INSTITUTO FEDERAL DE CIÊNCIA E TECNOLOGIA DE PERNAMBUCO
Campus Jaboatão dos Guararapes
Divisão de Pesquisa e Extensão e Pós-Graduação
Gestão em Tecnologia da Informação e Comunicação

RODOLFO LIMA DOS ANJOS

LEI GERAL DE PROTEÇÃO DE DADOS: UMA PROPOSTA DE IMPLANTAÇÃO E ADEQUAÇÃO ACESSÍVEL AOS PEQUENOS PROVEDORES DE ACESSO À INTERNET.

Jaboatão dos Guararapes

2022

RODOLFO LIMA DOS ANJOS

LEI GERAL DE PROTEÇÃO DE DADOS: UMA PROPOSTA DE IMPLANTAÇÃO E ADEQUAÇÃO ACESSÍVEL AOS PEQUENOS PROVEDORES DE ACESSO À INTERNET.

Trabalho de Conclusão de Curso apresentado ao Departamento de Pesquisa e Extensão e Pós Graduação como requisito obrigatório para obtenção do diploma de Pós-Graduação *Lato Sensu* Especialista em Gestão e Qualidade em Tecnologia da Informação e Comunicação do Instituto Federal de Ciência e Tecnologia de Pernambuco Campus Jaboatão dos Guararapes.

Orientador Prof. Ms. Nilson Cândido de Oliveira Junior

Jaboatão dos Guararapes

2022

FICHA CATALOGRÁFICA
Dados Internacionais de Catalogação na Publicação (CIP)
SIBI/IFPE Biblioteca Ariano Suassuna – Campus Jaboatão dos Guararapes

A599l
Anjos, Rodolfo Lima dos.
Lei geral de proteção de dados: uma proposta de implantação e adequação acessível aos pequenos provedores de acesso à internet / Rodolfo Lima dos Anjos; Prof. Ms. Nilson Cândido de Oliveira Júnior (orientador) . Jaboatão dos Guararapes, 2022.
86f.; il.
Trabalho de Conclusão de Curso (Especialização em Gestão e Qualidade em Tecnologia da Informação e Comunicação) IFPE - campus Jaboatão dos Guararapes.
Inclui referências.
1. Tecnologia da Informação 2. Brasil. [Lei geral de proteção de dados pessoais (2018)] 3.Proteção de dados. 4. Internet. 5. Provedores de serviços da Internet.
CDD 004.21

Catalogação na fonte elaborada pelo Bibliotecário Thiago Leite Amaro da Silva - CRB4/ 2.021

RODOLFO LIMA DOS ANJOS

LEI GERAL DE PROTEÇÃO DE DADOS: UMA PROPOSTA DE IMPLANTAÇÃO E ADEQUAÇÃO ACESSÍVEL AOS PEQUENOS PROVEDORES DE ACESSO À INTERNET.

Monografia apresentada ao Programa de Pós-Graduação em Gestão e Qualidade em Tecnologia da Informação e Comunicação do Instituto Federal de Ciência e Tecnologia de Pernambuco como requisito obrigatório para obtenção do título de Especialista em Gestão e Qualidade em Tecnologia da Informação e Comunicação.

Trabalho Aprovado. Jaboatão dos Guararapes, 09/02/22.

COMPOSIÇÃO DA BANCA		
	NOTA	**ASSINATURA**
Prof. Nilson Cândido de Oliveira Júnior (presidente da banca)	8	gov.br Documento assinado digitalmente Nilson Candido de Oliveira Jr Data: 10/02/2022 10:45:07-0300 Verifique em https://verificador.iti.br
Prof. Luciano de Souza Cabral (avaliador 1)	7	gov.br Documento assinado digitalmente Luciano de Souza Cabral Data: 10/02/2022 10:50:56-0300 Verifique em https://verificador.iti.br
Profa. Divanilson F. M. e Silva (avaliadora 2)	8	gov.br Documento assinado digitalmente DIVANILSON FRANCISCO MORAIS E SILVA Data: 10/02/2022 11:01:57-0300 Verifique em https://verificador.iti.br
NOTA FINAL	7,66	

AGRADECIMENTOS

Em primeiro lugar agradeço a Deus, por ser essencial em minha vida e estar ao meu lado como: meu guia e minha orientação em todos os momentos.

A minha mãe Dona Nalva, por todo sacrifício, apoio e esforço para transmitir uma boa educação, índole e caráter social.

Ao Professor e Orientador Nilson Cândido, pelo suporte que foi importante para a elaboração deste trabalho.

E aos meus colegas que se tornaram amigos a partir da sala de aula, em especial a Geraldo Torres, Glaudston Mota e Jurandy Santos por todo companheirismo, colaboração, compreensão, cooperação e parceria que tivemos ao longo desta jornada e tudo que realizamos juntos desde o início do curso.

A toda equipe de Professores e Funcionários do IFPE que demonstraram grandeza em me ajudar no crescimento como pessoa e como profissional, tornando o período dentro da instituição o mais interessante possível.

“o pó retorne à terra, de onde veio,
e o espírito volte a Deus, que o concedeu.”
(Eclesiastes, 12:7)

Resumo

O cenário mundial vem mudando em relação a proteção de dados pessoais. E no Brasil não poderia ser diferente, visando estabelecer direitos e responsabilidades de todos os envolvidos foi criada a Lei Geral de Proteção de Dados. Portanto, o presente trabalho foi elaborado para alcançar o propósito principal que é propor um guia de implantação da LGPD acessível para adequação dos pequenos provedores de acesso à internet, para tal serão enfrentados alguns desafios importantes como a necessidade de um planejamento através de etapas e procedimentos, possibilidade de investimentos e a adequação de políticas de proteção de dados em alguns setores da empresa, desta forma, se faz necessário o desenvolvimento de um instrumento que auxilie na utilização das melhores práticas existente no tocante a proteção de dados. Esse trabalho é baseado nas legislações de proteção de dados vigente, com o suporte de conceitos e práticas reconhecidas em vários países abordando técnicas e referências; direcionando empresas na implantação e na condução da proteção de dados. Por fim vale ressaltar, que o tema abordado envolveu os mais diferenciados campos como: tecnologia, gestão e do direito.

Palavras-Chaves: LGPD, Segurança, Tratamento, Dados, Internet.

Abstract

The world scenario has been changing regarding the protection of personal data. And in Brazil it could not be different, aiming to establish rights and responsibilities of all involved, the General Data Protection Law was created. Therefore, this work was designed to achieve the main purpose, which is to propose an accessible LGPD implementation guide for the adaptation of small internet access providers, for which some important challenges will be faced, such as the need for planning through steps and procedures , possibility of investments and the adequacy of data protection policies in some sectors of the company, thus, it is necessary to develop an instrument that helps in the use of the best practices in terms of data protection. This work is based on current data protection legislation, with the support of concepts and practices recognized in several countries addressing techniques and references; guiding companies in implementing and conducting data protection. Finally, it is noteworthy that the topic addressed involved the most different fields such as: technology, management and law.

Keywords: LGPD, Security, Treatment, Data, Internet.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS

ANATEL	Agência Nacional de Telecomunicações
ANPD	Autoridade Nacional de Proteção de Dados
DPO	Data Office Protect
GDPR	General Data Protection Regulation
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
LGPD	Lei Geral de Proteção de Dados
PDCA	Plan Do Check Act
RIPD	Relatório de Impacto à Proteção de Dados
SGPI	Sistema de Gestão da Privacidade da Informação
SGSI	Sistema de Gestão de Segurança da Informação
TIC	Tecnologia da Informação e Comunicação

SUMÁRIO

1 INTRODUÇÃO

É impossível ignorar o quanto o advento da internet modificou o modo de vida desde as atividades mais simples, passando pelo estilo de vida, até o trabalho. Dessa forma, a rede mundial de computadores traz as diversas possibilidades de utilização, como a oportunidade do aprendizado, a liberdade de comunicação entre outras. Tal facilidades traz consigo um aumento no volume de tráfego de dados, e a atenção sobre os mesmos que circulam pela internet.

Nesse contexto de desenvolvimento da internet uma evolução foi necessária para a proteção de dados, e no Brasil não poderia ser diferente através da lei 13.709/2018 (Lei Geral de Proteção de Dados). Na forma de atender os problemas advindos com a internet no que tange a proteção e a privacidade dos dados, visando a proteção das informações quanto ao tratamento, o uso, a manutenção, a guarda e o compartilhamento realizado, e viabilizando o amparo as pessoas sejam elas físicas ou jurídicas.

Com isso advêm as responsabilidades dos provedores de acesso à internet, sobre como se adequar à lei geral de proteção de dados e compreender o impacto causado no seu funcionamento. Faz parte dessa pesquisa encontrar um formato de implantação e adequação desta lei, onde o trabalho será obrigatoriamente guiado pelas áreas: gestão, tecnologia e direito. Cada área terá uma contribuição importante para a implantação, sendo difícil que apenas uma delas solucione as demandas dos pequenos provedores de acesso.

Neste trabalho, buscou-se reunir dados e informações com o propósito de responder o seguinte problema de pesquisa: Quais as etapas e procedimentos que melhor se adequa a uma proposta de implantação da lei geral de proteção de dados no ambiente dos pequenos provedores de acesso à internet.

1.1 Formulação do Problema de Pesquisa

Com as mudanças ocorridas nos perfis do usuário e da internet, foi verificada a necessidade de alterações na composição da proteção de dados, ou seja, a internet mudou parâmetros, conectando e aproximando as pessoas que estão ficando cada vez menos sós e deixando a vida cada vez menos privada. Essa realidade exige uma maior atenção sobre a privacidade e a proteção de dados, pois tendo em vista a importância dos dados na era digital, podemos afirmar que hoje os dados são o interesse predominante de qualquer instituição, pois através da coleta e do tratamento, os dados são usados para atender aos mais diversos interesses.

A preocupação com a proteção de dados no Brasil se formaliza através da concepção da lei geral de proteção de dados a LGPD, criada para garantir que os direitos fundamentais a proteção de dados fosse protegida em todo o território nacional no âmbito público e privado. A regulamentação vem para transformar todo o contexto que envolve o tratamento de dados pessoais dos cidadãos brasileiros.

Após a promulgação da LGPD questões relacionadas aos dados pessoais passou a vigorar em todo território nacional, dessa forma verificou-se uma demanda expressiva por parte de todos os setores da sociedade para iniciar o processo de adequação as questões relativas ao tratamento de dados, ao direito dos titulares dos dados, as responsabilidades e a segurança, enquadramento que também inclui os pequenos provedores de acesso à internet como parte integrante e importante do universo da comunicação e da informação, nesse sentido, os provedores terão que se adaptar ao novo ambiente digital.

Sendo um pequeno provedor de acesso à internet definido como qualquer organização que ofereça serviços de acesso, participação ou utilização da internet, o provedor também atua com serviços: e-mail, hospedagem de sites, *cloud* entre outros. Dada a definição acima existe a preocupação deste trabalho com a real situação dos pequenos provedores perante a lei geral de proteção de dados, onde os mesmos podem apresentar uma fragilidade e um completo desalinhamento com as políticas de proteção de dados, neste contexto, o desalinhamento produz um efeito danoso. A

ausência de uma correta ação nos processos como a coleta, o tratamento, o arquivamento, o anonimato, e a exclusão dos dados, faz com que os provedores estejam numa situação de completa clandestinidade e amadorismo perante a proteção de dados.

Conforme enfatizado acima, fica demonstrado que a implantação da lei geral de proteção de dados provocará mudanças na rotina dos pequenos provedores de acesso à internet, sendo a melhoria e a evolução partes importantes deste processo de proteção.

A importância das mudanças que se faz necessário para a implantação da LGPD e a ausência de um guia de implantação direcionado para os pequenos provedores de acesso à internet, criam barreiras para as adequações. Assim questionamentos surgem dentro do ambiente dos pequenos provedores de acesso à internet, por exemplo: Quais ferramentas e materiais tecnológicos serão necessários? Quanto custará implantar? O que será implantado? Será necessário contratar pessoas? Será necessário comprar equipamentos?

1.2 Objetivo

Tendo a consciência dos desafios para a proteção de dados, o presente trabalho volta-se para o desafio de adequar o ambiente do pequeno provedor a lei geral de proteção de dados. Neste trabalho serão apresentados as proposições, ações e procedimentos, baseados nas melhores práticas referentes a proteção de dados. Além do comprometimento com o desenvolvimento de uma proposta para a implantação de um plano de adequação à lei geral de proteção de dados, este trabalho tem como objetivo disponibilizar um guia contextualizado para a implantação da LGPD em um pequeno provedor de internet, onde serão abordados fundamentos, artefatos e mecanismos necessários para o desenvolvimento, estruturação e documentação do processo de implantação.

Com isso a proposta de um plano de implantação para adequação a LGPD surge para os provedores de forma integral e acessível. Para este propósito vale destacar e ter em mente que fatores como: aplicabilidade, economicidade e praticidade são condições primordiais para que transpareça ao pequeno provedor clareza ao usar o plano de implantação. Neste contexto vale ressaltar que a atual proposta se preocupar com as várias penalidades e sanções que os pequenos provedores podem sofrer caso não ocorra a adequação.

A implantação deste trabalho trará um fluxo de ações tendo como base a tecnologia, a gestão e o direito para atender em especial aos pequenos provedores. Outros pontos de importância que se faz necessário é saber lidar com a falta de recurso, saber conduzir o impacto da LGPD dentro do ambiente, alcançar as diretrizes impostas e sempre atualizar os parâmetros da proteção de dados. Tendo objetivo específico de compreender os obstáculos e as atuais dificuldades enfrentadas pelos provedores de acesso à internet com relação à lei geral de proteção de dados. Pesquisar e identificar um formato mais adequado de modelo de implantação a ser utilizado nos pequenos provedores de acesso à internet. Identificar mecanismos que visam facilitar a adequação dos requisitos da lei de proteção de dados.

1.3 Justificativa

Um provedor de acesso à internet tem os deveres segundo a legislação de proteger constantemente os dados e a privacidade dos usuários, de forma ininterrupta e mantendo os níveis de segurança dentro da rede.

> Brasil. Decreto nº 8.771, de 11 de maio de 2016. Regulamenta o art. 13, “Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes:
>
> I - O estabelecimento de controle estrito sobre o acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários;
>
> IV - O uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes.” (BRASIL, 2014).

A ausência da incorporação das políticas de proteção de dados dentro de uma empresa, pode causar danos diversos, de acordo com a lei geral de proteção de dados (BRASIL, 2018), assim estão dispostas: I - Advertência, com indicação de prazo adoção de medidas corretivas; II – multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitados, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; III – multa diária observando os limites citado anteriormente. IV – publicação da infração após devidamente apurada e confirmada a sua ocorrência.

As penalidades seguem conforme o disposto V – bloqueio dos dados pessoais a que se refere a infração até a sua regularização; VI – eliminação dos dados pessoais a que se refere a infração; X – suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; XI – suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; XII – proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

No tocante ainda sobre os impactos causados com a implantação da lei geral de proteção de dados, Teffé e Viola (2020) citam os benefícios da implantação da LGPD sobre a aplicação de base legal: previne e controla fraudes garantindo a segurança da rede e da informação; melhoria de produtos e serviços; produz ações mais adequadas e personalizadas a seus clientes; ainda segundo o Serpro (2020) existe: o destaque em relação à concorrência; mais credibilidade no mercado pela conscientização da proteção dos dados pessoais; melhoria na reputação e imagem da empresa no mercado. A implantação da lei geral de proteção de dados em um ambiente de provedor de acesso à internet requer uma gestão, utilizando o controle e a melhoria contínua nos processos, garantindo ao ambiente estabilidade e segurança na proteção de dados.

Para a implantação e adequação da lei geral de proteção de dados, segundo Pessoa (2016) será então necessário um esforço multidisciplinar, através das áreas de: (gestão, segurança da informação, TI e jurídica). Segundo Teixeira (2020) os métodos que auxiliam no processo de adequação as legislações de proteção de dados são encontrados de forma limitada e superficial, com a edição de poucas doutrinas e pouco aprofundada a matéria, todavia a partir de uma interpretação analógica da LGPD, assim como da importação de métodos bem-sucedidos de países que possuem certa solidez e adaptação a legislação pertinente, acabam, auxiliando no correto gerenciamento da informação, e assim do processo de adequação a Lei Geral de Proteção de Dados (LGPD).

Conforme abordagens já relacionadas, a novidade do tema e consequentemente a pouca quantidade de materiais traz a necessidade de elaborar este trabalho que pretende auxiliar neste processo de adequação da proteção de dados. Conforme mencionado anteriormente a sintonia e o alinhamento de diversas áreas do conhecimento, traz a possibilidade de atingir o objetivo de tornar público um guia de implantação, utilizando procedimentos, etapas, processos, ferramentas e funções necessária para a adequação. Este procedimento visa uma proposta direta e fácil, em acordo com as contribuições apresentada por outros autores.

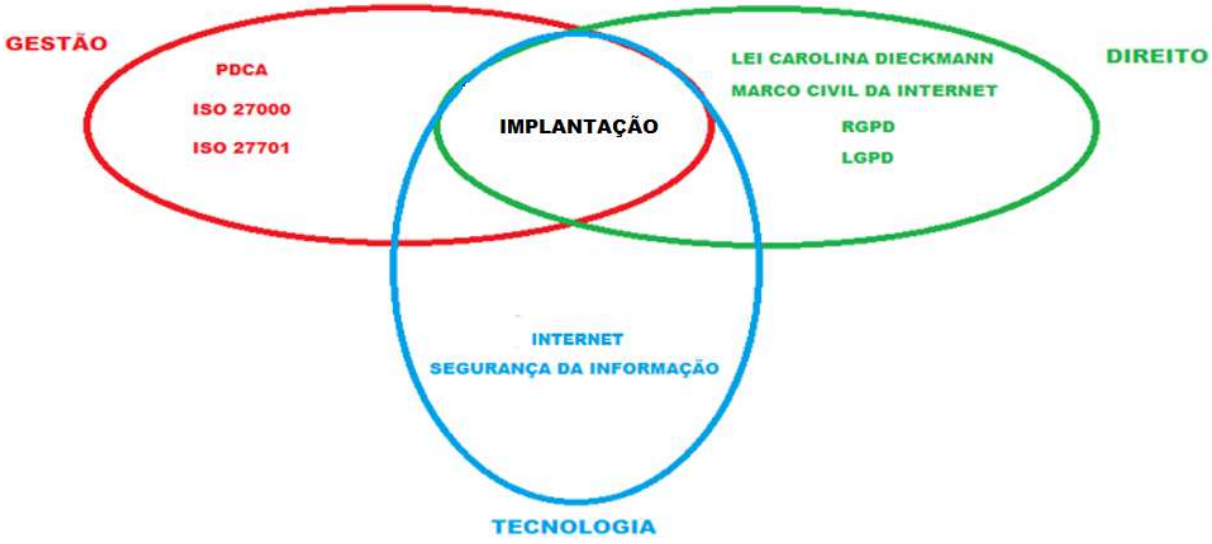
1.4 Estrutura da Monografia

O trabalho de conclusão de curso é constituído em 6 capítulos. Segue uma narrativa através de uma breve explanação. No capítulo 1 foi abordado o problema a ser pesquisado, os objetivos básicos e específicos, a motivação, os desafios e a relevância do tema para os pequenos provedores de acesso. No capítulo 2 é fundamentada a teoria através da revisão das literaturas que contempla os aspectos e conceitos sobre proteção de dados. Já no capítulo 3 foi demonstrado a metodologia de pesquisa com as etapas e definições da pesquisa. Nos capítulos 4 e 5 foi descrito a proposta de implantação da LGPD no ambiente dos pequenos provedores de acesso. No capítulo 6 deu-se início a conclusão sobre a proposta do trabalho. E por fim, todo material de pesquisa através das referências de autores e pesquisadores utilizados neste trabalho.

