os sistemas computacionais com foco em segurança, se tornando um especialista em cybersecurity. Já o outro hacker existente, chamado o Black Hat, este sim, é um criminoso sem ética que utiliza seu conhecimento para

fins maliciosos invadindo o sistema computacional e coletando ilegalmente os dados pessoais e muitas vezes até ameaça o controlador ou operador da empresa a ter que pagar imensos valores em moedas bitcoin, caso o estabelecimento não pague, os criminosos apagam os dados ou divulgam na internet no intuito de prejudicar a vítima (DONDA, 2020).

No Brasil e no mundo, hackers estão sempre atacando virtualmente estabelecimentos públicos e privados. Muitas empresas estão sendo vitimadas destes ciberataques, um deles o chamado ransomware, um tipo de malware que restringe o acesso ao sistema infectado com uma espécie de bloqueio, em seguida cobrando um resgate em criptomoedas para que o acesso ao sistema computacional de determinada empresa invadida possa ser restabelecido, que torna praticamente impossível o rastreamento dos criminosos que podem virem a receber o valor (SOUZA, 2018).

Segundo informações do portal de notícias G1 (2021), o site do Ministério da Saúde, também foi alvo de ataques cibernéticos de ransomware. Na madrugada da sexta-feira, do dia 10-12-2021, o aplicativo e a página do ConecteSUS, plataforma que mostra comprovantes de vacinação contra a Covid-19 – foram invadidos por hackers. O problema também afetou o sistema de notificação de casos da doença.

A queda dos sistemas do SUS teve reflexos pelo país: em Salvador, onde o comprovante começou a ser exigido na rodoviária, passageiros não conseguiram embarcar. No Piauí, houve filas para a vacinação, no Acre, quem perdeu o comprovante em papel não consegue tomar a 2ª dose ou a dose de reforço; o mesmo aconteceu no Oeste de Santa Catarina. O governo do Tocantins diz que não consegue notificar casos e mortes de Covid. Ataques como estes sempre estão acontecendo, por falta de profissionais treinados e de investimentos de equipamentos sofisticados que favoreçam à proteção do sistema de dados em reter estes tipos de ataques cibernético (G1, 2021).

2.2 A CONFORMIDADE LGPD NO AMBIENTE CORPORATIVO

No Brasil, espelhado na Lei Europeia surgiu a Lei Geral de Proteção de Dados - LGPD, 13.709, DE 14 DE AGOSTO DE 2018, dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Assegura os direitos de proteção de dados digitais de todas as entidades, seja ela por pessoa física ou jurídica de autonomia pública ou privada no Estado Brasileiro. Estas normas devem ser observadas por todos os órgãos administrativos da União, Estados e Municípios. Com a evolução da tecnológica, modelos de negócios foram a principal motivação para o surgimento desta regulamentação de proteção de dados pessoais, tendo o papel de colocar regras necessárias, limitar abusos, definir os padrões e sessões administrativas em caso de não cumprimento com a Lei da LGPD (DONDA, 2020).

A Lei da LGPD terá grande importância para o Brasil tanto para as instituições públicas como privadas, porque as instituições irão se preocupar em resguardar as informações de forma segurança longe de acessos não autorizados por parte terceiros.

Segundo Pinheiro (2020), o motivo que inspirou o surgimento de regulamentações de proteção de dados pessoais de forma mais consistente e consolidada a partir dos anos 1990 está diretamente relacionado ao próprio desenvolvimento do modelo de negócios da economia digital, que passou a ter uma dependência muito maior dos fluxos internacionais de bases de dados, especialmente os relacionados às pessoas, viabilizados pelos avanços tecnológicos e pela globalização. Desse modo, houve a necessidade de resgatar e repactuar o compromisso das instituições com os indivíduos, cidadãos desta atual sociedade digital, no tocante à proteção e à garantia dos direitos humanos fundamentais, como o da privacidade, já celebrados desde a Declaração Universal dos Direitos Humanos (DUDH) de 1948.

A base deste pacto é a liberdade, mas o fiel da balança é a transparência. Sendo assim, as leis sobre proteção de dados pessoais têm uma característica muito peculiar de redação ao conjunto de princípio e de amarração com indicadores mais assertivos, de ordem técnica, que permitam auferir o compromisso se está sendo cumprido, por meio da análise de trilhas de auditoria e da implementação de uma série

de itens de controle para uma melhor governança dos dados pessoais (PINHEIRO, 2020).

