PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE CIÊNCIAS EXATAS E DA COMPUTAÇÃO
GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

LGPD ANÁLISE DOS IMPACTOS DA IMPLEMENTAÇÃO EM AMBIENTES CORPORATIVOS: ESTUDO DE CASO

VICTTOR HENRIQUE PEREIRA LIMA

GOIÂNIA
2020

VICTTOR HENRIQUE PEREIRA LIMA

LGPD ANÁLISE DOS IMPACTOS DA IMPLEMENTAÇÃO EM AMBIENTES CORPORATIVOS: ESTUDO DE CASO

Trabalho de Conclusão de Curso apresentado à Escola de Ciências Exatas e da Computação, da Pontifícia Universidade Católica de Goiás, como parte dos requisitos para a obtenção do título de Bacharel em Ciência da Computação.

Orientador: Prof. Dr. Fábio Barbosa Rodrigues

GOIÂNIA
2020

VICTTOR HENRIQUE PEREIRA LIMA

LGPD ANÁLISE DOS IMPACTOS DA IMPLEMENTAÇÃO EM AMBIENTES CORPORATIVOS: ESTUDO DE CASO

Este Trabalho de Conclusão de Curso julgado adequado para obtenção o título de Bacharel em Ciência da Computação, e aprovado em sua forma final pela Escola de Ciências Exatas e da Computação, da Pontifícia Universidade Católica de Goiás, em ____/____/_____.

_____

Prof. Ma. Ludmilla Reis Pinheiro dos Santos

Coordenadora de Trabalho de Conclusão de Curso

Banca examinadora:

_____

Orientador: Prof. Dr. Fábio Barbosa Rodrigues

_____

Prof. Me. Eugênio Júlio Messala Cândido Carvalho

_____

Prof. Dr. José Luiz de Freitas Júnior

GOIÂNIA
2020

AGRADECIMENTOS

Agradeço primeiramente a Deus, que me concedeu vida e saúde para concluir este trabalho.

Aos meus pais Maria Rodrigues de Lima Pereira e Cleomar Pereira, que me incentivaram e me deram suporte por todos os anos de graduação.

A minha irmã Helena Beatriz, que me deram suporte familiar.

A todos os meus professores, os quais eu tive a oportunidade de conhecer ao longo da vida e contribuíram para minha formação.

Ao meu orientador acadêmico professor Dr. Fábio Barbosa Rodrigues pelo apoio e confiança no desenvolvimento deste trabalho.

Sou grato a todo o corpo docente, à direção e à administração desta universidade.

"O maior inimigo do conhecimento não é a ignorância, é a ilusão do conhecimento".

(Stephen Hawking)

RESUMO

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018) dispõe sobre o tratamento de dados pessoais, inclusive por meios digitais, por pessoa natural ou jurídica. O objetivo deste trabalho é apresentar uma série de medidas que visam atender a conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) em uma empresa no Brasil. A partir de pesquisas bibliográficas, artigos, documentos e relatórios acerca do tema, o presente trabalho apresenta uma breve contextualização sobre o assunto e os motivos desse estudo, seguido de uma abordagem da LGPD, conceitos e seus principais aspectos, o método foi o estudo de caso na empresa Nexus Systemas. Com este estudo percebeu-se a importância da segurança e a privacidade dos dados em um ambiente corporativo, além das dificuldades encontradas no processo de implantação e adaptação dentro de ambientes corporativos. Este trabalho mostra a importância da lei para empresas e sociedade, trazendo mais clareza para empresas sobre a nova regulamentação de proteção de dados.

Palavras-chaves: Privacidade de Dados, Segurança da Informação, Gestão de Riscos.

ABSTRACT

The General Law on Personal Data Protection (Law No. 13.709 of August 14, 2018) provides for the processing of personal data, including by digital means, by natural or legal persons. The purpose of this work is to present a series of measures aimed at complying with the General Law on Personal Data Protection (LGPD) in a company in Brazil. From bibliographic researches, articles, documents and reports on the subject, the present work presents a brief contextualization on the subject and the reasons for this study, followed by a LGPD approach, concepts and their main aspects, the method was the case study in Nexus Systemas company. With this study we realized the importance of data security and privacy in a corporate environment, in addition to the difficulties encountered in the process of implementation and adaptation within corporate environments. This work shows the importance of the law for companies and society, bringing more clarity to companies about the new data protection regulations.

Keywords: Data Privacy, Information Security, Risk Management.

LISTA DE FIGURAS

Figura 1: Mapa países adequados a proteção de dados 14
Figura 2: Etapas da Fase de Elaboração do Relatório de Impacto 17
Figura 3: Ativos de uma empresa 21
Figura 4: Processo de gestão de riscos 22

LISTA DE TABELA

Tabela 1: Grupo de dados 31

LISTA DE QUADRO

Quadro 1: Comparativo obrigações operador e controlador 18

LISTA DE SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
ART	Artigo
CPF	Cadastro de Pessoa Física
IP	Protocolo Internet
ISO	Organização Internacional de Padronização
LGPD	Lei Geral de Proteção de Dados
PSI	Política de Segurança da Informação
GDPR	Regulamento Geral de Proteção de Dados
SI	Segurança da Informação
TI	Tecnologia da Informação
WEB	World Wide Web

SUMÁRIO

1 INTRODUÇÃO 11

2 FUNDAMENTAÇÃO TEÓRICA 13

2.1 Lei Geral de Proteção de Dados 13

2.2 Titular 14

2.2.1 Dados Pessoais 15

2.2.2 Dados sensíveis 16

2.2.3 Dados anônimos 16

2.3 Controlador, Operador e Encarregado 16

2.4 Princípios Gerais da Lei 19

2.5 Tratamento de dados 20

2.6 Segurança da Informação 20

2.7 Gestão de Riscos 21

2.7.1 Avaliação dos riscos 23

2.7.2 Tratamento e plano de resposta ao risco 23

3 APRESENTAÇÃO E ANÁLISE DOS IMPACTOS 25

3.1 Apresentação do cenário: Nexus Systemas 25

3.2 Descrição e análise da Nexus Systemas 26

3.3 Inconformidades encontradas 27

3.4 Solução para inconformidades encontradas 28

3.4.1 Nomeação de um encarregado 28

3.4.2 Plano de Conscientização em segurança 29

3.4.3 Mapeamento de dados 29

3.4.4 Política de segurança 32

3.4.5 Gestão de incidentes e vazamento de dados 34

3.4.6 Revisão de contratos 35

4 DISCUSSÃO 36

5 CONCLUSÃO 38

REFERÊNCIAS BIBLIOGRÁFICAS 40

1 INTRODUÇÃO

Nos últimos anos, o número de usuários com acesso à Internet e a quantidade de informações disponíveis aumentaram significativamente, esse aumento é relativo à facilidade que a Internet nos proporciona.

Com o desenvolvimento de novas tecnologias, a interação contínua entre dispositivos e pessoas agilizam o processo de troca de informações, gerando uma grande quantidade de dados que estão sendo armazenados e processados de modo que questões sobre segurança da informação sejam levantadas (RAPOSÔ, 2019).

Escândalos recentes sobre vazamentos de dados de empresas como *Faceboo*k, *Netshoes* e *Uber* deixaram expostos dados pessoais como nomes, endereços, números de cartões de crédito e colocaram em evidência os efeitos devastadores da falta de rigor com a segurança no tratamento de dados pessoais. Portanto, existe uma grande necessidade de adotar mecanismos eficazes para evitar possíveis vazamentos e garantir a segurança dos dados (FERNANDES, 2019).

Na Europa, após relatórios de espionagem e violação de dados de clientes envolvendo a *Cambridge Analytica* e o *Facebook*, iniciou discussões sobre regulamentos de segurança de dados, que inspiraram a formulação do Regulamento Geral de Proteção de Dados (GPDR), que regulamentava a União Europeia e impunha Medidas para aprovar legislação sobre segurança de dados pessoais (RAPOSÔ, 2019).