2 FUNDAMENTAÇÃO TEÓRICA

Para uma compreensão direcionada deste trabalho é importante uma verificação prévia do escopo e direcionamento que envolve a pesquisa. A seguir, na figura 1, estão os três pilares que representam a base da proposta de implantação: a gestão, o direito e a tecnologia. Estes pilares orientam e credenciam a pesquisa e são essenciais para a construção do guia de implantação, onde a utilização de livros, artigos relacionados e sites especializados, são fundamentais para a produção deste trabalho.

Figura 1 - Panorama de Revisão da Literatura



Fonte: O Autor (2020)

2.1 A Internet

A *Internet* proporcionou uma grande revolução nos meios de comunicação entre os mais diversos povos e culturas. Por ser um instrumento de alcance mundial e de extrema praticidade, facilita a pesquisa acadêmica, auxilia no trabalho e contribui para o desenvolvimento humano, levando informação às áreas mais remotas e de difícil acesso do planeta. Entretanto, até chegar ao estágio atual, várias foram as etapas de aprimoramento e desenvolvimento desta tecnologia.

Morais (2012, p. 42), afirma que:

> A Internet é, portanto, uma rede mundial de computadores ou terminais ligados entre si, que tem em comum um conjunto de protocolos e serviços, de uma forma que os usuários conectados possam usufruir de serviços de informação e comunicação de alcance mundial através de linhas telefônicas comuns, linhas de comunicação privadas, satélites e outros serviços de telecomunicações. Com o surgimento da World Wide Web, esse meio foi enriquecido, o conteúdo da rede ficou mais atraente com a possibilidade de incorporar além de textos, imagens e sons.

Com isso o surgimento da internet alterou drasticamente a forma como as interações humanas acontece em tempos atuais. Na medida em que o número de seus usuários se aproxima dos 4 bilhões, não resta dúvida quanto à importância da internet. A Internet tornou-se primordial no apoio à inovação, ao crescimento econômico e ao progresso sociocultural da sociedade. Desde suas origens nos anos 1960 como um projeto das forças armadas americanas, mais especificamente do DARPA (*Defense Advanced Research Projects Agency*), passando pela incorporação dos protocolos TCP/IP (*Transmission Control Protocol/Internet Protocol*) nos anos 1980 até os dias atuais, a internet cresceu exponencialmente e diversas questões sobre sua arquitetura, funcionamento, gerenciamento, privacidade e proteção de dados têm chegado à luz da discussão. (PINHEIRO, 2016).

No Brasil, a internet foi lançada oficialmente apenas em 1989 e foi fruto do desenvolvimento da Rede Nacional De Pesquisa (RNP), uma iniciativa governamental do Ministério da Ciência e Tecnologia, com o apoio de fundações de pesquisa dos estados de São Paulo, Rio de Janeiro e Rio Grande do Sul.

Para uma maior descrição e compreensão do tema, a norma da ANATEL traz mais informações basilares sobre as propriedades da internet:

> A Internet é organizada na forma de espinhas dorsais *backbones*, que são estruturas de rede capazes de manipular grandes volumes de informações, constituídas basicamente por roteadores de tráfego interligados por circuitos de alta velocidade. Interligadas às espinhas dorsais de âmbito nacional, haverá espinhas dorsais de abrangência regional, estadual ou metropolitana,

> que possibilitarão a interiorização da Internet no País. Conectados às espinhas dorsais, estarão os provedores de acesso ou de informações, que são os efetivos prestadores de serviços aos usuários finais da Internet, que os acessam tipicamente através do serviço telefônico. Poderão existir no país várias espinhas dorsais Internet independentes, de âmbito nacional ou não, sob a responsabilidade de diversas entidades, inclusive sob controle da iniciativa privada. (ANATEL, 1995).

Sobre o aspecto técnico a *internet* propaga-se através da tecnologia de comutação de pacotes, que nada mais é que a transmissão de pacotes de dados com determinado conteúdo de uma origem a um destino. É imprescindível ter em mente os três elementos para entender o funcionamento da rede: conteúdo, origem e destino. O pensamento principal é visualizar a internet como uma rede responsável por transmitir dados entre dispositivos. O modelo TCP/IP é uma maneira de demonstrar o ecossistema da Internet que envolve diversos atores.

A evolução da *internet* no mundo não se deve apenas pelo aumento das velocidades das conexões, mas também em sua cobertura considerando áreas rurais e urbanas caminhando para a universalização do acesso à rede. Neste cenário, esse aumento do número de usuários é o que justifica a necessidade do incremento da infraestrutura da rede, ou seja, manter em evolução não só a infraestrutura da rede, mas a privacidade e a proteção de dados, sendo um desafio real e necessário a ser enfrentado pelos provedores de acesso à internet na ampliação e modernização da internet.

2.2 A Segurança da Informação

A segurança da informação é de extrema importância em tempos de proteção de dados, uma vez que tudo gira em torno da informação. Alertar sobre os perigos constantes e entender como se proteger de eventuais danos e prejuízos é de suma importância para diminuir os crimes virtuais.

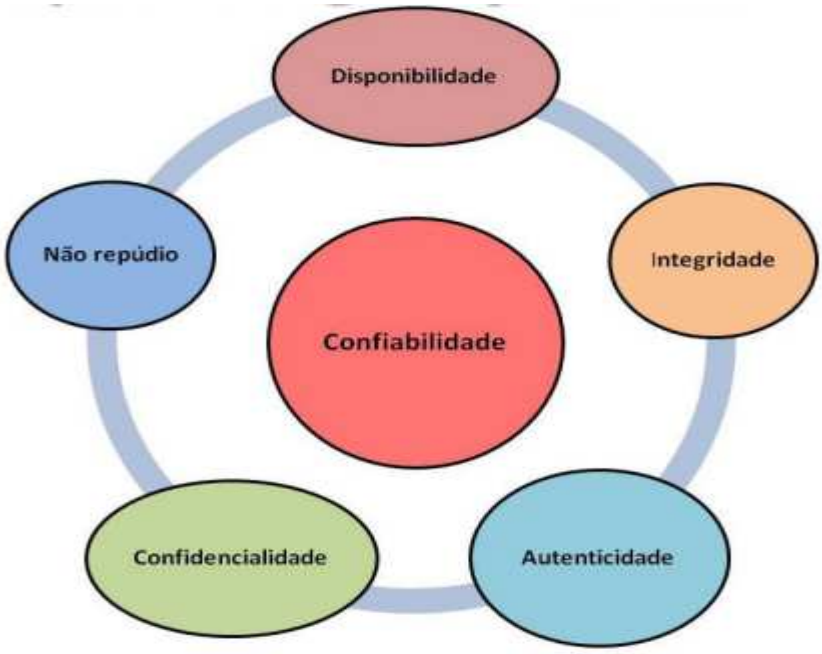
É preciso compreender que a segurança da informação se dá por um contexto maior, que vai além da engenharia de tráfego, dos firewalls e dos softwares de proteção. É importante ter uma visão mais ampla e estratégica do processo de segurança que deve ser integrado as ações de proteção de dados.

Para Ferreira (2003, p.162), a Segurança da Informação:

> Protege a informação de diversos tipos de ataques que surgem no ambiente organizacional, garante a continuidade dos negócios, reduz as perdas e maximiza o retorno dos investimentos e das oportunidades.

A segurança da informação está diretamente ligada a proteção e o objetivo de defender. As informações tem um alto valor para as pessoas e empresas, sendo assim a segurança da informação é montada nos pilares: da confidencialidade, integridade, disponibilidade e autenticidade. Esse conjunto orienta, normatiza e protege a informação, possibilitando que o negócio da empresa seja realizado e a sua missão alcançada. Com isso a política de segurança tem por objetivo definir ações e também princípios fundamentais de como a informação será utilizada (FONTES, 2010).

Figura 2 - Modelo dos Princípios de Segurança da Informação



Fonte: (Bertola, 2013)

Os conceitos de segurança da informação estão normatizados pela NBR ISO/IEC 17799. Campos (2007) observa a confidencialidade como:

> Propriedade que limita o acesso à informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação, onde a informação somente pode ser acessada por pessoas explicitamente autorizadas.

Sobre a Integridade:

> Quando uma informação é indevidamente alterada, intencionalmente ou não, tal como pela falsificação de um documento, da alteração de registros em um banco de dados, ou qualquer coisa que altere a informação original de maneira indevida, configura um incidente de Segurança da Informação por quebra de integridade (CAMPOS, 2007).

A explanação sobre a Disponibilidade informa que:

> Quando a informação não é acessível nem mesmo por quem é de direito, como no caso da perda de documentos, quando há sistemas de computador "fora do ar" ou, ainda, em função de ataques de negação de serviço a servidores de rede ou servidores Web, ou seja, quando esses servidores estão inoperantes em resultado de ataques e invasões, então isto é um incidente de Segurança da Informação por quebra de 18 disponibilidade. Mesmo as "quedas" de sistemas não provocadas, ou seja, não intencionais, configuram quebra de disponibilidade (CAMPOS, 2007).

Se faz necessário uma análise sobre a Autenticidade:

> A autenticidade, consiste na veracidade da fonte das informações. Por meio da autenticação é possível confirmar a identidade da pessoa ou entidade que presta as informações (CAMPOS, 2007).

E com isto Bertola (2013), complementa através da Confiabilidade:

> É demonstrar ao usuário/cliente a fidelidade e a boa qualidade da informação com a qual ele estará trabalhando.

Por fim Ferreira e Araújo (2006), ainda adicionam o seguinte conceito de Segurança da Informação:

> Não repúdio: o usuário que gerou ou alterou a informação (arquivo ou e-mail) não pode negar o fato, pois existem mecanismos que garantem sua autoria.

Para esse universo de segurança da informação os provedores de acesso têm o desafio de apresentar uma conexão rápida e segura para seus clientes. Essa segurança deve ser de ponta a ponta. Para isso, revisão das políticas de segurança, adequação à lei geral de proteção de dados (LGPD) e a utilização de ferramentas de segurança são fundamentais para um bom ambiente.

Os provedores de acesso em quase sua totalidade utilizam sistemas; e esses sistemas em alguma etapa do processo fará o tratamento dos dados pessoais, e caso esse sistema sofra qualquer tipo de falha, de alguma forma as atividades e o trabalho serão afetados e algum prejuízo ocorrerá. Sendo assim, para minimizar as ocorrências de falha e indisponibilidades, é importante que seja utilizado pelos provedores de acesso políticas de segurança que cumpram com os requisitos definidos.

Com esse panorama sobre a área de segurança da informação é possível visualizar as importâncias desse conceito para as características desse trabalho de implantação, sobre uma forte preocupação com os conceitos e da sua importância no ambiente dos provedores de acesso à internet.

2.3 A ISO/IEC 27701 e ISO/IEC 27000

A ISO/IEC 27001 foi lançada no Brasil em dezembro de 2019, tendo um foco para a privacidade da informação. A norma tem uma atenção voltada para uma gestão da privacidade da informação, contribuindo assim para a adequação à lei geral de proteção de dados. Essa norma especifica requisitos e fornece as diretrizes para o estabelecimento do contexto da privacidade dentro das organizações. A norma amplia os requisitos da ISO 27000, levando em consideração a proteção da privacidade dos titulares de dados pessoais (FARIAS JUNIOR, 2019).

A ISO/IEC 27000 vem servindo de apoio às empresas, organizações e entidades de vários setores. Por ser um padrão internacional de segurança, as normas da ISO 27000 se tornam uma das bases na implementação da proteção de dados, pois é uma ferramenta de controle. Quando a empresa utiliza a família ISO 27000, ela passa a contar com um sistema de melhoria contínua, que garante importantes medidas (CABRAL, 2020).

A família ISO 27000 incorpora as atividades de melhoria utilizando os princípios do ciclo PDCA. Permitindo também atender os incidentes e os problemas de segurança que envolve a proteção de dados. Um sistema de gestão que atende a

segurança deve proteger os dados fornecendo um modelo para implementação, operacionalização, monitoração e manutenção.

Figura 3 - Modelo SGSI utilizando o ciclo PDCA

Fonte: (Palma, 2016)

A informação tem que ser preservada com cautela por meio de normas e técnicas de políticas de segurança, do mesmo modo que os fundos monetários e patrimônios (FONTES e ARAÚJO, 2008).

A preservação da informação é indispensável, e a acessibilidade deve ser apenas para pessoas autorizadas que dispõem de tal permissão. Caso a informação seja acessada por um indivíduo não autorizado, sucede a ruptura da confidencialidade, podendo ocasionar falhas imensuráveis para todos os envolvidos (ISO/IEC 27001, 2013).

Vale ressaltar que um dos fundamentos necessários para que os pequenos provedores de acesso à internet alcancem os valores da privacidade e da proteção de dados passa pela utilização das práticas da família ISO 27000. Com isso é necessário o suporte de um padrão, e a Norma ISO 27000 traz parâmetros que

fundamentam com outras normas as necessidades da nova legislação (CABRAL, 2020).

A relação da ISO 27701 com a ISO 27001 surgiu como base na necessidade de criação de uma extensão da ISO 27001, trazendo requisitos e controles específicos para assegurar a privacidade no tratamento de dados pessoais. Ao combinar a ISO 27701 e a ISO 27001, as organizações podem construir uma fundamentação e se preparar para à lei geral de proteção de dados, pois muitos dos elementos da ISO 27701 são mapeados diretamente para aspectos da LGPD.

A Metodologia para a conformidade com o SGPI – Sistema de Gestão da Privacidade da Informação se dá através dos requisitos relacionados na ISO/IEC 27701. Esta metodologia pode ser utilizada por todos aqueles que realizam algum tipo de tratamento de dados. Uma organização que cumpre os requisitos desta metodologia irá gerar evidências documentais de como tratar os dados pessoais. Estas evidências também podem ajudar no relacionamento com outras partes interessadas, inclusive com a autoridade nacional de proteção de dados. Esta metodologia é aplicável a todos os tipos e tamanhos de organizações, incluindo as companhias públicas e privadas, entidades governamentais e organizações sem fins lucrativos (DONÁ, 2020).

A ISO/IEC 27701 contém um mapeamento detalhado e orientações específicas para implementar requisitos e controles requeridos pela LGPD. Focando sempre em segurança da informação e proteção da privacidade (DONÁ, 2020).

Por meio de controles e medidas de prevenção a ISO 27701 poderá ajudar as organizações a tratar com as questões de privacidade, evitando casos de uso indevido dos dados pessoais, através da melhoria contínua. Sendo guiada pelos princípios da: segurança, conscientização e responsabilidade, essas condições são inegociáveis para que a privacidade seja estabelecida de forma consistente com os requisitos apresentados pela legislação de proteção de dados, e ao mesmo tempo, de acordo com um padrão reconhecido internacionalmente (FARIAS JUNIOR, 2019).

2.4 Lei Carolina Dieckmann - Lei nº12.737 de 30 de novembro de 2012

Em 2012, fotos de uma conhecida atriz brasileira nua foram divulgadas na internet, após uma invasão de seu smartphone. O episódio rendeu um alerta debate sobre a exposição de pessoas na internet e resultou na aprovação da Lei nº 12.737, de 30 de novembro de 2012, que acresceu ao código penal a tipificação da conduta de invasão de dispositivo informático. A lei passou a ser conhecida como Lei Carolina Dieckmann.

A invasão adveio da execução de um programa malicioso (malware) recebido no e-mail da vítima, permitindo o acesso dos criminosos em seu dispositivo, que por sua vez efetuaram a cópia dos arquivos contendo fotos íntimas da atriz e posteriormente a extorquiram sob a ameaça de divulgação destes arquivos, fato que acabou se consumando. Não se trata de uma situação isolada, registros são relatados constantemente pelo Brasil e atingem todas as pessoas expondo ao constrangimento. Configurando um problema relevante sobre a proteção e a privacidade.

O sigilo pessoal compreende: sigilo de domicílio, de correspondência, e de dados: pessoais, bancários, fiscais e telefônicos. Por isso o sigilo de dados em geral é relacionado as informações que podem revelar aspectos da privacidade de determinado indivíduo. Os dados aqui mencionados também foram incorporados mais tarde em várias leis. Esses dados são referentes às informações telefônicas, bancárias e fiscais da pessoa, bem como à sua orientação sexual, crença religiosa e ao valor de sua remuneração (BRASIL, 1988).

Neste sentido, a Lei Carolina Dieckmann adicionou ao código penal o artigo 154-A, que determina, conforme Brasil (2012):

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

Desta forma, a Lei nº 12.737, de 30 de novembro de 2012, foi o primeiro passo com objetivo de proteção no tocante a intimidade e a privacidade do usuário no âmbito da rede mundial de computadores, essa lei também contribuiu para os primeiros passos na responsabilidade dos direitos e deveres da sua atuação, no que corresponde sobre a proteção dos dados.

2.5 Marco Civil da Internet - Lei nº12.965 de 23 de abril de 2014.

O marco civil da Internet foi regulamentado em 2014 pelo Decreto-lei nº.12.965, o qual manteve e adicionou diretrizes de privacidade, proteção de dados e liberdade de expressão, em seu art. 5º, inciso I, o marco civil define a internet como "o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para o uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes" (BRASIL, 2014).

De fato, o marco civil da internet se preocupa em abordar diversos direitos, garantias e deveres relativos à rede mundial de computadores, nesse sentido, informa Teixeira (2016, p. 84):

> Preocupado com a possibilidade de eventualmente haver alguma limitação à liberdade de expressão ou alguma violação da privacidade dos usuários da internet, o Marco Civil expressa que a garantia a esses dois direitos constitucionais é condição para o pleno exercício do direito à acesso à rede mundial de computador. Ou seja, a violação a esses direitos implica em quebra da própria finalidade do advento do Marco Civil enquanto uma lei federal que objetiva tutelar os usuários da internet.

Desta forma, o marco civil da internet estabeleceu diversos direitos, demonstrando uma preocupação e a necessidade de proteger os usuários. Sendo um princípio fundamental no uso da internet. É importante que os dados, os registros, a guarda, e a conexão por parte dos provedores de acesso estejam protegidos. Diante disto é preciso que "a garantia do direito à privacidade, a proteção dos dados e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet" (BRASIL, 2014).

A proteção ao sigilo das comunicações privadas no âmbito da internet é imprescindível conforme a legislação, pois garante o direito aos usuários observando-se o dever de indenizar moral ou materialmente, aos danos causados por aquele que viola este direito. Na sequência, nos incisos VII, VIII, IX e X do artigo 7º do marco regulatório reforçam essa ideia (BRASIL, 2014).

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> (...)
>
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
>
> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
>
> a) justifiquem sua coleta;
>
> b) não sejam vedadas pela legislação; e
>
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
>
> IX - Consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
>
> X - Exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;(BRASIL, 2014).

Percebe-se que todos estes incisos em linhas gerais apresentam determinadas ações para os pequenos provedores de acesso à internet, caso algum tratamento de dados seja de responsabilidade dos mesmos. O inciso VII aponta a impossibilidade de fornecimento de dados a terceiros sem consentimento expresso, o VIII cita que há uma necessidade de transparência na relação de tratamento dos dados coletados com os usuários, o inciso IX, por sua vez, trata da exigência de consentimento expresso em cláusula contratual destacada e, por último, o inciso X informa que o usuário que deseje contratar uma outra prestadora poderá requisitar ao antigo provedor que não mantenha seus dados pessoais nos registros.

