DOI:

GUIDELINES FOR THE IMPLEMENTATION OF CHAPTER VII OF THE LGPD IN ORGANIZATIONS BASED ON THE PRACTICES OF MOSE COMPETENCE

ORIENTAÇÕES PARA A IMPLEMENTAÇÃO DO CAPÍTULO VII DA LGPD NAS ORGANIZAÇÕES A PARTIR DAS PRÁTICAS DO 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
Provide a set of guidelines for the implementation of Chapter VII of the LGPD from MOSE practices
Possibility to offer organizations a set of guidelines that help the organization to implement chapter VII of the LGPD using the MOSE
Literature Review, Asset Mapping and Guidelines for LGPD Implementation from the MOSE Model.
Guide with guidelines for the implementation of Chapter VII of the LGPD based on the best practices of the MOSE.
Reference material for implementing the LGPD in organizations of all sizes and consequently improving the current scenario, making more companies adapt to the LGPD.
Avoid fines that may harm the existence of organizations, in addition to keeping the company on an equal footing with the competition that will use adherence to the LGPD as a competitive advantage

Key words: MOSE Competence, LGPD, Implementation, Guidelines, Data Protection

Resumo
Fornecer um conjunto de orientações para a implementação do Capítulo VII da LGPD a partir das práticas do MOSE
Possibilidade de oferecer para as organizações um conjunto de orientações que ajudem a organização a implementar o capítulo VII da LGPD usando o MOSE
Revisão da Literatura, Mapeamento de Ativos e Orientações para a Implementação da LGPD a partir do modelo MOSE.
Guia com orientações para a implementação do Capítulo VII da LGPD a partir das boas práticas do MOSE.
Material de referência para implementação da LGPD em organizações de todo porte e por consequência melhorar o cenário atual, fazendo com que mais empresas se adequem à LGPD.
Evitar multas que venha a prejudicar a existência das organizações, além de manter a empresa em igualdade com a concorrência que venha a usar a aderência com a LGPD como diferencial competitivo

Palavras-chave: MOSE Competence, LGPD, Implementação, Orientações, Proteção de Dados

Guidelines for the Implementation of Chapter VII of the LGPD in Organizations based on the Practices of MOSE Competence

ABSTRACT: The LGPD is the brazilian law that deals with the protection and privacy of the data of natural persons. Failure by organizations to comply with the law can generate fines of 2% of the company's revenue. Even so, surveys and reports show that most organizations are not LGDP-compliant. In this scenario, it is necessary to provide a set of guidelines for implementing the LGPD. In the formulation of this guide, the MOSE Competence quality model was used, which aims to favor the success of enterprises through its practices and objectives. Thus, this work brings as a result, a set of guidelines for the implementation of Chapter VII of the LPGD based on the MOSE practices, thus seeking to help organizations adapt to this new law.

Keywords: MOSE Competence, LGPD, Implementation, Guidelines, Data Protection.

Orientações para a Implementação do Capítulo VII da LGPD nas Organizações a partir das Práticas do MOSE Competence

RESUMO: A LGPD é a lei brasileira que trata da proteção e privacidade dos dados das pessoas naturais. A não adequação à lei por parte das organizações pode gerar multas de 2% do faturamento da empresa. Mesmo assim, pesquisas e relatórios mostram que a maioria das organizações não está adequada à LGDP. Neste cenário faz-se necessário o fornecimento de um conjunto de orientações para a implementação da LGPD. Na formulação desse guia, usou-se o modelo de qualidade MOSE Competence que tem por objetivo favorecer o sucesso dos empreendimentos por meio de suas práticas e objetivos. Assim, este trabalho traz como resultado, um conjunto de orientações para a implementação do Capítulo VII da LPGD a partir das práticas do MOSE, buscando assim ajudar as organizações a se adequarem a essa nova lei.

Palavras-chave: MOSE Competence, LGPD, Implementação, Orientações, Proteção de Dados.

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

1. INTRODUÇÃO

A publicação da Lei Geral de Proteção de Dados (LGPD) em 2018 (Brasil, 2018) e, consequentemente após a sua promulgação, somada com a probabilidade de aplicações de multas (Brasil, 2018), fez com que as organizações públicas e privadas reavaliassem os seus processos internos referentes ao tratamento de dados para que, desta forma, adequassem-se à nova lei. Entretanto, uma pesquisa feita pela Akamai em agosto de 2020, envolvendo 400 empresas brasileiras, apontou que 64% dessas empresas não estavam em conformidade com a LGPD (AKAMAI, 2020), isto é, a Lei Geral de Proteção de Dados estava próxima de ser promulgada e as organizações ainda não estavam aderentes a ela. Também em 2020, a Codeby realizou uma pesquisa com cerca de 130 profissionais, atuantes em áreas como tecnologia, educação, jurídica, saúde, dentre outras, perguntando qual era a sua maior dificuldade com a LGPD, onde 42% responderam que a dificuldade estava na falta de informação sobre o assunto (CODEBY, 2020).

Baseado nessas informações, procurou-se formular questões com o objetivo de ajudar na melhora do cenário apresentado. Assim, chegou-se à primeira questão: com qual modelo de qualidade é possível implantar a LGPD e, assim, melhorar o cenário atual? A resposta satisfatória para essa pergunta foi respondida no trabalho de DE SOUZA e OLIVEIRA (2021), que concluiu que 33% da implementação das práticas do MOSE Competence têm 100% de aderência com o capítulo VII da LGPD. Diante dessa resposta foi possível formular uma segunda questão: é possível implementar o Capítulo VII da LGPD a partir das práticas do modelo de qualidade MOSE Competence?

Seguindo nessa direção, este trabalho justifica-se pela possibilidade de oferecer para as organizações um conjunto de orientações que ajudem a organização a implementar o capítulo VII da LGPD usando o MOSE. Assim, foi escolhido o MOSE por se tratar de um modelo com foco no sucesso de empreendimentos de qualquer tipo e porte, mas que possui em sua estrutura dimensões para gestão, qualidade, talento humano, inovação, cliente e mercado, e sociedade e ambiente, que são essenciais para prover uma maturidade e capacidade nos processos de empreendimentos como esses (ROUILLER, 2017).

