DOI:

APPLYING THE LGPD IMPLEMENTATION APPROACH USING THE MOSE COMPETENCE

APLICAÇÃO DA ABORDAGEM DE IMPLEMENTAÇÃO DA LGPD USANDO O MOSE COMPETENCE

Maykon Araújo De Souza
UFPA - UNIVERSIDADE FEDERAL DO PARÁ - ORCID: https://orcid.org/0000-0001-7930-6384
Sandro Ronaldo Bezerra Oliveira
UFPA - UNIVERSIDADE FEDERAL DO PARÁ - ORCID: https://orcid.org/0000-0002-8929-5145

Abstract
Present an application of the LGPD implementation approach using the MOSE (Guiding Model for Enterprise Success) from a scenario.
Possibility to offer organizations an application model that helps the organization to implement chapter VII of the LGPD using MOSE.
Case Study and SWOT Analysis
Results of a case study applying the MOSE to the implementation of the LGPD.
Prior to the application of the Guide, Bank Z had 10 weaknesses that were reduced to one, ie 90% of the weaknesses were remedied by the application of the Guide.
It is suggested to use the proposed guide in real companies and scenarios so that, in this way, the approached process can be improved, in addition to improving the scenario of Brazilian companies that still need to implement the LGPD in their organization.

Key words: LGPD, MOSE Competence, Applying, Case Study, Evaluation

Resumo
Apresentar uma aplicação da abordagem de implementação da LGPD usando a MOSE (Modelo Orientador para o Sucesso do Empreendimento) a partir de um cenário.
Possibilidade de oferecer para as organizações um modelo de aplicação que ajude a organização a implementar o capítulo VII da LGPD usando o MOSE.
Estudo de Caso e Análise de SWOT
Resultados de um estudo de caso aplicando a MOSE para a implementação da LGPD.
Antes da aplicação do Guia o Banco Z tinha 10 fraquezas que foram reduzidas para uma, isto é, 90% das fraquezas foram sanadas pela aplicação do Guia.
Sugere-se a utilização do guia proposto em empresas e cenários reais para que, desta forma, melhore-se o processo abordado, além de melhorar o cenário das empresas brasileiras que ainda precisam implantar a LGPD na sua organização.

Palavras-chave: LGPD, MOSE Competence, Aplicação, Estudo de Caso, Avaliação

Applying the LGPD Implementation Approach using the MOSE Competence

ABSTRACT: LGPD will be fully enacted in august of this year, but reports indicate that most brazilian organizations are not yet adherent to the law. Provide an improvement in the scenario pointed out by the surveys. The first work was able to prove a relationship between the assets of Chapter VII of the LGPD and the MOSE Competence quality model, the second article by the authors of this work presented a set of guidelines for the implementation of Chapter VII in organizations based on the practices of MOSE. Now, the work presented here is intended to apply the authors' previous work in a simulated scenario in which Bank Z is a financial organization interested in complying with the general data protection law. In the end, this implementation was evaluated using the SWOT analysis that showed the elimination of 90% of the weaknesses regarding data protection, security and privacy in the organization.

Keywords: LGPD, MOSE Competence, Applying, Case Study, Evaluation.

Aplicação da Abordagem de Implementação da LGPD usando o MOSE Competence

RESUMO: A LGPD será promulgada em sua plenitude em agosto de 2021, mas relatórios apontam que a maioria das organizações brasileiras ainda não está aderente à Lei. Diante disso, procurou-se formular uma série de trabalhos que permitisse a implementação da LGPD nas organizações para, assim, prover uma melhora no cenário apontado pelas pesquisas. O primeiro trabalho conseguiu provar uma relação entre os ativos do Capítulo VII da LGPD e o Modelo de Qualidade MOSE Competence, o segundo artigo dos autores deste trabalho apresentou um conjunto de orientações para a implementação do Capítulo VII nas organizações a partir das práticas do MOSE. Agora, o trabalho aqui exposto tem por finalidade aplicar o trabalho anterior dos autores em um cenário simulado, no qual se tem o Banco Z como uma organização financeira com o interesse em se adequar à Lei Geral de Proteção de Dados. Ao final, essa implementação foi avaliada utilizando a análise SWOT que mostrou a eliminação de 90% das fraquezas referentes à proteção, segurança e privacidade dos dados na organização.

Palavras-chave: LGPD, MOSE Competence, Aplicação, Estudo de Caso, Avaliação.

Agradecimentos: Este trabalho pertence ao projeto SPIDER/UFPA (*http://www.spider.ufpa.br*).

1. INTRODUÇÃO

Este artigo está sendo escrito há poucos dias (julho de 2020) da promulgação dos artigos 52, 53 e 54 da LGPD (Lei Geral de Proteção de Dados), que são referentes às sanções administrativas. Assim, a partir da promulgação dos artigos citados, qualquer organização que descumpra a Lei estará sujeita à multa de até 2% do faturamento limitado a R$ 52 milhões por infração (BRASIL, 2018). Mesmo diante desse cenário, muitas instituições ainda não estão aderentes à LGPD, como mostra o relatório da Akamai feito em agosto de 2020 com a participação de 400 empresas brasileiras. O relatório mostrou que 64% das empresas não estavam em conformidade com a LGPD (AKAMAI, 2020). Outro número alarmante é mostrado pelo levantamento da BluePex, empresa nacional da área de segurança da informação, que aponta que só 2% das pequenas e médias empresas consideram-se totalmente preparadas para as normas da LGPD (BLUEPEX, 2020).

Então, com base nessas informações, procurou-se formular um trabalho de pesquisa para proporcionar uma melhora no cenário apresentado. Diante disso, é apresentada neste artigo uma aplicação da abordagem de implementação da LGPD usando a MOSE (Modelo Orientador para o Sucesso do Empreendimento). Nesse sentido, este trabalho justifica-se pela possibilidade de oferecer para as organizações um modelo de aplicação que ajude a organização a implementar o capítulo VII da LGPD usando o MOSE. A escolha do modelo de qualidade MOSE deu-se por se tratar de um modelo com foco no sucesso de empreendimentos de qualquer tipo e porte, o que está alinhado com a LGPD, pois essa abrange organizações de todos os tamanhos e tipos. Além disso, o MOSE possui em sua estrutura dimensões para gestão, qualidade, talento humano, inovação, cliente, mercado, sociedade e ambiente, que são essenciais para prover uma maturidade e capacidade nos processos de empreendimentos como esses (ROUILLER, 2017).

A pesquisa proposta por este trabalho é de natureza aplicada, onde os estudos e resultados gerados serão aplicados em um contexto simulado. Quanto aos objetivos, a pesquisa caracteriza-se como exploratória com um estudo sobre a Lei Geral de Proteção de Dados e do Modelo Orientador para o Sucesso do Empreendimento, implementação de leis de proteção de dados e trabalhos relacionados na literatura. Os procedimentos utilizados são a pesquisa bibliográfica e estudo de caso, aplicando também o método indutivo para a generalização da aplicação proposta para outras organizações e áreas de negócio além do contexto apresentado.

O restante deste artigo está organizado da seguinte forma: na Seção 2 é apresentada uma abordagem de uso da MOSE para a implementação da LGPD; a aplicação da abordagem de implementação da LGPD a partir das práticas do MOSE é apresentada na Seção 3; e, por fim, na Seção 4 são apresentadas as conclusões deste trabalho.

2. ABORDAGEM DE USO DA MOSE PARA A IMPLEMENTAÇÃO DA LGPD

O trabalho de DE SOUZA e OLIVEIRA (2021b) chegou a um conjunto de orientações para a implementação da LGPD a partir das práticas do modelo MOSE. Isso só foi possível graças ao primeiro trabalho dos autores que verificou uma relação entre os dois normativos por meio da percepção de que dos “45 objetivos da competência da MOSE 15 deles (33%), com as devidas adequações, tem aderência total aos 4 artigos (100%) do Capítulo VII da LGPD, ou seja, apenas 15 objetivos de competência constantes na MOSE são necessários para implementar na sua totalidade os itens constantes no Capítulo VII da LGPD” (DE SOUZA e OLIVEIRA, 2021a). Assim, por meio disso, foi possível a construção deste trabalho aqui exposto que trata da aplicação da implementação apresentada no trabalho anterior dos autores.

3. APLICAÇÃO DA ABORDAGEM

Esta seção descreve como aplicar a implementação da LGPD conforme explicitado no trabalho de DE SOUZA e OLIVEIRA (2021b), que apresenta um conjunto de orientações para implementação da LGPD a partir do MOSE, tratado aqui como Guia.

