TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

ADRIANO DA SILVA LOURENÇO FINCO

DANIEL OLIVEIRA DA SILVA

DANILO NASCIMENTO BRITO

MATHEUS FREGNANI MACAUBA

WILLIAM FELIPE PAULO DA SILVA

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

APLICAÇÃO WEB PARA UMA ABORDAGEM NORTEADORA DE IMPLEMENTAÇÃO DA LEI

São Caetano do Sul / SP

2020

ADRIANO DA SILVA LOURENÇO FINCO
DANIEL OLIVEIRA DA SILVA
DANILO NASCIMENTO BRITO
MATHEUS FREGNANI MACAUBA
WILLIAM FELIPE PAULO DA SILVA

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

APLICAÇÃO WEB PARA UMA ABORDAGEM NORTEADORA DE IMPLEMENTAÇÃO DA LEI

Trabalho de Conclusão de Curso apresentado á FATEC São Caetano do Sul como exigência para a conclusão da graduação em Tecnólogo em Segurança da Informação.

Orientador: Me. Kleber da Silva Divino

São Caetano do Sul / SP
2020

FATEC – FACULDADE DE TECNOLOGIA "ANTONIO RUSSO"

TRABALHO DE CONCLUSÃO DE CURSO
TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

ADRIANO DA SILVA LOURENÇO FINCO
DANIEL OLIVEIRA DA SILVA
DANILO NASCIMENTO BRITO
MATHEUS FREGNANI MACAUBA
WILLIAM FELIPE PAULO DA SILVA

BANCA EXAMINADORA

_____

Prof.: Kléber Silva Divino – Orientador

_____

Prof.: Jacinto Carlos Ascêncio Cansado - Banca

_____

Prof.: Cléber Milanez - Banca

São Caetano do Sul / SP
2020

Dedicamos esse trabalho aos nossos amigos e familiares pelas alegrias, tristezas e dores compartilhadas. A todos os professores que nos acompanharam e auxiliaram durante toda a trajetória do curso.

AGRADECIMENTOS

Agradecemos aos nossos familiares que estiveram sempre nos apoiando e depositando sua confiança em cada um de nós, que nos motivaram quando desanimados e alegraram em meio às dificuldades que enfrentamos.

A todos os professores por nos proporcionar o conhecimento não apenas racional, mas a manifestação de caráter e afetividade da educação no processo de formação profissional, por tanto que se dedicaram a nós.

“A percepção do desconhecido é a mais fascinante das experiências. O homem que não tem os olhos abertos para o misterioso passará pela vida sem ver nada.”
(Albert Einstein)

RESUMO

O crescimento tecnológico em nível mundial vem se tornando cada vez mais frequente, e tem impactado efetivamente no cotidiano das cidades e pessoas. Principalmente no contexto da Segurança da Informação, que hoje está em grande expansão, pois não há como pensar em desenvolvimento tecnológico sem pensar em como esse desenvolvimento afeta de maneira intrusiva na realidade física e digital das pessoas. O Brasil está se adaptando a esse momento de desenvolvimento tecnológico no âmbito de privacidade e segurança digital pessoal com a criação da Lei Geral de Proteção dos Dados Pessoais (Lei 13.709/2018). Esse trabalho tem o intuito de, por meio de uma aplicação que utiliza qualquer navegador de internet, orientar gestores ou responsáveis na área de tecnologia para o planejamento da implementação da LGPD em suas organizações, com perguntas e respostas claras visando diminuir a dificuldade de compreensão e adequações necessárias perante a nova lei, assim gerando um retorno palpável sobre os pontos principais que podem não estar em conformidade.

Palavras-chave: Segurança da Informação, Privacidade Digital Pessoal, LGPD, Dados Pessoais.

ABSTRACT

Technological growth worldwide is becoming more and more frequent and has effectively impacted the daily lives of cities and people. Especially in the context of Information Security, which today is very expansion, as there is no way to think about technological development without thinking about how this development affects in an intrusive way in people's physical and digital reality. Brazil is adapting to this moment of technological development in the scope of privacy and personal digital security with the creation of the General Law for the Protection of Personal Data (Law 13.709 / 2018). This work aims to, through an application that uses any internet browser, guide managers or responsible in the technology area for planning the implementation of LGPD in their organizations, with clear questions and answers in order to reduce the difficulty of understanding and necessary adaptations in the face of the new thus generating a tangible return on key points that may not be in compliance.

Keywords: Information Security, Personal Digital Privacy, LGPD, Personal Data.

LISTA DE FIGURAS

LISTA DE TABELAS

Sumário

INTRODUÇÃO

Milhões de pessoas no Brasil conectam-se à internet diariamente para trocar informações, fazer transações bancárias, trabalharem remotamente, armazenar dados na nuvem, pesquisar, entre outras ações, assim formando uma grande gama de dados para as empresas responsáveis pelo resguardo dos dados pessoais de seus usuários. O grande desafio da era digital é a segurança da informação, que vem tomando um grande destaque na função estratégica de uma empresa, pois é essencial para um alicerce bem estruturado de qualquer organização. Diversas áreas estão caminhando para uma cultura cheia de inovações tecnológicas, que antes pareciam uma promessa tão distante, apenas em cenários de filmes futuristas, mas agora já faz parte da rotina de milhões de empresas.

Até meados de 2018 não existiam leis específicas para a proteção de dados pessoais no Brasil. Nesse contexto surge a LGPD, isto é, a lei Geral de Proteção de Dados Pessoais, que estabelece padrões e regulamenta a forma como as empresas, sejam elas de qualquer ramo, manipulam os dados pessoais armazenados de clientes, terceiros, colaboradores, ou seja, dados pessoais dos envolvidos diretamente com a organização nos seus processos de negócios. Quando relacionamos LGPD a empresas, logo nos vem à cabeça formulários, relatórios e contratos todos de forma eletrônica, porém a lei é válida não necessariamente só para a parte de armazenamento eletrônico, ou seja, dados registrados em qualquer meio físico, como papel, também são válidos. Convergindo com a realidade brasileira, torna-se necessário que as empresas se adaptem aos novos padrões de segurança da informação a serem seguidos, porém, pode-se tornar uma tarefa complexa devido ao fato da lei ser extensa, dessa forma surge a necessidade de uma abordagem simplificada dos requisitos legais apresentados para responder a pergunta: como adequar empresas à LGPD?

O presente estudo tem como objetivo específico analisar, por meio de uma aplicação WEB, o nível de conformidade de empresas à nova lei, de forma que funcione como uma consultoria, apontando os principais pontos que não estão em conformidade, trazendo assim um discernimento claro de forma a elaborar e dinamizar o processo de implementação. O Objetivo geral do trabalho é aprofundar o entendimento sobre a LGPD, ao mesmo tempo em que simplificamos os pontos críticos necessários para se estar em conformidade.

A metodologia utilizada compreende a estrutura de pesquisa explicativa, fontes bibliográficas e resultados qualitativos e quantitativos. O método foi desenvolvido de forma a analisar e identificar os fatos relacionados ao tema e aos seus objetivos propostos, de modo que estruture e conceda o entendimento claro. O levantamento bibliográfico foi realizado a partir de fontes secundárias, ou seja, livros, artigos, periódicos e textos disponíveis em sites confiáveis.

Ao decorrer do estudo será apresentado uma breve explicação sobre segurança da informação no primeiro capítulo, seus principais pilares, alguns conceitos importantes e exemplos de casos que realmente aconteceram, tudo para enfatizar e situar sobre o elo entre segurança da informação e LGPD. No segundo capítulo será apresentado, de forma objetiva, um apanhado sobre a LGPD, já no terceiro capítulo será abordado a implementação da LGPD e, por fim, no último capítulo será apresentado a ferramenta WEB.

1 SEGURANÇA DA INFORMAÇÃO

A expressão segurança da informação, em geral, tem sido associada a sistemas informatizados e aos dados que estes manipulam. Diz respeito a uma série de aspectos associados à tecnologia da informação, como por exemplo, controle de acesso a recursos, segurança em comunicação, gestão de riscos, políticas de informação, sistemas de segurança, diretrizes legais, segurança física, criptografia, dentre outros, porém, existem três pilares da segurança da informação: Confidenciabilidade, Integridade e Disponibilidade (KIM; SOLOMON, 2014).

Figura 1 – Pilares de segurança da informação

Fonte: Matsunaga, 2017

A segurança da informação é a proteção da informação quanto a vários tipos de ameaças, de modo a garantir a continuidade do negócio, minimizar os riscos, maximizar o retorno sobre o investimento e as oportunidades de negócio:

> Preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas. (NBR ISO/IEC 27002:2005).

De acordo com o relatório de informações de segurança cibernética, publicado em 2016 pela empresa Norton, 42.4 milhões de usuários brasileiros foram

afetados por crimes de natureza cibernética, um prejuízo financeiro de 10.3 bilhões de dólares (NORTON, 2016). Em uma comparação global com 21 países, dentre eles Canadá, Estados Unidos, Alemanha, França, Itália, Japão e Reino Unido, 689.4 milhões de usuários foram afetados pelo cibercrime, que gerou um prejuízo de 125.9 bilhões de dólares, isso demonstra o quanto somos vulneráveis e o quanto a busca por segurança, mesmo com leis nos protegendo, tem que ser incentivada.

1.1 Confidencialidade

Segundo Igor Matsunaga (2018) a confidencialidade é o pilar que está diretamente relacionado aos procedimentos e métodos que garantem o controle de acesso as informações sensíveis, assim restringindo os dados apenas a quem está autorizado. Outrossim, conforme Starling e Brown (2014), o pilar da confidencialidade é responsável pela preservação de acessos autorizados, disponibilizando-os as informações pertinentes, e, também, alternativas de proteção à privacidade individual e as informações proprietárias.

1.2 Integridade

Na visão de Benetti (2015), o pilar da integridade significa a garantia de que a informação sendo transferida ou armazenada está íntegra e será apresentada de forma correta para quem consultá-la a informação. Esse pilar é absolutamente crítico do ponto de vista operacional tendo em conta o volume de dados trafegadas em um ambiente empresarial e a crescente troca de informações, seu enfraquecimento leva a uma série de grandes impactos as organizações, como por exemplo, a ineficiência, isto é, gastar mais pelo mesmo resultado, gerando menor margem de lucro.

Conforme a ISO/IEC 27000:2018, integridade é obter a garantia de que as mensagens não sofreram alterações e, tampouco foram duplicadas, repetidas ou tiveram a sua ordem alterada.

1.3 Disponibilidade

Segundo Matsunaga (2018), a disponibilidade é o pilar que trata da acessibilidade dos dados e sistemas da empresa, ou seja, as informações devem estar sempre disponíveis.

De acordo com Benetti (2015), disponibilidade significa a garantia de que a informação está disponível sempre para quem necessitar da mesma. Esse pilar está intimamente relacionado com questões operacionais das companhias, já que todos os processos organizacionais dependem de uma busca de informações, sabendo isso, a indisponibilidade da informação tem a capacidade de parar completamente os processos, o que pode levar ao cessar do lucro, ou até prejuízo.

1.4 Autenticidade

Outro pilar muito importante, conforme Matsunaga (2018), é a autenticidade. Esse princípio trata de garantir que toda informação vem de uma fonte confiável para que tenham sua autoria e originalidade confirmadas com objetivo de garantir que a identidade do remetente da informação enviada.Ainda segundo Matsunaga (2018), a autenticidade garante que a identidade do emissor, com isso gera o não-repúdio, o não-repúdio ocorre quando se tem garantia de que o remetente da informação não poderá negar a autoria da informação (Irretratabilidade). É através da autenticidade que se garante que a mensagem é proveniente da fonte anunciada.