Essa pesquisa tem por objetivo fornecer um conjunto de orientações para a implementação do Capítulo VII da LGPD a partir das práticas do MOSE. Ademais, a pesquisa caracteriza-se como exploratória com um estudo sobre o MOSE e a Lei Geral de Proteção de Dados, implementação de modelos de qualidade para a aplicação de leis de proteção de dados e trabalhos relacionados na literatura. A avaliação da pesquisa ocorreu por meio da técnica de revisão por pares com a participação de um especialista com experiência em implantação da LGPD e implementação de modelos de qualidades em organizações públicas e privadas.

O restante deste artigo está organizado da seguinte forma: na Seção 2 é apresentada a fundamentação teórica sobre o MOSE, a LGPD e o Capítulo VII da Lei; os trabalhos relacionados são apresentados na Seção 3; na Seção 4 são abordadas as metodologias de pesquisa utilizadas no trabalho; a implementação da LPD a partir do MOSE é detalhada na Seção 5; por fim, na Seção 7 são apresentadas as conclusões deste trabalho.

2. FUNDAMENTAÇÃO TEÓRICA

Esta seção discorre sobre a base teórica necessária para o bom entendimento do artigo.

2.1 MOSE Competence

Conforme descrito por ROUILLER (2017), o MOSE (Modelo Orientador para o Sucesso do Empreendimento) é um modelo de qualidade que “foi desenvolvido com o objetivo de dar suporte a empreendimentos para que estes se desenvolvam de forma saudável para que,

desta forma, sejam capazes de se manter no atual ambiente de negócios". Esse modelo de capacidade considera empreendimento como qualquer atividade humana que tenha por objetivo produzir bens ou serviços.

Um dos pilares do MOSE Competence são as dimensões de competência. Segundo ROUILLER (2017), "as cinco dimensões de competência devem ser trabalhadas para melhorar a competência e a capacidade das pessoas na organização, e consequentemente melhorar a capacidade de resolução de problemas". As dimensões do MOSE são: Talento Humano, Gestão e Qualidade, Cliente e Mercado, Inovação, e Sociedade e Ambiente. Estas dimensões são o foco principal deste trabalho. Reforça-se ainda que o objetivo deste trabalho é atingir as organizações de todo tipo e tamanho e o MOSE é a escolha ideal para ajudar nesse objetivo, pois, segundo ROUILLER (2017) o modelo de qualidade foi desenvolvido para ser implantando em qualquer tipo de empreendimento, além de contar com diretivas para organizações de pequeno, médio e grande porte.

Para ROUILLER (2017), a dimensão Talento Humano (TH) "aborda os aspectos relacionados às responsabilidades de cada indivíduo no empreendimento, a sua contribuição para produção dos bens e serviços e o desenvolvimento do negócio". A autora diz que o modelo considera a organização como um organismo vivo e que as pessoas são a peça chave para o sucesso de um empreendimento. A dimensão Gestão e Qualidade (GQ) "aborda aspectos relacionados à gestão da produção de bens e serviços e do próprio empreendimento" (ROUILLER, 2017). Além disso, a dimensão trata de assuntos como lições aprendidas e melhoria continua de processos de gestão e produção.

A dimensão Cliente e Mercado (CM) é definida por ROUILLER (2017) como a responsável por "abordar temas como a estruturação do empreendimento para poder atender de forma satisfatória seus clientes, a análise constante do mercado e o impacto dos bens e serviços gerados nele". A autora complementa dizendo que um empreendimento deve ter foco na geração de valor para si e para os clientes. Outra dimensão abordada por ROUILLER (2017) é a Sociedade e Meio Ambiente (SA), que "trata dos aspectos da inserção do empreendimento na sociedade à qual pertence. Esta dimensão se preocupa também com os aspectos relacionados à responsabilidade social e Ambiental". A autora também diz que essa dimensão da competência é importante por fazer com que os colaboradores sintam-se parte de um ambiente no qual estão colaborando para a sua evolução. Por fim, a dimensão de Inovação (IN) "aborda temas relacionados a olhar o negócio (atual ou novo) sob uma nova perspectiva, potencializando as oportunidades observadas no mercado" (ROUILLER, 2017). A autora complementa que a partir dessa dimensão, o empreendimento tem a capacidade de olhar para o mundo sobre uma nova ótica com o objetivo de criar novas oportunidades por meio das soluções de problemas que irão aparecer durante a existência do empreendimento.

Para ROUILLER (2017), uma dimensão da competência é formada por "três elementos mandatórios e devem ser observados em uma unidade de negócio para que seja possível concluir que uma determinada competência foi adquirida". Estes três elementos são: Objetivos da Competência, que "detalham os objetivos que a unidade de negócio devem alcançar para atingir as competências do MOSE, ou seja, deve poder ser observado na unidade de negócio para alcançar uma determinada competência"; Resultados Esperados, que são formas de avaliar se um empreendimento atingiu ou não um objetivo da competência; e Indicadores Obrigatórios, que "detalham indicadores que devem ser analisados pelas pessoas da unidade de negócio quando se deseja atingir um determinado objetivo de uma competência". Este trabalho utiliza os Objetivos da Competência e os Resultados Esperados, pois o foco é a construção de um conjunto de orientações.

2.2 Lei Geral de Proteção de Dados (LGPD)

A Lei Geral de Proteção de Dados – LGPD foi publicada em 14 de agosto de 2018 e "dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (BRASIL, 2018).

A Lei Nº 13.853 de 8 de julho de 2019 trouxe em seu escopo a criação da ANPD (Agência Nacional de Proteção de Dados) e sobre as datas de entrada em vigor da Lei e seus artigos, ficando assim: os artigos 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B entraram em vigor dia 28 de dezembro de 2018 (BRASIL, 2018). Por sua vez a Lei 14.010, de 2020, diz que em 1º de agosto de 202 entra em vigor os artigos 52, 53, e 54 que tratam das sanções administrativas (BRASIL, 2018). Os demais artigos entraram em vigor quando fez 24 meses após a data da publicação da Lei, isto é, em agosto de 2020 (BRASIL, 2018). Assim, de forma resumida, a Lei está em vigor atualmente e a ANPD está criada. Aguarda-se somente a promulgação dos artigos referentes às sanções administrativas. Com isso, as empresas ganharam mais algum tempo para continuar com o seu processo de adequação à LGPD, tornando assim este artigo pertinente e atual.