> Os provedores responsáveis deverão proteger os registros, dados pessoais e as comunicações privadas dos usuários, cuja finalidade é a preservação da intimidade, da privacidade, da honra e da imagem dos usuários, sendo que a divulgação de tais informações se dará apenas através de ordem judicial, ressalvada a possibilidade das autoridades administrativas obterem os dados cadastrais, na forma da lei. (ABDET, 2015, p.10)

O marco civil da internet segue relatando sobre a proteção dos registros de conexão, comunicações e dados dos usuários, ao citar que:

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
>
> § 1o O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.
>
> § 2o O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.
>
> § 3o O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.
>
> § 4o As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais (BRASIL, 2014).

Quanto ao artigo 11, é importante destacar o § 3º, que indica.

> § 3o Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações (BRASIL, 2014).

Através do artigo 13 do Decreto nº. 8.771, de 11 de maio de 2016, o qual, estabelece alguns padrões e deveres por parte dos provedores para a segurança e sigilo dos dados pessoais e comunicações privadas.

> Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança:
>
> I - o estabelecimento de controle estrito sobre o acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários;
>
> II - a previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros;
>
> III - a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014; e
>
> IV - o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes (BRASIL, 2016).

Cabe ao provedor de conexão ou aqueles que possua sistema autônomo como por exemplo as universidades o dever de manter os registros de conexão em ambiente seguro e sob sigilo pelo prazo de 1 ano, sendo que tal responsabilidade não pode ser transferida para terceiros, e existe a possibilidade da autoridade: administrativa, policial ou do Ministério Público requerer a guarda dos registros de conexão por tempo superior.

Ainda sobre o registro de conexão é definido pelo marco civil da internet como: um conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para envio e recebimento de pacote de dados". O marco civil ao instituir a guarda dos registros orientou dois aspectos essenciais são eles: a vedação ao anonimato e a privacidade dos dados dos usuários (TEIXEIRA, 2016).

2.6 GDPR – General Data Protection Regulation

O parlamento europeu e o conselho da união europeia estabeleceram em harmonia as diretivas sobre a defesa do direito e da liberdade das pessoas em relação às atividades de tratamento de dados pessoais e a circulação de dados, fomentando assim o regulamento geral sobre a proteção de dados, com isso, a União Europeia passou a ter uma nova regulação, se tornando referência na matéria de proteção de dados.

Nas considerações iniciais documentadas na GDPR, explica-se que o regulamento deverá promover a equivalência do nível de proteção de dados entre diferentes países membros com fins de garantir um nível de proteção coerente e elevado, bem como a supressão de obstáculos à livre circulação dos dados na União Europeia (GDPR, 2016).

A GDPR passou a exercer o controle regulamentar sobre a proteção de dados nas empresas da União Europeia, como também em todas aquelas empresas que mantém qualquer tipo de relação comercial que envolva dados pessoais dentro do território europeu ou que lhes prestassem serviço (GDPR, 2016).

A GDPR está inserida num mundo em que os dados se tornaram centrais, sendo gerados de forma ultra rápida por usuários e seus vários dispositivos de modo a atrair o interesse não só de companhias privadas como também de entidades governamentais. Com sua legalidade sobre a proteção de dados, a GDPR fundamenta em seu art. 5º o princípio da integridade e confidencialidade, onde implica que os dados devem ser tratados com segurança, estando protegidos de tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental (GDPR, 2016).

A partir desse contexto surge os princípios quando da coleta e tratamento de dados pessoais, merecendo destaque os princípios: da finalidade, dos propósitos, da pertinência, da utilização não abusiva, como no art. 7º decretando o consentimento sobre a necessidade da coleta como parte do contrato; da identidade do responsável

pela coleta e tratamento. No art. 10, para o fim de se ter conhecimento daquele que faz uso das informações pessoais; e da segurança e por fim o art. 17, sobre o cumprimento de especificações mínimas de segurança a serem observadas pelos responsáveis sobre das informações pessoais (GDPR, 2016).

2.7 LGPD – Lei Geral de Proteção de Dados

A LGPD regulamenta o uso, a proteção, o tratamento e a transferência de dados pessoais em território nacional. Antes disso as empresas nunca mencionavam os riscos, malefícios, as perdas e as fragilidades dessa abertura que os meios digitais oferecem. Nesse ambiente digital em que as redes convergem cada vez mais, a LGPD dispõe sobre o tratamento de dados pessoais nos meios digitais, por pessoa física ou jurídica de direito público ou privado, com objetivo de proteger os direitos fundamentais.

Com isso a proteção de dados tem como fundamentos: o respeito à privacidade, a autodeterminação, a liberdade de expressão, de informação, de comunicação, de opinião, a inviolação da intimidade, da honra e da imagem. Neste cenário social digital realmente a *internet* abre as portas do mundo na palma da mão, dando acesso a amplo conhecimento informativo, interação global entre pessoas, facilidades e oportunidades. Por isso a LGPD aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que o tratamento e os dados pessoais objeto do tratamento tenham sido coletados no território nacional (BRASIL, 2018).

Neste cenário da lei geral de proteção de dados cabe ressaltar a importância dos atores para o funcionamento da proteção de dados: O titular dos dados - é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento; O controlador dos dados - definido como pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; O operador dos dados - é uma pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Ele processa e gerencia as informações de acordo com as regras

estabelecidas pelo controlado; ANPD - é o órgão da administração pública federal responsável por zelar, implementar e fiscalizar o cumprimento da LGPD no Brasil. Para exercer este importante papel, a autoridade possui autonomia técnica e decisória assegurada por lei.

O acesso à internet pode acarretar abusos e invasões de direitos fundamentais do usuário tais como: intimidade, privacidade e liberdade, violando seus direitos em favor do interesse das instituições, mas em seu artigo 6º a LGPD deixa claro que as atividades de tratamento dos dados pessoais deverão observar a boa-fé e os seguintes princípios: da finalidade, adequação, necessidade, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização.

O primeiro passo para o tratamento dos dados pessoais passa mediante o consentimento pelo titular, e o cumprimento das obrigações legais para situações de políticas públicas, para a proteção da vida e tutela da saúde, sendo esse consentimento fornecido por escrito ou por outro meio que demonstre a manifestação do titular. Vale ressaltar que em seu artigo 9º a LGPD o titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara e adequada, entre outras características previstas em regulamentação sobre a forma de lei (BRASIL, 2018).

O controlador somente poderá realizar o tratamento de dados pessoais para finalidades legítimas consideradas a partir de situações concretas que incluem: apoio e promoção de atividades do controlador, a proteção em relação ao titular e prestação de serviços que o beneficiem, respeitadas as legítimas expectativas e os direitos e liberdades fundamentais. Vale ressaltar que para os casos do tratamento de dados sensíveis somente poderá ocorrer nas seguintes hipóteses: em cumprimento de obrigação legal e regulatória, no compartilhamento para a administração pública, para estudos por órgão de pesquisa desde que seja garantido o anonimato dos dados, exercício do direito, proteção da vida e a garantia de prevenção à fraude e a segurança do titular (BRASIL, 2018).

Ainda sobre o tratamento de dados a LGPD faz uma observação para o caso de dados de crianças e adolescentes onde deverá ser realizado com o consentimento específico dado pelos país ou responsável legal, onde os controladores deverão manter pública a informação sobre os itens coletados e assim divulgar informações simples, clara e acessível a fim de proporcionar a informação necessária e adequada.

Conforme mencionado em outros momentos a LGPD aborda todo o ciclo de vida dos dados, e nos seus artigos 15 e 16 a legislação relata que o término do tratamento dos dados se apresenta ao ser detectado o fim do período do tratamento, após verificada a finalidade, por comunicado por parte do titular e por determinação da autoridade nacional de proteção de dados (BRASIL, 2018).

No que tange aos direitos dos titulares dos dados, é permito ao titular a qualquer momento obter do controlador: a confirmação da existência do tratamento, acesso aos dados, correção dos dados, anonimização, bloqueio, eliminação e revogação. Ainda sobre os direitos dos titulares os artigos 19 e 20 informam que: a verificação de existência e acesso aos dados poderá ser obtida através de requisição em formato simples, por meio de declaração seja eletrônica ou sob forma impressa. Com isso conforme mencionado acima o titular tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (BRASIL, 2018).

Um outro ponto descrito na LGPD é sobre a transferência internacional de dados no qual o artigo 33 esclarece que a transferência internacional somente é permitida para os casos: de países ou organismos internacionais que proporcionem grau de proteção dos dados; para outro controlador quando o mesmo oferece e comprova garantias de cumprimentos, para o caso de cooperação jurídica internacional entre órgãos, para a proteção da vida, quando autorizado pela autoridade nacional de proteção e dados, cooperação internacional, para necessidade de políticas públicas e quando o titular fornecer o consentimento (BRASIL, 2018).

Num outro momento da lei geral de proteção de dados o controlador e o operador devem manter registro das operações de tratamento, e a autoridade nacional de proteção poderá determinar ao controlador que elabore relatório de impacto à proteção incluído os dados sensíveis, no caso do operador o mesmo deverá realizar o tratamento segundo as instruções fornecidas pelo controlador.

Seguindo as orientações da LGPD o controlador deverá indicar o encarregado pelo tratamento dos dados pessoais, assim o encarregado deverá: aceitar as reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências, receber os comunicados da autoridade nacional de proteção de dados, orientar os funcionários e os contratados sobre as práticas de proteção de dados e executar demais ações (BRASIL, 2018).

Da seção de responsabilidades e do ressarcimento de danos segundo a LGPD cabe ao controlador e/ou ao operador realizar a reparação em razão de danos causados pela falha ao realizar o tratamento de dados, descumprimento da legislação e a realização de ações ilícitas. Os agentes de tratamento só não serão responsabilizados quando: de fato não estiverem realizando o tratamento dos dados que lhe foram atribuídos ou quando o dano é decorrente de culpa exclusiva do próprio titular.

Em relação a segurança e ao sigilo dos dados os agentes de tratamento devem adotar medidas de segurança e técnicas 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.

A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável os fatores de segurança e de sigilo. Ainda sobre tal questão os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta lei em relação aos dados pessoais, mesmo após o seu término do tratamento. Em seu artº 48 a LGPD ainda reafirma que o controlador deverá comunicar à autoridade nacional

e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares (BRASIL, 2018).

No que se refere as boas práticas e da governança a LGPD afirma em seu art. 50 que os controladores e operadores no âmbito das suas competências, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, regime de funcionamento, procedimentos, incluindo normas de segurança, padrões técnicos, obrigações específicas para os diversos tratamento, ações educativas, mecanismos supervisão e de mitigação de riscos entre outros aspectos relacionados.

Das penalidades e sanções administrativas a LGPD comunica aos agentes de tratamento de dados que em caso de detectada a infração serão aplicadas pela autoridade nacional às seguintes sanções administrativas aplicáveis: Advertência com indicação de prazo para adoção de medidas corretivas; multa simples de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil, limitada no total de R$ 50.000.000,00 (cinquenta milhões de reais) por infração; multa diária, observado o limite total; publicação da infração após devidamente apurada e confirmada a sua ocorrência; bloqueio dos dados pessoais a que se refere a infração até a sua regularização; eliminação dos dados pessoais a que se refere a infração (BRASIL, 2018).

A suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados (BRASIL, 2018).

A autoridade nacional definirá por meio de regulamentação estabelecer as sanções administrativas e infrações, que deverá ser objeto de consulta pública, e as metodologias que orientarão o cálculo do valor-base das sanções de multa. O valor da sanção de multa diária aplicável às infrações a esta lei deve observar a gravidade

da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional.

Sobre a autoridade nacional de proteção de dados (ANPD) a mesma foi criada, sendo um órgão da administração pública federal, integrante da presidência da república, onde é assegurada autonomia técnica e decisória à ANPD, sendo sua composição formada por: conselho diretor, conselho nacional de proteção de dados pessoais e da privacidade, corregedoria, ouvidoria, órgão de assessoramento jurídico, unidade administrativas e unidades especializadas.

Compete à ANPD: zelar pela proteção de dados pessoais, zelar pela observância dos segredos comercial e industrial observada a proteção de dados pessoais e do sigilo das informações, elaborar diretrizes para a política nacional de proteção de dados pessoais e da privacidade, fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, apreciar petições de titular contra controlador após comprovada pelo titular a não solução no prazo estabelecido, promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade, estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais (BRASIL, 2018).

Promover ainda ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional, dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial; solicitar a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta lei, elaborar relatórios de gestão anuais acerca de suas atividades (BRASIL, 2018).

Além de editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados

pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta lei, ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento, arrecadar e aplicar suas receitas e publicar, realizar o detalhamento dos recursos, realizar auditorias, ou determinar sua realização (BRASIL, 2018).

No âmbito da atividade de fiscalização, celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, comunicar às autoridades competentes as infrações penais das quais tiver conhecimento, comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal, implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta lei (BRASIL, 2018).

2.8 A Importância do Pequeno Provedor na Proteção de Dados

Quando um pequeno provedor de acesso à internet disponibiliza um serviço para a sociedade, sua atuação consiste em transmitir e receber dados por uma rede de comunicação. O pequeno provedor é um agente mediador na prestação de serviços de conexão, onde a sua estrutura é baseada em serviços relacionados ao funcionamento da internet, também definido como sendo: aquele que disponibiliza ao usuário um serviço de natureza tecnológica.

Através desse entendimento a legislação brasileira através do art. 9 do marco civil da internet informa que os provedores de acesso, provedores de trânsito ou quaisquer provedores de conexão têm o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distorção e distinção do conteúdo, origem e destino, serviço, terminal ou aplicação, ressalvando os casos em que pode haver necessidade técnica para que pequenos provedores possam melhor gerir as suas redes, e assim cumprir os níveis de qualidade de serviço contratuais exigidos. Essas práticas podem incluir a

priorização de aplicações mais sensíveis à latência e o bloqueio de aplicações que ofereçam ameaças à segurança da rede.

Por isso a melhoria constante na infraestrutura da rede dos pequenos provedores, é uma ação necessária para a manutenção dos princípios da proteção e privacidade dos dados, evitando qualquer necessidade de intervenção como consequência a discriminação de tráfego por parte dos pequenos provedores de acesso. Assim quanto melhor a infraestrutura do pequeno provedor menor será a necessidade de interferência tecnológica sobre os dados.

Além do uso de dados coletados para cadastro e demais ações, os provedores no Brasil são requisitados a armazenar os registros de acesso de seus clientes por um período de um ano, ou por maior período conforme solicitação das autoridades policiais, administrativas ou do Ministério Público, essa comunicação é realizada mediante ordem judicial onde o pequeno provedor deve fornecer informações de acesso do usuário que estava cometendo um suposto delito digital, mediante esses dados é possível a identificação e a localização do suspeito. Diante dessas analises, Jesus e Milagre (2016, p. 192) dispõe que:

> Com base nos dados fornecidos pelos provedores ou responsáveis pelos ativos de TI, pode a autoridade requerer uma busca e apreensão na sede ou domicilio do suposto autor do delito, para que as máquinas sejam coletadas adequadamente para a realização de perícia técnica (para a apreensão de instrumentos utilizados na prática de crime ou destinados a fim delituoso).

É importante ao pequeno provedor manter sua infraestrutura em bom funcionamento e segurança, tais informações como: dados pessoais, endereço, informações de pagamento, informação de fatura e etc; são dados que podem implicar em riscos a privacidade e a proteção, por isso a devida atenção é necessária.

Portanto o pequeno provedor de acesso tem a importância de proteger os dados dentro do seu domínio de rede, e oferecer disponibilidade e integridade, acompanhando de forma eficiente o funcionamento da rede, mas não possuindo diretrizes para verificar os conteúdos que tramitam pela rede. (COLAÇO, 2015, p.8).

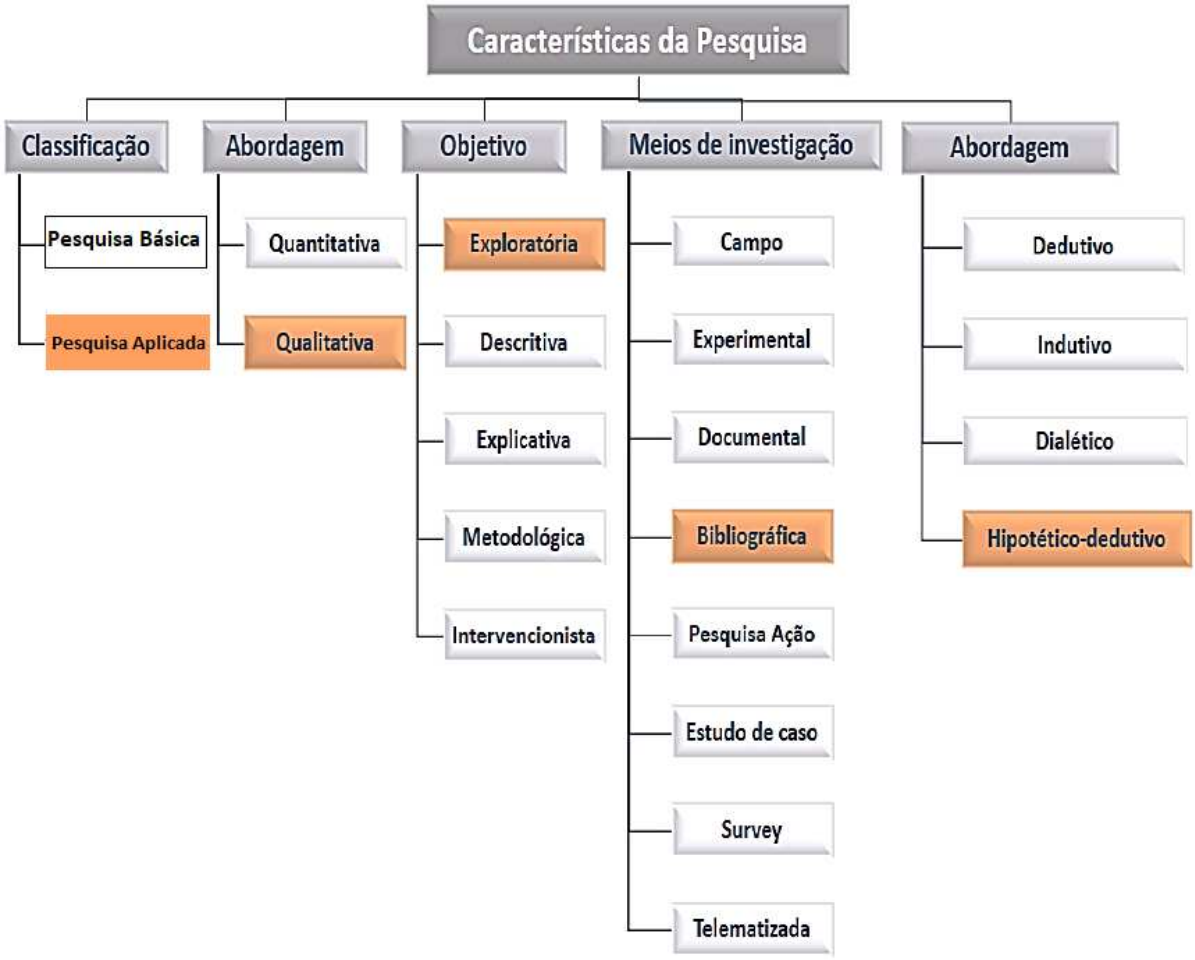
3 METODOLOGIA

3.1 Características da Pesquisa

De acordo Gerhardte e Silveira (2009, pg. 31), no que se refere a pesquisa os autores entendem que: "[...] não se preocupa com representatividade numérica, mas, sim, com o aprofundamento da compreensão de um grupo social, de uma organização, etc". Segundo os autores, ao se utilizar a metodologia qualitativa, o pesquisador terá duas ações de sujeito e objeto da sua pesquisa. Para os autores o objetivo da produção é fabricar informações aprofundadas e ilustrativas, sendo importante que nessa interação ela fomente novas informações.