A liderança de debate sobre o tema surgiu na União Europeia (UE), em especial com o partido The Greens, e se consolidou à promulgação do Regulamento Geral de Proteção de Dados Pessoais Europeu n. 679, aprovado em 27 de abril de 2016 (GDPR), com o objetivo de abordar a proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, conhecido pela expressão “free dada flow”. O regulamento trouxe a previsão de dois anos de prazo de adequação, até 25 de maio de 2018, quando se iniciou a aplicação das penalidades. Este, por sua vez, ocasionou um “efeito dominó”, visto que passou a exigir que os demais países e as empresas que buscassem manter relações comerciais com UE também deveriam ter uma legislação de mesmo nível que o GDPR. Isso porque o Estado que não possuísse lei de mesmo nível passaria a poder sofrer algum tipo de barreira econômica ou dificuldade de fazer negócio com os países da UE. Considerando o contexto econômico atual, esse é um luxo que a maioria das nações, especialmente as da América Latina, não poderia se dar (PINHEIRO, 2020).

Segundo a autora Patrícia Peck Pinheiro, na Europa, já estava previsto a Carta dos Direitos Fundamentais da União Europeia e no Tratamento sobre o Funcionamento da União Europeia; no Brasil, já tinha previsão no Marco Civil da Internet e na Lei do Cadastro Positivo, mas a questão ainda era, muitas vezes, observada de forma difusa e sem objetividade no tocante aos critérios que serão considerados adequados para determinar se houve ou não guarda, manuseio e descarte dentro dos padrões mínimos de segurança condizentes. Foi nisso que a nova legislação inovou, ou seja, padronizou, ou melhorou, normalizou, quase como uma norma ISO, o que seriam os atributos qualitativos da proteção dos dados pessoais sem a presença dos quais haveria penalidades (PINHEIRO, 2020).

Muitas instituições que utilizam dados de pessoas não imaginam a importância que a Lei da LGPD – Lei Geral de Proteção de Dados proporciona na proteção do estabelecimento empresarial, evitando assim, que os dados sejam vazados para terceiros. A empresa por mais despreparada que esteja financeiramente, precisa se adaptar ao novo sistema através de qualificações que favoreçam no aprendizado dos seus funcionários para que evite mais tarde penalidades à empresa no geral.

Conforme a Lei do Marco Civil da Internet sobre a proteção de dados pessoais: Art. 1º da LGPD, 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 (FIORILLO, 2017).

Donda (2020), o artigo 1º deixa claro que a lei se aplica ao tratamento de dados que seja feito por pessoa natural, física, ou pessoa jurídica, quando menciona pessoa jurídica, refere-se tanto a de direito público quanto privado: Pessoa jurídica de direito público, são entidades ligadas a União, estados, Distrito Federal, territórios, municípios e autarquias como INSS, já pessoas jurídicas de direito privado, dividem-se entre particulares e estatais. As particularidades são formadas por iniciativas privadas e constituídas apenas com recursos particulares; já as estatais são aquelas em que houve contribuição do Poder Público para o capital. Como por exemplo, temos empresas, fundações, associações (civis, religiosas etc.), cooperativas, políticas e outros.

Já no artigo 3º, Donda (2020) diz que a lei se aplica quando os dados estiverem sendo tratados em território nacional, ou se os dados tiverem sido coletados em território nacional, independentemente do país onde a sede da empresa ou do país onde estejam localizados os dados, sendo uma lei com alcance extraterritorial.

2.3 GOVERNANÇA COORPORATIVA E O ENCARREGADO DE PROTEÇÃO DE DADOS

A governança em TI no ambiente corporativo de uma empresa, é um conjunto de boas práticas em manter um perfeito funcionamento de uma organização. Uma boa governança em TI, significa assegurar que os dados pessoais estejam protegidos com boas ferramentas de segurança e medidas de segundo plano em serviços de recuperação rápida caso haja percas dos danos. Manter uma boa administração em segurança é utilizar serviços de backup para que a empresa não venha ficar com indisponibilidade no serviço se houver algum dano nos dados individuais ou coletivos (PINHEIRO 2020).