3. TRABALHOS RELACIONADOS

Foi realizada uma busca na literatura especializada com o objetivo de encontrar trabalhos publicados relacionados à implementação de uma lei de proteção de dados nas organizações a partir de modelos de qualidade, *frameworks* ou outras tecnologias. Neste sentido, foram encontrados trabalhos referentes à implementação da LGPD e da lei europeia GDPR (*General Data Protection Regulation*).

ROUILLER (2020) apresenta o *framework* MOSE.LGPD que, segundo a autora, "promove a implantação da LGPD em ciclos incrementais que proporcionam o aumento da capacidade e maturidade da organização na sua execução, cumprimento e aprimoramento". Esta forma de implementação é orientado pelo MOSE, isto é, a partir da implementação do MOSE, pode-se aferir que a LGPD foi atendida de alguma forma.

Os pesquisadores LOPES, GUARDA e OLIVEIRA (2019), por sua vez, propõem verificar se o processo de adequação das organizações é de alguma forma facilitado pela implementação da ISO 27001. Essas verificações e validações são feitas por meio da análise dos dois normativos e buscas em sites de discussão sobre a implementação da GDPR pela ISO 27001. O trabalho conseguiu comprovar que, apesar da ISO 27001 não atender completamente a GDPR, uma organização que tenha implementado essa ISO pode simplificar o seu processo de adequação.

O trabalho (TRUONG *et al.*, 2019) tem por objetivo de prover o gerenciamento de dados pessoais em conformidade com a GDPR por meio de uma solução baseada em *blockchain*. Isto deve ser feito por uma plataforma que permite que: o titular dos dados dê consentimento e permissão para o uso dos seus dados; garante que somente as partes autorizadas processem os dados pessoais; todas as atividades sejam registradas em um livro-razão imutável que usa contrato inteligente e criptografia. Assim, qualquer violação ocorrida com os dados será gravada como uma informação que não poderá ser modificada futuramente, o que facilita a descoberta de descumprimentos da Lei.

TORRE *et al.* (2020) propõem um modelo conceitual para caracterizar o conteúdo da informação previsto pela GDPR para as políticas de privacidade e uma abordagem assistida por Inteligência Artificial (IA) para classificar o conteúdo da informação em políticas de privacidade do GDPR. Essas abordagens foram validadas por meio de um

estudo de caso que teve uma precisão de 85%. Com esse trabalho, os autores pretendem, com o uso de IA, validar se determinada política empresarial está de acordo com a GDPR.

O trabalho de RIBEIRO e CANEDO (2020) faz uso dos métodos *Multi-Criteria Decision Analysis* (MCDA), *Preference Ranking Organization Method for Enrichent Evaluation* (PROMETHEE II) e *Analytic Hierarchy Process* (AHP) para selecionar a melhor alternativa para a implantação dos critérios de segurança da LGPD na Universidade Federal de Brasília (UNB). Aplicando esses métodos, os pesquisadores descobriram que o risco à privacidade dos dados é um dos temas com maior prioridade para a implementação de uma política de segurança de dados pessoais na UNB.

Por fim, o trabalho de SILVA, CALEGARI e GOMES (2019) cita o problema de aderência entre sistemas web descentralizados com a nova Lei Geral de Proteção de Dados brasileira Para ajudar as empresas com a dificuldade de se manterem aderentes à LGPD, os pesquisadores apresentam o *Sfinge Guardian Framework* que fornece uma estrutura de autorização refinada em conformidade com a LGPD para aplicativos web descentralizados.

O artigo aqui apresentado tem por objetivo realizar a implementação da LGPD por meio das práticas do MOSE usando como referência a LGPD, isto é, pega-se artigo por artigo do Capítulo VII da Lei e, a partir deles, procura-se implementá-los usando os objetivos da competência do MOSE com base no mapeamento de DE SOUZA e OLIVEIRA (2021). Assim, consegue-se aferir o quanto da LGPD foi implementado utilizando o MOSE. Diferente dos trabalhos de ROUILLER (2020) e LOPES, GUARDA e OLIVEIRA (2019), que seguem uma abordagem oposta, isto é, a partir dos normativos por eles escolhidos, seja MOSE.LGPD ou ISO 27001, entende-se que a LGPD foi atendida ou a sua implementação será facilitada de alguma forma, ficando, desta forma, impossível saber quanto de uma lei de proteção de dados foi implementada. Ademais, os outros trabalhos necessitam que a organização tenha implementado uma lei de proteção de dados para que seus trabalhos façam sentido. Dito isso, nota-se que o diferencial da implantação da LGPD a partir das práticas do MOSE proposta neste trabalho é a possibilidade de fornecer um conjunto de orientações para a implementação da Lei que atenda organizações de todos os tipos e tamanhos, não excluindo assim as organizações que estão começando. Desta forma, este artigo propõe um conjunto de orientações que implementa o Capítulo VII da LGPD em sua plenitude, passando pelas fases de planejamento, execução, monitoramento e controle e melhoria contínua.

4. METODOLOGIA DE PESQUISA

Esta seção descreve qual a metodologia de pesquisa adotada neste artigo.

4.1 Revisão da Literatura

A construção deste trabalho passou pelas seguintes fases de revisão da literatura: estudos sobre o MOSE Competence e a LGPD. Na sequência foi escolhido o capítulo da LGPD que poderia ser implementado por um modelo de qualidade. Então, foi escolhido o capítulo VII, sob a justificativa de: ter em seu escopo um viés passível de implementação em relação aos outros capítulos que apresentam definições, direitos e garantias da Lei; por abranger a área de interesse de estudo dos autores, pois trata da segurança da informação e das boas práticas organizacionais que são assuntos presentes no escopo da Ciência da Computação. O próximo passo foi buscar na literatura por trabalhos relacionados a este.

