Estudo de caso da implantação da LGPD em uma empresa paraibana

Maria Madalena Gomes de Pontes

Centro de Ciências Aplicadas e Educação – Universidade Federal da Paraíba (UFPB)
Caixa Postal: 58297-000 – Rio Tinto – PB – Brasil

maria.madalena@dcx.ufpb.br

Abstract*. Concerns about privacy and protection of personal data have increased around the world, spreading the discussion and creation of specific laws that regulate the use of this data. This paper seeks to present the guidelines of the legislation that regulates the activities of processing personal data in Brazil (Law 13.709 - LGPD), as well as a case study of the implementation of the law in a company from Paraíba, mentioning the changes that have been made to fit in, and the challenges they experienced.*

Resumo. A preocupação quanto à privacidade e proteção de dados pessoais tem aumentado no cenário mundial, propagando a discussão e a criação de leis específicas que regulamentem o uso destes dados. O presente trabalho busca apresentar as diretrizes da legislação que regula as atividades de tratamento de dados pessoais no Brasil (Lei 13.709 – LGPD), assim como contempla um estudo de caso da implantação da lei em uma empresa paraibana, mencionando as mudanças que vêm sendo feitas para se adequar, e os desafios vivenciados por ela.

1. Introdução

Em um mundo globalizado, é perceptível como as informações fazem parte do nosso dia a dia. Devido ao acelerado avanço da tecnologia e com o advento da internet, diversas mudanças foram ocasionadas na sociedade, com notáveis impactos nas relações humanas e organizacionais [Garnier e Padilha 2019].

A disponibilização de dados pessoais ocorre de forma constante, seja ao efetuar uma compra em loja virtual, se inscrever em plataformas de ensino, ou se cadastrar em um portal de entretenimento. Esse cenário com intenso e rápido fluxo de dados aumenta o desafio de inviolabilidade da privacidade dos indivíduos.

O atual contexto mundial de pandemia do COVID-19 impulsionou ainda mais o fluxo de informações, alavancando o risco de utilização indevida ou abusiva dos dados pessoais. Diante deste panorama, percebe-se a importância de se adotar medidas para proteger essas informações, pois uma violação pode ocasionar vários danos ao cidadão. Vale salientar que, na Constituição Federal Brasileira, o direito à proteção de dados é reconhecido como um direito fundamental.

A preocupação quanto à privacidade e proteção dos dados pessoais tem aumentado em cenário mundial, propagando a discussão e criação de leis próprias para regulamentar o uso destes dados. Conforme aponta Pinheiro (2021, p.48), a importância

Trabalho de conclusão de curso, sob orientação da professora Vanessa Farias Dantas submetido ao Curso de Licenciatura em Ciência da Computação do Centro de Ciências Aplicadas e Educação (CCAE) da Universidade Federal da Paraíba, como parte dos requisitos necessários para obtenção do grau de Licenciada em Ciência Da Computação.

de uma legislação específica sobre proteção de dados pessoais advém do atual modelo de negócios da sociedade digital, tendo a informação como principal moeda de troca para que se possa adquirir algum serviço ou produto.

Gomes (2019) destaca que "o mercado internacional vê com bons olhos países que tenham interesse pela proteção de dados dos seus cidadãos, o que pode facilitar as negociações entre as nações que já possuem leis específicas." Adotar medidas de proteção de dados está se tornando um diferencial competitivo entre as empresas e entre os países.

Uma legislação de proteção de dados traz benefícios tanto para as empresas quanto para os titulares dos dados: as empresas ganham com experiência em boas práticas de segurança da informação e no tratamento de dados de forma responsável, e os titulares dos dados ganham com a garantia de que suas informações serão tratadas de forma adequada [Gomes 2019].

Este trabalho tem como problemática uma nova legislação em vigor, à qual as empresas brasileiras necessitam se adequar. Neste cenário, o objetivo é apresentar as diretrizes da legislação brasileira que regula as atividades de tratamento de dados pessoais (Lei 13.709 – LGPD), e relatar um caso de adequação à lei, apresentando as mudanças que vêm sendo adotadas em uma empresa paraibana para cumpri-la e os desafios vivenciados.

Portanto, a fim de abordar a temática, o artigo está dividido da seguinte forma: a seção 2 apresenta a Lei Geral de Proteção de Dados, e a seção 3 discorre sobre a implementação da LGPD em uma empresa paraibana. Por fim, a seção 4 contempla as considerações finais.