O controlador ou operador no exercício de suas atividades em caso de danos nos dados, é obrigado a repará-lo, ou seja, será penalizado pela Lei a ter que pagar

indenização ao titular conforme o Art. 42 da LGPD. É importante manterem serviços de segurança para evitar riscos ou danos ao patrimônio empresarial, garantindo a segurança durante todo o ciclo de vida dos dados pessoais (BRASIL, 2018).

Segundo Pinheiro (2020), Art.42. “Assim como no GDPR, Artigos: 24, 25, e 26, a lei brasileira traz em sua previsão o caráter solidário da responsabilização do controlador e do operador”, e complementa:

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

Referindo aos Art.46 e Art.50 da LGPD – Lei Geral de Proteção de Dados, sobre Governança, os agentes de tratamento devem adotar medidas de segurança, técnicas administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perdas, alteração, comunicação ou qualquer forma de tratamento inadequado (DONDA, 2020).

Com a política de segurança inserida na empresa, os funcionários conhecerão medidas de proteção e não deixarão vulnerabilidades, evitando invasões na rede interna do ambiente corporativo. Uma das medidas de boas práticas de governança a ser adotada como por exemplo: evitar a inserção de pen driver em portas USB, não abrir links de e-mail desconhecidos, proteger senhas pessoais. Conhecer as ameaças é de fundamental importância para evitá-las (DONDA, 2020).

Treinamentos e campanhas de conscientização nas organizações favorecerão no conhecimento dos colaboradores na adequação à LGPD em boas práticas de governança. Com uma boa educação em segurança de dados, diminuirá as chances da empresa ser multada por falta de conhecimento dos funcionários, além de saber sobre o ciclo de vida destes dados no processo de validação da base legal se ainda é válido realizar o tratamento, quem pode realizar o uso, e definir quais são as regras de acesso, quando deve ser arquivado e por quanto tempo, ou quando deve ser excluído em qual condição, conforme o Art.50:

A melhor forma de garantir a segurança e a integridade dos dados, é protegendo e mantendo seguros através de backup. Havendo algum desastre ou ataques de hackers e que venha a interromper o serviço da empresa, com o backup o sistema será reativado rapidamente e não haverá indisponibilidade por muito tempo

no serviço. “Sistemas de recuperação contra desastre fazem uso de tecnologias de backup, aplicação e/ou redundância de software ou hardware”.

O encarregado de proteção de dados deve monitorar as atividades de tratamento de dados da empresa, de forma a garantir que elas estejam em conformidade com a LGPD. Nesse sentido, todas as decisões e instruções pelo encarregado devem ser passadas primeiro para o controlador, uma vez que ele é o responsável pelas decisões envolvendo o processo de proteção de dados. É importante lembrar que o respeito a essa hierarquia é fundamental, visto que ações em desconformidade com a LGPD podem resultar em sanções milionárias (PINEHIRO, 2020).

Portanto, toda empresa que desempenha alguma atividade em qualquer parte do processo de tratamento de dados, deve ter um encarregado de proteção de dados (DPO), este encarregado pode ser qualquer pessoa física ou Jurídica, desde que conheça as regulamentações estabelecidas pela Lei Geral de Proteção de dados (LGPD).

3 METODOLOGIA

O presente estudo utilizou como método de pesquisa, livros, fontes da internet, artigos científicos, questionário elaborado na plataforma Google Forms, questionário ficou disponível por 30 minutos no dia 21-02-2022. Os respondentes da pesquisa foram os colaboradores que fazem parte das empresas provedoras de internet, Nateltelcom e FibraTel.

A fundamentação teórica do estudo se deu através de pesquisas em artigos científicos, sites confiáveis, guias e leis publicadas pelo congresso nacional. Os estudos inclusos na pesquisa são de natureza quantitativa e qualitativa. De acordo com Gil (2002), a pesquisa é caracterizada também como descritiva e exploratória. Descritiva por buscar, através de pesquisas em revistas de universidades brasileiras, jornais, decretos e portarias, descrever as características e o comportamento de um determinado grupo. A apresentação dos dados se deu através de tabelas, para facilitar a compreensão e análise das relações entre o referencial teórico investigado e a prática percebida in loco.