3.1 Objetivo

O objetivo deste trabalho é mostrar a execução e aplicação do conjunto de orientações para implementação da LGPD a partir do MOSE em conjunto com o Guia de DE SOUZA e OLIVEIRA (2021b). Para isso, devem-se executar os seguintes objetivos secundários:

- Definir um cenário simulado para a aplicação do Guia;
- Definir personas interessadas no resultado da simulação;
- Definir papéis e responsabilidades dentro do cenário simulado;
- Realizar uma análise sobre os elementos selecionados utilizando a técnica de análise SWOT (*Strengths, Weaknesses, Oppotunities e Threats*).

3.2 Metodologia

Nesta etapa do trabalho foi executada uma série de atividades bem definidas, como apresenta a Figura 1. A execução dessas atividades permitiu a elaboração de um cenário fictício para a execução da simulação objetivada, permitindo que uma análise SWOT fosse executada sobre as informações obtidas por meio da execução do processo proposta.

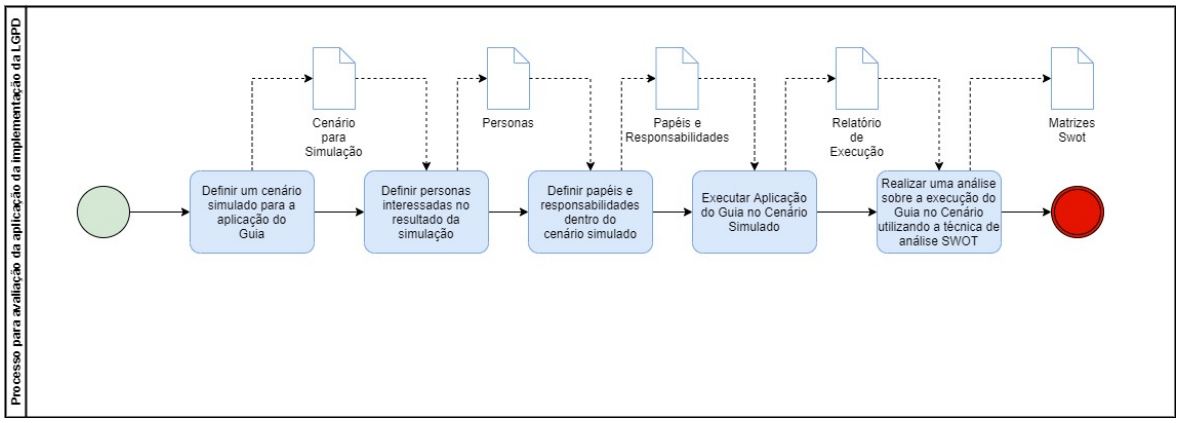

Figura 1. Metodologia da execução e análise da simulação
Fonte: Autor (2021)

Inicialmente, fez-se necessário definir um cenário para a aplicação do Guia. O cenário foi definido tomando por base uma instituição financeira, um banco, chamado aqui de Banco Z. A principal motivação para criar um cenário de simulação focada nesse tipo de instituição tem relação com o porte, a complexidade do seu processo de tratamento de dados, as ameaças ao negócio em caso de vazamentos de dados, dentre outros. Em resumo, os dados dos clientes de um banco são os principais ativos da organização. Diante disso, supõe-se que a implementação da LGPD é uma prioridade. Desta forma, acredita-se que esse cenário esteja alinhado com o trabalho aqui proposto.

Com base no cenário definido, foram criadas as personas interessadas na implementação da LGPD na organização. Assim, pelo aspecto positivo, têm-se desde a alta administração do Banco até o próprio cliente que tem o interesse de que seus dados estejam seguros na instituição. Por outro lado, pelo aspecto negativo, tem-se a

concorrência que pode se aproveitar da não implementação da LGPD no Banco Z como uma vantagem competitiva nos seus programas de marketing.

Após a definição das personas, o próximo passo é a definição dos papéis e responsabilidades dentro do cenário simulado. Nessa etapa serão conhecidos os participantes do processo de aplicação do Guia na instituição, bem como seus papéis, responsabilidades dentro do cenário proposto. Desta forma, ficará visível e de fácil compreensão qual individuo atuará em determinado processo e como isso se encaixa dentro da visão macro da implementação da LGPD.

Depois das definições de cenário, personas e papéis e responsabilidades, é chegada a hora de executar o Guia proposto por DE SOUZA e OLIVEIRA (2021b) no Banco Z. Essa etapa segue o passo a passo indicado no Guia. Desta forma, é criada uma instância da implementação do Guia no Banco Z, ao passo que é gerado um relatório de execução juntamente com um diagrama do Banco Z em que se têm os inter-relacionamentos entre personas, papéis e responsabilidades, LGPD e MOSE trazendo um panorama geral que demonstra como a Organização ficou após a implementação da LGPD a partir das práticas da MOSE.

Por fim, foi executada uma análise SWOT para avaliar a aplicação do Guia na instituição financeira. O objetivo principal da análise é o de identificar forças, fraquezas, oportunidade e ameaças da aplicação do Guia de DE SOUZA e OLIVEIRA (2021b) no Banco Z e assim apresentar aspectos positivos e negativos dessa aplicação.

3.3 Planejamento

Esta seção tem como foco principal apresentar o cenário de simulação e as suas principais característica.

3.3.1 Cenário

Para a execução e aplicação do Guia é necessário definir o cenário. A aplicação do Guia será realizada no Banco Z S.A., que é uma instituição financeira atuante em todo território brasileiro que conta com 93 mil colaboradores espalhados por cinco mil agências, além disso, contabiliza em sua carteira o total de 54 milhões de clientes, isso faz com que seu lucro bruto anual fique em torno dos R$ 30 bilhões. Assim, esses números caracterizam esse Banco como uma organização de grande porte (SEBRAE, 2013). A partir desse personagem central do cenário é possível perceber o quão importante é a adequação dessa organização à LGPD, pois essa trata de dados de milhares de colaboradores e milhões de clientes. Outro ponto para levar em consideração é que por se tratar de uma empresa de sociedade anônima de capital aberto, o Banco Z tem de prestar contas com os acionistas sobre os procedimentos que está realizando para mitigar os riscos da não adequação à LGPD.

Após o entendimento sobre a organização a qual será aplicado o Guia, o próximo passo é definir o contexto do cenário. Assim, em setembro de 2018 o Banco Z colocou como pauta das reuniões a implementação da LGPD na organização. Desta forma, em um primeiro momento fez-se os levantamentos necessários para entender o impacto da implementação da Lei, bem como os riscos da não implementação da lei no prazo de 48 meses. Assim, após o levantamento que teve como resultado de que a organização deveria o quanto antes está aderente a Lei Geral de Proteção de Dados, tendo em vista o elevado risco ao negócio. O Banco Z procurou uma forma, um guia para que orientasse a organização nessa nova empreitada. Então, chegou ao conhecimento da diretoria o Guia de DE SOUZA e OLIVEIRA (2021b) e ficou decidido de que seria esse o documento a ser utilizado na implementação da LGPD na empresa.

3.3.2 *Personas*

O Quadro 1 apresenta as duas principais *personas* para compor o cenário simulado. De um lado tem-se a Presidente do Banco Z que tem como principal preocupação a implementação padronizada da LGPD no Banco com o objetivo de proteger a Organização de uma série de problemas inerentes ao não cumprimento da Lei. Do outro lado é apresentado um cliente do Banco, que, de maneira geral, tem receio em fornecer seus dados para as instituições e espera mais transparência por partes dessas, além de ter a expectativa de ter mais controle sobre seus dados capturados pelas empresas.

Quadro 1 – Personas relacionadas ao Cenário Simulado

Persona	Perfil	Expectativas
Paula Silva e Souza	• Presidente do Banco Z há cinco anos; • 39 anos; • Passa maior parte do tempo em reuniões relacionadas às melhorias e resoluções de problemas do Banco; • Demonstra interesse em tornar o Banco aderente à LGPD.	• Encontrar uma maneira padronizada de implementar a LGPD no Banco; • Conseguir mensurar o quanto da LGPD foi implementada no Banco; • Proteger o Banco de perdas de receitas advindas de pagamento de multas e custas judiciais; • Mitigar o risco de vazamento de dados e assim proteger a imagem do Banco, os dados dos clientes e evitar ataques dos concorrentes; • Aumentar a segurança dos ativos informacionais que transacionam no Banco; • Atender à expectativa dos acionistas; • Promover segurança e comodidade aos clientes do Banco Z.
Lucas Neves da Costa	• Cliente do Banco Z; • 29 anos; • Dentista; • Passa maior parte do	• Que as organizações sejam mais transparentes no que vão fazer com seus

Persona	Perfil	Expectativas
	tempo atendendo clientes no seu consultório; • Mantém a sua renda pessoal e profissional em sua conta bancária de pessoa física; • Tem o conhecimento básico em tecnologia da informação; • Tem restrições ao fornecer seus dados pessoais com receio de que seja feito mau uso deles.	dados; • Ter mais poder e autonomia sobre os seus dados; • Aprender sobre seus direitos, deveres e cuidados que deve ter ao fornecer suas informações para as instituições.