2. Lei Geral de Proteção de Dados (LGPD)

Decretada pelo Congresso Nacional em 2018, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) entrou em vigor em 18 de setembro de 2020, tornando-se um importante marco legal para o Brasil visando à privacidade dos indivíduos. A legislação tem como referência o Regulamento Geral de Proteção de Dados Pessoais Europeu (GDPR), e "dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade, e o livre desenvolvimento da personalidade da pessoa natural" [Brasil 2018].

A LGPD conjuga o cenário diversificado de legislações no país que tratam a proteção e privacidade dos dados, a exemplo do Marco Civil da Internet e do Código de Defesa do Consumidor, e traz uma regulamentação específica para o uso, proteção e transferência de dados pessoais no Brasil [Lima 2020].

Esta lei é aplicável 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: a operação de tratamento seja realizada no território nacional; a atividade de tratamento tenha como objetivo a oferta ou o fornecimento de bens, serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou os dados pessoais objetos do tratamento tenham sido coletados no território nacional [Brasil 2018].

Para o tratamento de dados pessoais, são definidos quatro papéis envolvidos, conforme exibido na Figura 01. O Titular é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. O Controlador é responsável pelas decisões referentes ao tratamento de dados pessoais, enquanto o Operador realiza o tratamento de dados pessoais em nome do controlador (os papéis de controlador e operador são caracterizados por pessoa natural ou jurídica, de direito público ou privado). Já o Encarregado de Dados é a pessoa indicada pelo Controlador e pelo Operador para atuar como canal de comunicação entre o Controlador, os Titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Figura 01 – Papéis na LGPD

Fonte: CRIA Tecnologia e Inovação 2020

O Art. 6º da LGPD estabelece dez princípios que devem fundamentar as atividades de tratamento de dados pessoais demonstrando boa-fé: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas [Brasil 2018].

Empresas brasileiras ainda não estão, em sua totalidade, agindo em conformidade com a legislação de proteção de dados, mesmo com a total vigência da LGPD, incluindo a possibilidade de aplicação das sanções administrativas pela Autoridade Nacional de Proteção de Dados (ANPD) a partir de agosto de 2021 [LGPD Brasil 2021]. As penalidades vão desde advertência e multas associadas ao faturamento da organização, até a suspensão ou proibição, parcial ou total, do exercício da atividade de tratamento dos dados pessoais. Tais sanções poderão ser aplicadas para responsabilização por tratamento irregular de dados.

De acordo com Bisso *et al*. (2019), muitas empresas não estão adaptadas para a proteção dos dados, sendo imprescindível a divulgação e conscientização sobre o tema. A Fundação Dom Cabral (FDC) realizou um levantamento no primeiro semestre de 2021 com 207 empresas brasileiras, e o estudo aponta que 40% das empresas admitem não estarem adequadas às novas exigências da legislação de proteção de dados [Diário do Comércio 2021].

Para se adequar à LGPD é necessário elaborar um programa de conformidade. Este programa requer uma atuação multidisciplinar, que demanda estrutura tecnológica

de segurança da informação, governança normativa e contratual, além de ser necessária a capacitação de equipes [Oliveira et al. 2019, p.29]. Por ser um trabalho que envolve diversas áreas, é necessário que haja comprometimento entre todas as partes para que o programa possa fluir e atingir os objetivos esperados. O Governo Federal Brasileiro elaborou um guia com uma sequência de passos para um programa de Governança em Privacidade, apresentado na Figura 02.

Figura 02 - Etapas do Programa de Governança em Privacidade

Fonte: Governo Digital 2020

No entanto, para implantação desses programas, algumas dificuldades são apresentadas pelas empresas, seja de mudança cultural ou limitações financeiras. Conforme destaca Lima (2020), “nas empresas que já possuem boas práticas de governança implantadas em seus processos, a adequação ocorrerá de forma mais rápida, tendo em vista também que não dependerão de maiores investimentos”.

Por se tratar de uma legislação recente, a literatura possui poucos trabalhos que demonstrem casos práticos acerca do assunto, portanto a relevância deste trabalho é apresentar o que foi vivenciado por esta empresa durante seu programa de adequação.

3. Implementação da LGPD em uma empresa paraibana

Nesta seção será apresentado o contexto de uma organização paraibana e seu processo de adequação à legislação de proteção de dados, bem como os desafios vivenciados.

3.1. Apresentação e contexto da organização

Fundada em 1977, a EmpresaX[1], genuinamente paraibana, atualmente é uma das maiores indústrias avícolas do Nordeste, reconhecida por sua excelência em qualidade e respeito

[1] Nome fictício com o objetivo de manter sigilo das informações contempladas no trabalho

ao meio ambiente e às pessoas que compõem um time de mais de 2.000 colaboradores, incentivados diariamente à entrega com qualidade e ao aprendizado contínuo, e com mais de 10.000 clientes por todo o país.