Com o perfil de classificação aplicada, essa pesquisa concentra-se em torno do problema presente nas atividades das instituições, organizações, grupos ou atores sociais, onde a mesma está empenhada na elaboração de diagnósticos, identificação de problemas e busca de soluções, respondendo assim a uma demanda formulada por “clientes, atores sociais ou instituições”. (THIOLLENY, 2009, p. 36).

Figura 4 - Características da Pesquisa



Fonte: (LIRA, 2018).

Conforme Minayo (1994, p. 21), a pesquisa percebida como qualitativa "[...] trabalha com o universo de significados, motivos, aspirações, crenças, valores e atitudes, o que corresponde a um espaço mais profundo das relações, dos processos e dos fenômenos que não podem ser reduzidos à operacionalização de variáveis". Em razão disso, verifica-se essa pesquisa como abordagem qualitativa, conforme necessita a lei geral de proteção de dados, no que tange a adequação dos pequenos provedores de acesso à internet.

Numa outra questão, quanto ao nível de profundeza, verifica a pesquisa exploratória, em que um dos objetivos é diretamente proporcionar uma maior familiaridade com o tema. É necessário "desencadear um processo de investigação que identifique a natureza do fenômeno e aponte as características essenciais das variáveis que se quer estudar" (KÖCHE, 1997, p. 126).

Como ferramenta de inspeção, foi acionada a verificação bibliográfica para a localização de conteúdos sobre o assunto. Silva (2001), argumenta que a base está na análise da literatura já publicada em forma de livros, revistas, publicações avulsas, imprensa escrita e até eletronicamente, disponibilizada na *internet*.

Para o colhimento e abastecimento das informações sobre o tema, utilizou-se o parâmetro do fichamento. Este método tem como base a análise sobre diversas literaturas que referenciam o tema central. Após estas análises, as questões mais relevantes para a pesquisa, servirão como base para a proposta utilizada.

Tipos de fontes utilizadas:

> "Podem ser elaborados diversos tipos de fichas, como: bibliográfica: com dados gerais sobre a obra lida; citações: com a reprodução literal entre aspas e a indicação da página da parte dos textos lidos de interesse específico para a redação dos tópicos e itens da revisão; resumo: com um resumo indicativo do conteúdo do texto; esboço: apresentando as principais ideias do autor lido de forma esquematizada com a indicação da página do documento lido; comentário ou analítica: com a interpretação e a crítica pessoal do pesquisador com referência às ideias expressas pelo autor do texto lido. O Fichamento irá permitir: identificação das obras lidas, análise de seu conteúdo, anotações de citações, elaboração de críticas e localização das informações lidas que foram consideradas importantes" (SILVA, 2001, p. 42).

Este trabalho tem como objetivo geral, analisar e aprofundar quais os procedimentos, funções e proposições que melhor desenvolve uma proposta de guia para a implantação de um plano de adequação à lei geral de proteção de dados. Ao analisar legislações, metodologias de gestão e técnicas de segurança, foram abordadas 05 teses sobre os processos relacionados as ações de implantação, onde foi proposto um guia com etapas e procedimentos contextualizados para a implantação da LGPD, baseada nas melhores referencias acadêmica e de mercado.

3.2 Estruturação da pesquisa

Para Minayo (2002), o planejamento após a definição do tema não se apresenta de forma linear, sequencial, nem são estanques. Algumas vezes são concomitantes, outras, interpostas. Sendo importante uma estruturação desse planejamento, no qual muitas vezes é necessária uma ordem lógica para melhorar questões tais como os instrumentos, recursos e o tempo de pesquisa. Abaixo segue as ações elaboradas a fim de atender os propósitos deste trabalho:

A ação 1 tem por objetivo delinear o problema da pesquisa, ficando estabelecida a definição do problema a ser trabalhado, e a delimitação do escopo dentro do tema pretendido.

Na ação 2 através do *Snowballing* é iniciada uma busca por material onde o objetivo principal foi identificar os livros, teses e demais que estivessem em entendimento com o tema de uma maneira visível e detectada nos resumos dos trabalhos.

A ação 3 atua na revisão de literatura, com a coleta e análise dos conteúdos amplo das literaturas, constatando livros, metodologias e melhores práticas que poderiam ser utilizadas neste trabalho. Além disso, foi revisado materiais relacionados em: artigos publicados em revistas da área, blogs e sites especializados.

Na ação 4 em cima dos materiais revisados foi definido o escopo, a delimitação e definido os processos e funções que serão entregues como estrutura principal deste trabalho.

Com a ação 5 foi escolhido os modelos de implantação da lei geral de proteção de dados.

Na ação 6 foi avaliado os modelos selecionados de implantação da lei geral de proteção de dados, no qual a partir desses exemplares mais similares ao guia de

implantação para os pequenos provedores, foram analisadas e comparadas as literaturas e as teses citadas neste trabalho.

Na ação 7 foi definida as etapas para o guia de implantação, com objetivo de categorizar cronologicamente, as proposições e os procedimentos elaborados durante a construção do guia definindo a implantação que será entregue.

Por fim a ação 8 com a proposta do guia para implantação da lei geral de proteção de dados para os pequenos provedores de acesso à internet, na qual esta atividade se propõe a desenvolver como objeto principal deste trabalho.

Assim apesar de divulgada a proposta, não serão produzidos insumos necessários para a coleta de métricas e números, logo sua implantação não estará por completo nesta exposição.

3.3 Instrumentos de Pesquisa

3.3.1 Base dos instrumentos de Pesquisa

Dada a atualidade do presente tema onde o mesmo está em grande destaque nacional, como também as poucas produções literárias de adequação à proteção de dados, foram fatores determinantes para este trabalho que tem como principal objetivo contribuir neste processo de implantação. O levantamento inicial foi realizado através das legislações vigentes no Brasil e no exterior, num momento posterior foi realizada buscas em outras vertentes com o seguinte perfil: nas línguas inglesa e portuguesa, onde as alusões foram feitas em cima da proposta ou processo de implantação da lei geral de proteção de dados num ambiente de provedores.

Para coletar os artigos e teses, foram utilizados: o Google Acadêmico, o repositório da UFPE, o repositório da UFRGS, o repositório da UFMG, o repositório do CAPES e o repositório da UFRJ. Após as pesquisas iniciais através das *strings* de buscas, que podem ser vistas no quadro 1, foram pré-selecionados 22 trabalhos, e dentre estes, após uma análise mais criteriosa de proximidade como o tema central e

com as premissas definidas, foram escolhidos 5 trabalhos que possibilitaram inclusão e a construção de natureza corrente.

Quadro 1 - *Snowballing* e levantamento inicial

Observação	LINK	TÍTULO	AUTORES	FONTE	ANO	DOI/PUBLICAÇÃO
	https://scholar.google.com.br/scholar?hl=pt-BR&as_sdt=0%2C5&q=EMPRESAS+E+IMPLEMENTA%C3%87%C3%83O+DA+LGPD+-+Lei+Geral+de+Porte%C3%A7%C3%A3o+de+Dados&btnG=	Manual De Implementação Da Lei Geral De Proteção de Dados	Luciano Vasconcelos Leite - Christian De Lamboy - Marcelo Lapolla	Google Acadêmico	2019	https://scholar.google.com.br/scholar?hl=pt-BR&as_sdt=0%2C5&q=EMPRESAS+E+IMPLEMENTA%C3%87%C3%83O+DA+LGPD+-+Lei+Geral+de+Porte%C3%A7%C3%A3o+de+Dados&btnG=
Citado por 3 trabalhos (Goolge Acadêmico). Pesquisa em 10/11/2020	https://civilistica.emnuvens.com.br/redc/article/view/510	Tratamento de dados pessoais na LGPD: estudo sobre as bases legais	Chiara Spadaccini de Teffé - Mario Viola	Google Acadêmico	2020	https://civilistica.emnuvens.com.br/redc/article/view/510/384
Citado por 2 trabalhos (Goolge Acadêmico). Pesquisa em 15/11/2020	https://scholar.google.com.br/scholar?hl=pt-BR&as_sdt=0%2C5&q=IMPLANTA%C3%87%C3%83O+SEGURAN%C3%87A+DA+INFORMA%C3%87%C3%83O+LGPD&btnG=	Lei Geral de Proteção de Dados (LGPD): Guia de Implantação	Lara Rocha Garcia - Edson Aguilera Fernandes - Rafael Augusto Moreno Gonçalves - Marcos Ribeiro Pereira Barreto	Google Acadêmico	2020	https://books.google.com.br/books?hl=pt-BR&lr=&id=lS3sDwAAQBAJ&oi=fnd&pg=PA3&dq=IMPLANTA%C3%87%C3%83O+SEGURAN%C3%87A+DA+INFORMA%C3%87%C3%83O+LGPD&ots=WkQmpLVLSw&sig=4Qn97DSFDTuTCHEk2H_NNIlh0ww#v=onepage&q&f=false
	https://repositorio.ufpe.br/handle/123456789/3997	Responsabilidade do provedor pelos danos praticados na Internet.	Fernando Antônio de Vasconcelos	Google Acadêmico	2002	https://repositorio.ufpe.br/bitstream/123456789/3997/1/arquivo5663_1.pdf
	https://www.editorajuspodivm.com.br/cdn/arquivos/7c1ab637b2d1136fc1067a3992899546.pdf	EMPRESAS E IMPLEMENTAÇÃO DA LGPD - Lei Geral de Proteção de Dados	André Pedrosa Kasemirski - Rodolfo Ignácio Aliceda - Tarcisio Teixeira	Google Acadêmico	2020	https://www.editorajuspodivm.com.br/empresas-e-a-implementacao-da-lei-geral-de-protecao-de-dados-2021

Fonte: Adaptado Lira (2018).

A pesquisa transita pela importância dos trabalhos e autores escolhidos acima, no que diz respeito a legislação, gestão e segurança da informação, essas literaturas norteiam a didática sobre: a privacidade, a proteção de dados e a responsabilidade dos provedores. A apresentação dos resultados tem como parâmetro os trabalhos elaborados pelos autores, a proteção de dados dentro do ambiente dos pequenos provedores e os questionamentos atualizados sobre a proteção de dados.

4 PROSPOSTA DE IMPLANTAÇÃO DA LGPD AO PEQUENO PROVEDOR

4.1 Introdução

Ao longo desses últimos quatro anos, principalmente desde agosto de 2018, onde ocorreu a promulgação da lei geral de proteção de dados, iniciou-se uma verdadeira corrida das empresas de vários setores da economia para a implantação da LGPD, essa procura está gerando um impacto na busca por literatura, profissionais, materiais, ferramentas e outros recursos que são necessários à sua implantação e para os pequenos provedores de acesso à internet não poderiam ser diferentes.

Pautado sempre pelo recurso da literatura foi levantado monografias, artigos, teses, livros e outras fontes que apresentassem temas e características relevantes ao assunto deste trabalho, onde foi possível verificar uma crescente produção a partir de 2018, tendo relação com a entrada em vigor da lei geral de proteção de dados, sobre esses temas nota-se uma capilaridade, quase que exclusivamente em produções na língua portuguesa, se tornando cada vez mais popular no meio acadêmico. A figura abaixo representa o selecionamento dos trabalhos coletados, e que foram separados por temas e áreas do conhecimento, onde foram escolhidos os que apresentam maior proximidade, sendo importante para a fundamentação desse guia de implantação.

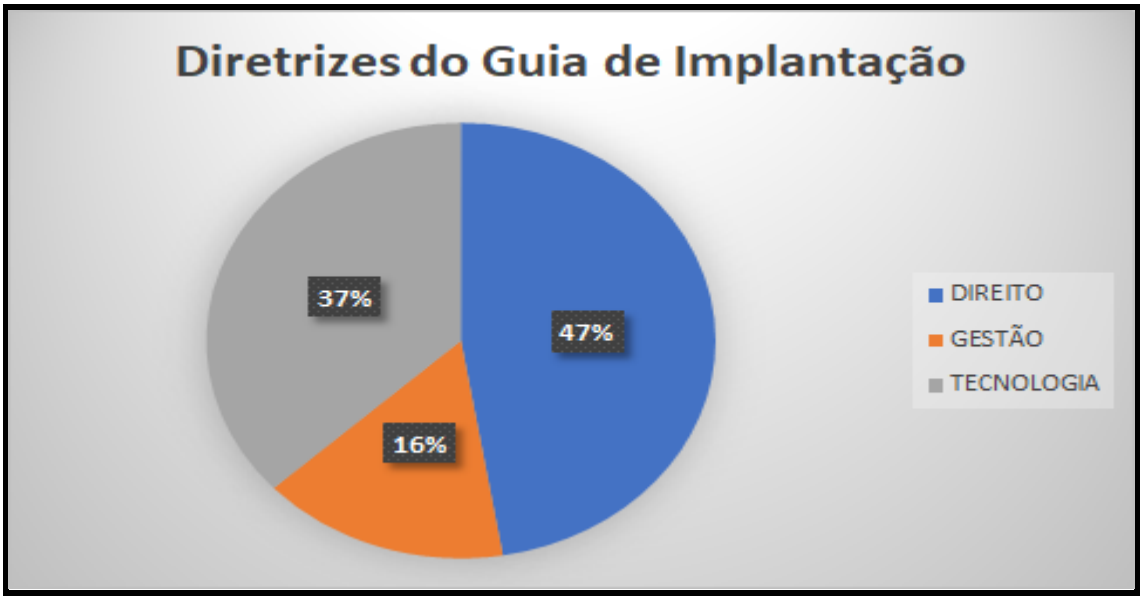
Figura 5 - Levantamento de pesquisa

LGPD/TRABALHOS	DIRETRIZES DO GUIA DE IMPLANTAÇÃO			TOTAL POR ASSUNTO
	DIREITO	GESTÃO	TECNOLOGIA	
RESPONSABILIDADE DOS PROVEDORES	3	0	0	3
ESTUDO DA LEGISLAÇÃO	1	2	0	3
IMPLEMENTAÇÃO/IMPLANTAÇÃO	3	1	0	4
SEGURANÇA E SISTEMA DA INFORMAÇÃO	0	0	4	4
REDE/NEUTRALIDADE/PRIVACIDADE	2	0	3	5
TRATAMENTO DOS DADOS/PROTEÇÃO DE DADOS	3	0	0	3
TOTAL DE TRABALHOS POR ÁREA DO CONHECIMENTO	12	3	7	
TOTAL	22			

Fonte: O Autor (2021).

Através da figura 6 pode-se identificar que o guia de implantação da lei geral de proteção de dados para os pequenos provedores de acesso à internet, sofre uma influência distribuída por áreas do conhecimento.

Figura 6 - Percentual das diretrizes do Guia de Implantação



Fonte: O Autor (2021).

Baseado nos registros encontrados, foram obtidos dois resultados de relevância referente ao objetivo central do trabalho que é um guia de implantação. Dentre os que mais se destacam tem-se a produção bibliográfica do (GARCIA, LARA ROCHA, 2020) com o título: Lei Geral de Proteção de Dados (LGPD): Guia de Implantação, no ano de 2020 no qual propõe uma implantação de um guia definido através de um framework e com os processos ajustados, e que apresenta um alinhamento com o tema deste projeto. Um outro trabalho importante foi o produzido por: Leite, Luciano Vasconcelos; De Lamboy, Christian; Lapolla, Marcelo (2019) que aborda o tema: Manual de Implementação da Lei Geral de Proteção de Dados, que também contribuiu com vários esclarecimentos para este trabalho. O trabalho de Teixeira (2020) com o título: Empresas e Implementação da LGPD – Lei Geral de Proteção de Dados, publicado em 2020 também constituiu como um ponto de encabeçamento para este trabalho, além das outras obras, sites e blogs que referenciam o tema.

4.2 Guia de Implantação da LGPD para os pequenos provedores

A apresentação do guia que ocorrerá dentro da sequência do trabalho, onde a mesma está alinhada com as melhores práticas da gestão de segurança da informação ISO 27001 e 27701, que tiveram suas exibições no tópico 2.3 deste trabalho. Como também as legislações pertinentes à proteção de dados: Lei Carolina

Dieckmann, Marco Civil da Internet, GDPR e principalmente a LGPD; além de um conceito tecnológico através da internet e da segurança da informação. Com isso serão detalhadas várias ações necessárias para que um pequeno provedor de acesso à internet implante a lei geral de proteção de dados, com os procedimentos e ações de acordo com o conjunto de conceitos supracitados. O ciclo de implantação proposto para o guia, é baseado no ciclo do PDCA, sendo um método interativo de gestão de quatro passos, utilizado para o controle e melhoria contínua de processos.

Figura 7 - Diagrama de Implantação

Fonte: O autor (2021).

4.3 Componentes do Plano em Etapas

A seguir, no quadro 2, está o plano desenvolvido com os 14 procedimentos e ações que compõem a proposta do guia de implantação da lei geral de proteção de dados aos pequenos provedores. Estas ações são provenientes dos estudos realizados e foram criadas em alinhamento com os sistemas de gestão de segurança da informação, ISO 27001, ISO 27701, as legislações vigentes: lei Carolina Dieckmann, Marco Civil da Internet, GDPR e a Lei Geral de Proteção de Dados e também uma abordagem tecnológica através da internet e da segurança da informação.

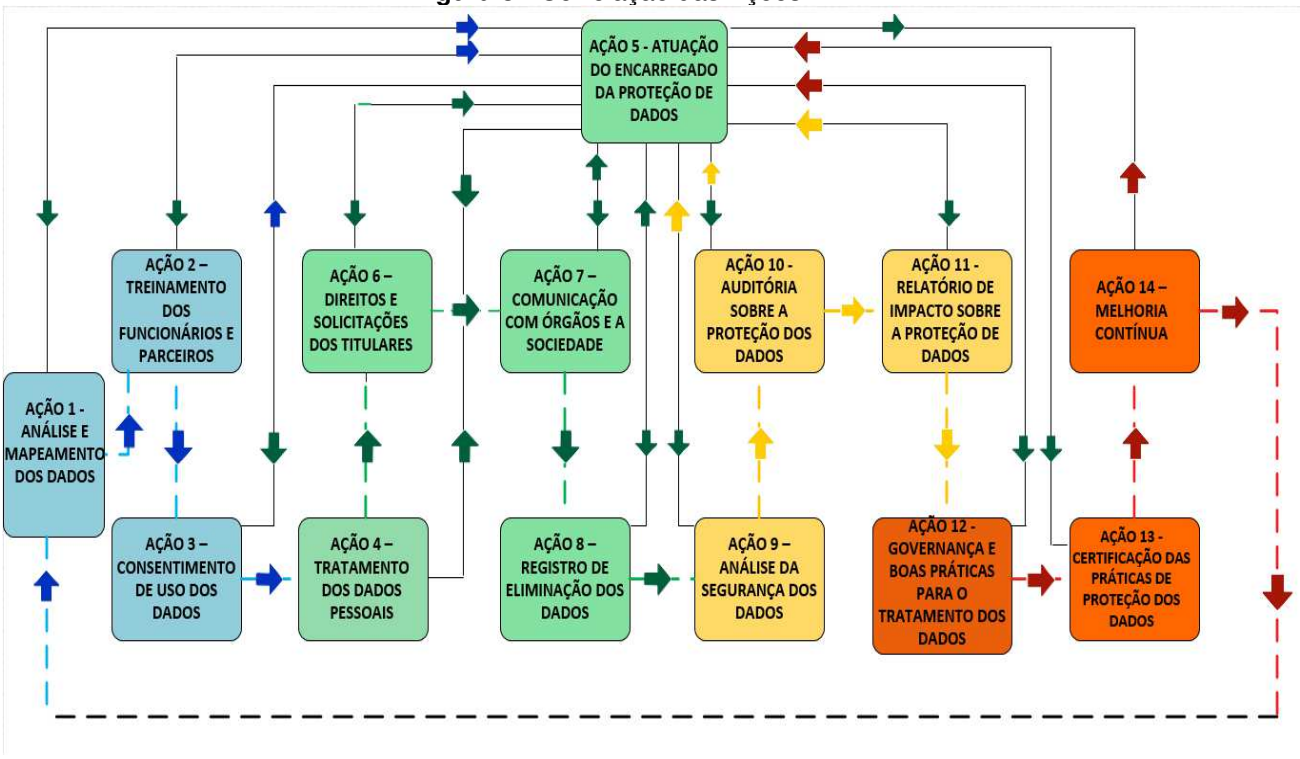
Quadro 2 - Plano de Ação Proposto.