Fonte: Autor (2021)

3.3.3 Papéis e Responsabilidades

Para melhor entendimento sobre o Banco Z, o Quadro 2 apresenta alguns papéis e responsabilidades presentes na Empresa.

Quadro 2 – Papéis e responsabilidades relacionadas ao Cenário Simulado

Papel	Responsabilidade
Presidente	Ter uma visão geral do ambiente interno e externo ao Banco Z e tomar todas as decisões relacionadas ao Banco. Participar de reuniões com a Diretoria Executiva para acompanhar de perto se o planejamento e as metas definidas estão sendo alcançadas. Ademais, tem o voto de minerva em pautas apresentadas em reuniões em que participa.
Diretor de Relacionamento com o cliente	Planejar, deliberar e apresentar em reuniões: pautas, temas e projetos relacionados à relação do Banco Z com os seus clientes.
Gerente de Segurança Corporativa	Responsável por tratar do planejamento, análise e deliberações relacionadas à segurança física e lógica do Banco Z.
Gerente de Compliance	Responsável por tratar do planejamento, análise e deliberações relacionados à adequação do Banco com a legislação e normas vigentes.
Gerente Jurídico	Responsável pela gestão estratégica jurídica do Banco
Gerente de Governança de TI	Responsável pelo Planejamento de TI, Gestão orçamentária de TI, Gestão da qualidade de TI, Contratação de soluções de TI, Gestão do catálogo de serviços de TI, Gestão de mudanças e liberações no ambiente, Gestão da arquitetura, Governança de Dados e Inovação.

Fonte: Autor (2021)

3.3.4 Execução

A execução do cenário simulado levou em consideração o trabalho de DE SOUZA e OLIVEIRA (2021b), que propõe um conjunto de orientações para a implementação do Capítulo VII da LGPD nas organizações a partir das práticas presentes no modelo de qualidade MOSE Competence. A execução aqui apresentada será dividida com foco na implementação de cada artigo do Capítulo VII: 46, 47, 48, 49 e 50; conforme organizado no trabalho dos autores. Desta forma, ao final será possível aferir o quanto da LGPD foi implementada no Banco Z. Será perceptível a preocupação de DE SOUZAS e OLIVEIRA (2021b) em formar uma estrutura base já no atendimento do artigo 46, assim o trabalho dos autores favorecem empresas que estão iniciando a implementação da LGPD.

Para uma melhor entendimento do contexto da implementação dos capítulos, entende-se que em determinado momento o Direito de relacionamento com o cliente do Banco Z, aqui denominado Diretor, levou para uma reunião da Diretoria com o Presidente uma pauta da importância da implementação da LGPD no Banco. Nesta reunião, ficou decidido que seria implementado a partir do trabalho, aqui denominado de Guia (DE SOUZA e OLIVEIRA, 2021b), ficando o Diretor como responsável pelo planejamento e pela execução da implementação. Assim, as seções a seguir demonstram como isso foi realizado.

3.3.4.1 Implementação do Artigo 46

Seguindo o que fora definido em (DE SOUZA e OLIVEIRA, 2021b), o Diretor levou para aprovação da diretoria e do Presidente do Banco a criação do Grupo de Trabalho LGPD (GT LGPD). O Diretor usou a justificativa dos autores para a criação desse grupo de trabalho, dizendo que "desta maneira, cria-se uma estrutura focada na implementação da Lei e a sua divulgação e promoção dentro da organização" (DE SOUZA e OLIVEIRA, 2021b). A criação do GT foi aprovada pela Diretoria e pelo Presidente do Banco.

No documento de criação do GT LGPD do Banco Z estavam definidos os papéis dos responsáveis por compor o grupo, então ficou definido, conforme o Guia, que o grupo seria composto por um Analista de Segurança da Informação, um Administrador e um Advogado especializado em Direito Digital. Também ficou definido que a chefia do GT LGPD ficaria na responsabilidade do Encarregado dos Dados. Além disso, neste mesmo documento ficaram definidas as seguintes responsabilidades do GT LGPD:

- Aprofundar os estudos e manter-se atualizados em relação à LGPD e outros normativos relacionados;
- Fomentar, realizar e promover palestras, workshops e outras atividades educacionais que envolva toda a organização, a fim de internalizar a LGPD na cultura organizacional;
- Pesquisar e indicar cursos, treinamentos e certificações para especialização dos agentes de tratamento e demais interessados;
- Quando demandado, analisar, validar, homologar e emitir relatórios de compliance de sistemas de informações com a LGPD;
- Sempre que possível, realizar estudos no mercado com a finalidade de inovar e/ou se antever as inovações que estão sendo praticadas pelas outras organizações no que se refere a novos processos e melhorias no cumprimento da Lei Geral de Proteção de Dados; e

- Assim, propor melhorias e inovações por meio da geração do Relatório de Propostas de Melhores Práticas no Cumprimento da LGPD que deve ser enviados e aprovados pela diretoria.

O GT LGPD, como sua atividade inicial, definiu um conjunto de passos a ser seguido para realizar o levantamento inicial para implementação da LGPD na organização. Esse levantamento é importante, pois fará com que o Banco Z entenda qual é o nível de maturidade da Organização para a implementação da LGPD. Assim, esse entendimento pode evitar que o Banco Z tenha custos desnecessários para implementar a Lei. A seguir serão apresentadas as atividades e as ações necessárias para o levantamento inicial, tendo como base (DE SOUZA e OLIVEIRA, 2021b).

- Realização de Diagnóstico Organizacional

Para o Guia, a realização do diagnóstico organizacional é importante para verificar qual é o nível de maturidade da organização em relação à proteção de dados, entender em qual estágio de adequação a organização está em relação à LGPD e aferir o nível de *compliance* de uma organização com a Lei Geral de Proteção de Dados. Para atender essa atividade, o GT LGPD realizou algumas ações conforme preconizado pelo Guia. As ações geraram os resultados vistos a seguir.

Foi feita uma pesquisa interna para levantar e documentar os seguintes itens: quais são os atos, normativos, regimentos, portarias, etc. que tratam de alguma forma sobre proteção de dados. Como resultado, averiguou-se que o Banco Z, por já ser regulamentado pelo Banco Central do Brasil, tinha internalizado em suas políticas de segurança o Normativo 023 – Segurança da Informação e das Comunicações criado em julho de 2018. Esse normativo trata dos seguintes temas: Metodologia De Gestão De Segurança Da Informação E Comunicações, Inventário E Mapeamento De Ativos De Informação, Gestão De Riscos De Segurança Da Informação E Comunicações, Gestão De Continuidade De Negócio Em Segurança Da Informação E Comunicações, Uso De Recursos Criptográficos Em Segurança Da Informação E Comunicações, Cópias De Segurança, Partes Externas, Planejamento Estratégico Da Informação, Controle De Descarte De Material Impresso E Digital, Indicadores De Desempenho Para A Gestão De Segurança Da Informação e Processo De Resposta A Incidentes De Segurança Da Informação. Além disso, são disponibilizados no Normativo os seguintes modelos de documentos: Termo de Responsabilidade, Plano de Segurança para Desenvolvimento de Sistemas, Checklist de Segurança para Desenvolvimento de Sistemas, Checklist de Descarte de Material Impresso e Digital, Termo de Uso de Recursos Criptográficos, Padrões Mínimos para Recurso Criptográfico Baseado em Algoritmo de Estado, Relatório de Comunicação de Incidente de Segurança em Redes Computacionais, Termo de Custódia dos Ativos de Informação relacionados ao Incidente de Segurança, Fluxo para Processo de Resposta a Incidentes de Segurança da Informação, Fluxo para Coleta e Preservação das Evidências, Fluxo para Comunicação as Autoridades Competentes, Fluxo para Comunicação entre o Banco da Amazônia e o CTIR Governo e Fluxo para Inventário de Ativos.