A Lei Geral de Proteção dos dados Pessoais (LGPD) é um novo paradigma, pois envolve a alteração da maneira como as empresas lidam com dados pessoais de pessoas físicas nos meios *online* e *offline* e tem a função de proteger os direitos fundamentais de liberdade e privacidade em qualquer relacionamento que envolva dados pessoais (SÁ, 2019).

Levando em conta os casos mencionados e o aumento da concorrência entre empresas, é importante que as empresas ajustem suas tecnologias para se enquadrar a Lei Geral de Proteção dos dados Pessoais e consequentemente garantir ao usuário plena consciência sobre a forma que os seus dados estão sendo armazenados e utilizados (RAPOSÔ, 2019).

A lei entrou em vigor no dia 16 de agosto de 2020, ainda há claramente muito debate sobre a adaptabilidade da tecnologia da informação as novas regras da LGPD, isso cria incerteza jurídica sobre como a lei será aplicada e quais ações devem ser tomadas para o cumprir a lei (RAPOSÔ, 2019).

O objetivo geral deste trabalho é um estudo de caso que analisará os impactos da aplicação da LGPD no cenário da empresa fictícia Nexus Systemas, visando se adequar à regulamentação estabelecida pela Lei Geral de Proteção de Dados.

A fim de alcançar o objetivo geral proposto, são elencados os seguintes objetivos específicos, este trabalho faz um estudo da lei, bem como suas características e padrões, com o propósito de apontar as suas necessidades, parâmetros de execução e aplicações, analisar quais as implicações da LGPD em ambientes corporativos, identificar e catalogar as ameaças a privacidade dos dados na empresa Nexus Systemas, analisar o impacto da padronização proposta da LGPD na gestão da segurança da informação relacionada às ameaças encontradas nos hábitos e processos da empresa.

O presente trabalho foi elaborado utilizando como metodologia a pesquisa bibliográfica.

Foi elaborada uma revisão de literatura baseada em informações nacionais e estrangeiras extraídas de livros, artigos científicos, teses, dissertações, como também de meios eletrônicos. Adiante foi exposto da lei e conceitos sobre segurança com o objetivo de entender seu processo de desenvolvimento.

Este trabalho está organizado em 5 capítulos, de maneira a se obter os objetivos citados no item 1, escritos de maneira clara e objetiva, visando facilitar o entendimento de todos os interessados no assunto.

No capítulo 2, serão abordados os conceitos teóricos utilizados como base para esta dissertação, iniciado com apresentação da lei seguindo das suas principais características para melhor entendimento. O capítulo 3 tem como objetivo desenvolver a análise evidenciando os impactos do novo padrão e detalhando sobre sua arquitetura e funcionamento.

O capítulo 4 expões a análise dos resultados do estudo realizado sobre o tema e seus resultados.

O capítulo 5 expõe as conclusões sobre o estudo detalhado do tema. Seguidamente, são apresentadas as referências bibliográficas, as quais foram fontes para os estudos.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Lei Geral de Proteção de Dados

"A Lei n° 13.709/2018 A Lei Geral de Proteção de Dados Pessoais (LGPD), foi criada com base no Regulamento Geral sobre a Proteção de Dados (GPDR), regulamento do direito sobre a privacidade e proteção dos dados pessoais, aplicável a todos os indivíduos na União Europeia" (MACIEL, 2019). A LGPD foi sancionada pelo ex-presidente Michel Temer, e está em vigência desde o dia 16 de agosto de 2020, para regular as atividades e a forma do tratamento dos dados pessoais no Brasil.

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

A LGPD alterar o Marco Civil da Internet no Brasil, que agora inclui o termo privacidade em seu sistema legal (SÁ, 2019).

De acordo com art. 1º da LGPD (Lei n° 13.709, de 14 de agosto de 2018) a lei se aplica a todo e qualquer tratamento de dados, por qualquer meio, seja realizado por pessoa natural ou pessoa jurídica de direito público ou privado:

> Art. 1°. a 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 livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

A LGPD está fundamentada nos direitos fundamentais de liberdade e de privacidade, como a livre iniciativa e o desenvolvimento econômico e tecnológico do país, de acordo com o Art. 2 da Lei nº 13.709, de 14 de agosto de 2018.

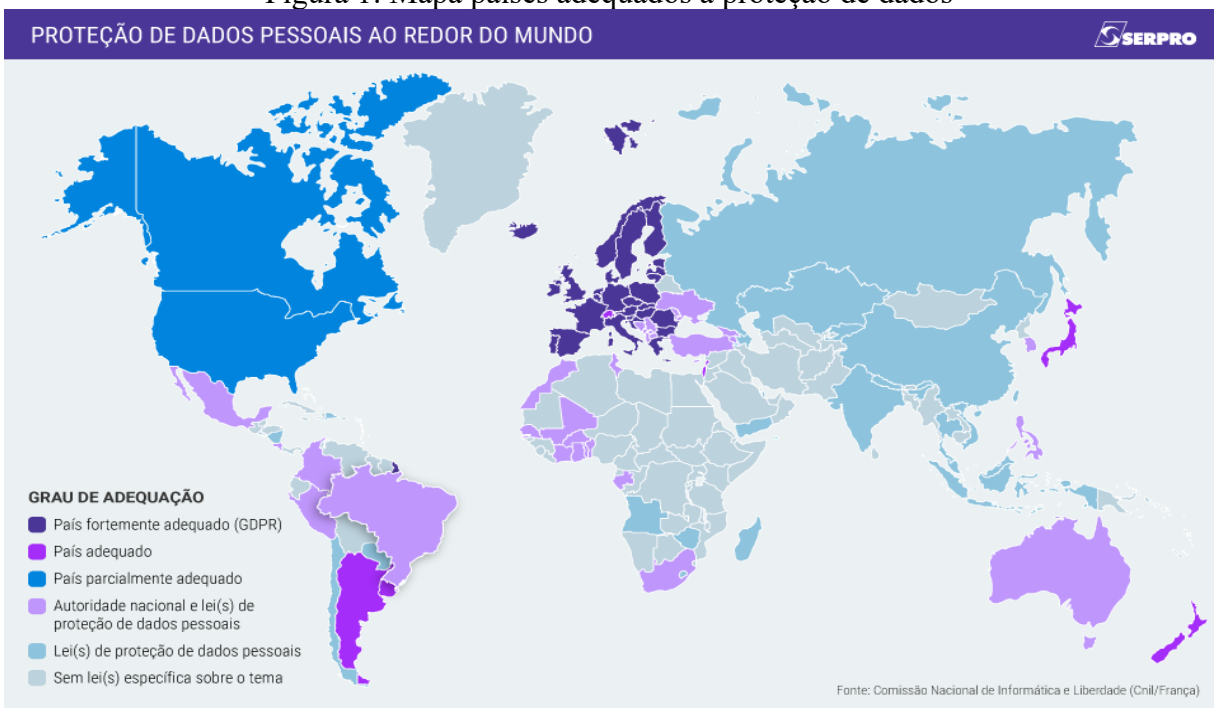
A lei estabelece todas as informações que identificam a identidade direta do titular ou tornam a identidade de uma pessoa natural e identificável como dados pessoais, assim como qualquer procedimento realizado em dados pessoais, como coleta, uso, acesso, transmissão, processamento, arquivamento e armazenamento, transferência, de acordo com o art.5 da Lei nº 13.709, de 14 de agosto de 2018 (BRASIL, 2018).

A lei exige que as atividades de processamento de dados pessoais obedeçam aos seguintes princípios: objetivo, suficiência, necessidade, acesso livre, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilidade e contribuição, Art.6 da Lei n°. 13.709 de 14 de agosto de 2018 (BRASIL, 2018).