4. RESULTADOS E DISCUSSÕES

As informações foram coletadas através de um questionário onde os colaboradores que fazem parte das empresas provedoras de internet, Nateltelcom e FibraTell informam que às regras estabelecidas pela Lei Geral de Proteção de Dados - LGPD no ambiente corporativo são seguidas em manter os dados seguros de seus clientes, também a equipe da empresa recebe orientações de segurança de dados, os programas da empresa são atualizados e protegidos de ataques de racks, neste questionário os resultados foram:

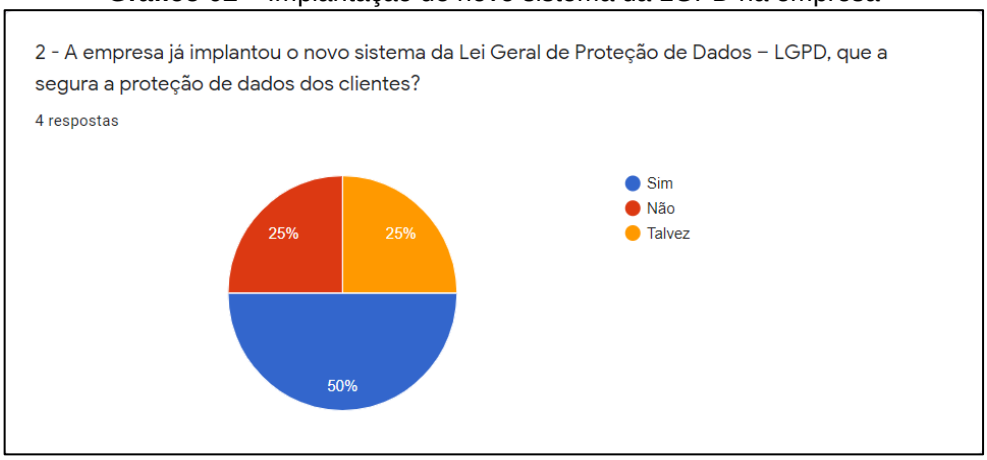
Na pergunta de número (1) 100% do pessoal entrevistado informou com a implantação da Lei LGPD melhorou mais ainda a segurança dos dados da empresa; na pergunta de número (2) 100% dos entrevistados 50% diz que já foi implantado o sistema da LGPD na empresa e outros 25% não sabem informar e os outros 25% não sabem de certeza se já foi implantado na empresa; pergunta de número (3) 100% informa que antes da aprovação da Lei LGPD os dados dos clientes já eram protegidos; pergunta (4) 100% informa que está seguindo o regulamento estabelecido pela Lei da LGPD; pergunta (5) 75% diz que na empresa existe Política de Segurança, ou seja, os colaboradores da empresa, são orientados a utilizarem antivírus confiáveis, não utilizar pen driver desconhecidos nas portas USB, não abri link de e-mail desconhecidos, cada pessoa tem a sua senha pessoal para utilização dos programas da empresa os outros 25% não sabem informar; pergunta (6) 100% informa que existe backup dos equipamentos e nos dados dos clientes na empresa; pergunta (7) 100% diz que existe controle de filtragem no firewall dos equipamentos de borda de internet da empresa; pergunta (8) 100% diz que já teve alguma tentativa de ataque de hacker na empresa; pergunta (9) 75% menciona que as tentativas destes ataques foi através de DDOS e 25% outros tipos de ataques maliciosos.

A seguir segue os gráficos apresentando de maneira gráfica os resultados obtidos com a coleta de dados.