Seguindo as ações indicadas no Guia, o próximo passo foi verificar se o Banco Z tem uma matriz de riscos corporativos. Nesta busca, não se encontrou nenhuma norma referente ao assunto, o mais próximo que se encontrou foi um normativo de risco de mercado, avaliação de risco de crédito e matriz de responsabilidade de acesso ao site *backup* da instituição. Assim, o GT LGPD tratou de colocar no planejamento a criação de uma norma interna para tratar do tema de riscos operacional na instituição.

Outra ação desenvolvida pelo GT LGPD foi o de fazer a verificação da existência ou não de um departamento, programa ou normativo que aborda a gestão de *compliance* na

Organização. Assim, feito pelo GT LGPD, seguindo o Guia, verificou-se, então, a existência da Gerência Executiva de Controles Internos que trata de *compliance* nos processos gerenciais e processos finalísticos. Apesar disso, o GT LGPD colocou no planejamento que deve ser criada uma Política de *Compliance* para o Banco Z.

Com essas ações, o GT LGPD finalizou o diagnóstico organizacional proposto pelo Guia. O Quadro 3 apresenta o resumo e resultado final desse diagnóstico.

Quadro 3 – Resumo do Diagnóstico Organizacional

Ação	Resultado	A fazer
Levantamento de normativos internos referentes à proteção de dados.	Foi encontrado Normativo 023 que trata da segurança da informação e das comunicações do Banco Z. A partir desse normativo, percebeu-se que o Banco está adiantado em relação à segurança dos dados.	Deve-se avaliar este normativo e verificar se ele é suficiente para atendimento da LGPD.
Verificar a existência de uma matriz de riscos.	Não foi encontrada nenhuma norma ou documento referente à existência de uma matriz de risco.	Deve-se criar uma norma interna para tratar sobre o tema de risco operacional na organização.
Verificar a existência de um departamento, documento ou normativo que trata de compliance.	Existe uma gerência executiva que trata de controles internos e compliance em processos gerenciais e finalísticos.	Deve-se criar uma política de Compliance.

Fonte: Autor (2021)

- Levantamento das áreas/sistemas que fazem tratamento de dados

O GT LGPD realizou o levantamento das áreas que fazem tratamento de dados no Banco Z, as informações podem ser verificadas no Quadro 4. Esse quadro foi montado a partir do ciclo de tratamento de dados com base no item do Artigo 5 da LGPD (BRASIL, 2018). Assim, pode-se fazer a relação entre a área presente no Banco e a fase no ciclo de tratamento de dados em que ela atua.

Quadro 4 – Levantamento das áreas/sistemas que fazem tratamento de dados

Sistemas	Fase no ciclo de vida do tratamento	Quantidade das áreas
Agências	Coleta	5.000
ATMs	Processamento.	25.000
Sistema de Cadastro	Retenção, Processamento, Eliminação.	1
Sistema de Crédito	Retenção, Processamento, Compartilhamento e Eliminação.	1
Sistema de Dossiê Eletrônico	Retenção, Processamento, Eliminação.	1

Sistemas	Fase no ciclo de vida do tratamento	Quantidade das áreas
Sistema de abertura de conta	Coleta, Processamento.	1
Site Institucional	Coleta, Processamento.	1
Sistema de Recursos Humanos	Retenção, Processamento e Eliminação.	1
Sistema de Segurança de acesso ao prédio por biometria	Coleta, Retenção, Processamento e Eliminação.	1

Fonte: Autor (2021)

A partir da análise do Quadro 4 o GT LGPD concluiu que o Banco Z possui muitas áreas que realizam o tratamento de dados e que devem ser incluídas dentro do planejamento da implementação da LGPD.

- Definir o escopo da implantação da LGPD

Nesta etapa o GT LGPD definiu o escopo que, posteriormente, foi aprovado pela Diretoria e pela Presidência. Assim, o escopo ficou definido conforme apresentado no Quadro 5.

Quadro 5 – Escopo da implantação da LGPD no Banco Z

Documento de Escopo de Projeto			
Nome do Projeto	**Implementação da LGPD no Banco Z**	Responsável	**Encarregado dos Dados - GT LGPD**
Objetivo	*Stakeholders*	Documento de suporte	Reguladores
Para que o Banco Z fique aderente a Lei Geral de Proteção de Dados	**- Presidência - Diretoria - Colaboradores -Empresas parceiras - Colaboradores - Acionistas - Clientes do Banco**	**- Orientações para a Implementação do Capítulo VII da LGPD nas Organizações a partir das Práticas do MOSE Competence (De Souza e Oliveira, no prelo).**	**Lei Geral de Proteção de Dados (Lei 13.709/2018)**
Início	**25/07/2021**	Fim	**25/07/2023**
Áreas/Sistemas do escopo	**Agências**	**Sistemas de cadastros**	**Sistemas de crédito**
	Sistema de Dossiê Eletrônico	**Sistema de Abertura de Conta**	**Site Institucional**
	Sistema de Recursos Humanos	**Sistema de Segurança de acesso ao prédio por biometria**	**Caixas de autoatendimento (ATMs)**
Pessoas ou Grupo do Escopo	**Colaboradores das agências**	**Analistas de sistemas responsáveis pelos**	**Parceiros responsáveis pelos sistemas/ATMs do**

		sistemas do escopo	**escopo**
Executores			
- GT LGPD **- Agências** **- Gerência Executiva de Segurança da Informação** **- Gerência Executiva de Sustentação Sistemas de Informação** **- Gerência Executiva de Produção** **- Gerência Executiva de Relacionamento com os clientes** **- Gerência Executiva de Controles Internos** **- Gerência Executiva de Governança de Tecnologia da Informação**			

Fonte: Autor (2021)

- Criar e apresentar o *Roadmap* da implantação da LGPD na Organização

Nesta etapa o GT LGPD criou o *Roadmap* da implantação da LGPD no Banco que, posteriormente, foi aprovado pela Diretoria e pela Presidência.

- Criar e apresentar o Documento de Criação do Projeto

Nesta etapa o GT LGPD criou o Documento de Projeto da Implantação da LGPD que, posteriormente, foi aprovado pela Diretoria e pela Presidência.

Findo a etapa de definições e criações de Documentos, o Guia aponta que devem ser definidos os papéis e responsabilidades dos que participarão da implantação da LGPD no Banco. Assim, o GT LGPD conseguiu aprovar e indicar com a Diretoria os dois principais papéis que irão tratar da LGPD no Banco no dia a dia da Organização, conforme apresentado no Quadro 6.

Quadro 6 – Papéis que tratarão a LGPD no Banco

Papel	Responsabilidade
Encarregado dos dados	Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; Receber comunicações da autoridade nacional e adotar providências; Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares. (BRASIL, 2018). Chefiar e coordenar as ações do GT LGPD.
Operador	Responsável por fazer o tratamento de dados em nome do controlador (Banco Z). Este pode ser um colaborador interno ou externo à Organização e/ou todo aquele intervém em alguma etapa do processamento dos dados.

Fonte: Autor (2021)

Com os papéis definidos, o GT LGPD conseguiu adicionar cursos e treinamentos para os operadores, conforme preconizados pelo Guia. Além disso, seguindo recomendações, foi possível definir etapas de monitoramento e controle desses

treinamentos, visando verificar se eles surtiram os efeitos desejados e surtiram os impactos positivos dentro da organização.

Até aqui, o Guia montou uma base estrutural no Banco Z para que esse conseguisse evoluir com a implantação da LGPD. Observou-se a criação da estrutura do GT LGPD, foi realizado um diagnóstico da Organização para entender o nível de maturidade dela em relação à proteção de dados, foi designado um Encarregado dos Dados e foram detidos os operadores do Banco. Passada essa etapa, o próximo passo do GT LGPD foi definir e elaborar o PRISP (Plano de Respostas a Incidentes de Segurança e Privacidade). Então, o GT LGPD criou um documento contendo esse Plano e que, posteriormente, foi aprovado pela Diretoria. O GT LGPD modelou o processo contido no PRISP que pode ser apreciado na Figura 2. Com isso, o GT LGPD conseguiu atender o Artigo 46 da LGPD segundo (DE SOUZA e OLIVEIRA, 2021b).