4.2 Mapeamento do MOSE para a LGPD

A primeira fase do trabalho de pesquisa, no qual este artigo faz parte, tinha o objetivo de responder à seguinte questão de pesquisa: existe uma correlação entre os normativos

MOSE e LGPD? Para isto, foi necessário estudar a fundo os dois normativos, fazer um mapeamento inicial e submeter o mapeamento para revisão por pares com um especialista. Após a revisão por pares, foram feitas as correções apontadas e, por fim, publicou-se o trabalho (DE SOUZA e OLIVEIRA, 2021), que teve como resultado "a percepção de que dos 45 objetivos da competência do 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". Diante dessa confirmação foi possível evoluir a pesquisa para a próxima fase, que trata da implementação da LGPD a partir do MOSE.

4.3 Implementação da LGPD a partir do MOSE

Após a publicação do artigo mencionado anteriormente e com a validação de que existe uma relação entre os normativos MOSE e LGPD, foi possível ir para a fase de construção do conjunto de orientações para a implementação da LGPD a partir do MOSE. Nesta fase, iniciou-se pela reciclagem no estudo sobre LGPD e a MOSE. Em relação à implementação desses dois normativos, encontrou-se na literatura os guias operacionais para a adequação à LGPD disponibilizados pelo Governo Federal do Brasil (BRASIL, 2020). Desses guias disponibilizados, aprofundou-se os estudos no Guia de Elaboração de Programa de Governança e Privacidade e no Guia de Boas Práticas – LGPD. Além disso, encontraram-se outros guias de implementação da LGPD para a complementação do estudo e melhor entendimento de uma estrutura ideal para à adequação de uma organização à LGPD.

Com base nos estudos das estruturas e com o conhecimento já adquirido no Modelo MOSE e na própria LGPD, foi-se então para a construção do conjunto de orientações para a implementação da LGPD a partir das práticas da MOSE. O conjunto de orientações foi construído capítulo a capítulo da LGPD, isto é, iniciou-se pela implementação do capítulo 46 utilizando os objetivos da competência do MOSE mapeados em (DE SOUZA e OLIVEIRA, 2021). Ao finalizar o capítulo 46, esse passou pela revisão por pares com o especialista, que propôs as correções por meio do formulário de revisão por pares. Assim, sucessivamente ocorreram com os outros artigos do Capítulo VII: 47, 48, 49 e 50. Feito esse processo com o capítulo VII, teve-se pronto o conjunto de orientações revisado e finalizado.

5. IMPLEMENTAÇÃO DA LGPD A PARTIR DO MOSE

Esta seção apresenta a abordagem de implementação dos ativos do capítulo VII da LGPD a partir do modelo de qualidade MOSE Competence. Antes disso, será descrito o cenário que será o ponto de partida e o alicerce para essa pesquisa. Para melhor entendimento deste trabalho, a implementação será apresentada de forma que os ativos da LGPD sejam atendidos na sequência, a saber: Artigo 46, Artigo 47, Artigo 48, Artigo 49 e Artigo 50. Desta forma, esta seção ficou estruturada conforme o Quadro 1, com base no mapeamento proposto em (DE SOUZA e OLIVEIRA, 2021).

Quadro 1 – Mapeamento dos objetivos da competência do MOSE para a LGPD

Artigo LGPD	Objetivos da Competência mapeados do MOSE
46	GQ.1, GQ.2, GQ.4, TH.1, TH.2, TH.6, TH.8, CM.9
47	TH.1
48	CM.8, CM.9, GQ.7, GQ.3
49	GQ.6, CM.3, CM.4
50	GQ.3, GQ.1, GQ.2, CM.7, TH.1, TH.6, GQ.9, GQ.4, GQ.7, IN.1, GQ.6, CM.4, CM.9

Fonte: (DE SOUZA e OLIVEIRA, 2021).

Para um bom entendimento do Quadro 1, na coluna sobre Objetivos de Competência as siglas de letras referem-se o nome das áreas de competência da MOSE relatadas na Seção 2, já as numerações representam os objetivos de competência constantes nestas áreas. A proposta de abordagem será apresentada a partir do ativo da LGPD e seguirá com os respectivos objetivos da competência, práticas e artefatos que devem ser utilizados na implementação deste ativo.

5.1 Ativo LGPD: Artigo 46

Este ativo da LGPD diz que é responsabilidade dos agentes de tratamentos, controlador e operador, a adoção de medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Essas medidas deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução (BRASIL, 2018). Os objetivos da competência citados no Quadro 1 devem ser implementados em conjunto para a obtenção dos resultados esperados do artigo 46 da Lei. As subseções a seguir detalharão esta implementação.

5.1.1 GQ.1 Estruturas básicas para a gestão da unidade de negócio são estabelecidos e mantidos

O objetivo da Competência GQ.1 está contido na dimensão Gestão e Qualidade da MOSE. Essa dimensão aborda dois aspectos principais: (1) gestão da unidade de negócio e da produção de bens e serviços, (2) qualidade dos bens e/ou serviços produzidos.

Conforme descrito em (ROUILLER, 2017), entende-se que gestão da unidade de negócio trata do controle das atividades que são executadas e o fornecimento de informações para tomadas de decisões. A autora assevera ainda que a gestão envolve planejamento, monitoramento e controle dos parâmetros necessários para realizar as entregas previstas nos acordos estabelecidos. Desta forma, é possível entregar qualidade dos bens e/ou serviços produzidos.

Então, para que essa implementação obtenha sucesso, é necessário que a empresa estabeleça e mantenha uma estrutura básica para as unidades de negócios que serão impactadas pela legislação. Assim, é sugerido que seja criado um Grupo de Trabalho para tratar da implantação da LGPD (GT LGPD) na organização. Desta maneira, cria-se uma estrutura focada na implementação da lei e a sua divulgação e promoção dentro da organização. A próxima seção que trata do objetivo da competência GQ.2, tratará de forma mais aprofundada sobre os papéis e responsabilidades das estruturas de gestão acima.

Assim, fica definido que o Grupo de Trabalho com foco na LGPD (GT LGPD) é o responsável pelo primeiro passo da organização em direção à implementação da LGPD. Um grupo de trabalho é uma reunião de pessoas para a realização de uma tarefa específica e em que cada um dos membros contribui com o grupo de acordo com suas capacidades individuais. Está definição está de acordo com o propósito da criação deste grupo de trabalho, pois é necessário unir pessoas que detém conhecimento em determinadas áreas específicas no escopo da LGPD e da MOSE para tratar do início do processo de implantação da Lei. Sugere-se aqui um grupo de especialistas, não se limitando a estes, nas áreas de Segurança da Informação, Administração e Direito Digital.