AÇÃO	PROCESSO	RESULTADO	FASE
1	Análise e Mapeamneto dos Dados	Verificar a atual estrutura e procedimentos, como também percorrer todo o fluxo de dados e assim elaborar um estudo com adequações.	PLANEJAMENTO
2	Treinamento dos Funcionários e Parceiros	Condicionar todos os envolvidos com a proteção dos dados, para obter conhecimento sobre a LGPD.	
3	Consentimento de Uso dos Dados	Elaborar um modelo de autorização para o tratamento dos dados.	
4	Tratamento dos Dados Pessoais	Realizar atividades de manipulação dos dados.	EXECUÇÃO
5	Atuação do Encarregado da Proteção de Dados	Realizar atividades para estabelecer a proteção dos dados.	
6	Direitos e Solicitações dos Titulares	Compreender e Atender as solicitações dos titulares.	
7	Comunicação com Órgãos e a Sociedade	Criar uma comunicação de forma objetiva com os orgãos de proteção dos dados e a sociedade.	
8	Registro de Eliminação dos Dados	Realizar ação de exclusão de todos os dados quando solicitado pelo titular.	
9	Análise da Segurança dos Dados	Verificar e propor melhorias de segurnaça para proteção dos dados.	CHECAGEM
10	Auditória sobre a Proteção de Dados	Averiguação dos processos que envolve a proteção dos dados, para identificar a ausência ou não das conformidades.	
11	Relatório de Impacto sobre a Proteção de Dados	Produzir informações sobre o processo de proteção dos dados, informando possíveis ponto de correção.	
12	Governança e Boas Práticas para o Tratamento dos Dados	Administrar com as melhores práticas as ações de proteção dos dados.	AÇÃO
13	Certificação das Práticas de Proteção de Dados	Buscar o reconhecimento das boas práticas relacionadas a LGPD.	
14	Melhoria Contínua	Atualizar processos e tornar o ambiente de dados mais adequação à proteção.	

Fonte: O Autor (2021)

Na figura 7 abaixo, são apresentadas as correlações das ações com o plano de ação do quadro 2, a fim de definir em que esfera do ciclo PDCA está a respectiva ação da implementação.

Figura 8 - Correlação das Ações



Fonte: O Autor (2021).

5 PROCEDIMENTOS E AÇÕES

Ação 01 – Analise e Mapeamento dos Dados

A primeira ação deste guia consiste em realizar uma verificação de como se encontra a real situação da proteção dos dados dentro do ambiente do pequeno provedor de acesso, caberá ao pequeno provedor e ao encarregado de proteção de dados realizar um estudo que deverá verificar o funcionamento desde a coleta dos dados até a exclusão.

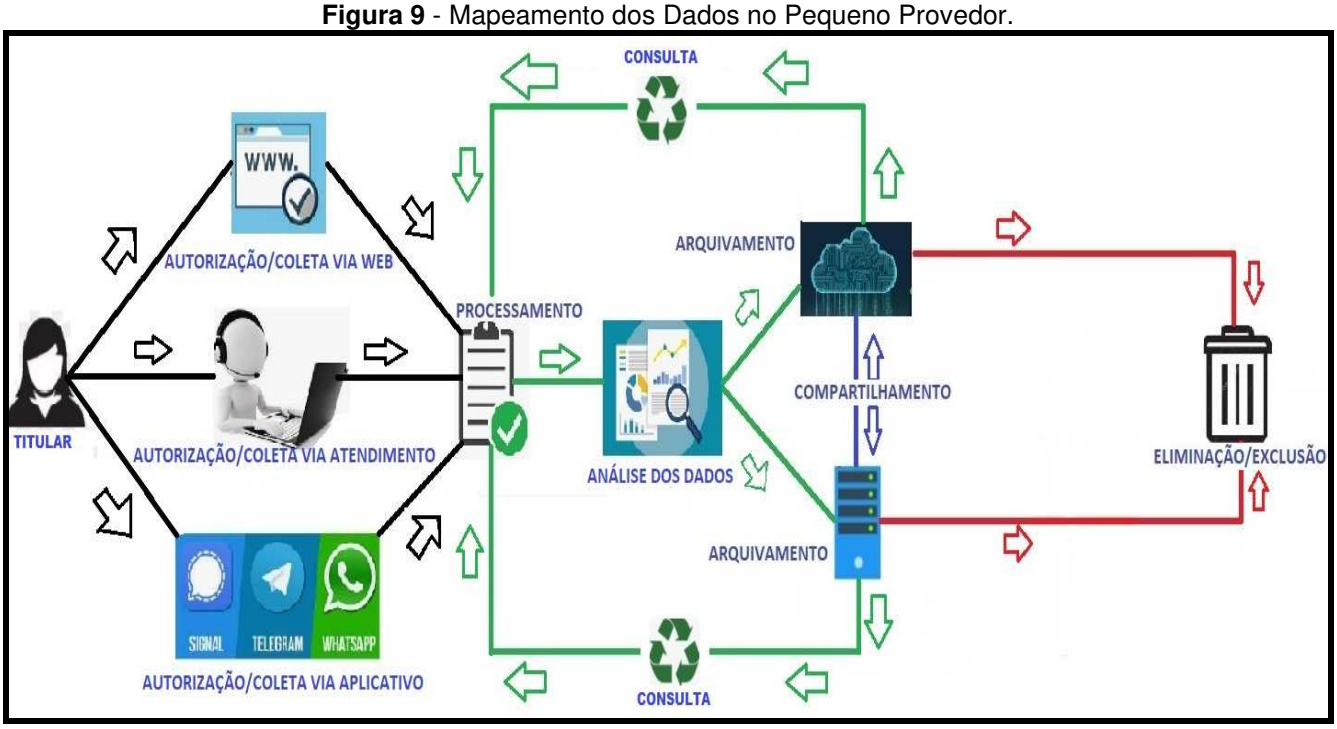
As não conformidades que forem encontradas deverão ser estruturadas em um documento que registrará o ambiente do pequeno provedor reunindo todas as informações possíveis sobre os processos utilizados atualmente.

Para análise inicial é preciso obter as seguintes informações sobre os dados dos titulares e os processos utilizados tais como: Quais são os dados utilizados, os tipos de dados coletados, qual é a finalidade do tratamento desses dados; o que é feito com os dados após o término de seu tratamento; onde estão armazenados os

dados, como foram coletados os dados, qual o fluxo dos dados, como é o acesso aos dados, quem os coleta, onde são guardados, como serão eliminados, como é feito o compartilhamento dos dados a terceiros, como está a base legal dos contratos existentes dos pequenos provedores, como estão as interações dos processos de TI com outras áreas do pequeno provedor, verificar a maturidade dos processos, observar os controles de acessos e os processos de desenvolvimento, Identificar os pontos fracos, verificar as medidas de segurança na proteção de dados pessoais, verificar o modo de contrato realizado com as empresas parceiras e terceiras.

Essas informações obtidas após análise são importantes para o registro e para atender as futuras necessidades como também na produção do mapeamento dos dados dentro do pequeno provedor. Após verificação de todos os caminhos percorrido pelos dados será possível elaborar o mapeamento conforme modelo abaixo, onde inicialmente o titular dos dados faz um primeiro contato com o pequeno provedor para registro dos dados, esses dados podem ser coletados através de vários meios como: web, atendimento via telefone e aplicativo de comunicação. Feita a coleta os dados serão processados/cadastrados no sistema do pequeno provedor que em seguida dará a devida analise/tratamento aos dados conforme necessidade do pequeno provedor e em acordo com a LGPD, durante a vigência do tratamento poderá ocorrer o compartilhamento visando ações de desempenho, segurança e backup. Os dados ainda podem consultados normalmente pelo pequeno provedor/controlador pelo período vigente de tratamento, e ao final serem excluídos conforme orientações da LGPD.

Figura 9 - Mapeamento dos Dados no Pequeno Provedor.



Fonte: O Autor (2021).

O artigo 37 da lei geral de proteção de dados determina que o controlador e o operador devem manter registro das operações de tratamento dos dados pessoais que realizarem, esses registros acabam ajudando no mapeamento. Também é fundamental no caso de haver compartilhamento de dados com terceiros, detalhar o mapeamento feito pelo lado do terceiro.

Com isso a estrutura do pequeno provedor deve ser verificada e compreendida de como estão os dados e como eles foram coletados e tratados. Após o processo de análise e mapeamento dos dados é possível que o pequeno provedor tenha a dimensão do que a empresa trata e como a empresa está tratando os dados.

Ação 02 - Treinamento dos Funcionários e Parceiros

Os funcionários e parceiros que trabalham de forma direta e indireta no pequeno provedor passarão por um importante processo de conscientização sobre a proteção de dados. O treinamento dos funcionários e parceiros são de grande importância para a implantação da LGPD, os pequenos provedores, nesta etapa da implantação, devem treinar seus colaboradores com objetivo de transmitir à importância da proteção e da privacidade dos dados. Abaixo segue os fatores que devem fazer parte do treinamento:

1 – Disseminar o conhecimento, os responsáveis pela proteção de dados do pequeno provedor devem ajudar aos seus colaboradores a obterem o conhecimento necessário, desenvolvendo a conscientização contínua, e com isso modificando a cultura do pequeno provedor, para que seja garantido o amadurecimento desta política de proteção.

2 – Divulgar ações de segurança e proteção dos dados, evitando e minimizando ameaças; evitar o uso inadequado de ferramentas tecnológicas e aplicativos, e evitar o compartilhamento indevido.

3 - Promover a cultura da privacidade e preservar os dados pessoais. É preciso envolver todos os setores que fazem parte do pequeno provedor.

4 - Utilizar o aprendizado sob medida, com base em situações reais do dia a dia do pequeno provedor e com suas respectivas funções e demonstrar para os funcionários o que muda na prática em seu dia-a-dia.

5 – Atualizar sempre que necessário a documentação do treinamento, criando um cronograma para monitorar a regularidade dos treinamentos.

6 - Convém, que os treinamentos possam ser elaborados de forma simplificada, sem fugir do real conceito, e sempre que possível trazendo analogias com outros conceitos mais simples e intuitivo.

7 - Relacionar a proteção de dados já na integração de novos colaboradores, ou seja, treinamento feito com os recém contratados.

8 – Estimular os funcionários a participar de workshops, cursos, encontros e capacitações propostas pela empresa, com objetivo de ampliar a cultura da proteção de dados dentro do ambiente de trabalho.

9 - Adotada uma campanha de comunicação regular, promovendo os aspectos da norma, utilizando divulgação em mural, e-mails, vídeos, posts e etc.

10 - Elaborar atividades periodicamente para verificar se os colaboradores estão envolvidos com o tema proteção de dados.

11 - Sempre que possível, gerar evidências sobre os treinamentos, por exemplo: através de questionários a serem aplicados ao término das apresentações.

12 - Definir de forma clara os setores que poderão ter acesso aos dados, bem como o modo de utilização de tais informações, estabelecendo penalidades em caso de uso indevido de dados.

13 - Apresentar alguns casos de violações de dados, e o impacto destas nas respectivas organizações.

14 - Designar ao encarregado da proteção dos dados pesquisar por assuntos e demais temas pertinentes a proteção de dados, de modo a aperfeiçoar o programa de treinamento com base nas melhores práticas de mercado.

Além de ajudar as operações do pequeno provedor de acesso a atuar em conformidade com a lei, o treinamento dos colaboradores sobre a LGPD fará com que a empresa seja bem vista pelo mercado, garantindo maior segurança e confiabilidade para a empresa e para os seus clientes. Os dados serão mais protegidos, o risco de sofrer com vazamento e roubo de dados será muito menor. Por fim, é importante lembrar que todos os envolvidos são responsáveis pela segurança dos dados de uma empresa.

Ação 03 – Consentimento de Uso dos Dados

O artigo 8º da LGPD explica que o consentimento de uso dos dados deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. A obrigação de comprovar a solicitação e fornecimento do consentimento é do pequeno provedor e não do titular, sendo importante que o consentimento seja solicitado para fins específicos, conforme disposto no Art. 8º. Caso necessário cabe

ao pequeno provedor solicitar uma nova permissão ao titular dos dados, e especificar o novo propósito.

Caso em situações particulares no que tange o tratamento de dados de crianças e adolescentes, o pequeno provedor deverá realizar o consentimento específico, devendo o aceite ser realizado por pelo menos um dos pais ou pelo responsável legal. É primordial que os pequenos provedores utilizem a comunicação de forma transparente sobre quais tipos de dados serão coletados, e o objetivo de sua utilização. Para as situações de dados sensíveis o consentimento deve seguir o registro da manifestação de vontade do titular de forma específica e destacada, dando ciência do conhecimento sobre as finalidades específicas daquele tratamento, explicando sobre como os dados serão tratados. No apêndice A está disponível um modelo de consentimento para uso dos dados ao qual serve como referência aos pequenos provedores de acesso.

Ao manifestar sua aceitação com o presente termo, o titular consente e concorda que o pequeno provedor de acesso, doravante denominado controlador, tome decisões referentes ao tratamento de seus dados pessoais, bem como realizar operações como: produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Vale lembrar ao pequeno provedor que o titular pode solicitar revogação, a qualquer momento do consentimento cedido anteriormente.

O pequeno provedor pode usufruir de ferramentas que vem sendo utilizada atualmente, ao qual o titular terá acesso direto as políticas de proteção de dados, e caso esteja de acordo o titular realizará o aceite de forma não explícita. Tal tipo de consentimento, além da ação positiva do usuário, precisa ser necessariamente requisito de obviedade e publicidade para ser considerado válido. Não poderá ser considerado implícito quando o termo digital for de difícil percepção e compreensão.

Abaixo estão os possíveis casos em que o pequeno provedor deve pedir o consentimento para o tratamento de dados pessoais:

1 - Para a execução de políticas públicas, ou seja, solicitações de tratamento de dados advindas da Anatel ou do Ministério das Comunicações, bem como para a realização de estudos por órgãos de pesquisa como por exemplo o IBGE.

2 - Para cumprimento de obrigações legais ou regulatórias do pequeno provedor: é o caso do armazenamento dos registros de conexão pelo pequeno provedor, como determinado pelo Marco Civil da Internet, ou ainda o armazenamento de ligações telefônicas dos clientes para a central de atendimento do provedor.

3 - Para questões contratuais ou de procedimentos preliminares relacionados a contratação dos serviços de internet, os provedores trabalham com contratos de adesão com clientes e devem inserir expressamente essa política de tratamento dos dados pessoais.

4 – Realizar tratamento através de ordem judicial expressa regular de direito ou em processo judicial, administrativo ou arbitral, ou seja, o tratamento de dados específico para o cumprimento de atividade de investigação policial ou cumprimento de ordem judicial para repressão de ilícito penal.

5 - Em caso de legítimo interesse do pequeno provedor, desde que não se sobreponha aos direitos e liberdades fundamentais dos titulares dos dados. Pode-se citar como exemplo, compartilhamento com empresas terceiras para fins de prevenção à fraude, marketing direto, proteção da integridade física do titular, dentre outras possibilidades.

6 - Tratamento para proteção de crédito, ou seja, o tratamento de dados para que o provedor se certifique do crédito do cliente e da cobrança de uma dívida, por exemplo, é uma das possibilidades expressas da LGPD. Assim, por exemplo, o envio de dados de cobrança pode ser realizado normalmente e não depende de consentimento prévio do cliente.

Dessa forma, incluir informações com vocabulário denso na política de consentimento, assim como ocultá-las, dificultando o seu acesso e compreensão por meio de textos com letras pequenas, são condutas que não devem ser praticadas pelo pequeno provedor de acesso. A lei suprime essa possibilidade, garantindo maior transparência e objetividade no consentimento conforme em seu artigo 7º. Esta etapa de consentimento é valiosa para a sequência da vida dos dados, então saber lidar com o consentimento dos diferentes tipos de titulares e de dados, traz ao pequeno provedor estabilidade e confiança ao seu ambiente de operação.

Ação 04 – Tratamento dos Dados Pessoais

Toda operação realizada com dados pessoais seja qual for o ambiente é considerada tratamento de dados. Para que os pequenos provedores de acesso realizem o tratamento dos dados pessoais de seus clientes, é fundamental compreender que ações como: coleta, classificação, armazenamento, anonimização, entre outras são considerados tratamento de dados, cabe ao pequeno provedor ter prudência ao tomar as decisões referentes ao tratamento de dados. Por essa questão este guia elenca abaixo as orientações de como realizar o tratamento dos dados:

1 – Antes de realizar o tratamento dos dados o pequeno provedor ou o encarregado deve disponibilizar um documento prévio ao titular dos dados a finalidade do tratamento, descrevendo o propósito legítimo e especifico.

2 – O pequeno provedor periodicamente deve realizar atualizações nas práticas de tratamento, a fim de proporcionar maior segurança e proteção dos dados.

3 – Tem a obrigatoriedade de garantir ao titular a realização de consultas facilitadas e gratuita sobre a forma e a duração do tratamento.

4 – Cabe ao pequeno provedor manter durante o tratamento dos dados a exatidão, clareza, relevância e atualização dos dados.

5 – Demonstrar transparência garantia que as informações serão precisas e facilmente acessível sobre a realização do tratamento.

6 – Manter sempre a segurança dos dados, protegendo os dados pessoais de acessos não autorizados e demais situações ilícitas.

7 - A realizar medidas para evitar a ocorrência de danos decorrente do tratamento de dados pessoais.

8 – Impedir qualquer tipo de abuso que implique sobre os titulares dos dados.

9 - Sobre a atividade de compartilhamento aconselhasse ao pequeno provedor descrever o propósito desta ação e elaborar o termo de compartilhamento.

Com isso é importante lembrar que essas atividades relacionadas são fundamentais para um bom desempenho no tratamento dos dados. Sendo atividades sempre em observâncias com a legislação.

Ação 05 – Atuação do Encarregado da Proteção de Dados

Nesta etapa de adequação da LGPD, as atividades do encarregado da proteção de dados serão importantes para o ambiente do pequeno provedor de acesso. A LGPD em seu Art. 5º, inciso VIII, conceitua o encarregado como: 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). Segue abaixo as atribuições que deverão ser desenvolvidas pelo encarregado “DPO” conforme propõem este guia de implantação alinhado com a lei geral de proteção de dados:

- O encarregado será responsável por estabelecer o processo de conformidade, implantação e manutenção dos processos relacionados a LGPD.
- O encarregado da proteção de dados terá que identificar e compreender dentro do ambiente do pequeno provedor todo o ciclo de vida dos dados tanto de uma perspectiva técnica, sabendo identificar possíveis riscos de segurança, quanto

da perspectiva jurídica, identificando as exigências legais aplicáveis a cada etapa do processo.