3.3.4.2 Implementação do Artigo 47

O Artigo 47 tem por foco o de responsabilizar qualquer pessoa que intervenha durante o tratamento dos dados. Assim, conforme indicado no Guia, o GT LGPD abriu uma demanda com a Gerência de Recursos Humanos para adicionar os cargos de Encarregado de Dados e Operadores, bem como suas respectivas responsabilidades de acordo com o Quadro 6, no Documento de Plano de Cargos e Salários. O GT LGPD também formulou um Termo de Responsabilidade e Confidencialidade de Acesso de Dados Pessoais para ser distribuído e assinado pelo operador externo à Organização, empresas parceiras terceiras. Esta indicação está no Guia e o GT LGPD utilizou o mesmo *template* fornecido pelo documento, alterando somente as partes no que diz respeito ao Banco Z.

3.3.4.3 Implementação do Artigo 48

O Artigo 48 trata diretamente dos canais e as formas de comunicação de uma Organização com a Agência Nacional de Proteção de Dados (ANPD), os titulares de dados e as partes interessadas no tratamento de dados. Assim, seguindo as indicações do Guia, ficou já definido, como pôde ser visto no Quadro 6, que o Encarregado é o responsável pelas comunicações relacionadas à proteção dos dados. Outra indicação do Guia que foi atendido pelo Banco Z foi a criação de uma página no site institucional do Banco que trata especificamente sobre a Governança de Dados da Instituição. Ali estão o nome, o telefone e o e-mail do Encarregado; um espaço onde o titular pode fazer petições referentes aos seus direitos sobre os seus dados; uma área no qual serão colocadas as notícias sobre vazamento de dados, evitando assim propagações de notícias falsas.

Além disso, o GT LGPD elaborou o Documento de Notificação de Violação de Dados que será utilizado, conforme Figura 2, na etapa pertencente ao Encarregado no processo de Recuperação de Incidentes de Segurança. Esse documento contém as seguintes informações, além de informações padrões como responsável pelo tratamento e informações sobre o Encarregado dos dados: I - a descrição da natureza dos dados pessoais afetados; II - as informações sobre os titulares envolvidos; III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; IV - os riscos relacionados ao incidente; V - os motivos da demora, no caso de a comunicação não ter sido imediata; e VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Por fim, o GT LGPD também elaborou um modelo do Registro de Operações de Tratamento de Dados Pessoais (RoPA) para que, segundo (BRASIL, 2018), o controlador e o operador mantenham registros das operações de tratamento de dados pessoais que realizarem. Assim, foi criado a planilha RoPA, conforme o Quadro 7, e, em seguida,

distribuída para os responsáveis pelas áreas/sistemas apresentados no Quadro 4 para que esses fizessem preenchimento solicitado no documento.

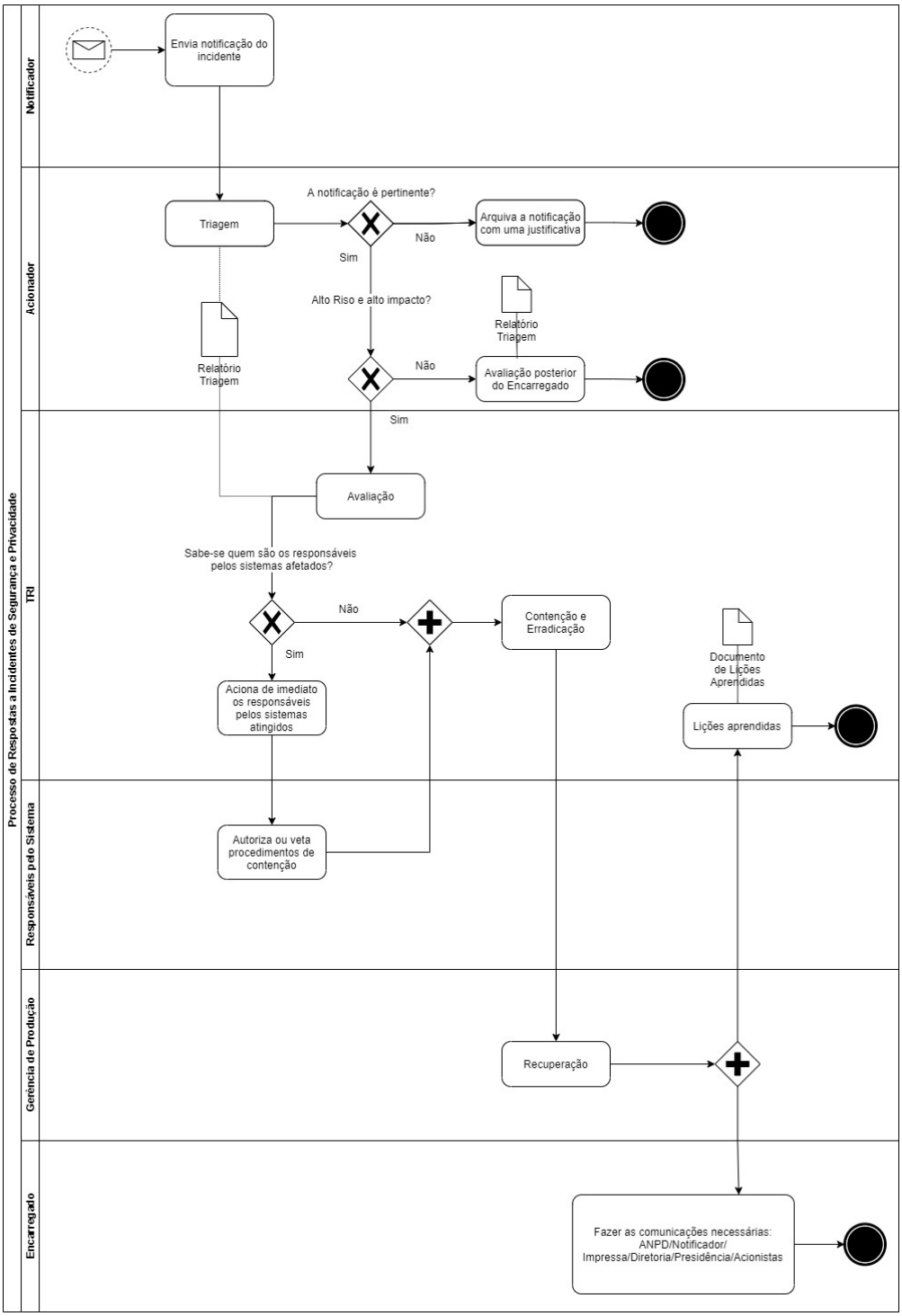

Figura 2 – Processo de Recuperação de Incidentes de Segurança no Banco Z
Fonte: Autor (2021)

Quadro 7 – Modelo do RoPA do Banco Z

Registro de Operações de Tratamento de Dados Pessoais (RoPA)	
Identificação do Processo	Código; Agente de tratamento no fluxo (controlador e operador); Área; Departamento; Responsável pelo departamento; Finalidade do tratamento; Detalhamento do tratamento; Tratamento automatizado (0 – sim, 1 – não); Quantitativo de Dados (> 1000, > 10000, etc.);
Sobre os Dados Pessoais	Código; Agente de tratamento no fluxo (controlador e operador); Área; Departamento; Responsável pelo departamento; Finalidade do tratamento; Detalhamento do tratamento; Tratamento automatizado (0 – sim, 1 – não); Quantitativo de Dados (> 1000, > 10000, etc);
Sobre os Sistemas	Origem do dado; Sistemas em que os dados transacionam; Operadores; Sistema(s) que armazena o dado.
Suporte Físico	Existe suporte físico (0 – não, 1 – sim); Segurança de suporte físico (0 – não, 1 – sim).
Transmissão e Compartilhamento Dos Dados Pessoais	Transmissão Interna (0 – não, 1 – sim); Transmissão Externa (0 – não, 1 – sim); Compartilhamento Dados (0 – não, 1 – sim); Compartilha com outras instituições (0 – não, 1 – sim); Ocorre a transferência Internacional dos dados pessoais (0 – não, 1 – sim).

Fonte: Autor (2021)

3.3.4.4 Implementação do Artigo 49

O Artigo 49 trata dos sistemas de informações. Estes devem estar aderentes à Lei. Assim, o GT LGPD seguiu as quatro etapas sugeridas pelo Guia com o objetivo de tornar os sistemas do Banco Z em *compliance* com a LGPD: 1ª fase – levantamento de sistemas ativos; 2ª fase - verificar a necessidade de atualização ou não desses sistemas, bem como a viabilidade técnica e financeira de atualizar o sistema de informação ou optar pela compra de outro que esteja aderente à LGDP; 3ª fase - executar a atualização e/ou compra de novos sistemas de informações; 4ª fase - monitorar, controlar e realizar melhorias contínuas nesses sistemas para que sempre fiquem aderentes às atualizações legislativas e normativas referentes à privacidade e proteção de dados dos titulares.