5.1.2 GQ.2 Abordagens para gestão de equipes da Unidade de Negócio são estabelecidas e mantidas

Definir estruturas básicas de gestão para implementação da LGPD é uma forma de concretizar o objetivo da competência GQ.1. Nesta seção será melhor detalhada a estrutura

de gestão criada. ROUILLER (2017) diz que este objetivo da competência está preocupado com a gestão do objeto de estudo em si. Diante disso, a organização, após definida as estruturas de trabalhos propostas no GQ.1, deve elencar quais colaboradores devem assumir os postos de trabalhos das estruturas criadas, bem como suas responsabilidades e atividades dentro da organização.

As funções do GT LGPD iniciam-se antes da implantação da LGPD na organização. Deve ser realizado um mapeamento inicial para identificar a maturidade da organização em relação à Lei Geral de Proteção de Dados, Gerenciamentos de Riscos e Segurança da Informação. Este mapeamento é importante para construção do *Roadmap*, definição do escopo da implantação e construção do cronograma de implantação da LGPD na organização. Assim, inicia-se a fase de concepção da implantação da LGPD na organização com as seguintes atividades dispostas no Quadro 2 a serem cumpridas pelo GT LGPD. As atividades descritas no Quadro 2 usam como base a proposta de SILVA (2020) em seu trabalho com implantação da LGPD em instituições de ensino. Entendendo o quadro, têm-se a coluna Atividade que conterá as atividades a serem exercidas pelo GT LGPD, por sua vez a coluna Descrição mostra mais detalhes dessa atividade. A coluna Ações diz respeito às ações que devem ser realizadas pelo GT LGPD para cumprimento da respectiva atividade e, por último, a coluna Artefatos sugere artefatos que podem ser criados para documentar o que foi realizado na atividade.

Quadro 2 – Levantamento inicial para a implementação da LPGD na organização

Atividade	Descrição	Ações	Artefatos
Realizar Diagnóstico Organizacional	Realização de estudos sobre a organização para verificar qual é o seu nível de maturidade em relação à proteção de dados, qual o tamanho da sua estrutura em relação aos dados que serão tratados, em qual estágio de adequação a organização está em relação à LGPD. Este levantamento inicial tem por objetivo entender o tamanho da organização e saber o que ela já tem de compliance com a LGPD antes mesmo da implementação da Lei para evitar custos com tempo e recursos desnecessários.	Levantar e documentar as seguintes informações sobre a organização: natureza jurídica, segmento de atuação, porte da empresa, tipo de gestão ou governança adotada, organograma, quais são os terceiros ou parceiros da organização, quais são as políticas públicas ou projetos sociais que a organização participa e as legislações que afetam a instituição.	Documento de Levantamento Inicial Sobre a Organização.
		Deve-se fazer uma pesquisa interna e levantar e documentar os seguintes itens: quais são os atos, normativos, regimentos, portarias, etc. que tratam de alguma forma sobre proteção de dados.	Documento de Listagem de Normatização Interna sobre Tratamento de Dados na Organização.
		Para verificar a maturidade da organização em relação à mitigação de risco, deve-se verificar e documentar a existência ou não de uma matriz de risco corporativos.	Documento de Análise e Verificação da Matriz De Risco Organizacional.
		Deve-se verificar e documentar a existência ou não de um departamento, programa ou normativos que abordam a gestão de complice dentro da organização.	Documento de Análise e Verificação de Programas de Complice Existentes.

Atividade	Descrição	Ações	Artefatos
Realizar um levantamento das áreas que realizam tratamento de dados	Realização de um levantamento das áreas que realizam tratamento de dados com intuito de fechar o escopo da implementação da LGPD nessas áreas.	Após realizar o levantamento das informações sobre a organização com o objetivo de verificar como a organização está atualmente dentro do contexto da LGPD e quais ajustes e implementações a serem propostos. Deve-se realizar o levantamento de todas as áreas da organização que tratam dos dados pessoais, isto é, áreas que coletam, processam, transferem ou recebem dados dos titulares, além de identificar os responsáveis pelo tratamento de dados, seja colaborador, terceiro, parceiro ou sistema de informação.	Relatório de Levantamento das Unidades Organizacionais que realizam tratamento de dados pessoais e os seus Respectivos Responsáveis pelos Tratamentos.
Definir o escopo da implantação da LGPD	Definição do escopo da implantação da LGPD que irá guiar as outras atividades de implementação da LGPD.	Após o levantamento das áreas que realizam tratamento de dados é possível definir o escopo da implantação da LGPD. O escopo deve abranger todas as áreas que tratam dados, bem como colaboradores, terceiros, parceiros e qualquer outra pessoa e/ou Sistema que intervenham nos dados pessoais em algum momento no decorrer do tratamento de dados.	Documento da Definição de Escopo da Implantação da LGPD na Organização.
Criar e apresentar o Roadmap da implantação da LGPD na Organização.	Criação e apresentação do Roadmap de implantação da LGPD na organização.	Planejar e definir o Roadmap da Implantação da LGPD na Organização de acordo com o Levantamento Inicial do porte, maturidade, nível de complice da organização com a LGPD, as práticas de Segurança da Informação e mapeamento das áreas que fazem tratamento de dados.	O Roadmap de implantação da LGPD na organização.
Criar o Documento de Projeto da Implantação da LGPD e submetê-lo à alta administração avaliar a viabilidade do projeto.	Criação e submissão do projeto de implantação da LGPD para aprovação da alta administração.	O Documento de Projeto da Implantação da LGPD na Organização é documento que guiará toda a implantação da LGPD, é nele que estão definidos as fases, o custo, o tempo e os marcos para verificação de melhorias da implantação da LGPD, por isso nesse documento deve conter todos os artefatos produzidos anteriormente: Documento de Levantamento Inicial Sobra a Instituição, Documento de Listagem de Normatização Interna sobre Tratamento de Dados na Organização, Documento de Análise e Verificação da Matriz De Risco Organizacional, Documento de Análise e Verificação de Programas de Complice Existentes, Relatório das estruturas organizacionais que fazem tratamentos de dados na instituição, Documento da Definição de Escopo da Implantação da LGPD na Organização, Roadmap de implantação da LGPD na organização. Este documento também deve ter um espaço para assinaturas da alta administração aprovando o projeto de implantação da LGPD na empresa, bem como a garantindo o seu compromisso com essa implantação de forma explicita e inequívoca, seja pela transmissão de e-mails, portarias, etc., para que assim, seja criado e fortalecida a cultura de proteção de dados.	Documento de Projeto de Implantação da LGPD.