A empresa está presente em outros estados nordestinos, possuindo filiais em Rio Grande do Norte, Pernambuco, Piauí e Sergipe. Tem como atividade principal a criação de frangos para corte, e atividades econômicas secundárias: produção de pintos, produção de ovos, criação de peixes em água doce, criação de camarões em água doce, abate de aves, fabricação de produtos de carne, preparação de subprodutos do abate, fabricação de alimentos para animais, comércio atacadista de alimentos para animais, comércio atacadista de aves abatidas e derivados, comércio atacadista de pescados e frutos do mar, comércio atacadista de produtos alimentícios em geral, comércio atacadista de mercadorias em geral (com predominância de insumos agropecuários), comércio varejista de carnes (açougues), comércio varejista de outros produtos não especificados anteriormente.

É evidente que, para o cumprimento das atividades da empresa, diversos processos necessitam realizar o tratamento de dados pessoais, sendo as áreas de RH, Compras e Comercial as que lidam com maior fluxo de informações de colaboradores, fornecedores e clientes, respectivamente, e o setor de TI que suporta tecnologicamente todas as áreas da empresa. Diante desse cenário, a EmpresaX entendeu a importância e a necessidade de adequar seus processos à Lei Geral de Proteção de Dados (LGPD), e, para auxiliar na implantação do programa de adequação, decidiu contar com consultoria externa especializada.

3.2. Etapas do programa de adequação

A consultoria contratada teve como escopo do seu trabalho: I. Desenvolvimento de *assessment*/auditoria, visando identificar lacunas e riscos para a adequação à Lei Geral de Proteção de Dados (LGPD); II. Implantação e organização do programa de privacidade para atender aos *gaps* identificados e adequação à lei; III. Implantação paralela dos controles de segurança da informação necessários à gestão de privacidade e controles adicionais de proteção da segurança da informação para aumento da maturidade.

3.2.1. Objetivos do programa

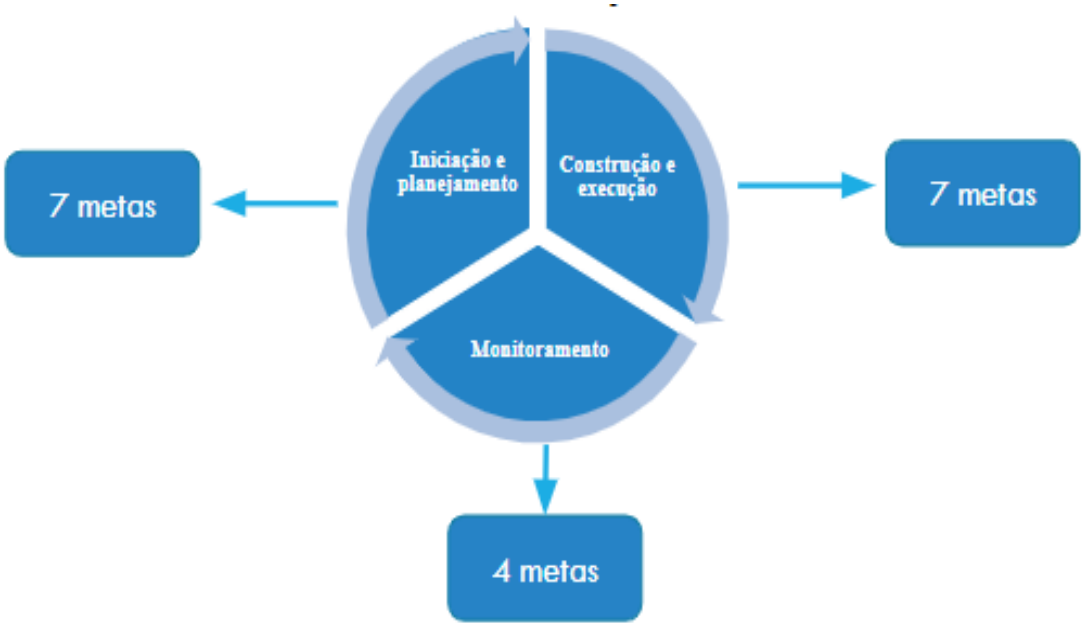
Foram elaborados **6 objetivos** para o Programa de Governança em Privacidade – PGP da empresa:

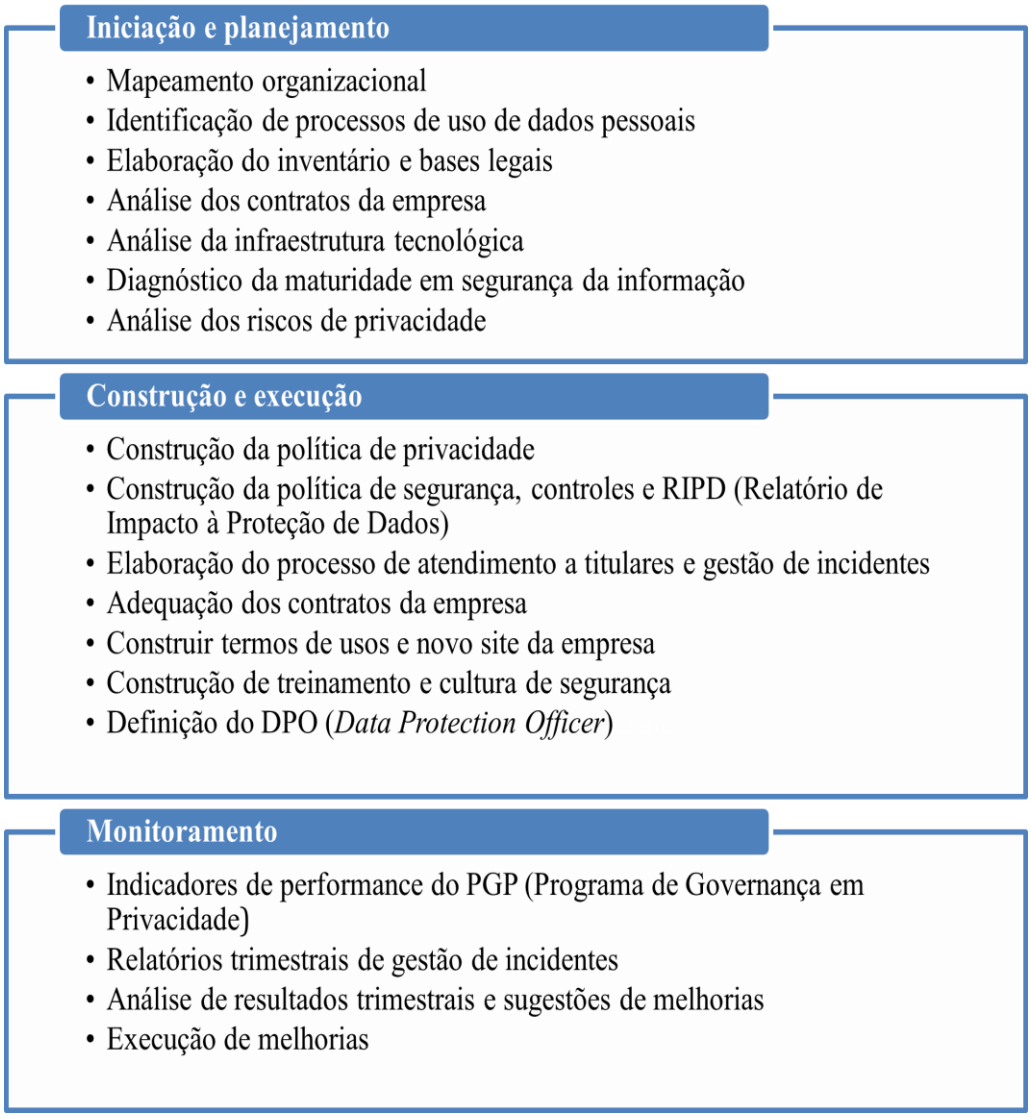
- **Política**: Desenvolver uma política de segurança e privacidade de acordo com as necessidades da empresa.
- **Processos:** Ajustar os principais processos operacionais visando a adequação à Lei Geral de Proteção de Dados (LGPD).
- **Salvaguardas:** Operar com ferramentas de proteção dos dados na infraestrutura tecnológica.
- **Gestão de incidentes:** Ter um processo de gestão de incidentes para atender as necessidades regulamentares e atuar na rápida contenção e remediação de problemas.

- **Transparência:** Trabalhar com um canal de comunicação com os clientes, colaboradores, parceiros e fornecedores através de ferramentas tecnológicas para atender as solicitações de direitos dos titulares.
- **Treinamento:** Treinar continuamente os colaboradores, redobrando a atenção e os cuidados no manuseio de dados pessoais na operação da empresa.