1.5 Conceito de Vulnerabilidade

Com base no NIST 800-30 (NIST, 2012) podemos definir vulnerabilidade como uma falha ou fraqueza nos procedimentos de segurança do sistema, design, implementação ou controles internos que podem ser exercidos (acionados acidentalmente ou explorados intencionalmente) e resultam em uma violação da segurança ou uma violação da política de segurança do sistema.

1.6 Conceito de Ameaça

Beal (2008, p.14) define ameaça como sendo a expectativa do acontecimento acidental ou proposital, causado por um agente, que pode afetar um ambiente, sistema ou ativo de informação. Os agentes podem ser o meio ambiente, pessoas más intencionadas, sistemas maliciosos, entre outros.

Segundo Torres (2015, p.15) há dois tipos de ameaças acidentais e propositais. Acidentais são falhas de hardware, desastres naturais, erros de programação entre outros, enquanto ameaças propositais caracterizam-se como roubos, invasões, fraudes, dentre outros. Dentro do tópico de ameaças acidentais temos duas classificações diferentes, são elas Dias (2000, p.57):

- Ativas: envolve o ato de alterar algum dado.
- Passivas: envolve invasões, espionagem, mas sem alterar as informações.

1.7 Conceito de Ataques

Segundo Beal (2008, p.14), trata-se de um evento decorrente da exploração de uma vulnerabilidade por uma ameaça, já para Lopes (2019) um ataque é um movimento destrutivo gerado por *hackers*, em sistemas, redes ou infraestruturas utilizando de diferentes tipos de métodos e recursos para prejudicar seu alvo, ou por interesse próprio, sem a autorização ou permissão de acesso. Em outras palavras é a invasão não autorizada a qualquer tipo de informação, sistema, ou dispositivo de forma a concretizar a ameaça através de uma vulnerabilidade. A Cartilha de Segurança para Internet classifica e define alguns ataques, eles são (CERT.BR, 2017):

- **Engenharia social –** Técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações.

- **Varredura em redes (scan) –** Consiste em efetuar buscas minuciosas em redes, com o objetivo de identificar computadores ativos e coletar informações sobre eles como, por exemplo, serviços disponibilizados.

- **Negação de serviço distribuída (DoS ou DDoS) –** Negação de serviço, ou DoS (Denial of Service), é uma técnica pela qual um atacante utiliza um computador para tirar de operação um serviço, um computador ou uma rede conectada à Internet. Quando utilizada de forma coordenada e distribuída, ou seja, quando um conjunto de computadores é utilizado no ataque, recebe o nome de negação de serviço distribuído, ou DDoS (Distributed Denial of Service).

- **Força bruta (Brute Force) –** Consiste em adivinhar, por tentativa e erro, um nome de usuário e senha de um serviço ou sistema. Invasão ou comprometimento – ataque bem sucedido que resulte no acesso, manipulação ou destruição de informações em um computador.

- **Desfiguração de página (Defacement) –** Consiste em alterar o conteúdo da página Web de um site.

- **Interceptação de tráfego (Sniffing) -** Interceptação de tráfego, ou sniffing, é uma técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos chamados de sniffers.

- **Ransomware -** Trata-se de um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (ransom) para restabelecer o acesso ao usuário.

- **Furto de identidade (Identity theft) -** O furto de identidade, ou identity theft, é o ato pelo qual uma pessoa tenta se passar por outra, atribuindo-se uma falsa identidade, com o objetivo de obter vantagens indevidas. Alguns casos de furto de identidade podem ser considerados como crime contra a fé pública, tipificados como falsa identidade.

- **Phishing -** É o tipo de técnica por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.

1.8 Casos reais de ataques cibernéticos

Abaixo será apresentado alguns casos sobre ataques cibernéticos e vazamento de dados através dos métodos e técnicas citadas anteriormente.

1.8.1 *Wannacry*

De acordo com PROOF (2017), WannaCry foi descoberto durante um ataque massivo em diversos países em 12 de maio de 2017. Segundo diversos reportes, foram afetados no total mais de 300.000 sistemas em pelo menos 150 países foram severamente danificados. O ataque afetou uma grande gama de setores, incluído sistema de saúde, governo, telecomunicação e indústria de gás e óleo.

Esse tipo de ataque cibernético não é novo e seu efeito imediato nas empresas é conhecido após os precedentes sofridos pelo Google em 2010 ou pela Sony Pictures em 2014 (PROOF, 2017): a paralisia do computador do sistema e o pedido de pagamento de um resgate. No entanto, além dos efeitos meramente econômico-financeiros e da paralisação técnica dos processos das empresas, de duração efêmera, as crises de reputação que possam surgir são o verdadeiro problema que enfrentam.

Figura 2 – Impactos causados pelo ataque Wannacry

Fonte: PROOF, 2017

A dificuldade de se proteger contra Wannacry foi de sua habilidade de se espalhar para outros sistemas utilizando “worm componentes” (componentes minhoca). Essa característica faz com que o ataque seja mais efetivo e que a vítima não tenha um mecanismo de defesa que reaja rapidamente e em tempo real, ou seja, o WannaCry tem um componente para criptografar os arquivos da máquina baseado em criptografia de chave pública (PROOF, 2017).

1.8.2 *Edward Snowden*

Segundo Greenwald (2014), o caso Snowden pode ser considerado como a maior quebra de privacidade digital da história, tendo em vista o fato do agente ativo ser a Agência de Segurança Nacional do governo dos Estados Unidos, a prestigiosa NSA (National Security Agency), em parceria com uma agência de inteligência britânica, a GCHQ (Government Communications Headquarters), e as vítimas variarem de cidadãos americanos a governos externos e todas as linhas comunicações regentes de seus países tendo suas comunicações espionadas. A NSA espionava quase todo o tráfego de informações dos cidadãos americanos através de um software chamado PRISM que possibilitava identificar toda a interação de determinado usuário na internet. Isso foi possível através da invasão de links de comunicação de duas das maiores empresas de tecnologia americanas: Google e Yahoo. Após da invasão dos links, o sistema monitorava todo o tráfego de informação presente e com isso possibilitava à agência espionar não só a atividade online de usuários americanos, mas também de todos ao redor do mundo que tinham suas informações compartilhadas através desse link.

Greenwald (2014) ainda diz que outro sistema, o XKeyscore, estaria hospedado em várias localidades ao redor do mundo, em países como Rússia, China, e em grande quantidade na América Latina e até mesmo no Brasil. A principal característica desse sistema e questionavelmente a mais ofensiva é a sua habilidade de explorar falhas de aplicativos presentes em grandes quantidades de aparelhos interceptando informações de usuários e expondo toda a sua atividade online.

O caso Snowden teve consequências políticas que levaram representantes da Agência Nacional de Segurança dos Estados Unidos a responderem

questionamentos do senado sobre suas atividades. Pedidos de verba para novos projetos foram negados, as relações com aliados do Governo Americano foram estreitadas e a preocupação global sobre existir uma entidade que vigia cada passo de cada usuário no mundo aumentou, levando o ex-presidente dos Estados Unidos, Barack Obama, a rever e propor mudanças na forma como a agência americana atuava (GREENWALD, 2014)

Mediante aos fatos descritos e técnicas utilizadas para a obtenção de dados de propriedade individual, é possível visualizar a vasta quantidade de métodos e procedimentos que são utilizados de maneira infratora para a obtenção de dados de pessoas. O que nos leva a pensar, se existem medidas regulatórias embasadas por lei, que nos asseguram, que nossas informações estão recebendo as devidas tratativas de segurança. Nesse contexto surgiu a Lei Geral De Proteção De Dados que será analisada no próximo capítulo.

2 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Segundo o Artigo Um Novo mundo de Dados (SILVA, 2017), apesar da infinidade de recursos disponíveis na internet para utilização de pessoas e para fins pessoais, o fluxo constante de informações geradas por pessoas é muito grande. A cada acesso, dados são solicitados em vários tipos de plataformas, e a exigência é que se forneçam informações padrões como nome, idade, endereço, cep, número de telefone, dentre outros vários tipos de solicitações, o que faz com que divulguemos informações que, na verdade, não são necessárias para o conteúdo que queremos acessar.

Portanto, poderíamos nos questionar: Quais sãos os métodos utilizados para o tratamento destes dados? Quem é o responsável por eles? O que acontece com tais dados após a confirmação das informações e o acesso ao conteúdo requerido? As respostas podem parecer sem fim quando paramos para pensar nas medidas por trás da tela. Por isso, vários países ao redor do mundo têm se precavido com controles “internos” que regulamentam processos que passam dentro de seu território, de modo a buscar formas de proteger algo que tem sido considerado como o novo petróleo (CAVALCANTI, 2019) do mundo, os dados. Em paralelo, o Brasil em 14 de agosto de 2018 aprovou a lei que traz consigo os mesmos princípios desenvolvidos na GDPR, qual seja a Lei 13.709/2018, também conhecida como a Lei Geral de Proteção de Dados (LGPD), e que tem como principal objeto, regulamentar diretrizes que firmem o compromisso do tratamento dos dados dos brasileiros, incluindo normatização para quaisquer que sejam os tipos de empreendimentos que quiserem se utilizar e usufruir deles.

2.1 Classificação e conceitos sobre dados

Segundo o texto do Art. 1º da LGPD, a lei traz consigo um conjunto de tratativas e normas relacionadas aos dados de brasileiros, denominados “titulares”. Para cada dado, existe uma classificação que determina a fragilidade e quais são os tipos de dados que a compõem, além de sua importância, como se verifica nos três tipos de dados estabelecidos pelo artigo 5º, incisos I, II e III do referido diploma legal (BRASIL, 2018):

Dado pessoal: Informação relacionada a pessoa natural identificada ou identificável;

Dado sensível: Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Dado anonimizado: Dado relativo à titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

Assim, com base nessa classificação, são originadas diferentes formas de tratamento por parte da lei, guiando os responsáveis sobre como agir no tratamento destes dados. Ainda, segundo o artigo 5º, inciso X da LGPD, a definição de tratamento de dados é:

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

A LGPD também define como controladores, operadores e encarregados os responsáveis pelo tratamento dos dados, por ordem de responsabilidade sobre os dados tratados, conforme consta em seu artigo 5º, incisos VI, VII e VIII (BRASIL, 2018):

Controlador: Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

Operador: Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

Encarregado: Pessoa indicada pelo controlador e operador para atual como canal de comunicação entre o controlador, os titulares dos dados, e a Autoridade Nacional de Proteção de Dados (ANPD);

Vale mencionar que, pela análise do referido artigo 5º da lei 13.709/2018 (BRASIL, 2018), muitos outros conceitos importantes relacionados ao tema foram estabelecidos, devendo tal artigo sempre ser utilizado como referência e parâmetro para se definir a abrangência e correta aplicação desta lei.