Fonte: (SILVA, 2020).

Além das atividades definidas anteriormente, o GT LGPD, de maneira transversal à implantação da LGPD na organização e durante toda a vida da organização, terá a

responsabilidade de: 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 LGPD; e assim, propor melhorias e inovações por meio da geração do Relatório de Propostas de Melhores Práticas no Cumprimento da LGPD que deve ser enviado e aprovado pela diretoria.

5.1.3 GQ.4 Melhorias são identificadas e implementadas

Este objetivo da competência está relacionado com a melhoria das práticas GQ.1 e GQ.2. A implementação definida não tem por objetivo ser um padrão de implantação da LGPD nas organizações, por isso se faz necessário um estudo inicial sobre a organização para entender seu porte e seu nível de maturidade em relação à LGPD, para assim definir um escopo de trabalho. Por isso, é necessário que durante o processo de implantação da LGPD sejam definidos marcos que podem ser reuniões em períodos pré-estabelecidos no Documento do Projeto para que sejam verificados pontos de controle e melhorias.

ROUILLER (2017) exemplifica as seguintes práticas, que neste contexto servem como sugestão: analisar as melhorias identificadas e registradas pelo GT; priorizar e selecionar as melhorias que podem ser implementadas nas práticas de implantação da LGPD; planejar a implementação das melhorias selecionadas; implementar as melhorias selecionadas e observar o impacto de sua adoção.

5.1.4 TH.1 Papéis e responsabilidades dos colaboradores são definidos comunicados e aprovados

Após o levantamento das informações sobre a instituição e a criação do Documento de Projeto de Implantação da LGPD, o próximo passo é definir os papéis e responsabilidades dos colaboradores, parceiros e terceiros na implantação da LGPD na organização. Para isso, deve-se usar o Objetivo da Competência TH.1 da MOSE Competence. ROUILLER (2017) deixa claro o que se espera da implementação do TH.1: “espera-se para este objetivo que todos os papéis e responsabilidades dos colaboradores da unidade de negócio do empreendimento estejam definidos, tenham sido comunicados a eles e os mesmos tenham aprovado as responsabilidades a eles atribuídas. É importante também que estejam claras para todos os colaboradores as responsabilidades de cada membro (ou de cada perfil de trabalho) para o desenvolvimento de suas atividades e a comunicação que deve ser realizada entre eles”.

Assim, o primeiro papel a ser definido na implementação da LGPD na organização é a do DPO (*Data Protection Office* ou Encarregado). O Encarregado é definido pela LGPD (BRASIL, 2018) como “pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)”. Este papel deve ser ocupado por um colaborador, empresa terceirizada ou parceiro de negócio que entenda o fluxo de dados da organização, pois esse conhecimento será necessário durante a implantação da LGPD e posteriormente para que o DPO execute as atividades exigidas para ele na LGPD, quais sejam: “I - Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - Receber comunicações da autoridade nacional e adotar

providências; III - Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV - Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares." (BRASIL, 2018). Nessa fase é importante alocar o DPO no Grupo de Trabalho da LGPD para que este consiga, juntamente com os seus pares manter-se focado em assuntos relacionados à Lei dentro e fora da organização.

A partir do Relatório de Levantamento das Unidades Organizacionais que realizam tratamento de dados pessoais e os seus Respectivos Responsáveis pelos Tratamentos é necessário definir quem sãos os responsáveis pelos tratamentos de dados. A LGPD determina que os agentes de tratamento são os controladores (organização) e os operadores (realiza o tratamento de dados em nome do controlador) (BRASIL, 2018). As atribuições dos agentes de tratamento devem ser as mesmas preconizadas na LGPD (BRASIL, 2018): "Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse. Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente à suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial. Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados. Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria". Assim, fica explicitado o papel dos controladores e operadores no tratamento d dados.

5.1.5 TH.2 Necessidades de capacitação são identificadas e tratadas

Após definir as responsabilidades dos operadores de dados e demais responsáveis pelo tratamento de dados, é necessário que o GT LGPD realize o treinamento inicial com todos esses colaboradores. O treinamento inicial tem por objetivo iniciar uma mudança na cultura da organização, fazendo com que todos os envolvidos no tratamento de dados conversem a mesma língua e estejam na mesma sintonia em relação à importância da implantação da LGPD na organização. Assim, é necessário que o GT explique questões como impactos da LGPD no dia a dia dos colaboradores, mudanças nos processos de tratamentos de dados, deixar todos cientes das etapas do *Roadmap* e prepará-los para as atividades futuras que a implantação irá exigir. O Artefato a ser gerado nessa etapa é o Plano de Capacitação para a LGPD.

5.1.6 TH.6 Programas (e/ou ações) de capacitação e ações motivacionais são estabelecidos e mantidos

Este objetivo da competência tem a finalidade de padronizar os programas de capacitação. Desta forma, é necessário que a organização tenha um Plano Semestral de Capacitação (PSC). Este plano deve contemplar todos na organização que estão envolvidos nos tratamentos de dados pessoais para participar de maneira frequente e planeja de treinamentos relacionados à LGPD.

Para isso, no início de cada semestre, o GT deve se reunir e formatar o PSC, que deve indicar os treinamentos necessários para que os colaboradores e terceiros responsáveis pelo tratamento de dados devem fazer para manter a organização sempre atualizada e aderente à legislação. O Plano deve conter a lista de treinamentos que devem

ser realizados no semestre e o orçamento com os custos desses treinamentos a serem aprovados pela diretoria.