Gráfico 01 – Importância da LGPD para a melhoria de segurança dos dados

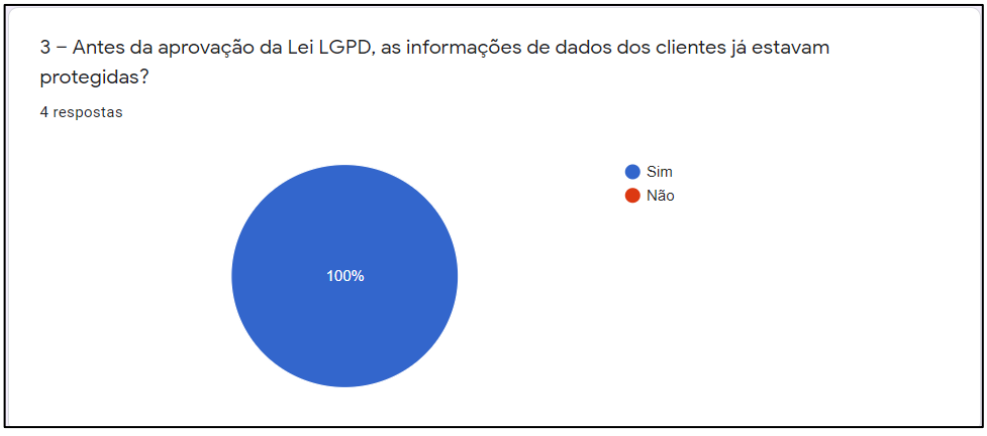
Fonte: Dados da Pesquisa

Gráfico 02 – Implantação de novo sistema da LGPD na empresa



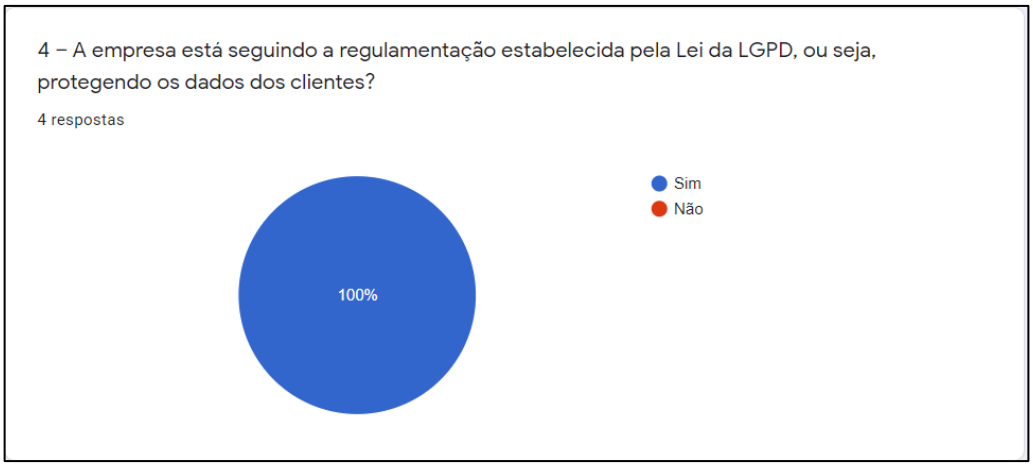
Fonte: Dados da Pesquisa

Gráfico 03 – Proteção de dados antes da aprovação da LGPD



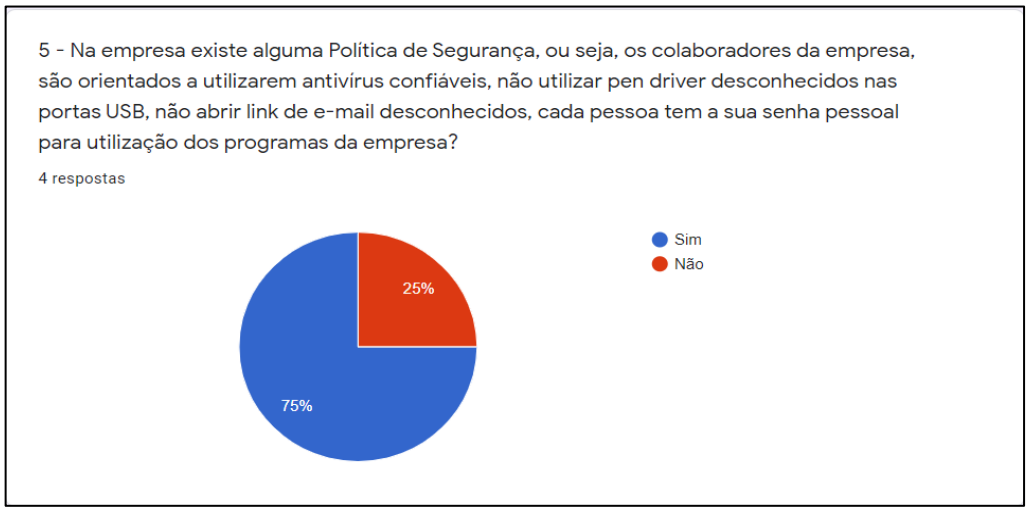
Fonte: Dados da Pesquisa

Gráfico 04 – Atendimento da regulamentação pela empresa



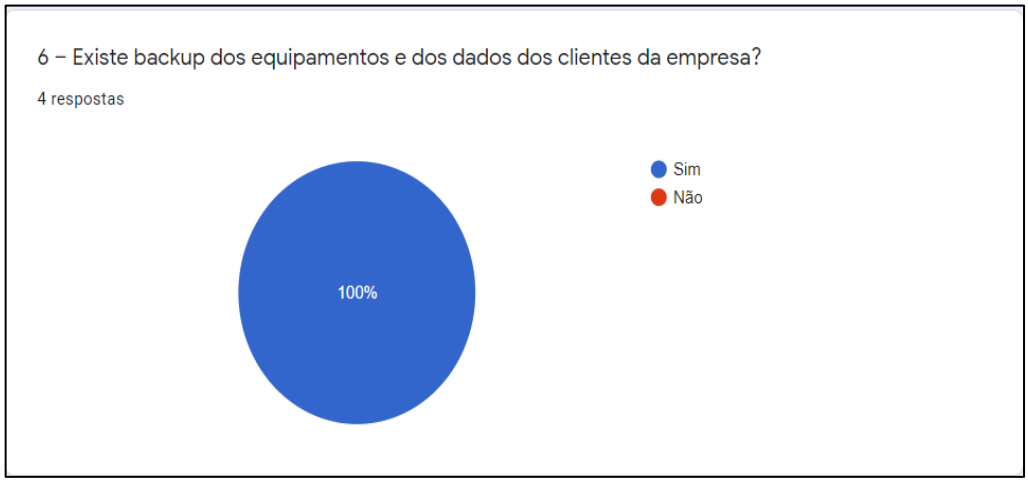
Fonte: Dados da Pesquisa

Gráfico 05 – Política de Segurança na empresa



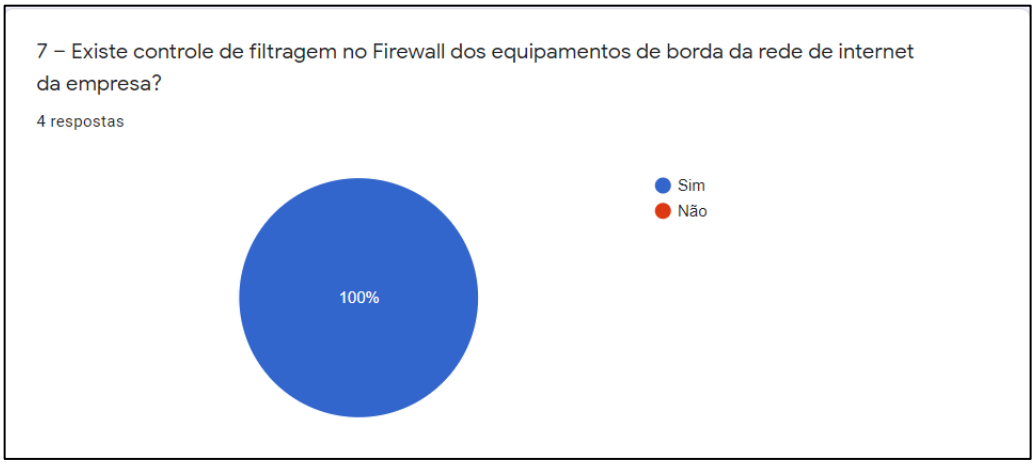
Fonte: Dados da Pesquisa

Gráfico 06 – Backup de equipamentos e dados na empresa



Fonte: Dados da Pesquisa

Gráfico 07 – Controle de filtragem no Firewall de equipamentos de borda da rede

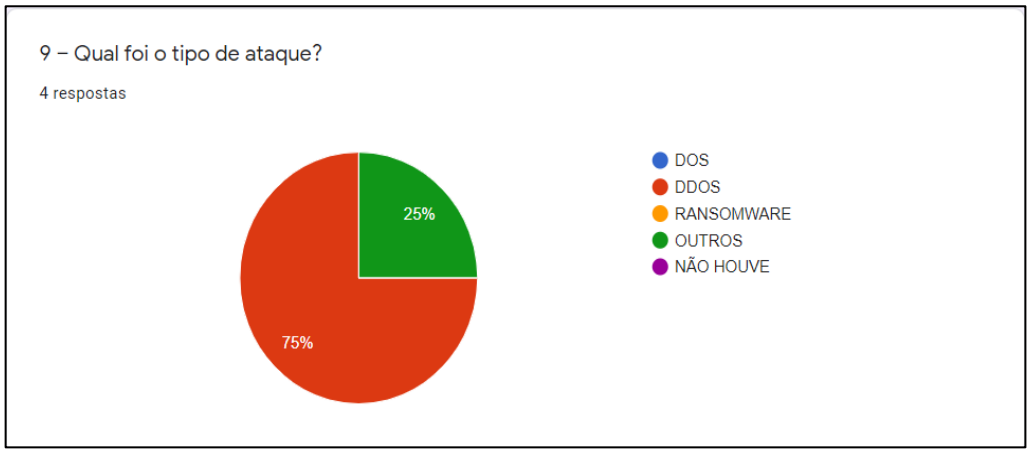


Fonte: Dados da Pesquisa

Gráfico 08 – Tentativas de ataque de hacker na empresa

Fonte: Dados da Pesquisa

Gráfico 09 – Tipo de de ataque de hacker na empresa



Fonte: Dados da Pesquisa

5. CONSIDERAÇÕES FINAIS

Este trabalho da LGPD – Lei Geral de Proteção de Dados, foi desenvolvido com o intuito de aprofundar conhecimentos sobre à importância da segurança de dados já que os autores do estudo atuam na área de TI - Tecnologia da Informação e estão sempre trabalhando e se deparando com dados de pessoas.