2.2 Direitos do titular

Dentre os diferentes âmbitos abrangidos pela lei, a perda ou mal gerenciamento dos dados, trouxe uma visão fixa sobre a responsabilidade de empresas, tanto do setor privado quanto do setor público, sobre a manipulação dos dados dos titulares. E, diante deste cenário, é possível verificar que houve um enfoque maior quanto às medidas para que o cuidado com os dados tratados seja feito de maneira mais cuidadosa e responsável, favorecendo a privacidade dos titulares dos dados. Esse destaque é visível na deliberação dos direitos dos titulares sobre seus dados, abordados no artigo 18º (BRASIL, 2018), entre eles:

1º Acesso:

- Direito do titular de solicitar a exportação de cópias dos dados coletados;
- Informações sobre o modo de coleta e armazenamento;
- Possibilidade de selecionar um período de intervalo de informação;
- Especificar formatos de envio dos dados do solicitante (titular) para o Controlador;

2º Cancelamento:

- Requisição de exclusão dos dados pessoais;
- Requisição de anonimização ou bloqueio dos dados;
- Revogação do consentimento;

3º Retificação:

- Atualizar, ou consertar dados;

4º Explicação:

- Esclarecimento sobre os elementos ou decisões automatizadas dadas a partir de dados do titular;

5º Portabilidade:

- Solicitar transferência de dados entre plataformas ou de uma para outra;

Assim, através desses direitos, a lei busca em sua essência tratar com o dever e a responsabilidade dos controladores, mesmo que sejam órgãos públicos, conforme os artigos 31º e 32º, para que trabalhem em prol do cuidado, e com a responsabilidade de realizar quaisquer evento que envolvam dados dos titulares de maneira a priorizar a segurança de ambos, já que a lei também prevê sanções ao não cumprimento

dessas normas, conforme o artigo 42º e 52º e seguintes. As possíveis sansões administrativas são:

- Multa Simples
- Multa Diária
- Advertência
- Bloqueio de dados pessoais
- Publicização da infração
- Eliminação dos dados pessoais

Portanto, é possível notar que a LGPD trouxe diversos direitos protetivos para os titulares de dados e, também, diversos deveres restritivos para os controladores, operadores e encarregados pelos dados, como se nota pela leitura dos artigos 37º a 41º, o que demonstra a preocupação com a privacidade, sigilo e proteção de tais dados e de seus titulares. Aliás, a mesma preocupação está bem demonstrada nos princípios em que se fundamenta esta lei, como a qualidade de dados, a segurança e a prevenção, dentre outros estabelecidos no art. 6º.

2.3 Abrangência da LGPD

Como toda lei, medidas cabíveis são necessárias para a garantia de execução da mesma, e mediante a isso, a abrangência pelas quais a lei interage e se concretiza é de igual importância às suas medidas, segundo Priscilla Silva, Pesquisadora de Direito e Novas Tecnologias no Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio), o escopo da aplicação da lei gira em torno da teoria expansionista que resguarda uma abrangência extraterritorial demonstrando que o tratamento de dados (coletados, compartilhados, ou armazenados em solo brasileiro) obtido de brasileiros em território nacional, ou de turistas, por exemplo, que transitam no nosso país, precisa estar debaixo e em conformidade com os requisitos estipulados pela lei. Porém, quais seriam esses requisitos? Qual seria a abrangência de aplicação desta lei? Segundo o Artigo 3º, incisos I, II e III, esses requisitos são:

> Art. 3º Esta Lei 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:

> I - a operação de tratamento seja realizada no território nacional;
> II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência
> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional. (BRASIL, 2018)

A lei também traz consigo, além das abrangências já descritas, há também atribuições dadas aos *controladores* sobre o seu papel como responsável pelo tratamento dos dados. Muitas empresas de diversos ramos tem realizado grandes e variados tipos de gerenciamento dos dados em busca da proporção de facilidades que oferece, são infinitos os tipos de tratamentos que podem ser gerados e manejados a partir deste resultado, mas muito mais do que isso, é grande a responsabilidade daqueles que utilizam deste recurso, e a lei de forma bem clara, traz de maneira direta, quais requisitos precisam ser atendidos para que tais procedimentos aconteçam. Segundo o artigo 7º (BRASIL, 2018):

- Provar que o consentimento do titular foi obtido em conformidade com a LGPD
- Manter o registro de todas as operações de tratamento de dados pessoais que realizar
- Elaborar um relatório de impacto à proteção de dados, caso solicitado pela ANPD
- Informar o titular caso seja feita alguma alteração no tratamento dos dados
- Responder solidariamente junto com o *operador* caso haja danos a terceiros por violação a LGPD

Também são abordadas situações em que, em processos judiciais, os *controladores* não serão acometidos pelas sanções, conforme o artigo 43º, inciso I, II e III (BRASIL, 2018):

- Os *controladores* não realizarem o tratamento dos dados do titular
- Embora tenham realizado o tratamento de dados pessoais que lhe é atribuído, não houve violação à legislação de proteção de dados
- Seja comprovado que o dano sofrido é recorrente de culpa exclusiva do titular dos dados ou/e terceiros.

A aplicabilidade da lei é regida e busca em todo o seu conteúdo, trazer limites e responsabilidade para informações que hoje não possuem nenhum tipo de vistoria ou regimento. O funcionamento é fundamental para que se crie controles e a garantia de que os dados estão sendo transitados de maneira segura e consciente tanto pelo controlador, quanto pelo titular dos dados. No próximo capítulo será apresentado alguns métodos para que a implementação da LGPD venha acontecer de maneira efetiva.

3 IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS

Para Prata (2019), não existe uma implementação definitiva em termos de LGPD para empresas, tampouco uma metodologia oficial onde possamos nos embasar para a implementação da LPGD, pois empresas são organismos vivos com finalidades diferentes, e isso implica diretamente na questão da implementação, já que é possível que observemos que, no caso de implementações existem recursos e áreas diferentes. Então por que, após um descritivo introdutório, este trabalho iria possuir um tema tão controverso como implementação e desenvolvimento da LGPD? Pois, apesar da aparente controvérsia, o fato é que, com base em estudos, utilizamos de recursos disponibilizados por outros profissionais que norteiam uma possível implementação inicial que faça com que, através desses pilares da lei, seja possível se encaminhar rumo a resposta da grande pergunta: Como se adequar à Lei Geral de Proteção de Dados?

Segundo Lima (2019), existem alguns passos sugestivos que servirão para a criação de um fluxo de implementação que serão utilizados como base para o desenvolvimento deste capítulo, sendo eles:

1 – Definição do projeto
2 – Inventário e Classificação dos Dados
3 – Adequação de Políticas e Processos

Através desta abordagem, muitos âmbitos que são legíveis dentro de qualquer empresa serão abrangidos trazendo uma simplificação do que precisará ser feito, ou por onde começar.

3.1 Definição do projeto

É de extrema importância que, como todo projeto, exista a necessidade da criação de um projeto, onde sejam-se alinhados os passos que precisaram ser cumpridos para o alcance da conclusão do projeto e são esses passos:

3.1.1 *Criação de um Escopo*

A Criação de um Escopo para o projeto é um dos pontos iniciais para uma boa implementação, é necessário que sejam delimitados vários pontos gerais onde serão discutidos recursos, responsabilidades e o desenvolvimento do projeto em uma visão macro (Vieira 2019).

3.1.2 *Responsabilizações*

Segundo Lima (2019) essa fase inicial terá que ser regida por um DPO (Data Protect Officer) ou Encarregado pelo Tratamento dos Dados, que será responsável pelos dados e pela criação de métodos que envolvem todos o contexto de dados dentro da empresa, e seus dados para contato deverão estar dispostos em locais onde será possível a visualização pública, para que, caso exista a necessidade de tratativas de usuários, ele possa ser contactado, o que confere na solicitação a Lei a respeito de um profissional responsável pelo Tratamento dos Dados, também será responsável pela criação da equipe de trabalho que estará envolvida intimamente com o projeto de implementação.

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

3.1.3 *Criação Comitê de Proteção de Dados*

Também haverá a necessidade da criação de um Comitê de Proteção de Dados. Tais profissionais terão um papel fundamental para a viabilização de todos os processos de implementação da Lei na empresa, por isso, devem fazer parte do círculo das principais áreas dela, principalmente as áreas que possuem uma grande demanda de dados circulados. Há um organograma que reflete no resultado deste comitê, apresentado por Lima (2019)

3.1.4 *Treinamento de recursos e atribuições*

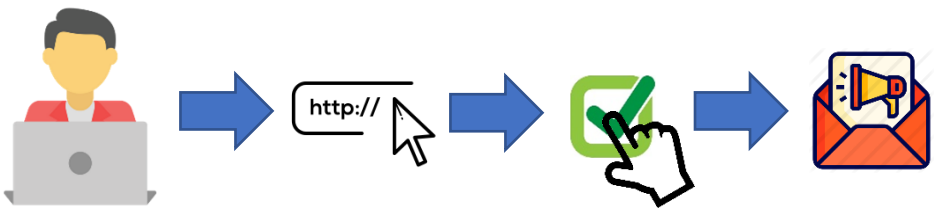
Mediante a criação da equipe, há uma recomendação de que, tais integrantes passem por um conjunto de treinamentos que os façam emergir dentro do contexto da LGPD, de maneira a abrangê-los em diversos assuntos como privacidade, gerenciamento de dados de usuários e consentimento dos titulares dos dados. Temas que introduzam os fundamentos da lei, para que, de maneira mais prática, cada profissional de cada área consiga associar esses temas com os processos realizados em suas respectivas áreas. A figura 3 representa a estrutura da equipe de um DPO.

Figura 3 – Equipe DPO

Fonte: Lima, 2019

Após feito os treinamentos, a equipe pode realizar reunião para as devidas atribuições e responsabilidades diversificadas que envolvem cada área da empresa. É recomendado que a partir desta reunião, já sejam criadas e discutidas metas para todos os envolvidos, é de suma importância que cada a equipe como um todo tenha um forte relacionamento comunicativo, já que cada etapa de mudança dos processos precisa ser feita e visualizada por todos os âmbitos da equipe, onde uma propaganda de marketing utilizando dados de pessoas que acessaram o site pela última vez, irá precisar dos olhares tanto do setor de marketing, quanto do setor jurídico para que o cliente tenha ciência de que permitiu essa ação, e quais pontos da lei estão sendo abordados, por exemplo.

Figura 4 – Fluxo de informação



Fonte: Elaborado pelo autor

3.1.5 *Consentimento Hierárquico*

A necessidade de que haja um consentimento geral da empresa, a começar da mais alta diretoria da empresa, de acordo com Lima (2019), pois a adequação impactará de maneira abrangente no negócio, o que consequentemente vai atingir toda as áreas, por isso a recomendação de que todo o C-Level (executivos de alto escalão de uma empresa) empresa esteja em consonância com o projeto.

3.1.6 *Contratação de consultoria terceirizada*

Caso a empresa veja a possibilidade de contratação de recursos terceirizados para a implementação da Lei Geral de Proteção de Dados, Lima (2019) recomenda um modelo de questionário elaborado pela GDPR Academy (LIST, 2020), onde são realizados questionamentos primordiais para uma validação correta de que o recurso a ser contratado possui os conhecimentos e gerenciamento técnico para adquirir a adequação da contratante à Lei.

> Lista de perguntas a serem feitas a um consultor da Lei Geral de Proteção de Dados
> Questões gerais:
> 1. Qual é a sua experiência no campo da privacidade / proteção de dados?
> 2. Com quais indústrias ele está familiarizado?
> 3. Quantos clientes ele teve? Quais indústrias? Ele pode fornecer uma lista de referência?
> 4. Sua experiência está relacionada a pequenas empresas ou empresas maiores?
> 5. Qual é a reputação dele - o que outros consultores dizem sobre ele; o que seus clientes dizem sobre ele?
> 6. Qual é a sua experiência (de negócios) além do LGPD ou GDPR?
> 7. Ele fala a sua língua perfeitamente?
> 8. Ele fala idiomas falados internacionalmente (por exemplo, inglês, espanhol etc.)?
> 9. Ele tem experiência em gerenciamento de projetos?
> 10. Ele tem algum conflito de interesse?
>
> Perguntas sobre a experiência de proteção de dados:
> 1. Quantos projetos de conformidade com o LGPD ou GDPR ele terminou com êxito nos últimos dois anos?
> 2. Qual é a sua experiência em outros requisitos de proteção de dados (por exemplo, Lei de Proteção de Dados (2018), diretiva de Privacidade Eletrônica etc.)?
> 3. Qual foi o projeto de conformidade de LGPD mais complexo que ele já teve? Ele pode descrevê-lo brevemente?
> 4. Ele esteve envolvido em projetos que envolviam múltiplas jurisdições dentro e fora do Brasil?
> 5. Ele ajudou em algum caso de violação de dados?
> 6. Qual é a experiência dele na criação de inventários de atividades de processamento?