5.1.7 TH.8 Análises do impacto dos programas (e/ou ações) de capacitação são realizadas.

Os treinamentos listados no PSC devem ser monitorados quanto a sua eficácia. Diante disso, sugere-se associar os treinamentos aos processos de promoção de cargos, isto é, um dado colaborador só poderá participar de um processo de promoção de cargos relacionados à proteção de dados na organização se tiver participado de determinados treinamentos presentes no PSC.

5.1.8 CM.9 Incidentes são registrados, analisados e ações preventivas são realizadas

Este objetivo da competência atende de forma direta ao artigo 46, por isso, antes de tratar do CM.9 faz-se necessário a implementação dos demais objetivos da competência para que a organização tenha uma base sólida para poder tratar dos incidentes de violação de dados.

Deve-se definir primeiro o que é o incidente que trata do artigo 46. Apesar da LGPD não ser explícita sobre o que é um incidente, por sua vez GPDR (UE, 2016), que é a legislação que trata da proteção de dados na Europa, define incidente como: "uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento". Com esse conceito, entende-se que a necessidade da organização está preparada para eventuais incidentes e os tratem tanto de maneira proativa, isto é, encontrando formas de mitigar os incidentes ou de maneira reativa que é a tratativa do incidente após o ocorrido.

Nesse contexto, faz-se necessário que a organização formule e mantenha atualizado o seu Plano de Respostas a Incidentes de Segurança e Privacidade (PRISP) juntamente com uma Base de Dados de Incidentes (BDI). O Plano de Resposta a Incidentes de Segurança e Privacidade é um processo que descreve a forma como a organização irá responder a um incidente de segurança. Devido à gravidade do tema, a resposta da organização deve ser rápida e confiável. Deve-se primar também pelo resguardo das evidências para compor a Base de Dados de Incidentes, e, assim, entender o incidente atual e evitar que futuros incidentes ocorram pelos mesmos fatores. O Plano de Respostas aqui abordado trata-se de uma sugestão, a organização deverá usar para si o que for adequado para o seu volume de informações. A estrutura abordada a seguir teve por base a proposta da PROCEMPA (2020). Para o atendimento do PRISP, os seguintes itens devem ser atendidos:

Formação do Time de Resposta a Incidentes (TRI). Grupo formado pelos colaboradores da organização ou prestador de serviço que deve ser designado pela Diretoria da Organização com aval do GT. Os membros do TRI devem ter acessos, habilidades, responsabilidades, treinamento e conhecimentos específicos para responder aos mais variados tipos de incidentes. O perfil dos membros irá se moldar a partir do nível de maturidade da organização em incidentes, isto é, quanto mais madura a organização for e por mais casos de incidentes tiver passado, melhor ela saberá definir o perfil desses membros. Para este time, deve-se fazer parte no mínimo o DPO e um representante da área de Segurança da Informação.

Instalação e divulgação dos mecanismos de comunicação de incidente. Devem ser criadas, disponibilizadas e publicadas formas de notificação à organização quando ocorrerem incidentes. Isto é, informações do contato do DPO devem estar disponíveis e de fácil acesso ao público geral, assim, em casos de incidentes o DPO deve ser o primeiro a

ser informado, conforme estabelece o §1º, do Artigo 41, da Lei LGPD: "A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador" (BRASIL, 2018).

Instalação, configuração e definição de ferramentas de monitoria e alarmes. O TRI deve ter a sua disposição, canais pelos os quais podem ser acionados durante a ocorrência de um incidente. Assim, devem ser definidos por onde os membros do TRI serão convocados para resolver determinadas ocorrências, quer seja via telefone, via software de alerta de incidentes, SMS, etc.

Definição de um Plano de Comunicação de Incidentes. Deve-se criar e disponibilizar para o DPO um conjunto de documentos padrões de comunicação formal para que o Encarregado comunique o incidente para a ANPD, titulares de dados, imprensa e internamente, conforme prevê a LGPD (NBR ISO/IEC 27001, 2013).

O Plano de Respostas a Incidentes deve contar com os seguintes participantes: **Notificado** – pessoa ou sistema de monitoração que notifica o incidente; **TRI – Time de Resposta a Incidentes**, definido previamente; **Acionadores do TRI** – grupo que receberá notificações de incidentes em um primeiro momento para fazer a triagem; **Responsável por Sistema ou Controlador de Sistemas** – indicado para ser contatado e tem o poder de autorizar ou vetar procedimentos de emergência; **Equipe de Segurança da Informação** – emitirá o parecer quanto à gravidade do incidente, bem como levantar hipóteses sobre sua possível causa; **Encarregado pelo Tratamento de Dados Pessoais (DPO)** – responsável pela comunicação dos incidentes para as pessoas e entidades interessadas; **Grupo da área de sustentação de software** – atuam no desenvolvimento e implantação da solução do incidente, se esse for o caso.

Desta forma, o Plano de Resposta a Incidentes deve respeitar o fluxo a seguir:

Fase inicial: I - um novo incidente é notificado por pessoa externa ou interna ou por alarme de monitoração ou, ainda, outro meio definido; II - a notificação é recebida por Acionador do TRI.

Fase da triagem: III – o acionador do TRI deve fazer uma avaliação preliminar e decidir se a notificação é pertinente e verdadeira e assim seguir o fluxo ou não, ao verificar que a notificação não procede e, assim, descarta-la com as devidas justificativas; IV - na avaliação preliminar, devem ser buscadas informações sobre os sistemas que foram impactados, definir uma criticidade inicial, quais os danos aparentes e o risco da situação se agravar caso não tenha uma resposta de tratamento imediata; V - conforme a avaliação preliminar, incidentes que não envolvem sistemas online e que seguramente não apresentam riscos aumentados pela falta de ação imediata devem ser reencaminhados para posterior avaliação do DPO e da Equipe de Segurança da Informação, caso o sistema envolva dados pessoais; VI - em caso de incidentes que exigem resposta imediata, o TRI deve ser acionado.

Fase de avaliação: VII - esta fase contempla uma avaliação mais detalhada do incidente. Aqui deve ser feita a coleta de provas que estão relacionadas com o incidente: endereços de IP, credenciais envolvidas, transações de banco de dados realizadas, transferências de informação fora do padrão, métodos e vulnerabilidades exploradas, entre outras. A depender da complexidade do incidente, nesta fase devem ser envolvidos os especialistas dos ativos afetados e a equipe de Segurança da Informação. Os ativos afetados aqui podem ser sistemas de informação ou dados físicos como documentos, fichas cadastrais, etc.