Conhecer algo novo é de fundamental importância para o aprendizado do ser humano, algo que ninguém toma do educando, que se chama o conhecimento. Apesar de estar se adaptando com a Lei Geral de Proteção de Dados – LGPD, no ambiente corporativo, as tarefas executadas no dia a dia da empresa de armazenar e coletar dados pessoais, serão laboradas com mais responsabilidades, de forma segura, além do mais, sabendo que está sendo realizado compartilhamento de informações de maneira transparente com os integrantes da empresa conforme as exigências da regulamentação da LGPD, documentando, armazenando nos sistemas de software e hardware, ou seja, em disco rígido, banco de dados de forma que as informações estejam seguras.

A pesquisa constata a predominância de estratégias organizacionais no ambiente coorporativo, fazendo com que os integrantes da empresa, tenham conhecimento em segurança de dados, e que se adequem as situações que se dizem ser “complexas” de não estarem ainda preparados com as exigências dos regulamentos determinados pela nova Lei da LGPD, em manter os dados de pessoas protegidos.

Por isso, as estratégias deverão ser alinhadas com os aspectos subjetivos dentro da empresa, pois partem da percepção, da experiência e são moldadas socialmente por meio de valores compartilhados de todos funcionários do ambiente corporativo para que seja mais fácil a adequação da empresa com a LGPD – Lei Geral de Proteção de Dados.

REFERÊNCIAS

BRASIL. Constituição da República Federativa do Brasil de 1988.Brasília, DF: Presidência da República, [2016]