> 7. Ele interage com as autoridades de supervisão? Sob que circunstâncias?
> 8. Qual é o seu caminho educacional em proteção de dados? Quais certificados ele tem?
> 9. Ele ministra treinamentos sobre LGPD? Se sim, quantos treinamentos ele forneceu e para quantas pessoas?
> 10. Ele já publicou algum artigo de especialista? Quantos e onde?
> 11. Ele pode mostrar exemplos de documentação do LGPD que ele criou para alguns de seus clientes? (LIMA, 2019)

3.1.7 *Apresentação do projeto*

Após executados todos esses fatores, uma apresentação descrevendo todos os processos que serão desenvolvidos para a implementação deve ser feita, todos os integrantes da equipe, além da autarquia da empresa e se possível todos os seus colaboradores, para que todos tenham ciência dos planos abordados, além da conscientização de mudanças e adequações, além das fases envolvidas, os responsáveis, e a importância da participação total de todos os colaboradores.

3.2 Inventário e Classificação de Dados

O Conhecimento de todo o fluxo de dados da empresa é uma das etapas fundamentais para a adequação dos requisitos impostos pela Lei, por isso, recomenda-se uma atenção especial no decorrer deste processo. Segundo Vieira (2019), a melhor forma de implementar um inventário, é executar uma Avaliação Inicial de Privacidade dentro da empresa, segundo ele “Essa etapa detalha como executar uma avaliação inicial do cenário atual de privacidade e proteção de dados de sua empresa”

3.2.1 *Avaliação Inicial de Privacidade*

Aqui é onde a busca pela compreensão do estado da empresa em termos de conceituais acontece. Como o setor de tecnologia e os outros setores lidam com os dados dos usuários, clientes, consumidores, *prospects,* funcionários, candidatos a vagas de empresas, parceiros e fornecedores da empresa? Como sua empresa lida com o tratamento de dados em um contexto geral?

Nessa etapa é criado um roteiro com o objetivo de criar uma visão macro dos pontos e campos de tratamento de dados, o foco aqui é melhorar a possibilidade de um inventário mais completo e tangível. Um mapa que possibilite um detalhamento posterior dos principais componentes deste diagnóstico.

Tabela 1 – Avaliação Inicial de Privacidade

Tratamento do dado	Quem coleta os dados?	O que é tratado?	Quando é iniciado o tratamento?	Quanto tempo irá durar o tratamento	Onde será realizado o tratamento	Qual o mecanismo/processo de segurança é utilizado no tratamento?	Há necessidade de tratamento?	Como é realizado o tratamento?
Coleta	Tecnologia da Informação	Dado Pessoal	Cadastro no site da empresa	3 anos	Banco de Dados interno	Criptografia no Banco de Dados	Sim, para envio de newsletters sobre promoções	Através de uma aplicação de webmail, do momento do cadastro, a aplicação insere o novo cadastrado em uma lista de pessoas cadastradas para que a cada nova noticia inserida no sistema, ele receba essas noticias
Coleta	Recursos Humanos	Dado pessoal sensível	Cadastro de funcionários	Até o desligamento do colaborador	Sistema de Recursos Humanos	Controle de acessos	Sim, Informações necessárias para o cumprimento da regulamentação trabalhista	Apartir do momento em que é feito o cadastro no sistema, suas informações são armazenadas no banco de dados do sistema para que caso haja necessidade de consulta, tais informações estejam disponíveis
Armazenamento	Tecnologia da Informação	Dado anonimizado	Acesso à intranet da empresa	3 anos	Banco de Dados interno	Criptografia no Banco de Dados	Sim, para elaboração de gráficos e controles regulamentados pelo Setor de tecnologia da Informação	A cada acesso à intranet da empresa, é criado um registro de acesso que é armazenado dentro do banco de dados para possíveis utilizações como comprovação maxima de acessos na intranet da empresa

Fonte – Elaborado pelo autor

3.2.2 *Relatório de Levantamento e Impacto de Dados*

Após a execução da Avaliação Inicial de Privacidade, é necessário que seja realizado o um relatório de impacto sobre os dados, segundo a exigência do artigo 38 da Lei.

> Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

Esse relatório possuí o intuito de relatar com mais especificidade cada procedimento de dados realizados da empresa e demonstrar em termos documentais um relatório de Impacto dos dados da empresa, segundo Lima (2019), está uma das etapas mais desgastantes de todo o projeto. Um modelo elaborado pela Family Links Network (PORTAL DA PRIVACIDADE, 2019), é utilizado por Lima (2019) como base para a elaboração do relatório.

Tabela 2 – Relatório de Levantamento e Impacto de Dados

Problema de Proteção de Dados	Código de Conduta	Levantamento dos Riscos	Medidas Mitigatórias	Conclusão
•*Especificação do propósito* •*O dado a ser coletado foi usado somente para um propósito específico?* •*O dado coletado será usado em algo mais, além do propósito específico?*	2.1 Propósito Específico	•Função Creep": Empresas podem querer ganhar mais com os dados coletados. •Na prática: As empresas podem ignorar ou não estão cientes de que não podem redirecionar dados pessoais (ou seja, usar os dados que originalmente coletaram para alguns propósitos adicionais) sem o consentimento novamente	•*Especifique/documente as finalidades para as quais os dados pessoais serão coletados /usados* •*Aumente a conscientização sobre a Lei Geral de Proteção de Dados, que prevê o princípio da especificação do propósito, e para processamento adicional, somente se parar fins compartilháveis com a finalidade original da coleta dos dados.* •*Melhorar o treinamento do pessoal em relação à especificação de propósitos/processamento adicional compatível.*	•Risco suficientemente mitigado. •Risco não mitigado, mas aceito. •Risco nem mitigado nem aceito.

Fonte – Lima, 2019

> Depois de entender as informações que você tem e onde as informações são armazenadas, você pode tomar decisões sobre o nível de segurança a ser aplicado, quem pode acessá-las, caso sejam criptografadas ou anônimas. A estratégia de segurança atual deve levar em conta que as regras de GDPR e LGPD são rígidas e que qualquer informação deve ser protegida onde quer que ela esteja, incluindo em dispositivos móveis, na cadeia de suprimentos ou com consultores (SUGDEN, 2018).

Finalizando esses dois relatórios, tanto o conhecimento da finalidade ou do porquê do tratamento dos dados, quanto à mitigação sobre seu impacto estarão de acordo com o Art. 50 da lei, garantindo o bom andamento da Implementação da LGPD.

3.2.3 *Incidentes*

Segundo Braz Junior (2019) em caso de vazamento de dados, existem pontos que normalmente serão considerados pela ANPD nos quesitos relacionados à segurança e ações comprovadas, esses pontos são:

- O tipo do incidente/vazamento
- O tipo de dados pessoais afetados
- A sensibilidade dos dados afetados
- O volume de dados afetados

• O número de titulares atingidos

• A natureza do processamento

• A facilidade ou não de identificação dos titulares (se por exemplo, os dados estavam criptografados ou anonimizados, o risco reduz)

• A gravidade das consequências para os titulares

• A extensão das consequências para os titulares

• Se houve menores entre os titulares

• Caso haja uma falha de confidencialidade, quais as possíveis intenções de quem perpetrou o ataque que gerou o incidente

Como resultado desta avaliação, os possíveis resultados com relação aos direitos dos titulares são:

• Não gera risco relevante

• Gera risco relevante

• Gera risco elevado

3.2.4 *Acessos interno e externo*

A partir do relatório elaborado, segundo Lima (2019), é possível visualizar de maneira centralizada, todos os pontos importantes dentro do contexto de dados da empresa, os relatórios nos darão uma ampla visão do que existe em contexto de informação dentro do negócio, pontos como impacto do dado, sensibilidade, tempo de duração e finalidade que são primordiais para o entendimento dos fluxos e processos que utilizam informação como recurso. E diante disso, a última etapa na ampla abordagem de Inventário e Classificação de Dados, é o controle dos acessos, com base nas informações disponíveis, é extremamente importante que seja feita uma análise de acessos tanto internos quanto externos dentro da empresa, de modo a realizar tratativas e revisões que não tenham verdadeiro propósito na permissão de determinados dados, bem como pessoas que já saíram da empresa, terceiros pessoas em férias ou de licença, entre outros.

3.3 Adequação de Políticas e Processos

Após a etapa de preparo e conhecimento de dados e processos, segundo Lima (2019), é necessário realizar a adequação destes à LGPD. Nessa etapa, serão feitas adequações, atualizações ou até mesmo a criação de processos e procedimentos que implique diretamente no fluxo vívido do negócio.

3.3.1 *Política de Privacidade*

Uma das primeiras adequações necessárias é na cultura organizacional da empresa, o contexto é novo, e sobrepõe muitos dos já existentes. Segundo Lima (2019), a empresa precisa buscar se inteirar com uma “Cultura de Privacidade”, onde vemos objetivos relacionados ao cuidado com o gerenciamento de todos os dados da empresa, a conscientização de colaboradores e da autarquia da empresa sobre privacidade e a priorização de um contexto seguro em termos de segurança da informação.

Segundo Lima (2019), a elaboração de uma Política de Privacidade, é um dos passos a caminho desta adequação, e é importante frisar a necessidade de que não é algo sobre um “termo de rede social” com centenas de linhas e até páginas em que o usuário começar a ler e para já na primeira página.

Abaixo utilizaremos alguns pontos da Política de Privacidade de uma empresa Multinacional chamada EATON, recomendada até mesmo por Lima (2019) pela sua clareza.

> POLÍTICA DE PRIVACIDADE, COOKIES E PROTEÇÃO DE DADOS
> Última atualização: 25 de maio de 2018
> A Eaton e suas afiliadas (coletivamente, "Eaton", ou "nós", “nos", "nosso") respeitam as suas preocupações com a proteção de dados pessoais e valorizam nosso relacionamento com você. Esta Política de Privacidade, Cookies e Proteção de Dados (a "Política") aplicam-se exclusivamente aos dados pessoais recolhidos através de sites da Eaton, páginas da web, portais, recursos interativos, aplicativos, linhas de suporte telefônico, e-mail, widgets, blogs e seus respectivos conteúdos, além do Twitter, Facebook ou outros sites de redes sociais, e seus respectivos conteúdos (coletivamente, os ’Sites"), mesmo acessados via computador, dispositivo móvel ou outro dispositivo (coletivamente, “Dispositivo").
>
> Esta Política descreve os tipos de dados pessoais que recolhemos por meio dos Sites e como esses dados pessoais podem ser utilizados e/ou com quem eles podem ser compartilhados. Esta política também descreve a maneira como você pode entrar em contato conosco para atualizar suas informações de contato, acesso e controlar o uso dos dados pessoais que coletamos em

> relação às nossas comunicações e atividades de marketing, ou obter respostas para as perguntas que você possa ter sobre nossas práticas de privacidade nesses Sites. Leia atentamente esta Política, porque, ao usar os Sites você está reconhecendo que compreende e concorda com os termos desta Política. Além disso, analise nossos Termos e Condições, que regem o uso dos Sites e qualquer conteúdo que você enviar a eles.
>
> COMO ENTRAR EM CONTATO CONOSCO
> Se tiver mais dúvidas ou comentários sobre esta Política, contate-nos:
> Escrevendo para:
> Eaton
> Aos cuidados de: Escritório de privacidade e proteção de dados Globais
> 1000 Eaton Boulevard
> Cleveland, Ohio 44122
> ou
> Via e-mail para: dataprotection@eaton.com
> Última atualização: 13 de outubro de 2017
> (LIMA,2019)

3.3.2 *Conhecimento e inicialização da política*

A política precisa conter as informações para o titular de maneira clara e objetiva, trazendo às claras: tipos de dados coletados, como esses dados serão utilizados ou compartilhados, além de maneiras de entrar em contato para atualizar informações, acesso e controle dos dados daqueles que quiserem.