Com a LGPD todas as organizações brasileiras, independente de seu porte, devem investir em segurança tecnológica para impedir violações de dados pessoais (ROCHA, 2019).

A Figura 1, apresenta o grau de adequação à proteção de dados pessoais no mundo:

Figura 1: Mapa países adequados a proteção de dados



Fonte: SERPRO (2020).

2.2 Titular

O titular dos dados é uma pessoa singular referida pelos dados, uma pessoa singular reconhecida ou identificável. Portanto, é possível obter a identificação de seu titular direta ou indiretamente (MACIEL, 2019).

A lei cria nove direitos para os titulares dos dados descritos no art. 18 e conferem aos indivíduos o direito de: 1. Confirmação da existência do tratamento dos seus dados. 2. Acessar seus dados. 3. Correção de dados incompletos, imprecisos ou desatualizados. 4. anonimizar, bloquear ou excluir dados, ou dados desnecessários ou excessivos que não estão sendo processados em conformidade com a LGPD. 5. Seus dados sejam portáveis, ou seja, entregues a outro serviço ou processador, se solicitado. 6. Ter seus dados excluídos. 7. Informações sobre entidades públicas e privadas com as quais o controlador compartilhou dados. 8. Informações sobre a possibilidade de negar o consentimento e as consequências disso. 9. Revogar o consentimento (BRASIL, 2018).

No art. 5° da LGPD, traz a definição sobre os tipos de dados, que estão definidos em 3 tipos, os dados pessoais, os dados pessoais sensíveis e dados anônimos.

2.2.1 Dados Pessoais

Os dados pessoais podem ser definidos como todo e qualquer dado referente a um indivíduo, no qual permita identificá-lo e obter informações de dados com base nas informações iniciais através de um nome, CPF (Cadastro de Pessoa Física), endereço, ou qualquer outro dado que permita identificar a pessoa física.

O Regulamento 2016/679 da União Europeia (General Data Protection Regulation - GDPR), uma das bases para a LGPD, em seu art. 4°, n.1, os dados pessoais foram definidos como:

> Dados pessoais: informação relativa a uma pessoa singular identificada ou identificável (<<titular dos dados>>); é considerado identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como, por exemplo, um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genético, mental, econômica, cultural ou social dessa pessoa singular.

Já segundo (MACIEL, 2019, p.19), os dados pessoais são definidos como:

> Dado pessoal é toda informação que pode identificar um indivíduo ainda que não diretamente. Portanto, incluem-se na referida definição, por exemplo, os números de Internet Protocol – IP, número de identificação de funcionário dentro de uma empresa, e até mesmo características físicas. Isso em razão da presença do léxico "identificável", que amplia a definição de dados pessoais.

2.2.2 Dados sensíveis

Segundo Maciel (2019, p.20) dados sensíveis estão relacionados aos seguintes dados: “origem racial ou ética, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural”.

Dados sensíveis são aqueles que possuem maior potencial para causar danos ao titular de dados, pois eles estão relacionados a questões sensíveis que podem levar a alguma discriminação.

2.2.3 Dados anônimos

Segundo o art. 5°, inciso III da LGPD dados anônimos são definidos: “III - Dado anônimo é aquele dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.” (BRASIL, 2018).

A anonimização realiza uma ocultação de informações sensíveis antes que estas informações sejam disponibilizadas para uso, sendo assim impossível obter a identificação do perfil que os dados pertenciam antes do processo.

2.3 Controlador, Operador e Encarregado

O art. 5°, inciso VIII e inciso IX, da LGPD traz a definição sobre o encarregado de dados, e dos agentes de tratamento, são considerados agentes de tratamento, os controladores e operadores.

O controlador pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Decisões relacionadas ao tratamento dos dados, registros sobre o tratamento dos dados, comunicação com a Autoridade Nacional de Proteção de Dados (ANPD), são algumas responsabilidades do controlador.

O controlador possui relação direta com o titular, ele deverá adotar medidas de boas práticas de segurança e governança o tratamento de dados esteja em conformidade com as diretrizes da LGPD. O controlador deverá manter registro de todas as informações referentes ao tratamento de dados, e para isso é necessário ferramentas adequadas para a documentação dos processos de tratamento de dados.

O relatório de impacto à proteção de dados pessoais consiste “na 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 riscos” (MACIEL, 2019, p.15). A Figura 2, apresenta etapas necessárias para criação do relatório de impacto:

Figura 2: Etapas da Fase de Elaboração do Relatório de Impacto

Fonte: GUIA (2020).

Segundo o art. 38° algumas medidas e dados que devem constar no relatório de impacto:

- A descrição dos tipos de dados coletados;
- A metodologia utilizada para a coleta e para a garantia da segurança das informações;
- Mecanismos de mitigação de riscos;

"O operador pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (BRASIL, 2018). O operador realiza as operações de tratamento determinadas pelo controlador. Em ambos os casos todos os registros das operações de tratamento de dados realizadas deverão ser documentadas.

O operador deve agir conforme as diretrizes do controlador, ele deve cumprir as regras que o controlador determina para o tratamento dos dados. No Quadro 1, é mostrado um comparativo entre algumas obrigações gerais que os controladores e os operadores devem seguir para se adequarem a lei:

Quadro 1: Comparativo obrigações operador e controlador

	OBRIGAÇÕES GERAIS PERANTE A LGPD	
	CONTROLADOR	OPERADOR
LIMITES PARA TRATAMENTO	Tratar dados com base legal definida	Tratar dados conforme propósito definidos pelo controlador
REGISTRO	Registro das atividades	Registro das atividades
RELATÓRIO DE IMPACTO	Elaborar relatório de impacto	Elaborar relatório de impacto
INCIDENTES	Comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.	Informar ao controlador casos de incidentes
BOAS PRÁTICAS DE SEGURANÇA	Adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito	Adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito
PROGRAMA DE GOVERNANÇA EM PRIVACIDADE	Implementar Programa de Governança em Privacidade, observadas a estrutura, a escala e o volume de suas operações, bem com o a sensibilidade dos dados	Receber e estar ciente do Programa de Governança adotado pelo controlador
DIREITOS DOS TITULARES	Atender aos direitos dos titulares	Atender aos direitos dos titulares

Fonte: adaptado (MACIEL, 2019, p.43).

A lei define o encarregado de dados como, pessoa designada pelo controlador e operador para atuar como um canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.

A função do encarregado de dados consiste em intermediar as ações entre o controlador, titulares de dados e a ANPD. O encarregado deve ter total liberdade para poder tratar as informações, realizar denúncias na existência de irregularidades, fiscalizar se as políticas adotadas pelo controlador e operador estão sendo cumpridas.

O encarregado de dados não pode sofrer nenhuma penalidade, segundo a lei o operador e controlador devem eleger o encarregado de dados, é recomendado que o encarregado de dados seja um terceiro para evitar conflitos internos e imparcialidade (CELIDONIO et al., 2020).

Segundo Celidonio et al. (2020), algumas atribuições que o encarregado deve executar são:

- Receber comunicações de órgãos reguladores e adotar as providências que couberem;
- Orientar os funcionários e os contratados da empresa a respeito das práticas a serem tomadas em relação à proteção de dados pessoais dos usuários;
- Manter registros de todas as práticas de tratamento de dados pessoais conduzidas pela empresa, incluindo o propósito de todas as atividades desenvolvidas;

2.4 Princípios Gerais da Lei

A LGPD possui 10 princípios, nos quais são essenciais para entendimento sobre como o tratamento de dados, os princípios são:

- Finalidade: Para o tratamento e uso dos dados é preciso existir um porque daquele dado ser tratado.
- Adequação: O tratamento tem que ter uma relação com a finalidade informada. Se os dados forem coletados não tiverem uma relação lógica com a finalidade, o dado não é para aquela finalidade.
- Necessidade: Esse princípio garante que mais dados sejam tratados de forma desnecessária.