BRASIL. **Lei nº 13.709**, de 14 de agosto de 2018, dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).

DONDA, Daniel. **Guia Prático de Implementação da LGPD**. Labrador, 2020

FIORILLO, Celso Antonio Pacheco. **O Marco Civil da Internet e o meio ambiente digital na sociedade da informação: Comentários à Lei n. 12.965/2014**. Saraiva Educação SA, 2017..

GIL, Antônio Carlos. Como elaborar projetos de pesquisa. 4 ed. São Paulo: Atlas, 2002.

LÓSSIO, Cláudio Joel Brito. **O compliance digital e a proteção de dados: preservando direitos na sociedade da informação**. 2020. Dissertação de Mestrado.

LÓSSIO, Claudio Joel Brito. **Proteção de dados e compliance digital**. Grupo Almedina, 2021.

LÓSSIO, Claudio Joel Brito; ALENCAR, Thomas Jefferson Lossio. A GAMIFICAÇÃO NO PROCESSO DE IMPLEMENTAÇÃO DA LGPD. **Campina Grande/PB**.

LÓSSIO, Claudio Joel Brito; NASCIMENTO, Luciano; TREMEL, Rosângela. **Cibernética jurídica**: estudos sobre direito digital. 2020.

OLIVEIRA, Maria. **Como fazer pesquisa qualitativa**. 2 ed. Petrópolis. Rio de Janeiro: Profissional e Tecnológica. Senac, Rio de Janeiro, 2013.

PINHEIRO, Patrícia. **Peck Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD) / Patrícia Peck Pinheiro – 2. ed. – São Paulo: Saraiva Educação, 2020.P14.

SOUZA, Kauan Richard Alves; MARZOCHI, Leonardo. **Insegurança de TI em órgãos municipais de atendimento ao público**. 2018.