> Leia atentamente esta Política, porque, ao usar os Sites você está reconhecendo que compreende e concorda com os termos desta Política. Além disso, analise nossos Termos e Condições, que regem o uso dos Sites e qualquer conteúdo que você enviar a eles.
> Geralmente, é possível visitar os Sites sem fornecer dados pessoais, salvo indicação em contrário nos próprios sites. Contudo, pode haver circunstâncias em que você pode ser convidado ou optar por fornecer dados pessoais que podem ser utilizados de modo razoável para contatá-lo ou identificá-lo pessoalmente (como seu nome, endereço residencial, número de telefone, dados de cartão de crédito ou endereço de e-mail (“Dados Pessoais") por meio dos Sites. Por exemplo, a Eaton pode coletar Dados Pessoais quando você se cadastrar nos Sites, solicitar informações, comprar produtos, enviar um currículo, fizer comentários ou participar de alguma promoção, pesquisa ou outro recurso dos Sites, ou comunicar-se ou interagir conosco de outra maneira. Os sites também podem pedir que você forneça outros dados pessoais sobre si mesmo, como dados demográficos (sexo, CEP, idade, etc.) ou determinadas informações sobre as suas preferências, uso do produto e interesses. Se combinarmos dados demográficos ou outros dados que coletamos sobre você como dados pessoais sobre você, nós trataremos as informações combinadas como dados pessoais de acordo com as leis aplicáveis, sujeitas à sua inclusão prévia, se e quando exigido pelas leis aplicáveis. Se você não deseja que seus dados pessoais sejam processados por nós, não os envie ou nos notifique a qualquer momento para excluí-los.
>
> COMO ENTRAR EM CONTATO CONOSCO
> Se tiver mais dúvidas ou comentários sobre esta Política, contate-nos:
> Escrevendo para:
> Eaton

> Aos cuidados de: Escritório de privacidade e proteção de dados Globais
> 1000 Eaton Boulevard
> Cleveland, Ohio 44122
> ou
> Via e-mail para: dataprotection@eaton.com
> Última atualização: 13 de outubro de 2017
> (LIMA,2019)

3.3.3 *Tratamento dos dados dos titulares*

Como determinado pela LGPD no Art. 18, o titular dos dados tem direito a solicitar diversas ações relacionadas aos seus dados, e por isso, a política da empresa precisa garantir que o mesmo, mesmo que desconheça a lei, possua esse conhecimento e direito.

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> I - confirmação da existência de tratamento;
> II - acesso aos dados;
> III - correção de dados incompletos, inexatos ou desatualizados;
> IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
> V - 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; (Redação dada pela Lei nº 13.853, de 2019) Vigência
> VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
> VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
> VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
> IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.
> § 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.
> § 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.
> § 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.
> § 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:
> I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou
> II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.
> § 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.
> § 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação

> seja comprovadamente impossível ou implique esforço desproporcional. (Redação dada pela Lei nº 13.853, de 2019) Vigência
> § 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.
> § 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor. (BRASIL, 2018).

Há a necessidade de possibilitar que as informações sejam repassadas para os titulares quando solicitadas, por isso, Lima (2019) recomenda que sejam elaborados métodos e processos que possibilitem a entrega dos dados do titular caso ele solicite-os, conforme o Art. 18 da LGPD.

3.3.4 *Utilização dos dados*

Segundo Lima (2019), tão importante quanto pedir consentimento, é necessário informar como serão utilizadas as informações coletadas. Em uma política de privacidade é necessário que o titular dos dados tenha ciência das metodologias utilizadas para captura de suas informações conforme o próprio Art. 18 da LGPD.

> A Eaton utiliza os dados pessoais e dados de uso que recolhemos através dos Sites para uma variedade de fins comerciais, incluindo, por exemplo, para: responder às suas perguntas e pedidos; fornecer-lhe acesso a determinadas zonas e recursos dos Sites; verificar a sua identidade; comunicar com você sobre sua conta e atividades sobre os sites e, em nosso critério, mudar qualquer política da Eaton; conteúdo sob medida, anúncios e ofertas fornecidas; enviar amostras, brindes, produtos e informações; processar pagamento por produtos e serviços comprados por você; processar pagamento por produtos ou serviços vendidos por você à Eaton; melhorar os Sites; desenvolver novos produtos e serviços; aplicações e transações de processos; e para fins de divulgação no momento em que você fornece seus dados pessoais ou de outra forma, com o seu consentimento. (LIMA,2019)

3.3.5 *Compartilhamento dos dados*

Outro ponto imprescindível na política é a ciência sobre o compartilhamento dos dados para outras empresas.

> Nós não forneceremos nenhum de seus Dados Pessoais a terceiros sem o seu consentimento específico, exceto conforme descrito nesta Política. Podemos compartilhar dados não pessoais, como estatísticas agregadas do usuário, dados demográficos e dados de uso com terceiros. Podemos também compartilhar seus dados pessoais nas seguintes circunstâncias: a terceiros prestando serviços em nosso nome. A fim de realizar os seus pedidos, para lhe disponibilizar vários recursos, serviços e materiais através dos Sites, e para responder às suas perguntas, podemos compartilhar seus dados pessoais ou dados de uso com terceiros que executam funções em nosso nome (ou em nome de nossos parceiros de negócios), como empresas ou indivíduos que: hospedam ou operam nossos Sites; analisam dados;

> fornecem atendimento ao cliente; enviam por correio amostras de produtos ou gerenciam pagamentos; anunciantes; patrocinadores ou outros terceiros que participam ou administram nossas promoções ou fornecem assistência de marketing ou promocional. Ao compartilhar seus Dados Pessoais com esses terceiros, exigimos que eles usem e protejam seus Dados Pessoais de maneira consistente com esta Política. (LIMA,2019)

3.3.6 *Acessos e escolhas*

Ainda em conformidade com o Art. 18 da LGPD, é importante que sejam informados sobre a possibilidade de fazer alterações, verificações ou correções nos dados coletados, assim o visitante fica ciente das opções que tem ao ver seus dados coletados na empresa.

> Você pode sempre nos instruir a não compartilhar seus dados pessoais com terceiros, para não usar seus dados pessoais para lhe fornecer informações ou ofertas, ou para não lhe enviar newsletters, comunicações de e-mails ou outras: (i) enviando-nos um e-mail para dataprotection@eaton.com, (ii) nos contatando por e-mail na Eaton, aos cuidados de: Global Data Protection and Privacy Office, 1000 Eaton Boulevard, Cleveland, Ohio 44122, EUA; ou (iii) seguindo as instruções de remoção na comunicação que você receber. Eaton não cobra por este serviço, e seu pedido de exclusão será processado dentro de 10-15 dias úteis a contar da data do recebimento. Para ajudar a proteger sua privacidade e segurança, tomaremos as medidas razoáveis para verificar sua identidade, como exigir uma senha e identificação de usuário, antes de conceder acesso aos seus dados pessoais.
>
> Se você deseja verificar, corrigir ou atualizar qualquer um dos seus Dados Pessoais reunidos através dos Sites, você pode fazê-lo entrando em contato conosco no endereço acima ou por e-mail. De acordo com a nossa manutenção de registros de rotina, podemos excluir certos registros que contenham dados pessoais que foram enviados através dos Sites. Não temos a obrigação de armazenar esses dados pessoais por tempo indeterminado e nos isentamos de qualquer responsabilidade decorrente de, ou relacionada à destruição desses Dados Pessoais. (LIMA, 2019)

3.3.7 *Transferência de dados pessoais*

Mediante à solicitação do titular, segundo Lima (2019), também precisa haver a necessidade de esclarecimento na política sobre a transferência de seus dados

> Dado que a Eaton inclui entidades localizadas em todo o mundo, processar seus dados pessoais e dados de uso envolve necessariamente a transmissão de dados em uma base internacional. Se você estiver localizado na União Europeia, no Canadá ou em outro lugar fora dos Estados Unidos, esteja ciente de que os dados pessoais e os dados de uso que coletamos podem ser transferidos para e processados nos Estados Unidos. Ao utilizar os Sites, ou nos fornecer quaisquer dados pessoais, você concorda com a coleta, processamento, manutenção e transferência desses dados pessoais e dados de uso para as entidades afiliadas da Eaton nos Estados Unidos ou em outros países, salvo a sua conformidade com as leis aplicáveis de proteção de dados pessoais.(LIMA, 2019)

3.3.8 *Segurança dos dados*

De acordo com o Art. 46 da Lei, é necessário que existam medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais e acessos, por isso, Lima (2019) recomenda a inserção destes métodos de maneira sucinta na política:

> Você tem os seguintes direitos relacionados à privacidade e proteção de dados:
> - Se desejar acessar, corrigir, atualizar ou solicitar a exclusão dos seus dados pessoais, você poderá fazê-lo a qualquer tempo, basta entrar em contato conosco por meio dos canais de contato mencionados na sessão “Como entrar em contato conosco” abaixo. Se preferir, você também pode atualizar seu perfil Eaton e os dados pessoais relacionados sempre que desejar. Para alterar essas informações, visite o centro de preferências.
> - Além disso, você pode objetar-se ao processamento dos seus dados pessoais, pedir para restringir o processamento dos seus dados pessoais ou requerer a portabilidade dos seus dados pessoais. Você pode exercer esses direitos entrando em contato conosco por meio dos canais de contato mencionados na sessão “Como entrar em contato conosco” abaixo.
> - Você tem o direito de cancelar os comunicados de marketing que enviamos, quando desejar. Para exercer esse direito, clique em “cancelar assinatura” ou no link “optar pelo cancelamento” nas mensagens de e-mail de marketing que enviamos para você. Para cancelar outras formas de marketing (como marketing postal ou telemarketing), entre em contato conosco por meio dos canais de contato mencionados na sessão “Como entrar em contato conosco” abaixo.
> - Da mesma forma, se coletamos e processamos dados pessoais com seu consentimento, você pode retirar seu consentimento quando desejar. Retirar seu consentimento não afetará a legitimidade do processamento realizado anteriormente à retirada, nem afetará o processamento dos dados pessoais executado com base em processos legítimos que dispensam sua anuência.
>
> Você tem o direito de reclamar à autoridade de proteção de dados sobre a coleta e uso que fazemos dos seus dados pessoais.
> Responderemos a todas as solicitações recebidas de pessoas físicas que desejam exercer seus direitos relacionados à proteção de dados de acordo com as leis de privacidade e proteção de dados em vigor. (LIMA, 2019)

3.3.9 *Base Legal*

Um ponto importante na política são as bases legais que regimentam todos os tratamentos realizados dentro da empresa, por isso também são recomendados dentro da política

> Nossa base legal para coleta e uso de dados pessoais descrita acima, depende dos dados pessoais considerados e do contexto específico em que os coletamos.