- Livre acesso, qualidade e transparência: O titular dos dados tem o direito de acessar seus dados a qualquer momento, esses devem claros, exatos, atualizados de acordo com a finalidade do tratamento.
- Segurança e prevenção: Os detentores dos dados devem tomar medidas para que nenhum dado seja acessado, exista perda, alteração ou que ocasione qualquer prejuízo.
- Não discriminação: Os dados não podem ser utilizados com finalidades, discriminatórias, ilícitas ou abusivas.
- Responsabilização: Os agentes (operadores e controladores) são responsáveis por garantir que todos os assuntos especificados na LGPD sejam atendidos.

2.5 Tratamento de dados

A lei define no art. 5°, inciso X tratamento como:

> Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, 2018).

A LGPD se aplica para todo o processamento de dados realizado por pessoas físicas ou jurídicas, onde a sua finalidade é para fins comerciais.

O consentimento é a principal ferramenta para que o tratamento de dados possa ser realizado. Através do consentimento o titular expressa que concorda com as ações de tratamento que serão realizadas com seus dados, garantindo assim o respeito ao direito e a liberdade de escolha (RIBEIRO, 2016).

O titular pode revogar o consentimento a qualquer momento, ele deverá comunicar ao encarregado de dados a sua decisão, e o encarregado de dados efetuará os procedimentos para a revogação junto ao controlador.

2.6 Segurança da Informação

Segurança da informação (SI) é definida como a proteção oferecida para um sistema de informação automatizado a fim de alcançar os objetivos de preservar a integridade, a

disponibilidade e a confidencialidade dos recursos do sistema de informação incluindo *hardware*, *software*, *firmware*, informações, dados e telecomunicações (STALLINGS, 2015).

Segundo a SI, a informação é um ativo de grande valor para as organizações, a função da SI é garantir que esses ativos estejam protegidos de qualquer ameaça ou acessos não autorizados, visando minimizar possíveis danos e manter a continuidade dos negócios em ambientes corporativos (ABNT, 2011).

A Figura 3, apresenta exemplos de ativos de uma organização, onde podemos observar que os ativos não estão restritos somente a informações, mas a tudo que gera valor para uma organização.

Figura 3: Ativos de uma empresa

Fonte: GUIA (2020).

A SI, está fundamentada em 3 pilares, a confidencialidade, integridade e disponibilidade. A confidencialidade é a garantia de que a informação esteja disponível apenas por pessoas autorizadas. A integridade assegura que os dados estejam em sua integridade e totalidade durante todo o seu ciclo de vida. A disponibilidade garante que os dados estejam disponíveis a qualquer momento, sem interrupções (STALLINGS, 2015).

Uma política de segurança é definida como um conjunto de normas e diretrizes baseadas em normas técnicas como a ISO/IEC 2005, ao qual uma instituição deve seguir para garantia e segurança de seus recursos e informações (VARGAS, 2020).

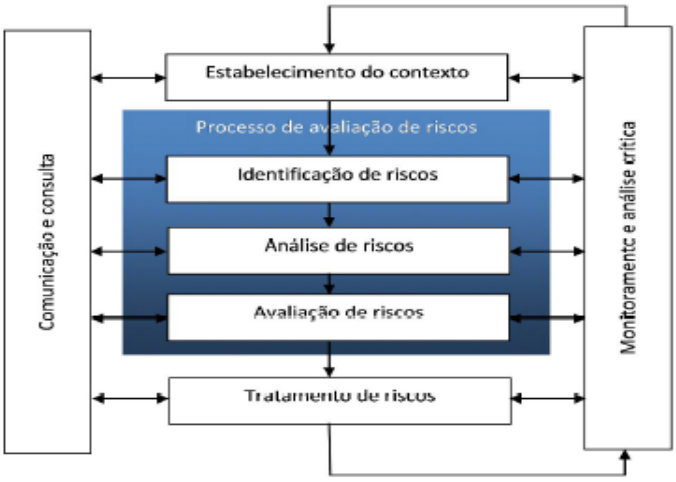
2.7 Gestão de Riscos

A gestão de riscos pode ser realizada com base na ISO 27005, a norma traz orientações e fornece o suporte para a implantação do processo de gestão de risco de Segurança da informação (ABNT, 2011).

A norma exige que as empresas constantemente executem análise de riscos, sempre que modificações forem executadas em seus processos, para que essa investigação seja feita com precisão, é preciso determinar parâmetros para o tratamento de riscos, assim detectaremos como os riscos serão medidos, dimensões dos riscos.

É preciso analisar a probabilidade dos riscos e a sua extensão (ROCHA, 2019). A Figura 4, apresenta como o processo de gestão de risco está estruturado:

Figura 4: Processo de gestão de riscos



Fonte: CALIXTO (2020).

O risco refere-se à possibilidade de uma ameaça ocorrer, como um evento ou situação incerta, que usará a vulnerabilidade de um ativo ou grupo de ativos para causar danos à organização, o que pode levar a um incidente (MONTEIRO, 2016).

Uma ameaça é uma violação potencial de segurança, que pode causar eventos que causam danos aos sistemas, geralmente eventos externos, que não estão sob o controle, ameaças podem ser classificadas como: ameaças naturais, ameaças involuntárias, ameaças voluntárias (MONTEIRO, 2016).

- Ameaças naturais: São questões relacionadas a natureza, como tempestades, incêndios entre outros.
- Ameaças voluntárias: vinculadas ao desconhecimento, como por exemplo: acidentes, erros, falta de energia, entre outros.

- Ameaças involuntárias: relacionadas a questões humanas, como hackers, vírus, invasores.

Dessa forma conhecemos o evento que estamos enfrentando, e podemos assim agir da melhor forma preventiva e rápida.

2.7.1 Avaliação dos riscos

Através do processo de avaliação dos riscos, é possível identificar eventos e suas causas, que possam gerar prejuízos e perda de ativos e determinar as medidas a serem tomadas (ABNT, 2011).

Segundo Calixto (2020), o mapeamento pode ser da seguinte forma:

> O mapeamento destas ações é efetuado com base na probabilidade e impacto de cada risco e atribuir pesos para cada risco, (Probabilidade e Impacto do Risco) que serão inseridos na fórmula: **RI** (Risco Inerente) = **NP** (Nível de Probabilidade) X **NI** (Nível de Impacto) (CALIXTO, 2020).

A probabilidade pode ser classificada como, muito baixa, baixa, média, alta e muito alta. Impacto como muito baixo, baixo, médio, alto, muito alto. Os pesos podem ser classificados de 1 a 10.

2.7.2 Tratamento e plano de resposta ao risco

A norma ISO 27005 define alguns métodos para o plano de resposta. Pereira e Bergamaschi (2018) como um plano de resposta a riscos: mitigação (ou redução); aceitação (ou tolerância); transferência (ou compartilhamento) ou evitando (ou eliminando) riscos:

- Mitigar o risco: Efetuar ações para reduzir a probabilidade e/ou impacto do risco. Se, caso o risco ocorrer, os impactos gerados serão menores e de mais fácil ajuste. Dessa forma, mitigar significa restringir os riscos a um nível aceitável pela organização (PEREIRA; BERGAMASCHI, 2018, p.14).

- Evitar o risco: Significa eliminar a ameaça na origem (PEREIRA; BERGAMASCHI, 2018, p.14).

- Aceitar o risco: São riscos toleráveis para a organização e os impactos são baixos, ações para esse risco não são realizadas (PEREIRA; BERGAMASCHI, 2018, p.14).