- Deverá ser a pessoa com maior domínio da LGPD dentro do ambiente do pequeno provedor, ou seja, apresentar um perfil adequado as suas atribuições e apresentar um bom relacionamento interpessoal a fim de evitar conflitos de interesse entre operador, controlar, titular e ANPD.
- Interpretar corretamente as diretrizes da autoridade nacional e ter condições de adotar as providências cabíveis.
- Ter autonomia técnica e profissional para que o encarregado possa trabalhar de maneira efetiva.
- Buscar o compromisso organizacional de estar em conformidade com os direcionamentos da LGPD.
- Orientar os funcionários e os terceirizados sobre aspectos da proteção de dados, como também participar, incentivar e instituir o comprimento dos processos de cultura, segurança, proteção e privacidade dos dados.
- Ser responsável pela elaboração do relatório de impacto sobre a proteção dos dados.
- Buscar a implementação do processo de privacidade por padrão em produtos e serviços.
- Ser o elo de comunicação entre a empresa, o titular dos dados e a Autoridade Nacional de Proteção de Dados – ANPD, aceitar solicitações, reclamações e comunicações dos titulares e da ANPD, prestar esclarecimentos e adotar providências.
- Monitorar a conformidade da organização, inclusive em auditorias, monitoramento da execução de contratos, atividades de conscientização e treinamento organizacional.
- Identificar e atualizar as atividades de tratamento dos dados.
- Orientar e manter a adequação dos contratos relativos as atividades com partes relacionadas a proteção e privacidade de dados.
- Promover ações de melhoria aos riscos de violações de privacidade;

- Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.
- Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

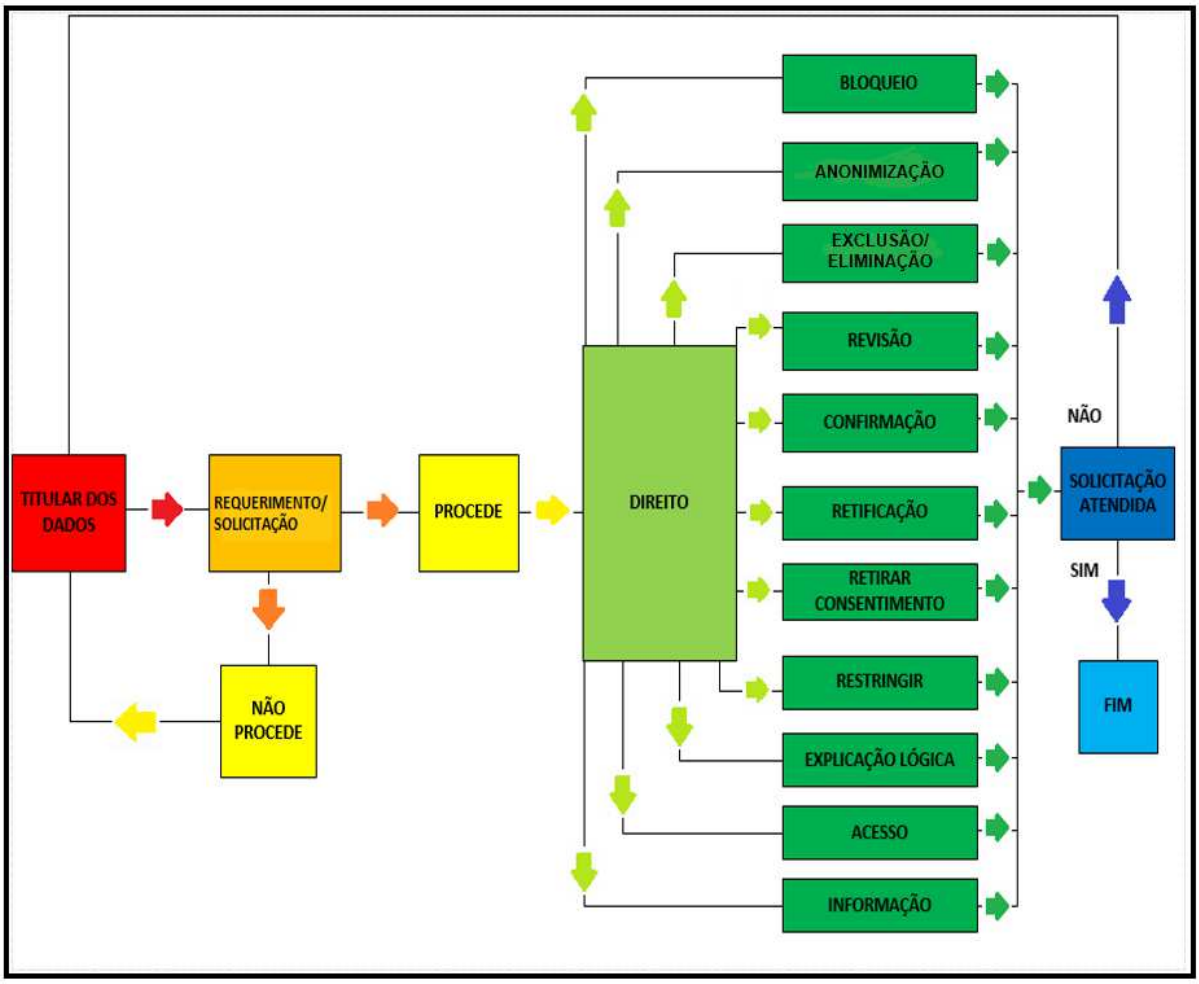
A lei geral de proteção de dados determina a divulgação pública de quem é o encarregado de proteção de dados, de forma clara e objetiva de preferência em site ou por outra plataforma de acesso livre para a sociedade.

Como foi visto durante esta etapa, a responsabilidade do encarregado da proteção de dados impacta em muitos aspectos. Assim, é importante que o pequeno provedor de acesso e o próprio encarregado estejam alinhados para todas as situações que podem ocorrer em relação ao tratamento de dados.

Ação 06 – Direitos e Solicitações dos Titulares

Nesta etapa será instruído ao pequeno provedor como proceder com as solicitações dos usuários. A legislação determina que através de requerimento físico ou digital o titular poderá realizar as solicitações, e o controlador, no caso o pequeno provedor deverá fornecer as informações claras e adequadas sobre os critérios e procedimentos utilizado. O direito do titular conferido na Lei Geral de Proteção de Dados está entre os artigos 17, 18 e 22. Dessa forma, será demonstrado a seguir o fluxograma das solicitações, que serve de mecanismo para a adequação, onde além de garantir a condução das solicitações do titular, terá importância nas atividades diária do pequeno provedor.

Figura 10 - Fluxograma das Solicitações dos Titulares dos Dados.



Fonte: (O Autor 2021).

Conforme demonstrado no fluxograma é essencial saber reconhecer se a solicitação feita pelo titular de dados está em conformidade com a LGPD e quando ela deve ser recusada, é importante ao pequeno provedor está atento ao que diz o artigo 18 da LGPD, neste artigo consta as especificações que deverão ser atendidas pelo controlador, questões que fogem deste artigo devem ser tratadas de forma particular e específica sempre com o respaldo da LGPD ou de outras legislações, e em último caso submeter a apreciação jurídica, uma vez aceita a solicitação através do requerimento/solicitação o provedor terá que verificar qual o direito que o titular solicita: retificação, anonimização, acesso, bloqueio, eliminação e etc; após o titular que receber o retorno da sua solicitação caberá ao mesmo verificar se as informações recebidas preenchem a necessidade questionada por ele, caso não o titular poderá

solicitar novamente um novo pedido de direito, desde que esteja em acordo com os princípios da LGPD.

Dentre os direitos e solicitações dos titulares vale apena fazer um destaque sobre a anonimização dos dados, esse direito é previsto em lei pela LGPD sendo uma técnica de processamento de dados que remove ou modifica informações que possam identificar uma pessoa. É importante lembrar ao titular dos dados que um dado considerado anonimizado só existe quando não há nenhuma maneira de voltar ao seu estado original, essa técnica resulta em dados anonimizados que não podem ser associados a nenhum indivíduo específico. Neste caso o pequeno provedor deve atender e realizar a desassociação dos dados do titular, ao mesmo tempo deve informar ao titular que uma vez os dados tornados anônimos os mesmos não serão considerados dados pessoais.

Atenções importantes para o pequeno provedor: ter um canal para recebimento das solicitações dos titulares dos dados, treinar os funcionários que farão essas ações, identificar o titular, gerenciar o tempo do recebimento e das respostas e utilizar ferramentas que protejam todo o processo, bem como facilitem a operação de resposta, de forma a cumprir todos os direitos dos titulares, ter um plano estruturado para responder às solicitações, reclamações e retificações.

Sugere-se que o pequeno provedor estabeleça um formulário físico ou digital que contenha a identificação do documento, a identificação do cliente, seu pedido e a data. A resposta do pequeno provedor deve vir acompanhada do número de protocolo aberto. Sugere-se que a resposta seja enviada por e-mail ao cliente ou que o serviço esteja disponível em um website. No apêndice B deste trabalho está proposto um modelo de formulário de solicitações dos titulares dos dados.

Ação 07 – Comunicação com Órgãos e a Sociedade

Em seu artigo 48 a lei geral de proteção de dados deixa expressamente claro: o controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, onde a comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar: A descrição da natureza dos dados pessoais afetados; As informações sobre os titulares envolvidos; A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; Os riscos relacionados ao incidente; Os motivos da demora, no caso de a comunicação não ter sido imediata; e as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. No apêndice C está demonstrado um modelo de comunicado sobre incidente.

A autoridade nacional ao verificar a gravidade do incidente poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao pequeno provedor de acesso, a adoção de providências, tais como: Ampla divulgação do fato em meios de comunicação e medidas para reverter ou mitigar os efeitos do incidente.

O trabalho de comunicação é estratégico e deve ser adotado pelos pequenos provedores de acesso à internet. É importante integrar as áreas e implementar ações adequadas ao cumprimento da LGDP, e assim desenvolver um procedimento preventivo de comunicação. A recomendação é fazer diagnósticos internos e mapeamento de potenciais riscos de comunicação, levando em consideração a comunicação de cada setor por onde passam os dados.

Os pequenos provedores terão que estar preparados para enfrentar situações de exposição na mídia. Então, é preciso instruir o encarregado da proteção de dados a criar um plano estratégico e preventivo de comunicação, específico para casos relacionados às falhas na proteção de dados pessoais. Se faz necessária como objetivo passar para todos os envolvidos o valor da transparência, essencial para todas as empresas que manipulam dados.

Ação 08 – Registro de Eliminação dos Dados

Nesta etapa de eliminação dos dados o encarregado da proteção de dados “DPO”, terá a atribuição de realizar quando solicitado pelo titular dos dados a eliminação dos dados sejam eles físicos ou digitais. O direito à eliminação de dados descrito no artigo 18 da lei geral de proteção de dados, estabelece que o titular dos dados pode solicitar ao controlador, a qualquer momento e mediante requisição a eliminação dos dados pessoais com o consentimento do titular.

Aconselha-se ao pequeno provedor de acesso à internet estabelecer um contato objetivo e direto com o titular no que corresponde ao tema exclusão de dados, ressaltando a importância da manutenibilidade e a disponibilidade no sistema para a realização destas atividades pertinente a privacidade e proteção de dados.

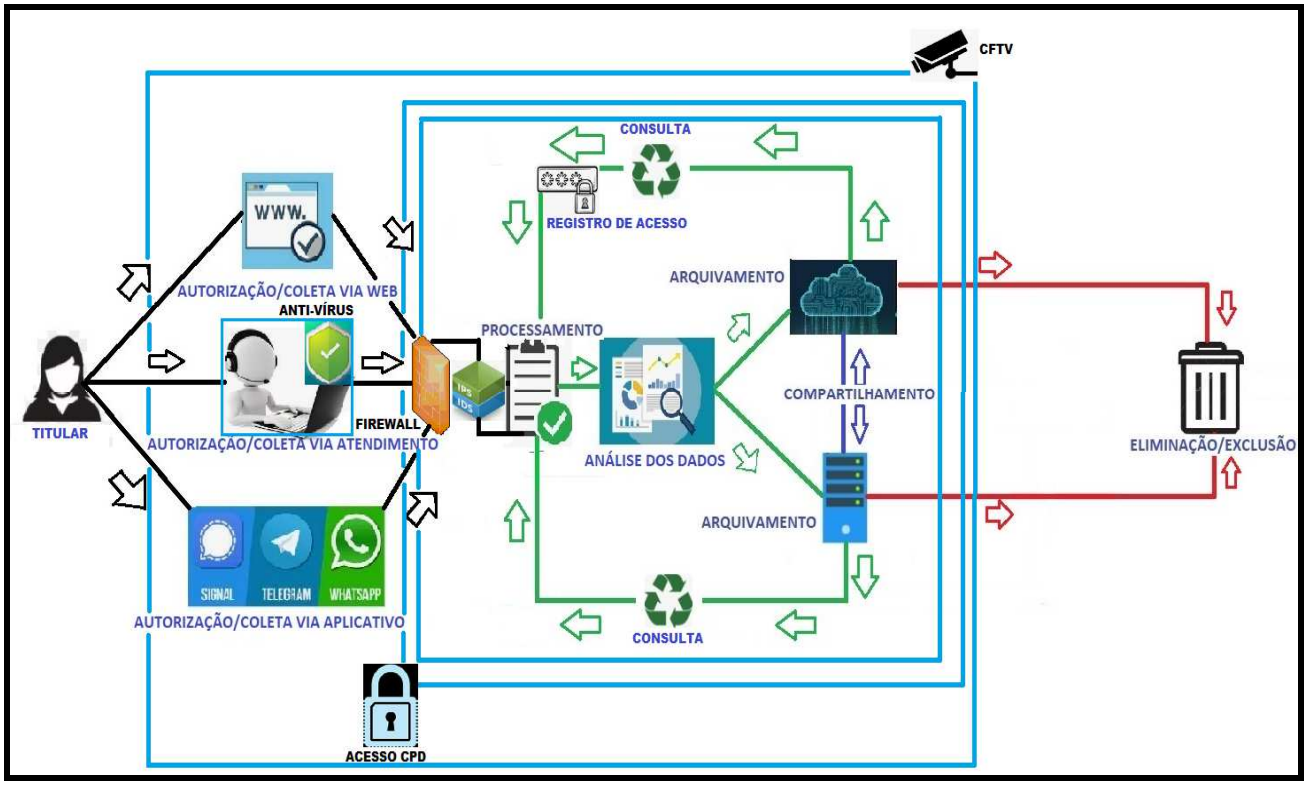
É importante reforçar que a revogação do consentimento, ou seja, a solicitação de exclusão dos dados, consiste em um direito do titular conforme legislação, podendo ser feito a qualquer momento pelo titular, mas há algumas ressalvas em que a eliminação dos dados pessoais precisa ser comprida independente da solicitação do titular conforme situações a seguir: cumprimento de obrigação legal ou regulatória pelo controlador; estudo por órgão de pesquisa (garantida, sempre que possível, a anonimização dos dados pessoais); uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados. Como trata-se de casos excepcionais, essas situações devem ser controladas pela Autoridade Nacional de Proteção de Dados (ANPD), prevista na LGPD. No apêndice D está disponível um modelo de requerimento para eliminação dos dados.

Ação 09 – Análise da Segurança dos Dados

Nesta parte do guia o pequeno provedor deve adotar ações de segurança e medidas de proteção de dados para mitigar os riscos. É importante estabelecer prioridades e tomar decisões, avaliando a sensibilidade dos dados, a vulnerabilidade do sistema e a probabilidade de ameaças.

Para o pequeno provedor as ações de segurança e as medidas de proteção combinada por meio de inteligência contra ameaças é uma ação para proteger esses ativos, processos e titulares. As políticas de segurança devem ser atualizadas regularmente. A ilustração abaixo exemplifica um modelo a ser seguindo pelos pequenos provedores.

Figura 11 - Modelo de Solução para Segurança dos Dados.



Fonte: O Autor (2021).

Os dados devem ser protegidos contra processamento não autorizado ou ilegal, também devem ser protegidos contra perda, destruição ou dano acidental. É importante ter o controle principalmente do acesso ao CPD restringindo o acesso e coletar logs dos acesso realizados, interagir com tecnologias de detecção e prevenção de intrusão, manter seus sistemas atualizado e principalmente verificar os registro de acesso ao sistema, fazer backup dos dados, fazer uma avaliação de impacto, estar atento a segurança física utilizando de circuito fechado de televisão “CFTV” para monitoramento em tempo real do ambiente do pequeno provedor, e também ao não compartilhamento de senhas, utilizar softwares de proteção antivírus conforme vimos

na figura acima, onde deve ser instalado nas máquina de todos os usuários dentro do provedor principalmente dos que estão realização as coletas dos dados dos titulares, o firewall para poder proteger todo a rede, softwares de controle e fazer escolhas compatível com a LGPD. A utilização conjunta dessas soluções no monitoramento de atividades é fundamental para que a segurança seja eficaz, saber o que está acontecendo em toda a rede é essencial para conter e evitar ataques.

Quando um pequeno provedor prioriza a proteção e a segurança em acordo com a lei geral de proteção de dados, ele tem uma maior chance não apenas de evitar o vazamento de dados, mas também de evitar multas e problemas de reputação. Corrigir sistemas e examinar possíveis falhas de segurança e aprender com os incidentes impedindo que isso aconteça novamente. É importante ao pequeno provedor considerar soluções que forneçam visibilidade a toda a rede utilizando logs, terminais e inteligência contra ameaças para detectar e entender rapidamente a fim de ajudar na resposta de forma rápida e eficaz.

Por fim é importante ao pequeno provedor ter um plano detalhado para eventuais situações, de forma que todos operem da mesma forma e evitem falhas de comunicação e procedimentos errados. Em caso de sucessivas falhas é essencial ter o *backup* para prover uma recuperação de dados de forma eficiente, seja por meio de um servidor externo, um HD externo ou na nuvem. O essencial é não abrir mão desse sistema de recuperação. Por fim deve-se sempre lembrar que essas ações citadas nesse tópico contribuem massivamente para uma implantação com segurança e proteção dos dados.

Ação 10 – Auditória sobre a Proteção de Dados

Neste processo o pequeno provedor de acesso passará por uma inspeção para revalidar seus conceitos, sistemas e procedimentos utilizados para a proteção de dados. Essa etapa visa demonstrar ao pequeno provedor que auditorias regulares produzem informações, que servem para aperfeiçoamento das práticas utilizadas para a proteção dos dados.

Por meio da auditoria o pequeno provedor deverá tomar conhecimento dos processos que não estão em conformidade e investigar através de diretrizes as oportunidades de melhorias. É necessário ao pequeno provedor compreender bem os métodos de auditoria como: processos, tarefas e etapas.

Efetuar uma auditoria é tipicamente um processo que é gerido por uma equipe de auditores que possuem elevado conhecimento técnico. Por isso, a auditoria não pode ser realizada por qualquer profissional, o pequeno provedor deve estar atendo na escolha do auditor ou empresa de auditoria. Esta equipe é encarregada de entrevistar os funcionários da empresa, e conduzir avaliações de vulnerabilidades, políticas de segurança, e analisar os sistemas de informação.