As etapas do programa foram inspiradas no modelo da metodologia **PDCA**, acrônimo de *Plan-Do-Check-Act*, que em português significa **Planejar-Fazer-Verificar-Agir**. O Ciclo PDCA pode ser descrito como um modelo implementado para melhorar a qualidade e a eficácia dos processos empresariais. Visando a simplificação e adequação deste modelo à realidade da empresa, foram utilizadas no PGP apenas 3 etapas para a sua estruturação, e cada uma delas contempla metas para a adequação da empresa para com o programa, conforme definido na Figura 3.

Figura 03 – Etapas e metas do PGP da EmpresaX





Fonte: Elaborado pela autora 2021

3.2.2. Etapa Iniciação e planejamento

No trabalho desta fase foram gerados os seguintes documentos e artefatos contidos no relatório de *assessment*:

- **Organograma da empresa e seus departamentos**: visão de toda a estrutura organizacional da empresa;

- **Identificação de processos que manipulam dados pessoais**: baseado no organograma gerado, foi possível identificar os departamentos e processos que utilizam dados pessoais.

- **ROPAS (*Record of Processing Activities* - Registro das operações de tratamento de dados pessoais):** este registro contém dados de contato e informações do agente de tratamento, área e processo, finalidades do

processamento, descrição das categorias e tipos de dados pessoais, sistemas utilizados na atividade, terceiros envolvidos na atividade, volume de dados, prazo de retenção, informações sobre transferência internacional de dados, riscos envolvidos no processo, medidas e salvaguardas para a proteção dos dados pessoais.

- **Análise de clausulados de contratos e sugestões**: foram analisados os contratos da organização no qual são realizados tratamento de dados pessoais, e indicado se já estavam em aderência à LGPD. Quando não estavam, foi realizado o indicativo de ajuste.

- **Identificação de *Privacy by default* (privacidade por padrão) com os fornecedores de *software***: foram solicitadas aos fornecedores dos sistemas utilizados na empresa informações sobre medidas/configurações de privacidade construídas/implantadas nos sistemas;

- **Análise de maturidade da Segurança da Informação:** foram realizados a análise, o diagnóstico e as recomendações para Segurança da Informação na empresa.

- **Análise da infraestrutura tecnológica que sustenta a empresa (inventário de ativos)**: foi elaborada uma tabela de recursos, sendo a origem de todo o trabalho de proteção e salvaguardas de Segurança da Informação na empresa. Ela possui toda a lista dos componentes a serem protegidos, e deve estar atualizada para um melhor controle. A referida tabela está segmentada em vários grupos de ativos, como por exemplo máquinas (desktops e notebooks), servidores, *smartphones*, equipamentos de CFTV, *switchs*, *links* de comunicação etc.

- **Identificação de riscos à privacidade:** foi elaborada uma tabela de riscos de privacidade baseada no conjunto dos processos que tratam dados pessoais, incluindo-se a classificação do risco, a probabilidade de ocorrência, e medidas de resolução.

3.2.3. Etapa Construção e Execução

Esta etapa possui 7 metas, e estão alicerçadas para atender 3 pontos fundamentais que são: gerenciamento dos direitos individuais, gerenciamento de consentimento e rastreamento de preferências; e prevenção a violações. Adicionalmente, foram construídos o repositório das informações e artefatos que foram gerados para implantação e acompanhamento do programa como:

- **Definição do DPO** (*Data Protection Officer* - encarregado de dados): os requisitos para o cargo obedeceram a um conjunto de responsabilidades inerentes à função com uma base multidisciplinar de conhecimentos necessários à realização de atividades. Foram exigidas habilidades, escolaridade e competências técnicas, tais como: ensino superior completo ou cursando (em finalização) nas áreas relacionadas à tecnologia da informação, direito ou administração; certificação em LGPD/GDPR; e conhecimentos técnicos específicos em direito

do consumidor, marco civil da internet normas ISO/IEC ABNT 27.001, 27.002, 27.005, 27.701, metodologia ágeis, gestão de projetos.

- **Política de privacidade**: o documento contém informações de forma objetiva e transparente acerca de como são coletados e utilizados os dados pessoais dos clientes e possíveis colaboradores quando acessam o *website* institucional.

- **Termo de consentimento para tratamento de dados pessoais de colaboradores:** são detalhadas no documento as finalidades para que a empresa utiliza as informações pessoais para o cumprimento do contrato de trabalho, informando também sobre o tratamento e utilização para contratação de terceiros visando à prestação de serviço e melhor entrega das atividades essenciais empresariais.

- **Avisos de privacidade**: foram elaborados avisos para áreas internas da empresa com algumas dicas, enfatizando o compromisso de todos com a segurança dos dados. Também visando à privacidade das pessoas que frequentam a empresa, sejam colaboradores, clientes ou fornecedores, foi elaborado um aviso para coleta de imagens em todos os locais que possuem monitoramento.