- Transferir o risco: Ocorre quando o risco não é de responsabilidade total de uma organização ou departamento, ou até mesmo quando a organização não possui acesso para modificar o cenário de risco. Em alguns casos, essa decisão pode ser registrada contratualmente (PEREIRA; BERGAMASCHI, 2018, p.14).

Após analisar cada método, será necessário mapear as ações que serão tomadas para cada etapa, o mapeamento deverá acompanhar o risco do início ao fim. Cada ação deverá ser comunicada e consultada visando compartilhar e documentar as ações e tratativas para todos os envolvidos.

Em ambientes corporativos o monitoramento e análise dos ricos são essenciais para acompanhamento e planejamento para novos métodos de ação para eventuais cenários.

3 APRESENTAÇÃO E ANÁLISE DOS IMPACTOS

3.1 Apresentação do cenário: Nexus Systemas

A Nexus Systemas empresa fictícia, foi fundada em 2008 na cidade de Goiânia em Goiás, com o objetivo de desenvolver sistemas para gestão pública. A empresa foi idealizada com o objetivo de otimizar os processos de gestão de sistemas para gestão pública, oferecendo o mais alto nível de qualidade e segurança.

A Nexus Systemas é umas das principais empresas no ramo de desenvolvimento de *softwares* para diversas áreas do setor público, com atividade nacional a Nexus Systemas está presente em diversos estados brasileiros, suas matrizes estão localizadas nos seguintes estados, Bahia, Goiânia, São Paulo e Rio Grande do Sul.

Em 2018, a empresa lançou o projeto de migração dos sistemas para o formato *web(World Wide Web)*, modernizando seus sistemas com novos recursos e atendendo as novas demandas do mercado com as tecnologias atuais.

A empresa é reconhecida por atuar na resolução de problemas complexos, com a tecnologia como pilar estratégico e inovação, eliminando assim problemas que evitam o crescimento das organizações de seus clientes.

Diante desse cenário, a empresa Nexus Systemas necessita entrar em conformidade com a legislação da LGPD, atendendo às principais orientações que está dividida em 10 capítulos, com 65 artigos (BRASIL, 2018). Para que seja possível a adequação a lei empresa contará com a consultoria externa que auxiliara todo o processo.

3.2 Descrição e análise da Nexus Systemas

Em decorrência da Lei 13.709/2018 Lei Geral de Proteção de Dados, a Nexus Systemas entendeu a importância e a necessidade de adequar seus processos a nova Legislação, de forma a manter a excelência e qualidade dos serviços e produtos oferecidos pela empresa.

A nova lei se aplica a todos aqueles que realizam tratamento de dados pessoais, e que envolvam um dos elementos a seguir:

I. Ocorrer em território nacional;
II. Que tenha por objetivo a oferta ou fornecimento de bens e serviços ou o tratamento de dados de indivíduos localizados no território nacional;
III. Em que os dados tenham sido coletados no território nacional.

A Nexus Systemas está enquadrada nos elementos citados anteriormente. A LGPD estipula sanções e penalidades para as empresas que não estão de acordo com a lei.

O foco principal da Nexus Systemas é o desenvolvimento de *software*, atualmente a empresa não possui um departamento ou pessoa responsável pela segurança da informação, as decisões são tomadas através de reuniões entre o diretor e o gerente de desenvolvimento, todas as decisões são tomadas de acordo com o surgimento dos incidentes. As decisões são repassadas para os outros gestores da empresa e cabe a eles aplicarem as medidas ao seu respectivo departamento.

A empresa possui diversas filiais e clientes em diversos estados brasileiros, atualmente a Nexus Systemas possui um grupo de 230 funcionários, existe uma grande porcentagem de funcionários com extenso vinculo empregatício, este grupo foi selecionado e observado durante alguns dias para observar como são seguidos os processos e a tomada de decisão durante suas atividades, foi observado que a maior parte dos processos e decisões tomadas por este grupo não seguem as orientações da segurança da informação, como senhas anotadas em papéis expostos em cima das estações de trabalho, executam arquivos recebidos por *e-mail* sem verificação do seu conteúdo, senhas de simples como de 1 ao 6.

Foi efetuada uma auditoria interna para observar a privacidade dos dados, durante a auditoria foi efetuada a verificação dos acessos e alterações, e constatado que a empresa não

possui definição de como essas informações serão armazenadas, categorização das informações, e não possui registros informando o tempo que de acessos e alterações das informações.

Os sistemas de gestão da Nexus Systemas possuem um grande fluxo de armazenamento de dados, foi observado que não é realizado nenhum processo para a distinção dos dados, se a informação apresenta dados sensíveis, se existe alguma restrição para acesso a essa informação. Os dados são armazenados mas não existe a informação do local onde os dados estão armazenados, não existe consentimento que permitam a captura e armazenamentos de tais dados.

Novos colaboradores ao ingressar na empresa recebem uma cartilha com recomendações gerais formuladas pela empresa, que contém alguns itens relacionados à segurança e privacidade dos dados, mas a empresa não possui políticas definidas e aprovadas para esse fim. Não existe um programa de treinamento sobre privacidade e proteção de dados para educar os funcionários sobre a importância da privacidade e da proteção de dados pessoais para que possam realizar o processamento de dados corretamente, reduzindo assim o risco de qualquer vazamento de dados.

Nexus Systemas possui diversos clientes e contratos com fornecedores, será necessário revisar os antigos contratos pois muitos contratos foram gerados antes da vigência da lei, será necessário a revisão desses contratos para que eles entrem em conformidade com a LGPD.

A empresa mantém um banco de dados contendo uma série de informações pessoais sobre seus clientes e funcionários. A empresa não possui nenhum tipo de medida para classificação de riscos, plano de ação para evitar os riscos, será necessário tomar algumas medidas para evitar vazamentos ou incidentes, que possam ameaçar a proteção desses dados e a imagem da empresa.

3.3 Inconformidades encontradas

Com base na análise, caso ocorra uma fiscalização da Autoridade Nacional de Proteção de Dados a Nexus Systemas não está em conformidade para atender as principais determinações da LGPD.

As inconformidades encontradas na Nexus Systemas em relação a LGPD são:

- Nomeação de um encarregado – Artigo 5°, inciso VIII - Lei 13.709/2018;

- Plano de conscientização em segurança – Artigo 50 °, Artigo 41 ° - Lei 13.709/2018;
- Mapeamento dos dados – Artigo 37° da Lei 13.709/2018;
- Política de segurança – Artigo 50 ° da Lei 13.709/2018;
- Revisão de contratos – Artigo 42 ° da Lei 13.709/2018;
- Gestão de incidentes e vazamento de dados – Artigo 38°, Artigo 48°, Artigo 50° da Lei 13.709/2018;

3.4 Solução para inconformidades encontradas

O cumprimento da nova regulamentação será um grande desafio, a empresa precisará revisar os processos internos e externos, a forma como os dados e informações são tradados e identificar as principais vulnerabilidades, isso tudo também envolve uma mudança na cultura da empresa e de seus funcionários.

3.4.1 Nomeação de um encarregado

O artigo 5° recomenda a nomeação de um encarregado de dados:

> Art. 5º Para os fins desta Lei, considera-se: VIII – encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) (BRASIL, 2018).

Um dos principais papéis da LGPD e para estruturação do projeto de adequação é a nomeação do encarregado de proteção de dados, o encarregado será responsável pela fiscalização e governança dos dados, esse papel pode ser indicado pelo controlador e escolhido internamente ou contratada de forma terceirizada, para atuar como um intermediador entre o controlador e os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

As informações a respeito do encarregado deverão ser disponibilizadas de forma clara, objetiva, em um local de fácil acesso para o titular dos dados, o encarregado irá comunicar-se

diretamente com o titular dos dados, ele será responsável por implantar e fiscalizar se as políticas estabelecidas pelo controlador e operador estão sendo cumpridas.