Assim, o GT LGPD reutilizou o Quadro 4, que já trazia consigo a listagem dos sistemas que fazem tratamento de dados no Banco, para atender a primeira fase. Após isso, para a fase 2, aproveitou-se o preenchimento do RoPA (Quadro 7) por parte das áreas da Empresa para verificar a necessidade de atualização ou compra de novos sistemas. Desta

forma, o GT conseguiu montar o Quadro 8 que apresenta as decisões tomadas pelo Grupo que sinalizou que a fase 4 será atendida a partir das atualizações da LGPD e que esse será o gatilho para iniciar a fase 1 novamente.

Quadro 8 – Decisões tomadas pelo GT LGPD sobre os Sistemas do Banco Z

Sistemas	Fase no ciclo de vida do tratamento	Atualiza ou Compra	Indicações
ATMs	Processamento.	Não se aplica	Não se aplica
Sistema de Cadastro	Retenção, Processamento, Eliminação.	Atualiza	Utilizar técnica de pseudoanonimização nos dados retidos de forma que os dados fiquem mascarados para terceiros sem acesso, mas que seja visível aos usuários com acesso ao dado. Utilizar trilha de auditoria no processo de eliminação dos dados.
Sistema de Crédito	Retenção, Processamento, Compartilhamento e Eliminação.	Atualiza	Utilizar técnica de pseudoanonimização nos dados retidos de forma que os dados fiquem mascarados para terceiros sem acesso, mas que seja visível aos usuários com acesso ao dado. Utilizar trilha de auditoria no processo de eliminação dos dados. Coletar aceite do Titular dos Dados autorizando o compartilhamento de suas informações com terceiros à Organização e Coletar assinatura do Agente de Tratamento terceiro que irá tratar os

Sistemas	Fase no ciclo de vida do tratamento	Atualiza ou Compra	Indicações
			dados. Utilizar trilha de auditoria no processo de eliminação dos dados.
Sistema de Dossiê Eletrônico	Retenção, Processamento, Eliminação.	Atualiza	Utilizar técnica de pseudoanonimização nos dados retidos de forma que os dados fiquem mascarados para terceiros sem acesso, mas que seja visível aos usuários com acesso ao dado. Utilizar trilha de auditoria no processo de eliminação dos dados.
Sistema de abertura de conta	Coleta, Processamento.	Atualiza	Coletar o aceite do Titular dos Dados para uso específico dos seus Dados em conformidade com a Politica de Privacidade e Tratamento de Dados.
Site Institucional	Coleta, Processamento.	Atualiza	Adicionar aceite de captura de cookies; Adicionar a área LGPD com informações do Encarregado, notícias sobre vazamentos de dados do Banco Z, espaço para petição do titular de dados e tira dúvidas; Adicionar a Politica de Privacidade e Tratamento de Dados.
Sistema de	Retenção,	Atualiza	Utilizar técnica de

Sistemas	Fase no ciclo de vida do tratamento	Atualiza ou Compra	Indicações
Recursos Humanos	Processamento e Eliminação.		pseudoanonimização nos dados retidos de forma que os dados fiquem mascarados para terceiros sem acesso, mas que seja visível aos usuários com acesso ao dado. Utilizar trilha de auditoria no processo de eliminação dos dados.
Sistema de Segurança de acesso ao prédio por biometria	Coleta, Retenção, Processamento e Eliminação.	Atualiza	Coletar o aceite do Titular dos Dados para uso específico dos seus Dados em conformidade com a Politica de Privacidade e Tratamento de Dados. Utilizar trilha de auditoria no processo de eliminação dos dados.

Fonte: Autor (2021)

3.3.4.5 Implementação do Artigo 50

O Artigo 50 trata da formulação de regras de boas práticas no tratamento dos dados por parte do Controlador, aqui no caso o Banco Z. Assim, seguindo as orientações do Guia, o GT LGPD criou o Programa de Governança em Privacidade – PGP que foi apresentado e aprovado pela Diretoria e Presidência do Banco. O PGP do Banco Z seguiu todas as etapas sugeridas no Guia e fez as devidas adequações para a realidade da Instituição. Assim como explicitado no Guia, o atendimento dos artigos anteriores atendem diversos itens, tais como: Nomeação do Encarregado; Alinhamento de Expectativas com a Alta Administração; Diagnóstico de Maturidade da Organização; Medidas de Segurança; Estrutura Organizacional e Gestão de Incidentes. Assim, aqui serão apresentados os itens como o GT LGPD aplicou os demais itens do PGP de DE SOUZA e OLIVEIRA (2021b), como: Levantamento de Contratos fechados com clientes, bem como com terceiros ou parceiras que fazem tratamento de dados; Políticas e práticas para proteção da privacidade; Cultura de segurança e proteção de dados e *Privacy by Design*; Relatório de Impacto à Proteção de Dados Pessoais (RIPD); Política de Privacidade; Adequação de cláusulas contratuais; Termo de uso e Inovação. Cujas instanciações para o estudo de caso realizado no Banco Z encontram-se a seguir:

- Levantamento de contratos fechados com os clientes, bem como com terceiros ou parceiras que fazem tratamento de dados e Adequação das cláusulas contratuais. O GT LGPD definiu novas cláusulas aderentes á LGPD para serem adicionadas aos contratos já vigentes e para comporem os modelos de contratos atuais;
- Políticas e práticas para a proteção da privacidade. O GT LGPD criou o documento de Políticas de Privacidade para serem adicionadas aos locais e sistemas que fazem coletas de dados para que, desta forma, o titular dos dados possa lê-lo e aceitá-lo. Assim, o Banco Z atende ao princípio de transparência, apresentando a sua real intenção no tratamento de dados;
- Termo de Uso. O GT LGPD criou o Termo de Uso dos sistemas que fazem coleta de dados dos usuários para coletar o aceite do usuário referente às informações presentes nele, como: aceitação dos termos e políticas; definições; arcabouço legal; descrição do serviço; direitos do usuário; responsabilidades do usuário e da Administração; mudanças no termo de uso; informações para contato; foro;
- *Privacy by Design e by Default*. O GT LGPD adicionou aos modelos de documentos de Análise e Requisitos de Sistemas itens referentes aos requisitos funcionais obrigatórios que protegem a privacidade do Titular dos Dados. Assim, a privacidade parou de ser somente um requisito não-funcional para algo que deve ser implementado nos projetos;
- Relatório de Impacto à Proteção de Dados Pessoais (RIPD). O GT LGPD atualizou o modelo do RoPA com as colunas "Mecanismos de Mitigação de Risco", "Medidas Adotadas para Salvaguarda dos Dados" para que as áreas responsáveis pelo tratamento de dados no Banco adicionassem a informação de quais mecanismos estão sendo utilizados para mitigação do risco em caso de vazamento dos dados, por exemplo, como foi solicitada a atualização dos sistemas para que esses mascarassem os dados, isso é um exemplo de um tipo de mitigação de dos riscos. Assim, foi possível atender a LGPD utilizando dois artefatos RoPA e RIPD de forma conjunta para mapear o tratamento de dados realizado na organização, além de apresentar o que a organização tem feito para reduzir os riscos em caso de um incidente de dados;
- Inovação. Foi agregada à função do GT LGPD a obrigatoriedade de manter-se atualizado com as práticas que o mercado vem adotando para se tornar aderente à LGPD com foco na redução dos custos e efetividade dos processos. Assim, ficou definido que o GT LGPD deverá participar de eventos nacionais que reúnem empresas para discutirem sobre a LGPD nas organizações financeiras, além de buscar treinamentos, workshops e palestras para que sejam trabalhados dentro da Organização com o objetivo de fomentar a cultura da proteção de dados com os demais colaboradores.

3.3.5 Avaliação

Para a avaliação da simulação será utilizada a análise SWOT que é uma ferramenta de avaliação estrutural e estratégica que tem como principal objetivo fazer uma análise nos ambientes internos e externos de uma organização apontando as forças, fraquezas, oportunidades e ameaças. A avaliação da simulação será feita em cada etapa da implementação da LGPD no Banco Z, isto é, será feita uma análise SWOT na Organização, no que diz respeito à segurança e privacidade dos dados, antes da

implementação do Guia, ou seja, antes do Banco implementar o Capítulo VII da LGPD, e, então, será feita uma análise SWOT do Banco após a implementação do Guia para que seja possível verificar como a organização evoluiu e reduziu suas fraquezas e ameaças e aumentou suas forças e oportunidades.