> Normalmente, coletaremos seus dados pessoais apenas (i) com o seu consentimento para fazê-lo; (ii) quando precisamos dos dados pessoais para celebrar um contrato com você; (iii) quando o processamento está de acordo com os nossos interesses legítimos e não menosprezam seus interesses relacionados à proteção de dados ou liberdades e direitos fundamentais. Em alguns casos, também somos compelidos a coletar seus dados pessoais ou podemos precisar dos seus dados pessoais para proteger seus interesses vitais ou de terceiros.
> Se solicitarmos seus dados pessoais com o intuito de cumprir uma exigência legal ou celebrar um contrato com você, este propósito será esclarecido em tempo oportuno e comunicaremos se o fornecimento dos seus dados pessoais é compulsório ou não (bem como sobre as possíveis consequências, caso os dados pessoais não sejam fornecidos). (LIMA, 2019)

3.3.10 *Consentimento*

O resultado da elaboração deve ser o termo de consentimento, que deve estar em consonância com a política para a elaboração do termo de consentimento, segundo Lima (2019), você deve atender os seguintes requisitos

> 3.3 Indique as atividades de processamento que ocorrem a qualquer momento em que você coleta dados pessoais
> 3.4 Se os dados pessoais não estiverem sendo obtidos diretamente, informe quais atividades de processamento estão ocorrendo
> 3.5 Avisos devem estar presentes sempre que dados pessoais forem coletados e em todos os pontos
> 3.6 Os dados devem incluir a identidade do controlador e do responsável pela proteção de dados por quanto tempo será mantido os direitos que o consumidor tem, o direito de registrar uma reclamação, os destinatários e as transferências de dados, uma declaração de que o consumidor tem o direto de retirar o consentimento a qualquer momento e também uma explicação de por que você ou um terceiro deseja coletar os dados (LIMA, 2019)

3.3.11 *Revisão e ajuste do ambiente de TI para obter o consentimento*

Mediante às exigências impostas pela lei, quanto ao direito dos titulares, cabe ao setor de Tecnologia da Informação, corresponder aos termos de consentimento e na capacidade de entrega de solicitações vindas dos titulares, Lima (2019) também demonstra isso em formato de requisitos para que seja possível a visualização preparo deste setor:

> 3.7 Confirmar a identidade de quem está solicitando os dados;
> 3.8 Dar aos consumidores a capacidade de solicitar seus dados pessoais;
> 3.9 Responder a pedidos de acesso a dados pessoais;
> 3.10 Rastrear e pesquisar os dados pessoais de um consumidor e entregá-los dentro de 30 dias;
> 3.11 Solicitar retificação e retificar quaisquer dados pessoais coletados;
> 3.12 Solicitar a exclusão dos dados pessoais de um consumidor;

3.13 Entender quais dados de controladores adicionais foram transferidos para terceiros;
3.14 Em caso de violação de dados, entrar em contato com essas entidades para excluir os dados;
3.15 Solicitar a restrição do processamento de dados e mostrar como e quando isto é feito;
3.16 Solicitar cópias e transmitir dados pessoais;
3.17 Encontrar dados pessoais e copiá-los em formatos legíveis por máquina;
3.18 Oferecer aos consumidores uma maneira de se opor aos dados que estão sendo coletados;
3.19 Interromper todo o processamento de dados e demonstrar sua conformidade; (LIMA, 2019).

Com isso, é possível visualizar o funcionamento das engrenagens que correspondem ao funcionamento das práticas e exigências solicitadas pela lei, com base no capítulo apresentado, teremos o retorno do atingimento das documentações e comprovações que cercam o empreendimento de razão quanto a manipulação dos dados de maneira correta, no final deste processo, será possível visualizar o atingimento dos pontos regimentais da LGPD, que giram em torno da empresa e garante que, mediante a uma auditoria, seja possível comprovar a execução dos regimentos, controles e cuidados no tratamento dos dados.

Tabela 3 – Exigências e comprovante de atingimento

Exigências	Comprovante de Atingimento
Art º 6 – Princípios sobre o tratamento de dados (motivo do tratamento)	Avaliação Inicial de Privacidade
Art º 7 - Requisitos sobre o tratamento dos dados (É consentido o tratamento dos dados?)	Política de privacidade
Art º 18 – Direitos do Titular	Política de privacidade
Art º 23 – Encarregado de dados	Responsabilizações
Art º 38 – Exigência de Relatório de Impacto	Relatório de Levantamento e Impacto de Dados

Fonte: Elaborada pelo autor

Como a exploração da necessidade de Implementação da LGPD exige que o ponto de partida seja dado pelos responsáveis pela empresa, ou melhor, os responsáveis que tenham como intuito o resguardo de sua empresa à Lei vigente. Foi criada uma plataforma avaliativa que possui o objetivo de questionar tal responsável sobre alguns pontos principais da lei, onde para cada resposta informada um relatório final informará quais pontos precisam de atenção, trazendo uma visão simples, porém prática sobre quão adequada essa empresa está.

4 APLICAÇÃO WEB

O desenvolvimento da aplicação WEB foi voltada para empresas que necessitam se adequar à LGPD. Para facilitar o entendimento e análise das empresas, criamos esta plataforma de pré avaliação baseada em um questionário que será respondido de forma simples, assim será gerado um relatório que terá informações suficientes para compreender se atualmente a empresa que respondeu o questionário está de acordo com à LGPD, o relatório também indica os pontos chaves que precisam ser alterados dentro da companhia, caso os tópicos abordados não estejam sem conformidade. Nesse capítulo explicaremos o funcionamento detalhado da ferramenta além de demonstrar a utilização da ferramenta e apresentar os resultados produzidos pela mesma.

4.1 Utilização da ferramenta

A ferramenta funciona na forma de um *website* e é necessário que o usuário se cadastre para utilizá-la. A plataforma foi desenvolvida usando PHP como principal linguagem de processamento no servidor, e o banco de dados escolhido para armazenamento de dados do sistema foi o SQLite, o motivo dessa escolha se dá na ausência da necessidade de realizar a configuração inicial do banco de dados em todo ambiente de desenvolvimento, como SQLite funciona na forma de arquivo ao invés de serviço, qualquer um com acesso ao código-fonte da plataforma consegue testa-la sem preparos adicionais com relação ao banco de dados, basta apenas compartilhar o arquivo SQLite utilizado.

Nos subcapítulos a seguir será explicado em detalhes como funciona a análise na plataforma e o processo para chegarmos ao relatório apresentado ao usuário, além dos preparos iniciais que foram necessários para que a ferramenta funcionasse.

4.1.1 *Preparos iniciais*

A análise feita pela ferramenta funciona nas repostas informadas pelos usuários no questionário, para que isso seja possível precisamos definir questões que a partir das respostas possamos definir o nível de conformidade de uma empresa, mas ao mesmo tempo essas perguntas precisam ser fáceis de interpretar, para que seja acessível a todos que necessitem auxiliar empresas em medir seu nível de

conformidade. A abordagem que tomamos para a criação das perguntas foi a extração de requisitos presentes na lei, simplificar os termos e transformar em perguntas de positivo ou negativo, assim podemos ter algo simples mas que ao mesmo tempo não foge do que a lei apresenta, algumas perguntas apresentam variações nas suas respostas, mas conceitualmente seguem a estrutura de positivo ou negativo.

As perguntas elaboradas podem ser categorizadas em três categorias: fluxo de dados, responsabilidades e políticas. Fluxo de dados envolve o controle e registro de quais caminhos a informação percorre dentro da empresa e por quais tratamentos ela passa dentro da empresa. Responsabilidades está atrelada definição e segregação de funções relacionadas ao fluxo de dados. Políticas engloba a criação e implantação da política de segurança e a criação e uso de políticas de privacidade para os produtos oferecidos pela empresa.

As perguntas não são armazenadas no banco de dados por conta da complexidade exigida, seria necessário criar relacionamentos entre questões e alternativas e entre alternativas e soluções, e o armazenamento de um relatório seria ainda mais complexo, já que seria necessário referenciar cada pergunta além de referenciar a alternativa para aquela questão. Evitando essa complexidade desnecessária optamos por número de questões fixo que seriam armazenadas em um arquivo JSON, e os relatórios seriam armazenados no banco de dados, mas sem referências complexas, mas sim usando um formato de pares chave-valor, onde a chave seria o número da questão e o valor seria o número da alternativa, assim conseguimos unir todos pares chave-valor representando as respostas informadas pelo usuário em um questionário e armazenar tudo no banco de dados na forma de texto.

4.1.2 *Análise*

Como já definido no capítulo anterior as perguntas e alternativas já foram definidas, mas vale atentar ao fato que para cada alternativa definimos uma “solução”, essa solução seria como uma resposta direta para a alternativa escolhida pelo usuário tendo como base a questão, exemplo: a questão “Com relação a classificação de dados ?” umas de suas alternativas é “Os dados não seguem nenhuma classificação especifica” e a solução definida seria “A empresa precisa definir um procedimento para que seja possível que qualquer um classifique os dados” , dessa forma o

mecanismo de análise só precisa relacionar a alternativa escolhida com a solução já proposta. A seguir mostraremos um passo a passo da utilização da ferramenta.

4.2 Utilização da ferramenta

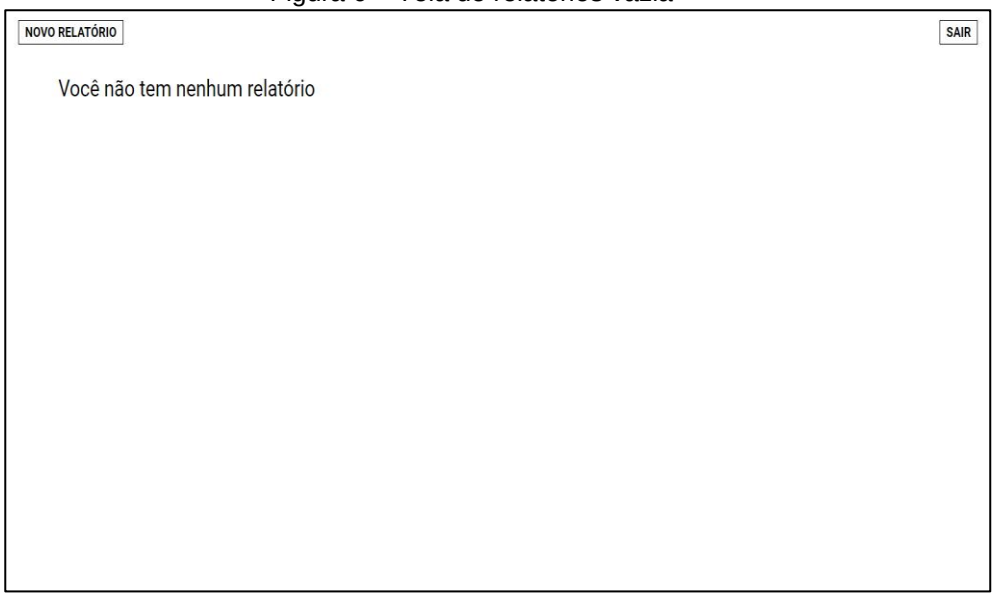
Na figura 5 podemos observar a tela inicial, onde as empresas podem efetuar o cadastro ou entrar na plataforma, caso tenham um cadastro.

Figura 5 – Tela de login

Fonte: Elaborado pelo autor

Caso a empresa já tenha algum relatório cadastrado ele ficará registrado em nosso banco de dados, caso seja o primeiro ela poderá clicar em no “Novo Relatório” para ter acesso ao questionário.