3.4.2 Plano de Conscientização em segurança

Um plano de conscientização de segurança da informação, tem como objetivo fornecer conhecimentos para todos os funcionários de uma empresa sobre segurança da informação (AFINAL, 2019).

O art. 50° da lei, recomenda que os agentes estabeleçam regras e boas práticas de governança sobre segurança de proteção de dados:

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais (BRASIL, 2018).

Os dados são o ativo mais importante de uma empresa, um plano de conscientização sobre segurança das informações deve estar ligado aos objetivos da empresa, ou seja, com sua missão e visão.

O plano deve conter programas educacionais voltados para a importância da privacidade e segurança dos dados, com treinamentos sobre possíveis ataques, treinamentos e palestras sobre engenharia social, cartilhas com informações sobre os principais ataques, testes de penetração e vulnerabilidades.

3.4.3 Mapeamento de dados

O mapeamento de dados é um documento que deve conter o mapeamento de todos os dados utilizados em cada atividade, bem como as informações de armazenamento, finalidade de uso, origem e método de coleta. Um dos principais objetivos do mapeamento de dados é estabelecer quais dados a empresa coleta, onde são coletados, a forma como são armazenados (BRANDAO, 2020).

No artigo 37 da LGPD, afirma que é dever do controlador e o operador manter os registros claros e completos das operações de tratamento de dados pessoais que realizarem. “Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.” (BRASIL, 2018).

A criação de grupos de dados é de extrema importância, já que ajudará a relacionar e entender melhor os dados que a empresa possui acesso.

O levantamento de atividades por departamentos é feito para entender quais dados são necessários para cada atividade, como armazená-los, como estão sendo utilizados, quem tem acesso a esses dados, outro ponto importante é evitar o armazenamento de dados que não estão sendo utilizados.

É importante dividir as atividades para que nenhum dado seja esquecido. Dados compartilhados também deve estar presente no agrupamento de dados, muitos desses dados são compartilhados com outros sistemas e áreas internas da empresa.

Podemos observa através da Tabela 1, a criação do grupo de dados do sistema interno de cadastro de colaboradores da Nexus Systemas, foram coletados todos os dados que o sistema realiza armazenamento, tratamento e compartilhamento com outros sistemas.

Tabela 1: Grupo de dados

Grupo de Dados	**Dados Envolvidos**
Documentação	CPF, RG, Nr°Reservista, Título de Eleitor, Certidão casamento, Nr° Convênio Médico, Nr° Convênio Odontológico, CNH, PIS, CTPS.
Dados pessoais	Nome, Data de nascimento, Sexo, Estado civil, Naturalidade, Nacionalidade, Etnia.
Dados familiares	Nome do cônjuge, Nome do pai, Nome da mãe, Nome dos filhos, Pensionista.
Informações bancárias	Conta, Agência, Banco, Conta FGTS, Tipo de conta.
Remuneração	Salário, % Variável, Remuneração variável, Benefícios.
Banco de Horas	Carga horária, Hora Extra, Horário de entrada e saída.
Lotação	Empresa, Cargo, Função, Líder imediato, Departamento.
Desempenho	Feedbacks recebidos, Desempenho, Plano de desenvolvimento individual, Perfil comportamental, Motivo Desligamento.
Contato	Telefone particular, Telefone corporativo, E-mail particular, E-mail corporativo.
Endereço	Endereço, Número, CEP, Bairro, Cidade, País, Complemento.

Fonte: Elaborado pelo autor, 2020.

Para elaboração do mapa de dados, deverá ser mapeado todos os dados sensíveis de cada grupo de dados e especificar qual a finalidade dos dados, local de armazenamento dos dados, tempo de armazenamento desses dados, com quem são compartilhados, se existe

alguma lei ou consentimento que permita a coleta desses dados, isso facilitará a etapa de levantamento de riscos.

É importante traçar os perfis comportamentais dos riscos, listando a probabilidade de ocorrência, o impacto caso risco ocorra, nível do risco para cada evento e perfil.

3.4.4 Política de segurança

O art. 50° da lei, recomenda que os agentes estabeleçam regras e boas práticas de governança sobre segurança de proteção de dados:

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

> "Nos dias de hoje, o PSI é aderido por uma grande parte das empresas em escala mundial, inclusive no Brasil. Semelhante aquelas empresas que ainda não tem um PSI, admitem a deficiência de realizar e instalar uma" (CAMPOS, 2007, P. 131).

A política de segurança da informação precisa determinar de fato o que pode ser feito com as informações, padrões a ser seguido dentro da organização, as possíveis entrada das informações, a verificação de acesso dessas informações sem infringir o princípio da confidencialidade, se os acessos podem ser efetuados de forma interna ou externa, determinar também os meios e quais os conseguirão fazer a transmissão e acesso a essas informações. A política deve definir em detalhes os requisitos e seu respectivo mecanismo, procedimento a ser executado.

Para Freitas e Araújo (2008), é essencial a criação de um comitê de segurança da informação, esse comitê deverá ser formado pelos responsáveis de inúmeros setores, como informática, jurídico, engenharia, infraestrutura, recursos humanos e outros setores essenciais.

O comitê será encarregado por divulgar e estabelecer os métodos de segurança, realização de reuniões regularmente, treinamentos sobre segurança da informação, ou seja, cujo objetivo principal é manter a segurança de todos os departamentos da empresa. "Compete que a política de segurança da informação possua uma gestão que abranja responsabilidade de gerenciamento definida para melhoramento, pesquisa crítica e análise da política de segurança da informação" (ABNT, 2005).

Para que a política de segurança consiga ser efetiva em uma empresa ela necessita de ter o apoio de todas as áreas envolvidas principalmente da parte gerencial da empresa, a implementação de uma política de segurança implica em uma grande mudança cultural na empresa principalmente para os colaboradores internos e externos da empresa.

É essencial que tenha uma preparação com todos os colaboradores, através de reuniões, informativos, debates e treinamentos, todas essas recomendações devem estar incluídas no plano de conscientização. O texto base que será apresentado aos colaboradores precisa ser escrito de uma forma objetiva e precisa, e que seja de fácil compreensão para evitar que os usuários tenham dúvidas e seja entendido por todos que tenham acesso ao documento. Destacaremos alguns itens essenciais que devem estar presentes em uma política de segurança da informação, conforme orientação abaixo:

- Política de senhas
- Termo de Uso dos Sistemas Internos
- Classificação da Informação
- Norma de Uso Aceitável de Ativos da Informação
- Gestão de Identidade e Controle de Acesso
- Acesso à Internet e Comportamento em Mídias Sociais
- Uso de Serviços de E-mail e Comunicadores Instantâneos
- Proteção Contra Códigos Maliciosos
- Uso de Equipamentos Computacionais Pessoais
- Acesso Remoto
- Monitoramento de Ativos e Serviços da Informação
- Resposta a Incidentes de Segurança da Informação
- Política de Backup

3.4.5 Gestão de incidentes e vazamento de dados

De acordo com o artigo 48 da Lei nº 13.709/18 (Lei Geral de Proteção de Dados), o controlador tem a responsabilidade de comunicar a autoridade nacional e ao titular qualquer incidente de segurança que possa acarretar risco aos titulares, devendo ser feita em prazo razoável, mencionando no mínimo:

> I - a descrição da natureza dos dados pessoais afetados;
> II - as informações sobre os titulares envolvidos;
> III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
> IV - os riscos relacionados ao incidente;
> V - os motivos da demora, no caso de a comunicação não ter sido imediata;
> VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Quanto ao plano de resposta a incidentes deve englobar a todos os funcionários da empresa, mesmo aqueles de baixo escalão, pois eles devem obrigatoriamente informar sobre qualquer irregularidade operacional relacionada a proteção de dados, podendo sofrer penalidades caso não haja a notificação, será necessário a criação de um fluxo de comunicação que facilite a chegada da informação sobre o vazamento de dados, para que medidas sejam tomadas. Prestadores de serviços que processam dados também devem ser integrados ao plano de resposta (CÂMARA, 2020).