Quando as análises da vistoria estiverem conclusas, os auditores produzirão o documento mostrando as conformidades e não conformidades encontradas no pequeno provedor. É importante ressaltar ao pequeno provedor que correções e atualizações técnicas podem exigir realocação de orçamento e aumento de equipe, ou podem exigir desenvolvimento de treinamento.

A verificação completa por meio da auditoria fornece ao pequeno provedor a qualificação das boas práticas, certificando que a empresa está em conformidade com os processos da LGPD. É importante lembrar que este é um processo necessário na estrutura da privacidade e proteção de dados para garantir que tudo esteja em conformidade.

Ação 11 – Relatório de Impacto sobre a Proteção de Dados

O relatório de impacto na proteção de dados deve ser incorporado dentro das políticas de proteção dos pequenos provedores. Este documento deve registrar os riscos presentes nas práticas de tratamento de dados, bem como identificar se as medidas e procedimentos de segurança implementados estão à altura dos riscos encontrados. Servindo como base para o cumprimento dos princípios da LGPD, o relatório tem o propósito de mitigar riscos, e deve ser produzido de tal forma que comtemple todo o ciclo de vida dos dados.

O processo de criação do relatório consiste basicamente na compilação de todas as informações relevantes que envolva os dados. Deste modo é necessário que todas as áreas que manipulam dados dentro do ambiente do pequeno provedor participem no desenvolvimento desta documentação. O relatório de impacto à proteção de dados deverá conter: a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta dos dados, os sistemas de tratamento utilizado, a finalidade do tratamento, avaliação sobre as operações de tratamento, avaliação dos riscos, avaliação de medidas de segurança, os procedimentos destinados a assegurar a proteção dos dados e demonstrar a conformidade com a lei.

A LGPD valoriza muito a prevenção dos riscos, com isso mesmo um pequeno provedor conduzindo um relatório de impacto à proteção de dados em modo autônomo isso demonstrará seu cuidado e proatividade com a segurança dos dados. Também é importante lembrar que a autoridade nacional de proteção de dados poderá solicitar ao pequeno provedor o relatório de impacto à proteção de dados pessoais.

Abaixo segue os benefícios que o pequeno provedor terá ao implementar em seu cotidiano o relatório de impacto a proteção de dados: proatividade na conformidade com a legislação, melhor funcionamento do sistema de gestão de segurança da Informação, maior compreensão dos riscos relacionados à proteção de dados pessoais, medidas e ações na melhoria do tratamento, impedir violações de dados, vazamentos, multas, sanções, danos à imagem e a reputação da organização.

De modo geral o relatório de impacto demonstra à Autoridade Nacional, aos clientes, fornecedores, parceiros comerciais, investidores ou autoridades de proteção de dados de países estrangeiros com os quais se deseje transferir os dados que o ambiente é efetivamente seguro para os dados pessoais. É importante ao pequeno provedor que ele esteja sempre atento as reuniões da ANPD, pois podem ocorrer atualizações nos regulamentos e nas resoluções que impactem na proteção de dados pessoais.

O pequeno provedor deve manter um alinhamento com o encarregado da proteção de dados, pois conforme em seu artigo 41 a LGPD afirma que é de

responsabilidade do encarregado de proteção de dados receber as comunicações da ANPD, e tomar as providências necessárias sendo assim o encarregado recebe o pedido e então dar andamento em conjunto com o pequeno provedor.

Por fim tentou-se passar ao pequeno provedor que o relatório de impacto à proteção de dados é algo importante, tendo em vista a quantidade de benefícios que o relatório traz, se tornando uma etapa relevante para o funcionamento da proteção de dados dentro do ambiente do pequeno provedor.

Ação 12 – Governança e Boas Práticas para o Tratamento dos Dados

De acordo com o artigo 7º da LGPD o tratamento de dados pessoais somente poderá ser realizado mediante o fornecimento de consentimento pelo titular. Todos os dados pessoais que forem coletados, utilizados e armazenados pela empresa devem obter essa autorização. O pequeno provedor de acesso tem obrigação e competência com relação ao tratamento de dados, podendo elaborar regras de boas práticas e governança para o tratamento dos dados. As regras devem ser atualizadas e publicadas de maneira periódica e podem ter o reconhecimento e divulgação da Autoridade Nacional de Proteção de Dados.

No Artigo 50 da LGPD os controladores e operadores, no âmbito de suas competências para o tratamento de dados pessoais, na forma individual ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam condições, procedimento, funcionamento entre outros. As normas de segurança e os padrões técnicos, são itens importante para a cultura da governança e boas práticas para a proteção de dados, os mecanismos internos de supervisão e de mitigação de riscos também são aspectos de relevância.

Para o pequeno provedor de acesso: o volume de sua operação, a sensibilidade dos dados tratados e a gravidade dos danos, são fatores que contribuem na implementação de um programa de boas práticas, demonstrando o comprometimento em adotar métodos e políticas que assegurem o cumprimento das normas. Assim as governanças e boas práticas consistem em descrever medidas com objetivo de minimizar erros do processo de tratamento dos dados.

Essa política de governança e boas práticas poderá servir como base para demonstrar a boa-fé do pequeno provedor de acesso, a diligência e o comprometimento da empresa em termos de governança, conformidade com a legislação e preocupação com a segurança e sigilo dos dados pessoais dos titulares e assim atenuar eventual sanção administrativa.

Ação 13 – Certificação das Práticas de Proteção dos Dados

Após passada as etapas anteriores é possível ao pequeno provedor validar os seus processos de proteção de dados através da certificação isso trará uma boa reputação ao pequeno provedor, pois a importância da certificação junto ao mercado pode ser uma mudança de posicionamento tornando o pequeno provedor diferenciado em relação aos demais.

O processo de certificação é feito através de avaliação de item como: adequação à lei, defesa a possíveis riscos, danos, incidente e vazamento. Visando cumprir regras de conformidades e contribuir para a proteção dos titulares. Inspecionar os processos e sistemas, verificar eventuais falhas de segurança, analisar setores, coletar informações, observar as formas de tratamento de dados, prestar contas aos entes públicos e regulatórios são processos que devem estar alinhados dentro do ambiente do pequeno provedor para a obtenção da certificação.

A certificação além de atestar os níveis de segurança e de capacidade no tratamento de dados, pode ser compreendida como uma validação realizada por uma instituição independente, dando o de acordo sobre as práticas de proteção de dados, ou seja, declarando que o pequeno provedor está em conformidade com as normas técnicas relacionadas com a LGPD. Nesse contexto caberá às entidades certificadoras, que possui tal escopo conceder certificados com prazos de validade, mediante o cumprimento dos critérios técnicos estabelecidos e parâmetros específicos.

Ação 14 - Melhoria Contínua

A melhoria contínua deve ser tratada no ambiente do pequeno provedor como uma atividade regular, sendo uma ação rotineira que irá examinar todos os processos de proteção e privacidade dos dados, com objetivo de revalidação dos tópicos. Abaixo estão os parâmetros utilizados:

- Analisar e garantir os processos da coleta de dados e as informações pessoais.
- Verificar e garantir os processos sobre o consentimento, propósito, legitimidade e especificação para coleta.
- Verificar e garantir os processos sobre os limites da coleta de dados do indivíduo.
- Verificar e garantir os processos de utilização do mínimo de dados necessários;
- Verificar e garantir os processos de tratamento das informações.
- Verificar e garantir processos da qualidade da privacidade e da proteção das informações pessoais;
- Verificar e garantir processos de transparência para aviso quanto aos incidentes de vazamento;
- Verificar e garantir processos para garantir os acessos dos titulares às informações;
- Verificar e garantir processos para registro das solicitações e prestação de contas de privacidade às pessoas.
- Verificar e garantir processos da segurança da informação.
- Verificar e garantir processos da proteção de dados na área recursos humanos.
- Verificar e garantir processos para gerenciamento das operações e comunicações.
- Verificar e garantir processos para gestão de incidentes
- Verificar e garantir processos para gestão da continuidade do negócio;
- Verificar e garantir processos de Conformidade.

O principal objetivo desta etapa dentro da proposta de implantação é avaliar e monitorar de forma contínua todos os aspectos específicos da proteção de dados e privacidade da organização (controles, políticas, procedimentos, práticas, etc.).

É importante lembrar que a gestão de proteção de dados é cíclica, devendo ocorrer periodicamente avaliações e melhorias; para sempre buscar a evolução dos serviços e qualidade garantidos assim a devida proteção e rastreabilidade dos dados.

6 CONCLUSÃO

Foi demonstrado ao longo deste trabalho o objetivo de implantar a proteção de dados dentro do ambiente dos pequenos provedores de internet, tendo como referência metodologias, fundamentos, princípios e frameworks reconhecidos e conceituados globalmente. Para tal, foi realizada uma ampla investigação sobre os desafios de implantar e adequar a proteção de dados, em sintonia com as áreas: gestão, tecnologia e direito que atualmente regem a proteção de dados, para minimizar qualquer vulnerabilidade ou dificuldade imposta pela falta dos diversos recursos.

No decorrer da produção da pesquisa foi possível verificar a dificuldade de encontrar ferramentas, trabalhos, suportes, teses e artigos publicados que relatassem sobre o assunto, visto que tal tema ainda é principiante nas literaturas vigentes. Essa novidade vem percorrendo de forma lenta dentro do mercado brasileiro sendo não só uma mudança cultural, mas de importância fundamental para o contexto nacional.

A proposta do guia de implantação, adicionada com as suas etapas e procedimentos, não foi legalizada em nenhum pequeno provedor, contudo as etapas mostram-se válidas no que diz respeito a legislação e a realidade do ambiente dos pequenos provedores. Neste contexto, pode-se verificar que o guia trará benefícios com sua utilização, por ser baseado nas práticas referenciadas pelas áreas da gestão, do direito e da tecnologia, tornando viável a possibilidade de cumprir os objetivos de quem busca implantar a proteção de dados.

Para validação deste guia, é necessário um estudo de caso com a implantação em um pequeno provedor de acesso à internet para analisar a efetividade das ações e métricas, assim como, estudos pós-implantação possibilite base para projetos e pesquisas que otimizem os temas aqui estruturados.

Neste contexto recomenda-se para trabalhos futuros o acompanhamento e a incorporação das normas e resoluções da ANPD para necessidades de novas adequações no ambiente de proteção de dados, buscar métodos e demais soluções

de segurança que protejam os dados pessoais, utilizar ferramentas de software que visem otimizar processos da proteção dos dados, analisar a utilização de outros métodos como ferramenta para a proteção dos dados pessoais e elaborar ações para verificação do ambiente de proteção de dados. Por todo exposto, o presente trabalho de conclusão de curso se alinha ao entendimento, de que a otimização dos processos de forma objetiva traz uma praticidade e usabilidade centralizando assim os objetivos deste trabalho as melhores práticas.

REFERÊNCIAS

ATHENA SECURITY. ATHENA SECURITY. **Entenda as responsabilidades do DPO na empresa**. São Paulo. 2020. Disponível em: < https://blog.athenasecurity.com.br/responsabilidades-do-dpo/ > Acesso em: 23 de nov de 2020.

AUCAR, L. **Política de privacidade de dados pessoais**. Juiz de Fora. 2020. Disponível em: < https://www.rheserva.com.br/politica-de-privacidade-de-dados-pessoais/ > Acesso em: 29 de nov de 2020.

AZEVEDO, J. P. B. **Análise de Segurança e Aperfeiçoamento de uma Rede Universitária de Telecomunicações**. Ilha da Madeira. Digituma. 2019. 184 p. Disponível em: < https://repositorio.uma.pt/handle/10400.13/2342 > Acesso em: 16 de nov de 2020.

BATISTELLA, C. **Por que o treinamento LGPD é importante para as empresas?**. São Paulo. 2020. Disponível em: < https://www.certifiquei.com.br/treinamento-lgpd/ > Acesso em: 21 de nov de 2020.

BHS. BHS. **Qual a relação entre segurança da informação e a Lei Geral de Proteção de Dados**. Belo Horizonte. 2020. Disponível em: < https://www.bhs.com.br/2020/03/11/seguranca-da-informacao-e-a-lei-geral-de-protecao-de-dados/ > Acesso em: 10 de dez de 2020.

BIDNIUK, V. B**. O Papel do DPO – DATA PROTECTION OFFICER (Encarregado)**. Porto Alegre. 2020. Disponível em: < https://www.federasul.com.br/o-papel-do-dpo-data-protection-officer-encarregado/ > Acesso em: 24 de nov de 2020.

BRASIL. Lei nº13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados. Diário Oficial da União**, Brasília, DF, v.01, n.01, 15 de agosto de 2018, 15 de agosto de 2018. Seção 1, página 59. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm >. Acesso em: 03 de jun. de 2021.

BRASIL. Lei nº12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil**. Diário Oficial da União, Brasília, DF, v.01, n.01, 24 de abril de 2014, Seção 1, página 1. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm >. Acesso em: 04 de nov de 2020.

BRASIL. Lei nº12.737, de 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos**. Diário Oficial da União, Brasília, DF, v.01, n.01, 03 de dezembro de 2012, seção 1, página 1. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm > Acesso em: 05 de nov de 2021.

Cabral, T. **ISO 27001 E LGPD: Entenda a sua relação para a proteção de dados da empresa**. São Paulo. 2020. Disponível em: < https://blog.athenasecurity.com.br/iso-27000/ > Acesso em: 19 de nov de 2020.

CÂMARA BRASILEIRA DE LIVROS. CÂMARA BRASILEIRA DE LIVROS. **Termo de Consentimento para Tratamento de Dados**. São Paulo. 2020. Disponível em: < https://servicos.cbl.org.br/termos-e-condicoes/ > Acesso em: 03 de dez de 2020.

CAVALCANTI, A. E. L.W.; LEITE, B. S. F., & BARRETO JUNIOR, I. F. **Sistemas de responsabilidade civil dos provedores de aplicações da internet por ato de terceiros: Brasil, União Europeia e Estados Unidos da América**. Santa Maria. Revista Eletrônica do Curso de Direito da UFSM. 2018. Disponível em: < https://periodicos.ufsm.br/revistadireito/article/view/28622 >. Acesso em: 20 mar. 2021.

CGI.BR. CGI.BR. **Princípios para a governança e uso da internet**. São Paulo. 2009. Disponível em: < https://principios.cgi.br/ >. Acesso em: 08 nov. 2020.

COPATI, M. **LGPD na prática: Como adequar seu negócio**. São Paulo. 2020. Disponível em: < https://blog.tivit.com/lgpd-na-pratica-como-adequar-o-seu-negocio > Acesso em: 29 de nov. 2020.

DAU, Gabriel. Jornal Contábil. 2020. **Primeiro passo para empresas se adequarem à LGPD**. São Paulo. 2020. Disponível em: < https://www.jornalcontabil.com.br/primeiro-passo-para-empresas-se-adequarem-a-lgpd/ > Acesso em: 28 de nov. 2020.

DIAS, P. Y. **Os Desafios do direito digital e das políticas públicas para proteger o direito à privacidade no âmbito da atuação dos provedores da internet**. Maringá. Revista Espaço Acadêmico. 2020. Disponível em: < http://periodicos.uem.br/ojs/index.php/EspacoAcademico/article/view/52117 >. Acesso em: 06 de nov. 2020.

DODT, C. **Como criar um Relatório de Impacto à Proteção de Dados Pessoais adequado a LGPD**. Blumenau. 2020. Disponível em: < https://www.profissionaisti.com.br/relatorio-impacto-protecao-dados-pessoais-lgpd/ > Acesso em: 05 de dez. 2020.

DONÁ, C. M; CELIDONIO. T., & NEVES, P. N. **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**. Curitiba. 2020. Disponível em: < https://www.brazilianjournals.com/index.php/BJB/article/view/18382 > Acesso em: 08 de dez. 2020.

DONEDA, D. C. M.; ALMEIDA, V. A. F. de. **Privacy Governance in Cyberspace**. Nova Jersey. 2015. Disponível em: https://ieeexplore.ieee.org/document/7111890?reload=true >. Acesso em: 11 de nov. 2020.

_____. **Da privacidade à proteção de dados pessoais**. 1. Ed. Rio de Janeiro: Renovar, 2006.

DURBANO, V. **Segurança da informação: o que é e 12 dicas práticas para garantir**. São Paulo. 2018. Disponível em: < https://blog.ecoit.com.br/seguranca-da-informacao/ > Acesso em: 11 de dez. 2020.

EXIN. EXIN. **GPRD – Importância do Treinamento das Equipes**. Utrecht. 2020. Disponível em: < https://www.exin.com/br-pt/gdpr-importancia-do-treinamento-das-equipes/ > Acesso em: 22 de nov. 2020.

FALEIROS JÚNIOR, J. L. M., LONGHI, J.V. R. **A Responsabilidade Civil dos Provedores de Busca de Produtos na Internet**. Rio de Janeiro. Revista da Faculdade de Direito da UERJ. 2020. Disponível em: < https://www.e-publicacoes.uerj.br/index.php/rfduerj/article/view/36191 > Acesso em: 08 de nov. 2020.

FERNANDES, J. C. **LGPD, uma visão propositiva da lei, oportunidade para maximização de performance, resultado e diferencial competitivo**. São Paulo. 2020. Disponível em: < https://ambitojuridico.com.br/cadernos/direito-internacional/lgpd-uma-visao-propositiva-da-lei-oportunidade-para-maximizacao-de-performance-resultado-e-diferencial-competitivo/ > Acesso em: 29 de nov. 2020.

FIGUEIREDO, T. T. M. G. de. **Da responsabilidade do subcontratante no âmbito do RGPD**. Porto. VERITATI. 2019. 55 p. Disponível em: < https://repositorio.ucp.pt/handle/10400.14/28688 > Acesso em: 17 de nov. 2020.

FILHO, A. S., e RODRIGUES, J. de S. C. **Certificate: a arte da certificação em LGPD**. 2020. Disponível em: < https://migalhas.uol.com.br/coluna/migalhas-de-protecao-de-dados/333202/certificarte--a-arte-da-certificacao-em-lgpd > Acesso em: 07 de dez. 2020.

REDEMPRESA. REDEMPRESA. 2020. **LGPD – Lei Geral de Proteção de Dados: O que sua empresa deve fazer?**. São Paulo. 2020. Disponível em: < https://fj.com.br/lgpd/#:~:text=Garanta%20um%20ciclo%20de%20Melhoria,de%20forma%20consentida%20(contratos)%3B&text=Garanta%20processos%20que%20estabele%C3%A7am%20os,dados%20do%20indiv%C3%ADduo%20(cookies)%3B > Acesso em: 26 de nov. 2020.

FUKUDA, L. M. **Segurança da Informação em IoT**. Curitiba. Repositório RIUT UTFPR. 2019. 39 p. Disponível em: < http://repositorio.roca.utfpr.edu.br/jspui/handle/1/19442 > Acesso em: 14 de nov. 2020.

GERHARDT, T. E; SILVEIRA, D. T. **Métodos de pesquisa**. Porto Alegre, Editora da UFRGS, 2009.

GONÇALVES, G. **Mais do que o consenso, LGPD exigirá mudança de comportamento**. 2019. Disponível em: < https://www.ecommercebrasil.com.br/noticias/mais-do-que-o-consenso-lgpd-exigira-mudanca-de-comportamento/ > Acesso em: 27 de nov. 2020.

GONÇALVES, M. S. **LGPD - Como atender as solicitações dos titulares de dados**. São Paulo. 2020. Disponível em: < https://www.lgpdbrasil.com.br/lgpd-como-atender-as-solicitacoes-dos-titulares-de-dados/ > Acesso em: 01 de dez. 2020.