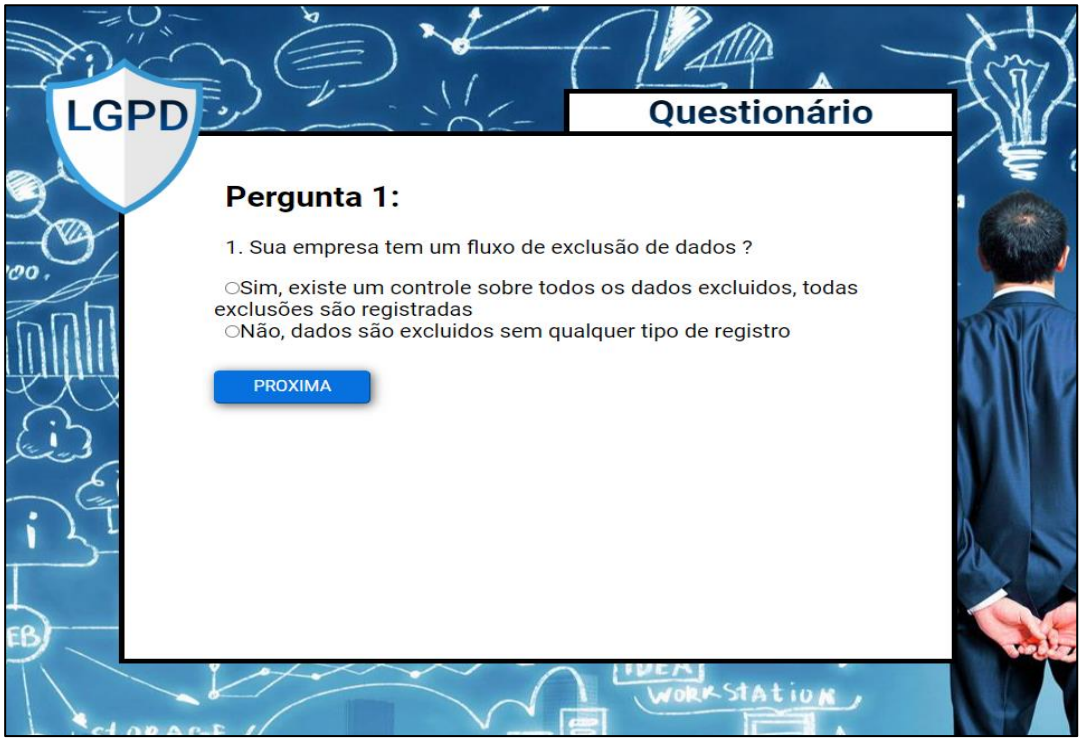
Figura 6 – Tela de relatórios vazia



Fonte: Elaborado pelo autor

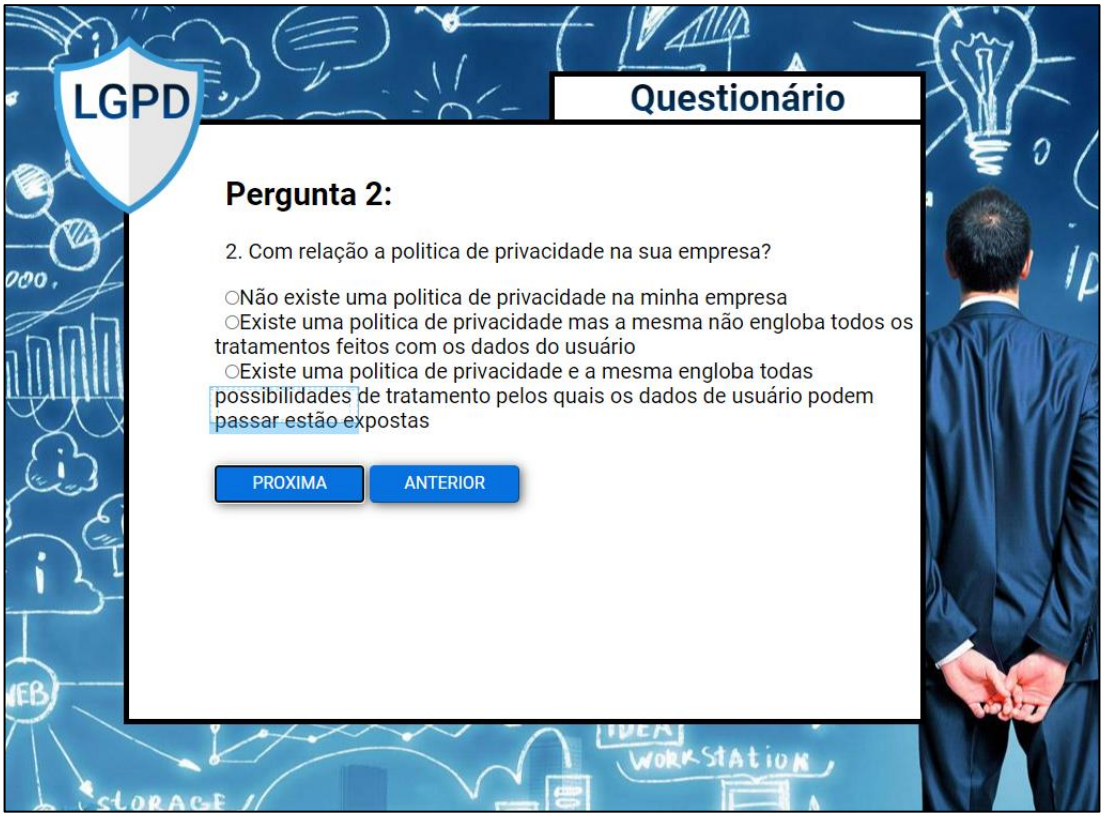
Já com acesso ao questionário, a empresa deverá responder a um banco de questões com apenas uma resposta por pergunta:

Figura 7 – Exemplo de questão 1



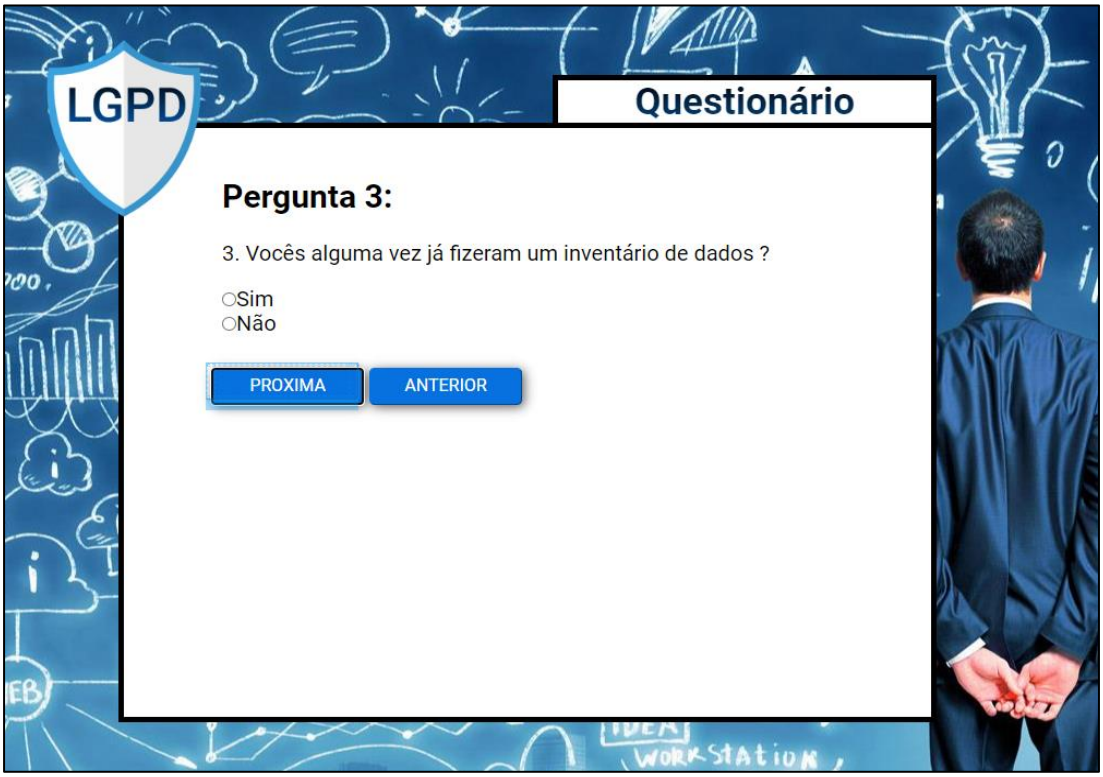
Fonte: Elaborado pelo autor

Figura 8 – Exemplo de questão 2



Fonte: Elaborado pelo autor

Figura 9 – Exemplo de questão 3



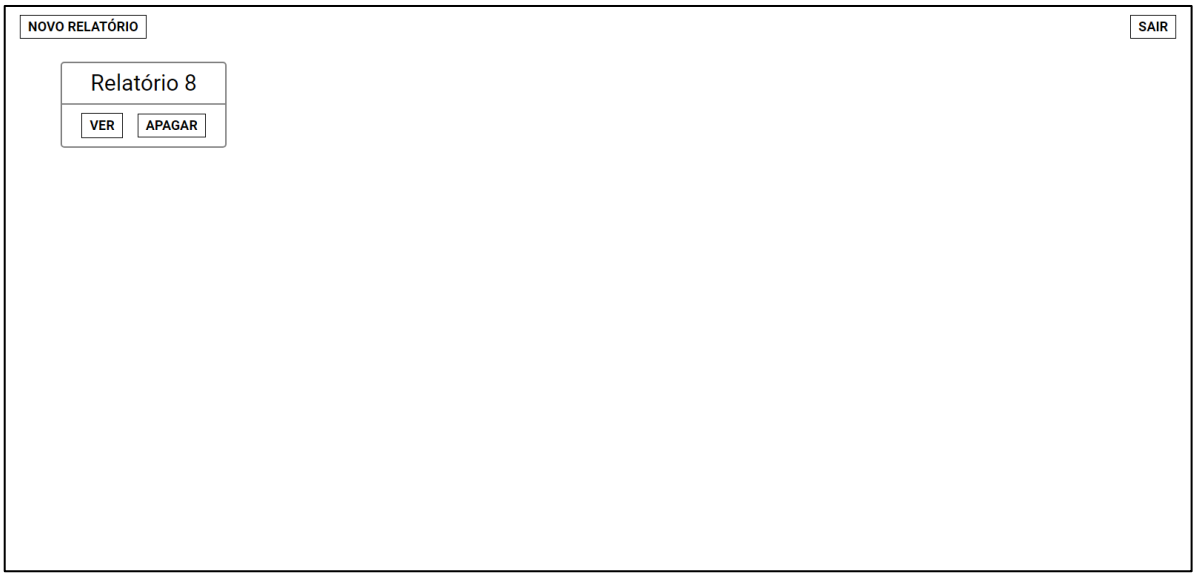
Fonte: Elaborado pelo autor

Ao final do questionário a empresa terá a opção de encerrar ou de retornar às perguntas anteriores. Caso deseje encerrar, será direcionado a página de relatórios e assim terá acesso ao mesmo.