Deve ser comunicado à autoridade nacional de proteção de dados e aos titulares quanto a qualquer incidente e vazamentos de dados. O controlador deve em conjunto com a autoridade nacional analisar qual será as medidas necessárias para neutralizar os riscos causados pelos incidentes. E quanto a comunicação aos titulares deve ser o mais transparente possível e de forma estratégica.

Relatório de impacto à proteção de dados pessoais de acordo com art. 5º da LGPD:

> 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.

O controlador deve manter o relatório de impacto à proteção de dados pessoais sempre que houver qualquer risco de que determinado tratamento de dados possa vir a causar danos ao titular, isso permite compreender os perigos envolvidos em cada incidente. O relatório é uma documentação que contém a descrição dos processos de tratamento de dados pessoais que podem causar riscos, bem como medidas e mecanismos de mitigação de risco. Com ele é possível comprovar os devidos cuidados para evitar tais risco no tratamento de dados.

De acordo a art. 38 da Lei Geral de Proteção de Dados Pessoais:

> Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
> Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

3.4.6 Revisão de contratos

O Artigo 42 da Lei Geral de Proteção de Dados, afirma que a responsabilidade por qualquer dano ou violação referente ao tratamento de dados é do controlador e operador.

E necessário efetuar à revisão dos contratos vigentes e de possíveis novos contratos que possam ser assinados. Qualquer contrato envolvendo o compartilhamento, uso, consulta de dados pessoais, caso ocorra violação da LGPD os responsáveis serão penalizados com as sanções previstas na lei.

O artigo 42 traz a seguinte afirmação: “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.” (BRASIL, 2018).

É recomendado a revisão jurídica e atualização das cláusulas de contratos com parceiros e fornecedores que realizem algum tipo de tratamento de dados, principalmente fornecedores de soluções em nuvem, e-mail marketing e mídias sociais, a responsabilidade por qualquer infração ou incidente de vazamento de dados será do controlador e operador.

Muitas empresas não possui uma estrutura para efetuar uma revisão, nesses casos a contratação de uma empresa de consultoria jurídica poderá auxiliar nesse processo.

4 DISCUSSÃO

O presente trabalho apresentou pontos importantes sobre a Lei Geral de Proteção de dados e identificou que é muito importante a preocupação referente a privacidade e proteção dos dados.

Durante o desenvolvimento do trabalho ficou evidenciado a importância de uma equipe de TI (tecnologia da informação) capacitada com os mais diversos tipos de profissionais para que se possa garantir a segurança dos dados, além da equipe ter conhecimentos sobre a LGPD. A lei traz no artigo 46, que os agentes de tratamento devem adotar medidas de segurança técnicas e administrativas, controles de acessos, mecanismo de segurança, e para isso uma equipe de TI é essencial.

Em um projeto que tem como premissa alterar a estrutura e a forma como os processos são conduzidos em uma empresa, a maior dificuldade será em relação a mudança na cultural da empresa. A complexidade da implantação de novos processos em organizações que já possuem uma cultura rígida por parte de seus colaboradores pode dificultar a adesão.

Ao longo da análise foi identificado a necessidade da revisão constante dos processos internos e externos da empresa, e em alguns casos será necessário ajustes simples, em outros casos ajustes de grande impacto. Na etapa de mapeamento de dados ficou evidenciado a importância da categorização dos dados, através do mapeamento será possível a identificação quais são os dados que a empresa possui acesso, quem são os responsáveis por determinados dados, se a empresa está coletando e armazenando somente os dados necessários ao qual foi indicado no consentimento de coleta dos dados.

Empresas que já possuem boas práticas de governança implantada em seus processos, a adequação ocorrerá de forma mais rápida, tendo em vista também que não dependeram de maiores investimentos. A colaboração de todos os funcionários e integração dos setores da empresa poderá diminuir a dificuldade dessa viabilização.

A nomeação de um encarregado de proteção de dados é um ponto bastante discutido em um processo de implementação da LGPD, a nomeação de um encarregado implicará geração de novos custos para as empresas, pois ele será o responsável por prestar assistência interna para os colabores da empresa, aos titulares de dados, sobre a praticas de tratamento de dados, verificar se está praticas estão em conformidade com a legislação e a política interna da empresa. Investimento em cursos de capacitação, certificações serão essenciais.

Empresas que não possuem um encarregado definido e efetuam algum tipo de tratamento de dados, deverão eleger um colaborador ou uma equipe capacitada para que possa atender essa função.

De acordo com os art. 49 e art. 50, as empresas deverão aderir normas e padrões de qualidade de boas práticas e da governança, a norma ISO 27001 por se tratar de um padrão relacionado à segurança da informação e possuir normas técnicas e obrigações específicas, é uma das normas que melhor se enquadra nesses requisitos, a norma possui mecanismos internos e externos, mitigação de riscos e outros aspectos necessários para o cumprimento da LGPD.

A criação do plano de conscientização para a instrução dos colabores e titulares de dados, com os conhecimentos sobre segurança e privacidade otimizará os processos e ajudará a evitar possíveis vazamento de dados e diminuir o risco de ameaças à segurança.

Outro ponto encontrado, as empresas devem efetuar auditorias internas e externas constantemente, revisar seus contratos, processos internos, e manter todos esses registros documentados. A LGPD traz recomendações para o tratamento realizado pelos meios físicos, o cuidado com documentos armazenados fisicamente, esses documentos também estão expostos a possíveis riscos, como, roubo de documentos, eliminação incorreta, cópias indevidas de documentos, armazenamento incorreto. Na ocorrência de auditorias perante a agência nacional de proteção de dados ser possível a comprovação que a empresa está em conformidade com a LGPD.

Um dos pontos positivos da lei, os titulares de dados terão maior segurança e garantia de que suas informações serão tratadas de forma adequada.

A lei também apresenta pontos negativos, como, o alto custo e investimentos na estrutura operacional da empresa, investimento em certificações, contratação de novos profissionais, aquisição de novos equipamentos para adequação da estrutura física da organização, esforço conjunto de todas as áreas da empresa para adequação principalmente na mudança de cultura da empresa, e as sanções trazidas no art. 52 da lei, onde, em razão de infrações e não cumprimento da lei, ficam sujeitos a multa simples, de até 2 % do faturamento da empresa, limitada, no total, a R$ 50.000.000.00.

5 CONCLUSÃO

Ao longo deste trabalho, foi possível observar que medidas para a proteção dos dados pessoais eram necessárias algum tempo no Brasil, tendo em vista que países da Europa já possuía o Regulamento Geral de Proteção de Dados (GDPR), impondo assim a necessidade de o Brasil ter a suas próprias medidas de proteção aos dados pessoais. Com a LGPD a proteção dos dados pessoais vai se fazer necessária para as empresas públicas e privadas.

A mudança cultural e adaptação às regras propostas pela nova lei não acontecem da noite para o dia. Em um projeto que tem como premissa alterar a estrutura e a forma como os processos são conduzidos na empresa, a maior dificuldade será em relação a mudança na cultura da empresa e o apoio de todos os envolvidos no processo, que tendem a oferecer resistência quando há necessidade de modificar hábitos já estabelecidos na organização.

A proposta deste trabalho foi um estudo sobre os impactos da implementação da LGPD em ambientes corporativos, no qual foi possível avaliar um estudo de caso, avaliando o que poderia ser feito dentro das normas previstas na LGPD, avaliando os possíveis caminhos que uma empresa pode adotar em relação aos dados coletados de seus clientes e em posse deste dados identificar como protegê-los. Este trabalho mostra a importância da lei para empresas e sociedade, trazendo mais clareza para empresas sobre a nova regulamentação de proteção de dados.