- **Política de Segurança da Informação (PSI):** documento que define claramente a finalidade, a direção, os princípios e as regras básicas do Sistema de Gestão da Segurança da Informação (SGSI) na empresa.

- **Política de gestão de incidentes**: esta política tem como objetivo preparar a empresa para lidar com a gestão de um incidente de segurança garantindo que responda de forma mais rápida, organizada e eficiente ao evento, minimizando suas consequências para todos os envolvidos.

- **Política de gestão de direitos dos titulares de dados**: tem como objetivo definir um processo e preparar a empresa para garantir os direitos dos titulares de dados.

- **Criação de aditivo de proteção de dados:** atendendo às necessidades impostas pela LGPD, a empresa criou uma Política de privacidade e proteção de dados para Fornecedores, além de um Aditivo contratual de condições gerais de tratamento de dados pessoais para clientes e fornecedores ativos a fim de cumprimento da legislação.

- **Material de treinamento e aculturação:** Foi desenvolvido material de treinamento e uma cartilha que explanam os principais pontos das políticas e diretrizes que devem ser seguidos na empresa. Além da cartilha desenvolvida na empresa, foram divulgadas para os colaboradores cartilhas adicionais desenvolvidas pelo CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil).

- **RIPD (Relatório de Impacto à Proteção de Dados)**: este documento visa descrever os processos de tratamento de dados pessoais que podem gerar riscos

às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

- **Controles básicos de segurança**

É seguido na empresa o framework de segurança cibernética NIST (*National Institute of Standards and Technology*- Instituto Nacional de Padrões e Tecnologia), que se refere a um conjunto de boas práticas que fornece uma estrutura de política de orientação sobre segurança, guiando as organizações do setor privado como podem avaliar e melhorar sua capacidade de prevenir, detectar e responder a ataques cibernéticos [GAT InfoSec 2021].

Existem quatro camadas de implementação descritas na estrutura de segurança cibernética do NIST. As quatro camadas são: Nível 1 (Parcial), Nível 2 (Risco informado), Nível 3 (Repetível), Nível 4 (Adaptável). Atualmente, é utilizada a camada de Nível 1 que é a mais aderente ao tamanho e operação da empresa, para implementação em um prazo de um ano na instituição.

O *framework* contempla diversas referências informativas, e a escolhida pela consultoria para ser aplicada na empresa foi o CIS *Controls* do grupo de implementação 01 (um) que consiste em dezoito controles, informados na Figura 04. Alguns dos controles já tiveram medidas contempladas, outros ainda não.

Figura 04 – Controles do CIS

01 - Inventário e controle de ativos da empresa	02 - Inventário e controle de ativos de *software*	03 - Proteção de dados
04 - Configuração segura de ativos e *software* da empresa	05 - Gerenciamento de contas	06 - Gerenciamento de controle de acesso
07 - Gerenciamento contínuo de vulnerabilidade	08 - Gerenciamento de *log* de auditoria	09 - Proteção de e-mail e navegador web
10 - Defesas contra *malware*	11 - Recuperação de dados	12 - Gerenciamento de infraestrutura de rede
13 - Monitoramento e defesa de rede	14 - Treinamento de consciência e habilidades em segurança	15 - Gerenciamento de provedores de serviços
16 - Segurança de *software* de aplicação	17 - Gerenciamento de resposta a incidentes	18 - Teste de invasão

Fonte: Elaborado pela autora 2021

3.2.4. Etapa de Monitoramento

Esta etapa possui o objetivo de um monitoramento constante da organização. Por esta razão, é acompanhada pelo comitê de Privacidade e Segurança da Informação da companhia, que reúne os principais interessados que lideram e que são responsáveis por atividades de tratamento de dados pessoais da instituição, com competência para analisar, discutir, sugestionar e aprovar a elaboração de normas, políticas, relatórios e documentos, correspondentes ao tema. O time possui reuniões periódicas, e nestas são reportados os indicadores de performance do programa.

3.2.5 Normas e *frameworks* de melhores práticas utilizadas no programa

Além do já comentado framework NIST (*Cybersecurity Framework*) utilizado para os controles de segurança, no programa também são usadas como guias de aderência, tanto na privacidade como na segurança, algumas normas existentes no Brasil para a gestão destas práticas. Alguns exemplos: ISO/IEC 27.001 – Sistemas de gestão da segurança da informação – Requisitos; ISO/IEC 27.002 – Código de prática para controles de segurança da informação; ISO/IEC 29134 – Avaliação de impacto de privacidade – Diretrizes; ISO/IEC 29151 – Código de prática para proteção de dados pessoais.