3.3.5.1 Análise SWOT antes da Implementação do Capítulo VII da LGPD

No contexto da implantação da LGPD no Banco Z, percebe-se que antes da implementação do Capítulo VII da Lei e usando como base o Guia de DE SOUZA e OLIVEIRA (2021b), o Banco apresenta dois pontos de força, dez pontos de fraqueza, dois pontos de oportunidades e dois pontos de ameaça, conforme ilustrado na Figura 3.

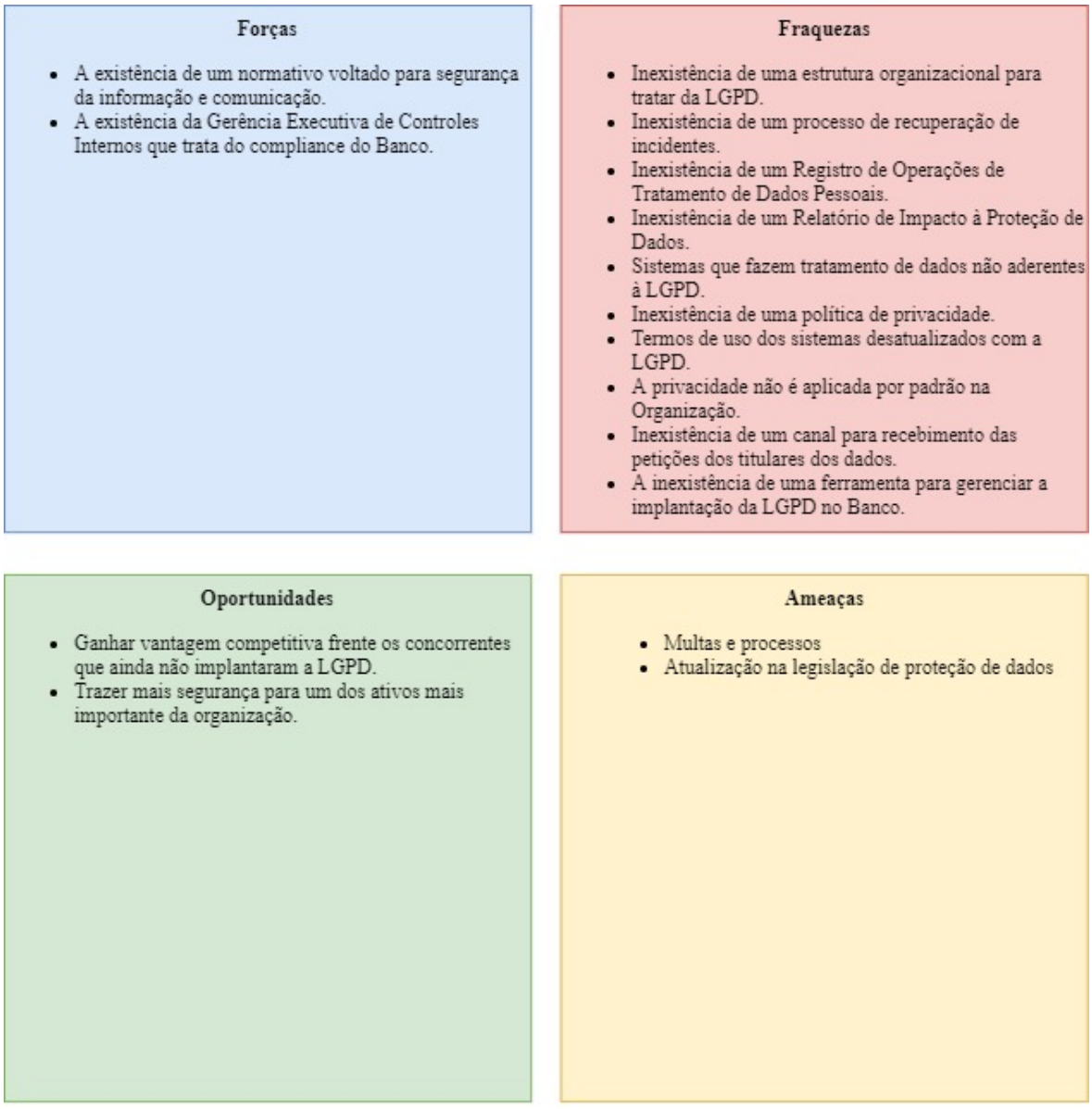

Figura 3 – Matriz SWOT antes da implementação do Guia
Fonte: Autor (2021)

3.3.5.1.1 Forças

Na primeira fase da implementação do Capítulo VII por meio do Guia, é feito um diagnóstico da organização para averiguar o seu nível de maturidade em relação à proteção de dados e a privacidade dos dados. Nesse diagnóstico, o GT LGPD levantou duas informações que são dadas como duas forças pela análise SWOT que são: a existência de um normativo voltado para a segurança da informação e comunicação, e a existência da Gerência Executiva de Controles Internos que trata do *compliance* do Banco. Assim, o Banco Z, mesmo não tratando de tópicos importantes da LGPD, já detinha uma base de segurança da informação e uma gerência voltada para *compliance* que no contexto da análise é visto como uma força.

3.3.5.1.2 Fraquezas

- Inexistência de uma estrutura organizacional para tratar da LGPD: o Banco não tem uma estrutura focada no tratamento da LGPD na Organização, isto faz com que não se tenha um foco na implementação da Lei;
- Inexistência de um processo de recuperação de incidentes: processo crítico e essencial em uma organização que está aderente à LGPD, pois um incidente que não seja tratado de maneira adequada pode trazer graves consequências para a empresa, como multas, perda de clientes, dentre outras;
- Inexistência de um Registro de Operações de Tratamento de Dados Pessoais: o RoPA é citado no Artigo 37 da LGPD e serve como prova do que a organização está fazendo para proteger os dados em caso de vazamento, por isso é essencial esse artefato em uma organização que realiza algum tipo de tratamento de dados;
- Inexistência de um Relatório de Impacto à Proteção de Dados: o RIPD é outro artefato exigido pela LGPD em seu Artigo 38, o qual pode ser solicitado a qualquer momento pela ANPD (BRASIL, 2018). Assim, é crucial que o Banco, por realizar tratamento de dados, tenha esse relatório disponível para caso seja necessário apresenta-lo para a ANPD;
- Sistemas que fazem tratamento de dados não aderentes à LGPD: por ainda não atender à LGPD, o Banco conta com diversos sistemas que fazem tratamento de dados, conforme levantamento do GT LGPD, mas esses ainda não detêm os mecanismos necessários de mitigação de riscos e proteção de dados condizentes com a legislação;
- Inexistência de uma política de privacidade: a Política de Privacidade é um documento que expressa como o Banco pretende realizar o tratamento de dados do titular. Assim, é crucial a existência deste documento para que o titular dê o seu aceite no momento em que entregar seus dados para instituição. Este documento também servirá de base para verificar se a Organização está realizando o tratamento de dados dentro do contexto previsto na Política;
- Termos de uso dos sistemas desatualizados com a LGPD: o Termo de Uso de qualquer produto ou serviço de uma organização que realiza o tratamento de dados deve estar aderente à LGPD uma vez que o titular dos dados deverá estar ciente de como o Banco irá realizar o tratamento de dados e, assim, dar o seu de acordo com o Tempo. Além disso, esse documento, assim como a Política de Privacidade, servirá como base para verificar se a Organização está realizando o tratamento de dados conforme acordado no Termo de Uso;
- A privacidade não é aplicada por padrão na Organização: o conceito de privacidade por padrão (*Privacy by Design*) torna a Organização alinhada com a proteção à

privacidade dos dados, uma vez que os seus produtos ou serviços estarão preocupados com a segurança dos dados desde a concepção. Esta também é uma preocupação da LGPD que traz essa informação no escopo da § 2º do Artigo 46, "as medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução" (BRASIL, 2018);

- Inexistência de um canal para recebimento das petições dos titulares dos dados: Com a promulgação da LGPD o titular dos dados passou a ter mais direitos sobre suas informações. Então, é crucial que uma organização que realiza o tratamento de dados disponibilize um canal de comunicação que seja de fácil acesso para que o titular de dados faça suas petições.