A análise realizada visa contribuir para os novos estudos acerca do tema e com a vigência da lei pode ser um documento útil para orientação e adequação.

O trabalho desenvolvido apresentou as seguintes contribuições:

- Poder ser utilizado como um documento de base para quem esteja pesando conhecer, especializar no assunto;
- Desenvolver uma análise sobre os principais aspectos de proteção referente a proteção de dados pessoais;
- Conhecimento sobre a lei e a aplicação em outros tipos de cenários e empresas;

As limitações encontradas durante o desenvolvimento do trabalho foram:

- Livros, artigos e documentos referente a lei e a área de tecnologia ainda são difíceis de ser encontrados;
- A lei pode haver muitas interpretações e ocasionando dificuldade no seu entendimento;

- Pelo pouco tempo de vigência da lei, as experiências são baseadas no regulamento europeu, na GPDR;

Após a conclusão deste trabalho pode-se analisar as limitações, contribuições e apontar a elaboração de trabalhos futuros como:

- Análise e implementação da LGPD em uma empresa real, com dados e problemas que podem ocorrer durante a sua implementação;
- Desenvolvimento de uma política de privacidade e Relatório de impacto com base na LGPD;
- Desenvolver uma análise sobre a importância da NBR ISO/IEC 27001 no processo de implementação da LGPD;

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001:2013. Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos**. Rio de Janeiro: 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 27005: **Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação**. Rio de Janeiro. 2011.

AFINAL, **o que é plano de conscientização em segurança da informação?** 2019. Disponível em: https://www.alertasecurity.com.br/afinal-o-que-e-plano-de-conscientizacao-em-seguranca-da-informacao/. Acesso em: 04 nov. 2020.

BRANDAO, Graziela. **O que é o mapeamento de dados?** 2020. Disponível em: <https://blconsultoriadigital.com.br/mapeamento-de-dados/#:~:text=Compartilhe!,LGPD%2C%20GDPR%2C%20CCPA).> . Acesso em: 27 out. 2020.

Brasil. Lei 13.709 de 14 de Agosto de 2018. **Dispõe sobre a proteção de dados pessoais e altera a Lei nº12.965, de 23 de abril de 2014 (Marco Civil da Internet)**. Diário Oficial da República Federativa do Brasil, 15 agosto de 2018. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 31 mai. 2020.

CALIXTO, MELISSA DA SILVA. **ANÁLISE DA IMPLANTAÇÃO DA GESTÃO DE RISCOS NA TECNOLOGIA DA INFORMAÇÃO: UM ESTUDO DE CASO.** 2020. Trabalho de Conclusão de Curso (Tecnólogo em Gestão da Tecnologia da Informação) - Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina, FLORIANÓPOLIS, 2020.Disponível em: https://repositorio.ifsc.edu.br/bitstream/handle/123456789/1668/Analise%20da%20implanta%C3%A7%C3%A3o%20da%20gest%C3%A3o%20de%20riscos%20na%20tecnologia%20da%20informa%C3%A7%C3%A3o%20-%20um%20estudo%20de%20caso.pdf?sequence=1&isAllowed=y. Acesso em: 11 nov. 2020.

CAMPOS, A. **Sistemas de Segurança da Informação**. 2 .ed. Florianópolis: Visual Books, 2007.

CÂMARA, FLÁVIA D S. **Lei Geral de Proteção de Dados Pessoais (LGPD) - aplicada às empresas de Contabilidade.** 2020. Trabalho de Conclusão de Curso (Graduação em Ciências Contábeis) - Universidade Federal do Rio Grande do Norte, Natal, 2020. Disponível em: https://monografias.ufrn.br/jspui/handle/123456789/10702. Acesso em: 11 nov. 2020.

CELIDONIO, Tiago et al. Metodologia para mapeamento dos requisitos listados na LGPD (Lei Geral de Proteção de Dados do Brasil número 13.709/18) e sua adequação perante a lei em uma instituição financeira - Um estudo de caso: Methodology for mapping and adequacy of the requirements listed in LGPD (Brazil Data Protection General Law number 13 709/18) in a financial institution - A case study. **Brazilian Journals of Business**, Curitiba, ano 2020, v. 2, n. 4, p. 3626-3648, 20 set. 2020. DOI 10.34140/bjbv2n4-012. Disponível em: https://www.brazilianjournals.com/index.php/BJB/article/view/18382. Acesso em: 11 nov. 2020.

FERNADES, Ana V. **EFEITOS DO VAZAMENTO DE DADOS SEGUNDO A LGPD**. 2019. Disponível em: https://4s.adv.br/blog/efeitos-do-vazamento-de-dados-segundo-lgpd/. Acesso em: 25 de maio de 2020.

FREITAS, F; ARAUJO, M. **Politicas De Segurança Da Informação: Guia prático para elaboração e implementação**. 2ed. Rio de Janeiro: Ciência Moderna LTDA, 2008.

GUIA DE BOAS PRÁTICAS LEI GERAL DE PROTEÇÃO DE DADOS (LGPD). [S. l.: s. n.], 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf. Acesso em: 21 nov. 2020.

MACIEL, Rafael Fernandes. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18).** 1. ed. Goiânia: RM Digital Education, 2019.

MONTEIRO, Sheila de Góes. **Gestão de riscos, Ameaças e Vulnerabilidades**. Estácio de Sá, Rio de Janeiro, 2018.

MONTEIRO, Sheila de Góes. **Fundamentos de Segurança da Informação**. Florianópolis: Estácio de Sá, 2016. 40 p.

PEREIRA, Helena Acácio Santini; BERGAMASCHI, Alessandro Bunn. **Manual de gestão de riscos do INPI**. Rio de Janeiro: Instituto Nacional da Propriedade Industrial, 2018.

RAPÔSO, Cláudio F L et al. **LGPD-LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS EM TECNOLOGIA DA INFORMAÇÃO**: Revisão Sistemática. RACE-Revista da Administração, v. 4, p. 58-67, 2019.

RIBEIRO, L. **Proteção de dados pessoais: Estudo comparado do regulamento 2016/679 do parlamento europeu e conselho e o projeto de lei brasileiro n. 5.276/2016.** Brasília, p. 5 – 24, 2016.

ROCHA, Camila P D et al. **Segurança da Informação: A ISO 27.001 como Ferramenta de Controle para LGPD**. Revista de Tecnologia da Informação e Comunicação da Faculdade Estácio do Pará, v. 2, n. 3, p. 78-97, 2019.

SÁ, MARCELO DIAS DE. **Análise do Impacto da Nova Lei de Proteção de Dados Pessoais nas aplicações de Internet das coisas:** Aplicações mobile do governo. 2019. Trabalho de Conclusão de Curso (Especialista em Informática) - Universidade Federal de Minas Gerais, Brasília, 2019. Disponível em: https://repositorio.ufmg.br/bitstream/1843/32040/1/MarceloDiasDeSa.pdf. Acesso em: 31 maio 2020.

SERPRO. Mapa da proteção de dados. Disponível em: https://www.serpro.gov.br/lgpd/menu/a-lgpd/mapa-da-protecao-de-dados-pessoais. Acesso em: 11 de nov de 2020.

STALLINGS, Willian.**Criptografia e segurança de redes**: princípios e práticas. 6. ed. São Paulo: Pearson Education do Brasil, 2015.

VARGAS, André Azevedo. **DESENVOLVIMENTO E USO DE UM FORMATO DE POLÍTICAS DE PRIVACIDADE NO CONTROLE DE ACESSO.** 2017. Trabalho Conclusão Curso (Bacharelado em Ciências da Computação) - Universidade Federal de Santa Catarina, Florianópolis, 2017. Disponível em: https://repositorio.ufsc.br/xmlui/handle/123456789/179929. Acesso em: 31 maio 2020.