3.3. Desafios vivenciados no programa de adequação

Toda nova prática traz consigo seus desafios, e com a LGPD não seria diferente. Muitas vezes, por falta de conscientização sobre os riscos, as pessoas não se protegem e acabam sendo as responsáveis por expor seus próprios dados. Esses descuidos acabam sendo reproduzidos no ambiente corporativo. A figura 05 apresenta os principais desafios vivenciados pela EmpresaX durante seu programa de adequação.

Figura 05 – Desafios durante o programa de adequação

Dificuldade dos colaboradores em adotar no dia a dia boas práticas de proteção dos dados
Resistência dos colaboradores quanto às medidas de segurança da informação adotadas
Baixo número de fornecedores em conformidade com a legislação
Dificuldade para organização de treinamentos em todas as filiais da empresa
Demonstrar a importância do engajamento de todos para que a organização cumpra as diretrizes da legislação

Fonte: Elaborado pela autora 2021

Durante a implementação de medidas para atendimento à LGPD na empresa, foi apresentada a dificuldade dos colaboradores em adotar no dia a dia boas práticas de proteção dos dados, tais como: não compartilhar, em hipótese alguma, contas e senhas com outras pessoas; não deixar senhas anotadas em *post-its* ou agendas; criação de senhas fortes; bloqueio de tela ao sair da seção de trabalho; não postar fotos de tela no ambiente de trabalho; evitar impressões desnecessárias e realizar o descarte adequado. Todas essas situações ocorrem pois a empresa ainda não adquiriu maturidade para a cultura de proteção de dados, é um processo gradual que requer engajamento de todas as áreas da companhia. Portanto, a fim de instruir os colaboradores foram expostas placas com boas práticas para proteção dos dados em todos os setores administrativos ou que manipulem dados pessoais.

Outro desafio encontrado no programa de adequação foi o baixo número de fornecedores em conformidade com a legislação, visto que a LGPD define obrigações para os agentes de tratamento, sendo que o controlador pode ser responsabilizado caso um operador infrinja as diretrizes da legislação. Com apoio da área de TI, foram solicitadas aos fornecedores dos softwares utilizados na empresa, informações sobre as medidas desenvolvidas em seus sistemas para a proteção dos dados pessoais, e foi perceptível a baixa maturidade de muitos fornecedores, que nem sequer tinham iniciado seus programas de adequação, e consequentemente não haviam tomado nenhuma medida visando à proteção dos dados. Para as novas contratações de fornecedores que tratarão de dados pessoais, está sendo realizada uma análise para verificar o atendimento à LGPD, e as empresas que já estão cumprindo as diretrizes da legislação possuem grande vantagem em relação às que não apresentam nenhuma medida.

Mediante a necessidade de implantação de medidas mais rígidas de segurança da informação, muitos colaboradores mencionaram que o setor de TI estava dificultando os processos da empresa, pois foram implantadas por exemplo, políticas que forçavam a criação de senhas fortes e sua troca periódica, havendo relatos de não conseguir lembrar de senhas com este padrão. Do mesmo modo, houve contrariedade com o bloqueio de acesso a determinados sites e a instalação de programas, em que apenas poderiam ser baixados softwares com a autorização do setor de TI, assim como a liberação de acesso a sites que previamente estivessem bloqueados, devendo informar qual a finalidade da navegação. Estes assuntos foram abordados no primeiro treinamento realizado, e serão reforçados nos próximos, para que os colaboradores se conscientizem das diretrizes corporativas estabelecidas, e do compromisso de cada um com a proteção dos dados.

Além dos desafios já citados, outra dificuldade foi a organização de treinamentos para disseminar a cultura de proteção de dados para todas as filiais da empresa que tenham colaboradores que manuseiam informações pessoais, pois alguns possuem pouco conhecimento em informática dificultando o acesso a plataforma de treinamento. Outra situação desafiante, foi demonstrar a importância do engajamento de todos para que a organização cumpra as diretrizes da legislação, sendo extremamente importante o apoio dos gestores para incentivar a participação nos treinamentos.

4. Considerações Finais

Ao decorrer deste trabalho foram apresentadas as diretrizes da legislação que versa sobre proteção de dados no Brasil e o processo pelo qual a EmpresaX vem passando para

cumprir os requisitos impostos pela legislação. A adequação à LGPD não tem finalização, pois trata-se de um trabalho contínuo, sendo sempre necessária a atualização dos processos e artefatos gerados durante o programa de adequação, assim como a conscientização dos colaboradores com intuito de demonstrar a relevância sobre o assunto e se promover uma mudança cultural de segurança e proteção de dados.