INFOCHANNEL. INFOCHANNEL. **Certificação em conformidade com a LGPD é emitida para a primeira empresa no Brasil**. São Paulo. 2020. Disponível em: < https://inforchannel.com.br/certificacao-em-conformidade-com-a-lgpd-e-emitida-para-a-primeira-empresa-no-

brasil/#:~:text=O%20primeiro%20certificado%20ISO%2027701,vigor%20esse%20ano%20no%20Pa%C3%ADs. > Acesso em: 07 de dez. 2020.

KOCHE, J. C. **Fundamentos de metodologia científica**. Petrópolis. Vozes, 2011.

KURBALIJA, J. **Uma introdução à governança da internet**. São Paulo. 2016. Disponível em: < https://cgi.br/media/docs/publicacoes/1/CadernoCGIbr_Uma_Introducao_a_Governanca_da_Internet.pdf >. Acesso em: 20 de maio. 2021.

LBCA. LBCA. **11 Passos para Implantar a LGPD na sua empresa**. São Paulo. 2019. Disponível em: < https://www.lgpdbrasil.com.br/10-passos-para-implantar-a-lgpd-na-sua-empresa > Acesso em: 07 de nov. 2020.

LINS, B. F. E. **Privacidade em tempos de internet: uma apreciação da dimensão econômica no tratamento de dados pessoais**. Brasília. 2018. Disponível em: < https://bd.camara.leg.br/bd/bitstream/handle/bdcamara/35379/privacidade_internet_lins.pdf?sequence=1&isAllowed=y > Acesso em: 13 de nov. 2020.

LIRA, L. S. **Gestão de serviços de TIC: uma proposta de implantação de uma central de serviços de baixo custo com ênfase em operações de TIC**. Jaboatão dos Guararapes. 2018. 88 p.

MAGRI, S. Sheilamagri. **Comunicação em tempos de LGPD – entenda os impactos da lei para a reputação de empresas**. 2020. Disponível em: < https://sheilamagri.blog/2020/09/14/comunicacao-em-tempos-de-lgdp-lei-geral-de-protecao-de-dados/ > Acesso em: 30 de nov. 2020.

MEIRELLES, E. **Boas práticas de segurança digital para ISPs**. São Paulo. 2020. Disponível em: < https://everestridge.com.br/boas-praticas-de-seguranca-digital-para-isps/ > Acesso em: 15 de nov. 2020.

MINUTO DE SEGURANÇA. MINUTO DE SEGURANÇA. **5 Melhores Práticas para a Prevenção da Violação de Dados em 2019**. 2019. Disponível em: < https://minutodaseguranca.blog.br/5-melhores-praticas-para-a-prevencao-da-violacao-de-dados-em-2019/ > Acesso em: 11 de dez. 2020.

MOURA, P.R., ANDRADE, D. C. M. **O Direito de Consentimento Prévio do Titular para o Tratamento de Dados Pessoais no Ciberespaço**. Goiânia. Revista de Direito Governança e Novas Tecnologias. 2019. Disponível em: < https://www.indexlaw.org/index.php/revistadgnt/article/view/5568 >. Acesso em: 07 de nov. 2020.

MULLER, M. **Quais são e para que servem as normas de segurança da informação?** São Paulo. 2017. Disponível em :<http://anyconsulting.com.br/wp-content/cache/page_enhanced/www.anyconsulting.com.br/normas-de-seguranca-da-informacao/_index_ssl.html_gzip > Acesso em: 20 de nov. 2020.

NETTO, T. **Boas Práticas de Governança na proteção de Dados: o Programa de Governança em Privacidade**. Rio de Janeiro. Instituto de Direito Real. 2020. Disponível em:

< https://direitoreal.com.br/artigos/boas-praticas-de-governanca-na-protecao-de-dados-o-programa-de-governanca-em-privacidade > Acesso em: 12 de dez. 2020.

NORONHA e NOGUEIRA ADVOGADOS. NORONHA e NOGUEIRA ADVOGADOS. **LGPD: Treinamento dos Colaboradores é Essencial – Importância do Treinamento das Equipes**. São Paulo. 2020. Disponível em: < https://noronhaadv.com.br/lgpd-treinamento-dos-colaboradores-e-essencial/ > Acesso em: 23 de nov. 2020.

OLIVEIRA, C. E. E. de. **Aspectos Principais da Lei nº 12.965, de 2014, o Marco Civil da Internet: subsídios à comunidade jurídica**. Brasília: Núcleo de Estudos e Pesquisas/CONLEG/ Senado, 2014. Disponível em:< https://www12.senado.leg.br/publicacoes/estudos-legislativos/tipos-de-estudos/textos-para-discussao/td-148-aspectos-principais-da-lei-no-12.965-de-2014-o-marco-civil-da-internet-subsidios-a-comunidade-juridica >. Acesso em: 15 de abr. 2021.

OLIVEIRA, F. N. S. C. de. **Gestão de riscos no direito fundamental à privacidade de dados pessoais no Processo Judicial Eletrônico/Diário de Justiça Eletrônico**. Brasília. Repositório RIUnB UnB. 2020. Disponível em: < https://repositorio.unb.br/handle/10482/39152 > Acesso em: 08 de dez. 2020.

BELLUNO. BELLUNO**. O Mercado de Pequenos Provedores de Internet no Brasil**. Caçapava do Sul. 2021 Disponível em: < https://bellunotec.com.br/blog/o-mercado-de-pequenos-provedores-de-internet-no-brasil/ > Acesso em: 10 de nov. 2020.

PALMA, F. **Sistema de Gestão de Segurança da Informação (SGSI)**. 2017. Disponível em: < https://www.portalgsti.com.br/2016/12/sistema-de-gestao-de-seguranca-da-informacao-sgsi.html > Acesso em: 20 de nov. 2020.

PESSOA C., OLIVEIRA C., e NUNES B. **Efeitos e Projeções sobre a Vigência da Lei Geral de Proteção de Dados (LGPD) e o Papel do Encarregado dos Dados Pessoais**. São Paulo. Revista CONTECSI USP. 2020. Disponível em: < http://contecsi.submissao.com.br/arquivos/6598.pdf > Acesso em: 09 de nov. 2020.

PINHEIRO L. **A Segurança da rede na nova realidade dos provedores de serviços**. São Paulo. 2017. Disponível em: < https://www.abranet.org.br/Artigos/A-seguranca-da-rede-na-nova-realidade-dos-provedores-de-servicos-1337.html?UserActiveTemplate=site#.X81GPdhKiM8 > Acesso em: 14 de nov. 2020.

RAMOS, P. **Arquitetura da Rede e Regulação – a neutralidade da rede no Brasil**. São Paulo: Biblioteca Digital FGV, 2015. Disponível em < http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/13673/Arquitetura%20da%20Rede%20e%20Regula%C3%A7%C3%A3o%20-%20a%20neutralidade%20da%20rede%20no%20Brasil%20(PHSR,%20vers%C3%A3o%20final).pdf?sequence=3 > Acesso em: 08 nov. 2020.

RESULTADOS DIGITAIS. RESULTADOS DIGITAIS. **LGPD para Pequenas e Médias Empresas: passo a passo para se adequar e evitar multas**. Florianópolis. 2020. Disponível em: < https://resultadosdigitais.com.br/materiais-educativos/ebooks/lgpd-para-pmes/?external=1 > Acesso em: 21 de nov. 2020.

RODRIGUES, C. **LGPD: Qual deve ser o plano das empresas para se adequar à lei em 2020?**. São Paulo. 2019. Disponível em: < https://tiinside.com.br/10/12/2019/lgpd-qual-deve-ser-o-plano-das-empresas-para-se-adequar-a-lei-em-2020/ > Acesso em: 27 de nov. 2020.

ROJAS, M. A. T. **Avaliação da adequação do Instituto Federal de Santa Catarina à Lei Geral de Proteção de Dados Pessoais**. Santa Catarina. 2020. Disponível em: < https://repositorio.ifsc.edu.br/handle/123456789/1433 > Acesso em: 09 de dez. 2020.

SABBAT, A. P. **O papel do "Encarregado" ou "Data Protection Officer" na LGPD**. São Paulo. 2019 Disponível em: < https://www.securityreport.com.br/destaques/o-papel-do-encarregado-ou-data-protection-officer-na-lgpd/#.X_z51dhKiM8 > Acesso em: 24 de nov. 2020.

SAMANTHA, A. **Segurança de dados e gestão de qualidade são focos na NDD**. Lages. 2020. Disponível em: < https://www.ndd.com.br/blog/nddcargo/iso-9001/ > Acesso em: 28 de nov. 2020.

SANTANA, F. **LGPD: implantação leva tempo**. Brasília. 2020. Disponível em: < https://modal.org.br/quanto-tempo-para-implementar-a-lgpd-na-minha-empresa/ > Acesso em: 28 de nov. 2020.

SERPRO. SERPRO. **O que são dados anonimizados, segundo a LGPD**. Brasília. 2020. Disponível em: < https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-anonimizados-lgpd#:~:text=O%20que%20s%C3%A3o%20dados%20anonimizados%2C%20segundo%20a%20LGPD&text=A%20Lei%20Geral%20de%20Prote%C3%A7%C3%A3o,n%C3%A3o%20se%20aplicar%C3%A1%20a%20ele. > Acesso em: 02 de dez. 2020.

SERPRO. SERPRO. **Nos casos em que a base legal utilizada seja o consentimento, é você cidadão que define se e como seus dados pessoais podem ser tratados por terceiros**. Brasília. 2020. Disponível em: < https://www.serpro.gov.br/lgpd/cidadao/seu-consentimento-e-lei > Acesso em: 03 de dez. 2020.

SILVEIRA, S. A.; AVELINO, R.; SOUZA, J. **A privacidade e o mercado de dados pessoais**. Rio de Janeiro, Liinc em Revista. 2016. Disponível em: < http://dx.doi.org/10.18617/liinc.v12i2.902. >. Acesso em: 10 de fev. 2021.

SILVA, E. L. da. **Metodologia da pesquisa e elaboração de dissertação**. 3 ed. Florianópolis. Atual, 2001.

SOUZA, W. I. de. **Proteção de dados pessoais do consumidor online**. 2017. Dissertação (Especialização em Direito do Consumidor e Direitos Fundamentais) – Faculdade de Direito, Universidade Federal do Rio Grande do Sul. Porto Alegre. 2017. Disponível em: < https://lume.ufrgs.br/handle/10183/179003 > Acesso em: 16 de nov. 2020.

TBOOM. TBOOM. **LGPD: Conheça os direitos dos usuários e deveres das empresas**. São Paulo. 2020. Disponível em: < https://tboom.net/blog/lgpd-conheca-os-direitos-dos-usuarios-e-deveres-das-empresas/ > Acesso em: 01 de dez. 2020.

TEFFÉ, C. S. DE, VIOLA, M. **Tratamento de dados pessoais na LGPD: estudo sobre as bases legais**. Rio de Janeiro. Civilistica. 2020. Disponível em:< http://civilistica.com/tratamento-de-dados-pessoais-na-lgpd/ >. Acesso em: 10 de nov. 2020.

TEIXEIRA, T. **Empresas e a implementação da lei geral de proteção de dados**. Salvador. Editora JUSPODIVM. 2020. 480 p. Disponível em: < https://www.editorajuspodivm.com.br/cdn/arquivos/7c1ab637b2d1136fc1067a3992899546.pdf >Acesso em: 18 nov. 2021.

TIINSIDE.TIINSIDE **ABRADi lança certificação para LGPD e cartilha de Proteção de Dados Pessoais**. São Paulo. 2019. Disponível em: < https://tiinside.com.br/29/08/2019/abradi-lanca-certificacao-para-lgpd-e-cartilha-de-protecao-de-dados-pessoais/ > Acesso em: 06 de dez. 2020.

BL CONSUTÓRIA. BL CONSULTÓRIA. **Série LGPD na Prática: O que é e como fazer um RIPDP – Relatório de Impacto à Proteção de Dados**. São Paulo. 2020. Disponível em: < https://blconsultoriadigital.com.br/serie-lgpd-na-pratica-ripdp-relatorio/ > Acesso em: 05 de dez. 2020.

VASCONCELOS K. **Os benefícios da implementação da LGPD**. Brasília. 2020. Disponível em: < https://www.serpro.gov.br/lgpd/noticias/2020/beneficios-riscos-lgpd-empresas > Acesso em: 18 de nov. 2020.

VIOLINO, B. **GDPR: 4 passos para uma auditoria em conformidade com a lei**. 2018. Disponível em: < https://computerworld.com.br/seguranca/gdpr-4-passos-para-uma-auditoria-em-conformidade-com-a-lei/ > Acesso em: 04 de dez. 2020.

WIKIPÉDIA. **Autoridade Nacional de Proteção de Dados.** 2019. Disponível em:<https://pt.wikipedia.org/wiki/Autoridade_Nacional_de_Prote%C3%A7%C3%A3o_de_Dados > Acesso em: 08 de nov. 2020

YANDRA, B. F. F. **A Responsabilidade do Provedor de Aplicação pelo Armazenamento e Fornecimento da Porta de Origem do Endereço IP, sob a ótica do Marco Civil da Internet**. Brasília. Caderno Virtual. 2019. Disponível em: < https://portal.idp.emnuvens.com.br/cadernovirtual/article/view/3462 > Acesso em: 09 de nov. 2020.

ZAMPERLIN E.; BORELLI A**. Segurança de dados: Boas práticas para mitigar riscos**. São Paulo. 2020. Disponível em: < https://blogbrasil.westcon.com/seguranca-de-dados-boas-praticas-para-mitigar-riscos > Acesso em: 10 de dez. 2020.

Apêndices

Apêndice A: MODELO DE CONSENTIMENTO DE USO DOS DADOS.

Tipo: Termo de Consentimento para Tratamento de Dados Pessoais.

TERMO DE CONSENTIMENTO PARA TRATAMENTO DE DADOS PESSOAIS

[NOME DO PEQUENO PROVEDOR DE INTERNET]

[ENDEREÇO DO PEQUENO PROVEDOR]

[TELEFONE E ENDEREÇO ELETRÔNICO DO PEQUENO PROVEDOR]

Este documento visa registrar a manifestação livre, informada e inequívoca pela qual o Titular

concorda com o tratamento de seus dados pessoais para finalidade determinada, em conformidade com a Lei nº 13.709 – Lei Geral de Proteção de Dados Pessoais (LGPD).

Ao manifestar sua aceitação para com o presente termo, o Titular consente e concorda que a

NOME DO PEQUENO PROVEDOR, CNPJ do Pequeno Provedor, Endereço do Pequeno Provedor, Telefone do Pequeno Provedor, E-mail do Pequeno Provedor, doravante denominado Controlador, realize o tratamento dos dados pessoais especificados (tabela 1. Tratamento de Dados Pessoais) com a finalidade de cadastrar o titular como usuário/cliente dos serviços de telecomunicações em sistema informatizado ou físico, assim quando necessários realizar demais ações que envolvam questões técnicas, financeiras e jurídica, pelo período de vigência da temporalidade do processo administrativo.

Dados do(a) Identificado(a):

Nome Completo do Titular: _____

Documento de Identidade: _____ CPF: _____

Tabela 1:Tratamento de Dados Pessoais:

Dados pessoais	
Finalidade	
Forma do tratamento:	
Duração do tratamento:	
Compartilhamento previsto:	
Legislação	

Estou ciente que nos termos da Lei nº 13.709, de 14 de agosto de 2018, meus dados serão mantidos em formato interoperável com a finalidade de cadastrar o titular como usuário/cliente dos serviços de telecomunicações em sistema informatizado ou físico, assim quando necessários realizar demais ações que envolvam questões técnicas, financeiras e jurídica, pelo período de vigência da temporalidade da prestação de serviço. Tomei conhecimento que tenho direito a obter NOME DO PEQUENO PROVEDOR, a qualquer momento e mediante requerimento, as seguintes informações sobre meus dados por ela tratados, com exceção daqueles que assegurem a segurança do Estado e da sociedade:

a) confirmação da existência de tratamento;

b) acesso aos dados;

c) correção de dados incompletos, inexatos ou desatualizados;

d) informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

e) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei nº 13.709;

f) portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos

comercial e industrial;

g) eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da Lei nº 13.709;

h) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

i) revogação do consentimento, estando ciente que tal revogação impossibilita a manutenção do cadastro de usuário externo em sistema informatizado de gestão de documentos da Universidade.

Cidade, UF. Em ___ de _____ de _____.

_____

Nome completo do Titular dos dados ou Responsável Legal

Apêndice B: FORMULÁRIO DE SOLICITAÇÃO DE INFORMAÇÕES.

Tipo: Modelo de Formulário de Solicitações e Direitos dos Titulares.

FORMULÁRIO
DE SOLICITAÇÃO DE INFORMAÇÕES DE DADOS PESSOAIS

Prezado(a) Sr(a).

De acordo com a Lei N° 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD) que (Dispõe sobre o tratamento e proteção de dados pessoais), **SOLICITO** a V.S.ª. exercer meu direito como **TITULAR DOS DADOS** para a seguinte situação:

(Confirmação de existência de tratamento;
( ) Acesso aos dados;
( ) Correção ou atualização dos dados;
( ) Anonimização, bloqueio ou eliminação de dados tratados em desconformidade com a lei;
( ) Informações das entidades públicas e privadas com as quais os dados foram compartilhados;
( ) Vedação de compartilhamento de dados;
( ) Exclusão de dados pessoais tratados com o consentimento;
( ) Revogação do consentimento;
( ) Oposição de tratamento de dados tratados com o Legítimo Interesse nos termos da Política de Privacidade;
( ) Outros _____

DADOS DO TITULAR SOLICITANTE

Nome completo:	
RG:	**CPF:**
E-mail:	**Celular:**

Dados necessário para localização perfeita do titular

Declaro sob as penas da lei, que são verdadeiras as informações prestadas neste formulário.

_____
Assinatura do titular

Apêndice C: MODELO DE COMUNICAÇÃO COM AS ENTIDADES.

Tipo: Comunicado Oficial sobre Incidente.

COMUNICADO OFICIAL

INCIDENTE DE CIBERSEGURANÇA

A propósito de supostos vazamentos de informações de beneficiários do Sistema divulgados na imprensa nas últimas semanas, a empresa esclarece que possui sistema de gestão operacional próprio, política de segurança da informação e mecanismos tecnológicos que visam garantir a privacidade, o sigilo e a proteção dos dados de seus beneficiários. A empresa informa que, até o presente momento, não tem conhecimento de ocorrências que fragilizem a segurança de dados de beneficiários desta operadora

Com relação à Lei Geral de Proteção de Dados Pessoais (LGPD). Como se trata de legislação de expressiva relevância, a empresa já vem trabalhando nas adequações necessárias para atuar em conformidade com os termos da Lei.

Em nota a empresa informa que as operações se mantêm absolutamente normais e que, devido à identificação de ocorrências em empresas fornecedoras um intenso esforço de correção e proteção de dados já está sendo empenhado minimizando qualquer efeito adverso à marca e às atividades

Atenciosamente,
Diretoria

Apêndice D: REQUERIMENTO DE ELIMINAÇÃO DOS DADOS.

Tipo: Registro de Eliminação dos Dados.

Pedido de eliminação de dados às empresas - LGPD

LOCAL, DATA .

À **Nome da Empresa**

Em atendimento à Lei Geral de Proteção de Dados (LGPD), por solicitação do titular _____ , inscrito no CPF sob nº _____ . solicita que os dados pessoais sejam eliminados em observância ao Art. 18, §6º e Art. 16 da LGPD.

Atenciosamente,