3.3.5.1.3 Oportunidades

Com os adventos da promulgação da LGPD, surgiram as seguintes oportunidades para a Organização:

- Ganhar vantagem competitiva frente os concorrentes que ainda não implantaram a LGPD: a implementação da LGPD na Organização tornou-se uma obrigatoriedade para as instituições financeiras, assim, o Banco Z sairá na frente da concorrência e aumentará sua vantagem competitiva no mercado em que atua;
- Trazer mais segurança para um dos ativos mais importantes da organização: a LGPD é um ganho para o cliente, mas um ganho ainda maior para a Organização, pois agora a proteção de dados tornou-se o foco principal, e, assim, os projetos que tenham esse escopo serão priorizados, trazendo mais segurança para o principal ativo da organização que são os dados dos seus clientes.

3.3.5.1.4 Ameaças

Por não está aderente à LGPD e por ser regulamentado pelo Banco Central do Brasil, o Banco Z tem que lidar com duas potenciais ameaças:

- Multas e processos: o Banco Z corre o risco de ter que pagar multas de até 2% do faturamento bruto anual conforme a LGPD (BRASIL, 2018), além de ter que arcar com custas processuais de processos movidos pelos titulares de dados;
- Atualização na legislação de proteção de dados: essa ameaça sempre estará presente, pois o Banco Z é uma instituição financeira que sempre estará sob constante ameaça do surgimento de novas regulamentações inerentes ao setor e, agora, pela própria LGPD.

3.3.5.2 Análise SWOT após a Implementação do Guia

Após a implementação do Guia pelo Banco Z, as fraquezas antes mapeadas tornaram-se forças e a ameaça de multa também foi eliminada, tendo em vista as implementações realizadas para a mitigação de risco, conforme mostra a Figura 4. Assim, tem-se agora 11 forças, 1 fraqueza, 2 oportunidades e 1 ameaça. Portanto, é perceptível que quase todas as fraquezas tornaram-se forças para o Banco Z no contexto da implantação da LGPD a partir da implementação do Guia. A única fraqueza que se manteve foi a inexistência de uma ferramenta ou sistema para gerenciar e acompanhar a implantação da LGPD no Banco.

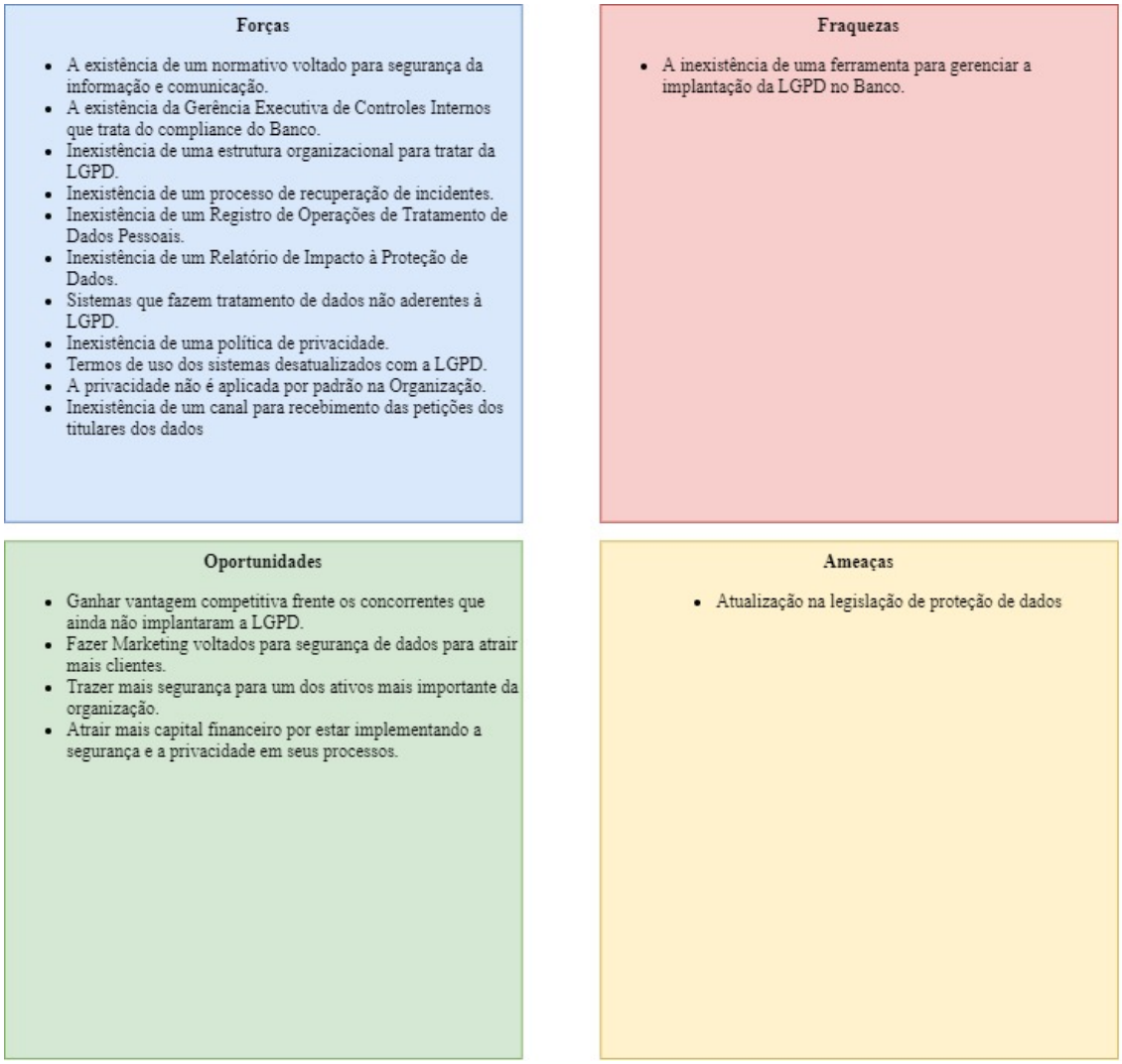

Figura 4 - Matriz SWOT após a implementação do Guia
Fonte: Autor (2021)

4. CONCLUSÕES

Mesmo após quase três anos da publicação da Lei Geral de Proteção de Dados, muitas organizações brasileiras não estão aderentes à Lei, segundo aponta os relatórios da AKAMAI (2020) e BLUEPEX (2020). Isso é alarmante, pois diversas empresas podem sofrer com sanções e multas advindas do descumprimento da Lei.

Este trabalho propôs-se a aplicar em um cenário simulado um conjunto de orientações para a Implementação do Capítulo VII da LGPD a partir das Práticas do MOSE Competence para que, desta forma, por meio de uma avaliação utilizando a análise SWOT fosse possível mostrar que a aplicação da implementação proposta trouxe resultados. Dentre eles, pode-se observar que antes da aplicação do Guia o Banco Z tinha 10 fraquezas que foram reduzidas para uma, isto é, 90% das fraquezas foram sanadas pela aplicação do Guia. Assim, com esse resultado sugere-se a utilização do guia proposto em empresas e cenários reais para que, desta forma, melhore-se o processo abordado, além de melhorar o cenário das empresas brasileiras que ainda precisam implantar a LGPD na sua organização.

Como trabalho futuro pretende-se expandir a implantação do Guia em outros diferentes cenários e realizar uma análise da sua eficácia no contexto da LGPD.

REFERÊNCIAS BIBLIOGRÁFICAS

AKAMAI. (2020). "Segurança, entrega na nuvem, desempenho". Disponível em *https://www.akamai.com*. Acesso em Julho/2021.

BLUEPEX. (2020). "Só 2% das PMEs estão preparadas para a LGPD, aponta pesquisa". Disponível em *https://www.bluepex.com.br/noticias/so-2-das-pmes-estao-preparadas-para-a-lgpd-aponta-pesquisa-2*. Acesso em Julho/2021

BRASIL. (2018). "Lei Geral de Proteção de Dados Pessoais (LGPD)". Disponível em *http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm*. Acesso em Julho/2021.

DE SOUZA, M. A. e OLIVEIRA, S. R. B. (2021a) "Adequação da MOSE® Competence para a Implementação do Capítulo VII da LGPD: Um Mapeamento dos Ativos de Segurança e Boas Práticas". Anais do Computer on the Beach, 12, 193-200. doi:https://doi.org/10.14210/cotb.v12.p193-200

DE SOUZA, M A. e OLIVEIRA, S. R. B. (2021b) "Orientações para a Implementação do Capítulo VII da LGPD nas Organizações a partir das Práticas do MOSE Competence". 18th CONTECSI VIRTUAL.

ROUILLER, A. C. (2017) "MOSE: Base de Competências". 2ª Edição. Recife, PE, Brasil.

SEBRAE. (2013) "Anuário do Trabalho na Micro e Pequena Empresa". 6a. ed.. Brasília, DF, Brasil.