É de suma importância o comprometimento e engajamento da liderança, pois servirão de reflexo para os demais setores. A maior dificuldade será sempre a resistência dos colaboradores para mudanças de hábitos já consolidados na empresa, e que, através das novas diretrizes impostas para atendimento à legislação, irão afetar seus cotidianos.

Vale também salientar que, para se atingir os objetivos do programa de adequação, faz-se necessário o apoio e investimento da alta gestão, primeiramente na contratação de profissionais especializados para orientar as atividades que devem ser realizadas na empresa, e a aquisição de ferramentas visando assegurar a proteção dos dados, bem como o investimento em treinamento e conscientização de colaboradores.

A contribuição deste trabalho para a área de Computação é o alerta para os profissionais de TI diante das diretrizes da legislação de proteção de dados, uma vez que essa é a área que suporta tecnologicamente as empresas ou desenvolve soluções de *software* para elas. Sendo assim, estes profissionais não podem se omitir diante da responsabilidade que possuem para atender os requisitos para a proteção de dados, sendo de extrema importância o conhecimento sobre o assunto. Além disto, o trabalho visa contribuir com novos estudos sobre o tema, tendo em vista que há poucas publicações que demonstrem casos reais, servindo como base para quem busca conhecer um exemplo prático com medidas para adequação à Lei Geral de Proteção de Dados e os desafios vivenciados.

Como trabalho futuro, poderá ser realizado um novo estudo de caso, através de uma auditoria interna, para avaliar o nível de maturidade da organização com as novas diretrizes estabelecidas, assim como verificar a eficácia dos controles implementados visando à proteção dos dados.

Referências

Bisso, Rodrigo et al. Vazamentos de Dados: Histórico, Impacto Socioeconômico e as Novas Leis de Proteção de Dados. In: ESCOLA REGIONAL DE REDES DE COMPUTADORES (ERRC), 17, 2019, Alegrete. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2019. p. 154-159. DOI: https://doi.org/10.5753/errc.2019.9230.

Brasil. Lei 13.709, de 14 de Agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da República Federativa do Brasil. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12/09/2021.

Diário do comércio. (2021). Estudo revela que 40% das empresas ainda não se ajustaram à LGPD. Disponível em: <https://diariodocomercio.com.br/economia/estudo-revela-que-40-das-empresas-ainda-nao-se-ajustaram-a-lgpd/#>. Acesso em: 11/09/2021.

Garnier, Cíntia Miele; Padilha, Tamyris Michele. Ética, privacidade e novas tecnologias: o impacto da lei de proteção de dados na sociedade. [S. l.]: Portal Migalhas, 23 set. 2019. Disponível em: https://www.migalhas.com.br/depeso/311142/etica--privacidade-e-novas-tecnologias--o-impacto-da-lei-de-protecao-de-dados-na-sociedade. Acesso em: 25/09/2021.

GAT InfoSec. (2021). Implementação do NIST *Cybersecurity Framework*. Disponível em: https://www.gat.digital/blog/implementacao-do-nist-cybersecurity-framework/. Acesso em: 15/11/2021.

Gomes, Heloisa dos Santos. LGPD: Uma análise dos impactos da Lei na cultura e tratamento de dados no Brasil. 2019. Trabalho de Conclusão de Curso (Tecnólogo em Análise e Desenvolvimento de Sistemas) - Universidade do Sul de Santa Catarina, 2019. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/11112. Acesso em: 13/09/2021.

LGPD Brasil. (2021). 74% das empresas brasileiras não estão preparadas para a LGPD. Disponível em: https://www.lgpdbrasil.com.br/84-das-empresas-brasileiras-nao-estao-preparadas-para-a-lgpd/. Acesso em: 13/09/2021.

Lima, Victtor Henrique Pereira. LGPD Análise dos impactos da implementação em ambientes corporativos: Estudo de Caso. 2020. Trabalho de Conclusão de Curso (GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO) - PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS, 2020. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/108. Acesso em: 12/09/2021.

Oliveira, A. P. de. et al. A lei geral de proteção de dados brasileira na prática empresarial. 2019. Revista Jurídica da Escola Superior de Advocacia da OAB-PR, Curitiba, v. 4, n. 1, maio, 2019. Disponível em: http://revistajuridica.esa.oabpr.org.br/wp-content/uploads/2019/05/revista-esa-cap-08.pdf. Acesso em: 13/09/2021.

Pinheiro, Patricia Peck. Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD). 3. ed. São Paulo: Saraiva jur, 2021. 176 p.