Figura 10 – Final do questionário

Fonte: Elaborado pelo autor

Figura 11 – Tela de relatório



Fonte: Elaborado pelo autor

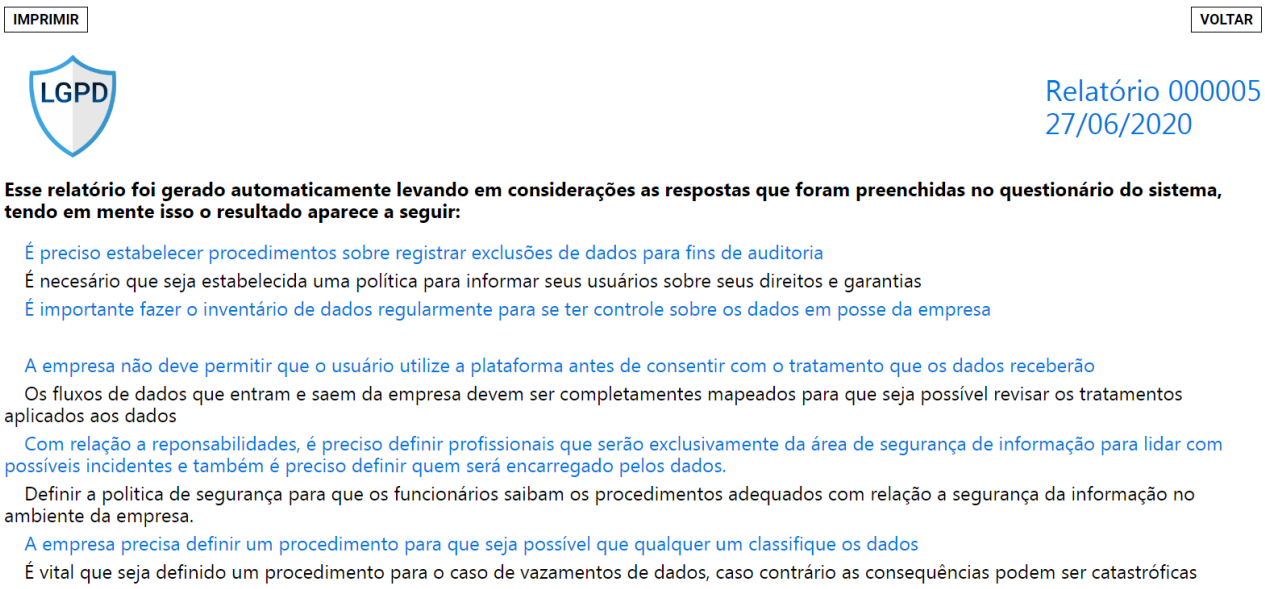
4.2 Resultado obtido

Ao encerrar o desenvolvimento da ferramenta chegamos aos resultados demonstrados nos subcapítulos anteriores. A ferramenta em sua versão final

apresenta para o usuário um relatório contendo informações sobre o estado da empresa em relação a conformidade com a LGPD, além de apresentar medidas a serem adotados nos casos de não conformidade. Esse relatório aborda fluxos de exclusão de dados, política de privacidade, inventário de dados, consentimento do usuário, definição de responsáveis e responsabilidades, políticas de segurança, classificação de dados e por fim, medidas para o caso de vazamento de dados, como é possível observar na figura 12, onde todos esses temas estão previstos na lei na forma de requerimentos.

O mecanismo de análise presente na ferramenta é simples, mas o ponto forte da ferramenta não está na análise feita pela plataforma, mas sim na análise feita nos preparos iniciais onde extraímos requisitos da lei e os convertemos em perguntas, definimos alternativas com base em cenários possíveis e, por fim, definimos soluções que seriam as melhoras medidas a serem tomadas em cada cenário. Isso tornou possível a criação de um sistema que gira em torno de um conceito simples, mas ainda sim pode ser de grande utilidade já que apresenta conceitos da LGPD de uma forma que mesmo pessoas com dificuldade de interpretar a lei, podem vir a entender a mesma através dessa ferramenta.

Figura 12 – Relatório final



Fonte: Elaborado pelo autor

5 CONSIDERAÇÕES FINAIS

De acordo com os objetivos propostos, e os estudos realizados ao longo da produção desse trabalho, foi possível elaborar uma solução de questionário que possui o intuito de nortear as bases principais exigidas no processo inicial de adequação e implementação da LGPD em organizações. De acordo com nossos estudos, não existe, até o momento da elaboração deste trabalho, uma metodologia oficial para a implementação definitiva da lei. Por isso, através das pesquisas foi possível observar a abrangência da lei nos diversos aspectos que envolvem o contexto de manipulação de dados dentro do nosso país, e quais as exigências impostas, de maneira a garantir o cuidado e a responsabilidade por parte dos responsáveis pelo tratamento de dados, na execução de seus interesses empresariais. Além de observar que, apesar da lei não permitir uma visualização clara, existem métodos específicos dentro do setor de tecnologia da informação que podem ser utilizados para a adequação da lei, se utilizados de maneira correta. Neste trabalho demonstramos como esses métodos existentes podem ser inseridos de maneira eficaz ao escopo do projeto de implementação da LGPD, além de criar uma plataforma avaliativa, onde é possível obter um resultado prático do quão adaptado o avaliado está nos principais pontos abordados da Lei Geral de Proteção de Dados.

REFERÊNCIAS

ABNT NBR ISO/IEC 27002. (2005). **Tecnologia da informação – Código de prática para a gestão da segurança da informação**. Rio de Janeiro: Associação Brasileira de Normas Técnicas.

BENETTI, Ticiano. **SEGURANÇA DA INFORMAÇÃO COMO GESTÃO DE RISCOS DE NEGÓCIO**. Disponível em: <https://ticianobenetti.wordpress.com/>. Acesso em: 24 Jan de 2020.

BRASIL. Lei nº 13.709, de 14 de Agosto de 2018. **Lei Geral de Proteção de Dados Pessoais**. Michel Temer. Brasília. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm> Acesso em: ago de 2019.

BRASIL. Lei nº 13.853, de 08 de Julho de 2019. **Autoridade Nacional de Proteção de Dados**. Jair Messias Bolsonaro. Brasília. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato20192022/2019/Lei/L13853.htm#art1> Acesso em: ago de 2019.

BRASIL. Medida Provisória nº 959, de 29 de Abril de 2020. **Prorroga a vacatio legis da Lei nº 13.709**. Jair Messias Bolsonaro. Brasília. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv959.htm> Acesso em: mai de 2020.

BRAZ JUNIOR, Marcilio. Considerações sobre a notificação de incidente de segurança da informação no contexto da lei geral de proteção de dados (e além). **Migalhas**, São Paulo, v. 1, n. 1, p. 1-1, 01 fev. 2019.

CAVALCANTI, Eduardo de Hollanda. **Proteção de dados, a vez do Brasil**. Disponível em:https://www.migalhas.com.br/dePeso/16,MI286295,71043;Protecao+de+dados+a+vez+do+Brasil. Acesso: 08 out de 2019

CERT.BR (Brasil) (Org.). **Cartilha de Segurança para internet.** 2017. Disponível em: <https://cartilha.cert.br/ataques/>. Acesso em: 20 Set. 2019.

CORREIA, Pedro Miguel Ribeiro; SANTOS, Susana Isabel da Silva; BILHIM, João Abreu de Faria. **Proposta de modelo explicativo das percepções sobre gestão e políticas públicas em matéria de cibersegurança e cibercrime**. 2017. 18 f. Artigo (Instituto Superior de Ciências Sociais e Políticas) - Universidade de Lisboa, Lisboa, 2017. Disponível em: <http://www.scielo.mec.pt/pdf/soc/v33/v33a06.pdf>. Acesso em: 30 maio 2018.

GOODMAN, Marc. **Future Crimes: Inside the Digital Underground and the Battle for Our Connected World**. 1. ed. [S.l.]: hsm, 2016. 504 p.

GREENWALD, Glenn. **Sem Lugar Para Se Esconder:** Edward Snowden, A Nsa e A Espionagem do Governo Americano. Nova York: Metropolitan Books, 2014. 288 p.

GROSS, Hyman. **The concept of privacy**. NYUL Rev., v. 42, p. 34, 1967.

KIM, D.; SOLOMON, M. G. **Fundamentos de Segurança de Sistemas de Informação**. Rio de Janeiro: LTC, 2014. 385 p. ISBN 978-0-7637-9025-7.

LIMA, Adriano Carlos de (comp.). Implementação e Desenvolvimento da LGPD. In: MALDONADO, Viviane Nobrega; LIMA, Adriano Carlos de; PRATA, Alexandre; VIEIRA, Vieira (2019); MONTANARO, Domingo; VIEIRA, Elba Lúcia de Carvalho; PALHARES, Felipe; GIOVANNINI JUNIOR, Josmar Lenine; SILVA, Sergio Aparecido Oliveira da; CAPANEMA, Walter Aranha. **LGPD Lei Geral de Proteção de Dados Pessoais**: manual de implementação. Manual de Implementação. São Paulo: Thomson Reuters, 2019. p. 133-166.

LIST of questions to ask a GDPR consultant. 2020. Disponível em: https://info.advisera.com/eugdpracademy/free-download/list-of-questions-to-ask-a-gdpr-consultant. Acesso em: 20 jun. 2020.

LOPES, Adriano. **O que é ataque cibernético?** 2019. Disponível em: <https://mundohacker.net.br/o-que-e-ataque-cibernetico/>. Acesso em: 14 out. 2019.

MATSUNAGA, Igor. **Os Pilares da Segurança da Informação**. Disponível em: <https://nsworld.com.br/os-pilares-da-seguranca-da-informacao/>. Acesso em: 15 Dez de 2019.

MENEZES, Karina (ed.). **Comparativo entre LGPD x GDPR**. 2019. Disponível em: https://guialgpd.com.br/comparativo-entre-lgpd-x-gdpr/. Acesso em: 12 ago. 2019.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **NIST 800-30**: Guide for Conducting Risk Assessments. 1 ed. Estados Unidos: Computer Security Division, 2012. 95 p. Disponível em: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>. Acesso em: 11 out. 2019.

NORTON. **Relatório de segurança cibernética: Norton Cyber Security Insights Report 2016**. Disponível em: <http://now.symassets.com/content/dam/content/pt-br/collaterals/datasheets/norton-cyber-security-insights-report2016.pdf>. Acesso em: 15 Outubro. 2019.

PRATA, Alexandre (org.). Preparação. In: MALDONADO, Viviane Nobrega; LIMA, Adriano Carlos de; PRATA, Alexandre; VIEIRA, Claudinei; MONTANARO, Domingo; VIEIRA, Elba Lúcia de Carvalho; PALHARES, Felipe; GIOVANNINI JUNIOR, Josmar Lenine; SILVA, Sergio Aparecido Oliveira da; CAPANEMA, Walter Aranha. **LGPD Lei Geral de Proteção de Dados Pessoais**: manual de implementação. Manual de Implementação. São Paulo: Thomson Reuters, 2019. Cap. 1. p. 105-132.

PROOF. **Threat Report – Wannacry 2017**. Disponível em:<https://d335luupugsy2.cloudfront.net/cms/files/9568/1507148257WannaCry_Threat-Reportd.pdf>. Acesso em: 15 Dez de 2020.

PORTALDAPRIVACIDADE (ed.). **Template for Data Protection Impact Assessment (DPIA)**. 2019. Disponível em: https://www.portaldaprivacidade.com.br/template-for-data-protection-impact-assessment-dpia/. Acesso em: 09 jan. 2019.

SILVA, Alexandre Pacheco Da (São Paulo). Fgv - Grupo de Ensino e Pesquisa em Inovação (org.). **UM NOVO MUNDO DE DADOS**: RELATÓRIO FINAL. 2017.

Disponível em: http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/28625/Um%20Novo%20Mundo%20de%20Dados%20-%20Relat%C3%B3rio%20Final.pdf?sequence=1&isAllowed=y. Acesso em: 29 ago. 2017.

SUGDEN, Martin. Classificação de dados é chave em GDPR e LGPD. **Tiforense.** São Paulo, p. 1-1. 10 dez. 2018.

VIEIRA, Claudinei (comp.). Preparação. In: MALDONADO, Viviane Nobrega; LIMA, Adriano Carlos de; LIGUORI FILHO, Carlos Augusto; VIEIRA, Claudinei; MONTANARO, Domingo; VIEIRA, Elba Lúcia de Carvalho; PALHARES, Felipe; GIOVANNINI JUNIOR, Josmar Lenine; SILVA, Sergio Aparecido Oliveira da; CAPANEMA, Walter Aranha. **LGPD Lei Geral de Proteção de Dados Pessoais: manual de implementação. Manual de Implementação**. São Paulo: Thomson Reuters, 2019. p. 35-104.