Fase de contenção e erradicação: VII - os responsáveis pelo ativo afetado devem ser procurados para orientar e se manifestar sobre os procedimentos de contenção e erradicação do incidente; IX - o objetivo das medidas de contenção é erradicar e limitar o

dano e isolar o ativo afetado para evitar mais danos. Caso o ativo seja uma Sistema de informação e conforme a necessidade e a autorização obtida, deverá ser realizado o desligamento de sistemas inteiros ou de funcionalidades especificas, avisando ao usuário desses sistemas, por meio de avisos, da indisponibilidade do sistema para manutenção. Esses procedimentos devem ser feitos com cuidado para não impactar as evidências, pois essas deverão ser usadas para identificar autoria, origem e método usado para quebrar a segurança.

Fase de recuperação: X - deve ser iniciado, caso exista, o Plano de Continuidade de Negócio dos sistemas impactados; XI - a recuperação é conjunto de medidas para restaurar os serviços completamente, onde e depender da circunstância e o tamanho do dano causado, essa retomada dos serviços pode ser feita de forma gradual, conforme viabilidade e decisão dos responsáveis pelo ativo atingido; XII - o DPO em posse dos relatórios emitidos pelo TRI, pela equipe Segurança e pelo responsável pelo ativo impactado deve passar essas informações para a equipe que irá desenvolver e instalar a solução para o incidente; XIII - as medidas identificadas na fase de Avaliação devem ser executadas, tais como restauração de *backups*, clonagem de máquinas virtuais, reinstalação de sistemas, abertura de Boletim de Ocorrência por roubo ou furto de informação.

Lições aprendidas: XIV - com o incidente contido e sua resolução encaminhada, o TRI deve agendar e conduzir uma reunião de Lições Aprendidas com o objetivo de discutir erros e dificuldades encontradas durante o tratamento do incidente. Nesta reunião também devem ser propostas melhorias que serão encaminhadas aos responsáveis para a definição sobre sua adoção.

Registro no Banco de Dados de Incidentes: XV - o TRI deve documentar o incidente na Base de Dados de Incidentes, detalhando as informações obtidas, linha do tempo, atores envolvidos, evidências, conclusões, decisões, autorizações expedidas, decisões tomadas e as lições aprendidas.

Fase da Comunicação: XVI - o processo do Plano de Respostas a Incidentes de Segurança e Privacidade (PRISP) se completa com a formatação do documento de comunicação que é dirigida a ANPD, quanto aos titulares de dados envolvidos, identificando os possíveis danos e as providências que foram e que estão sendo tomadas para mitigar esses danos. Essa comunicação deve apresentar alguns pontos previamente definidos no artigo 48: 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 proteção dos dados, observados os segredos comerciais e industriais; IV – os riscos relacionados ao incidente; V – os motivos da demora, no caso de a comunicação não ter sido imediata; VI – as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo (BRASIL, 2018).

Por fim, caso o incidente envolver a prática de algum ato ilícito, recomenda-se a apresentação de pedido para instauração de inquérito policial.

5.2 Ativo LGPD: Artigo 47

Este ativo da LGPD diz que os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se garantir a segurança da informação prevista na Lei em relação aos dados pessoais, mesmo após o seu término.

5.2.1 TH.1 – Papéis e responsabilidades dos colaboradores são definidos, comunicados e aprovados

ROUILLER (2017) espera como resultado desse objetivo de competência que “todos os papéis e responsabilidades dos colaboradores da unidade de negócio do empreendimento

estejam definidos, tenham sido comunicados a eles e os mesmos tenham aprovado as responsabilidades a eles atribuídas". Assim, uma forma de concretizar o artigo 47 é com a criação do Plano de Cargo e Responsabilidades para colaboradores internos da Organização. Para terceiros, parceiros ou qualquer outro que venha interferir no processo de tratamento de dados, deve-se criar o Termo de Responsabilidade e Confidencialidade de Acesso de Dados Pessoais.

O Plano de Cargos, Responsabilidades e Confidencialidade, onde geralmente a organização tem definido o seu Plano de Cargos e Salários, é o artefato que tem o foco no cargo, na responsabilidade e na confidencialidade do colaborador interno para com o tratamento de dados pessoais. Assim, o Plano de Cargos, Responsabilidades e Confidencialidade deve ser formatado pelo Grupo de Trabalho de Implantação da LGPD. Deve estar definido neste termo: nome do cargo – aqui deve ser definido o nome do cargo que estará presente na comunicação interna e externa da organização; responsabilidades – aqui devem ser definidas as responsabilidades do colaborador no tratamento dos dados, seja coleta, processamento, exclusão, alteração de dados, entre outras operações previstas na LGPD. cláusula de confidencialidade – aqui deve estar descrito cláusulas de confidencialidades específicas a serem resguardadas pelo colaborador durante o tratamento de dados. penalidades – aqui deve estar descrito as penalidades as quais o colaborador está sujeito em caso de comprovação de quebras de protocolos de segurança ou quebras de acordo de confidencialidade.

Já o Termo de Responsabilidade e Confidencialidade de Acesso de Dados Pessoais deve estar presente nos contratos da organização com empresas operadoras, isto é, terceiras ou parceiras ou qualquer individuo que tenha realizado o tratamento dos dados em nome do controlador (BRASIL, 2018). O termo tem o papel de garantir que os operadores que respondem em nome da empresa participem de situações relacionadas a tratamento de dados na organização. Assim, sugerem-se as seguintes cláusulas nos contratos, seguindo as diretrizes da NBR ISO/IEC 27002 (2013): (i) reconhecimento que em razão do uso das ferramentas tecnológicas disponibilizadas pela organização, o operador poderá ter acesso a diversas informações pessoais, sensíveis, estratégicas, comerciais, entre outras - confidenciais ou não - armazenadas nos sistemas informatizados sob a responsabilidade da organização; (ii) ter ciência de que as credenciais de acesso (login e senha) são de uso pessoal e intrasferível e de conhecimento exclusivo (é de inteira responsabilidade do operador todo e qualquer prejuízo causado pelo fornecimento da sua senha pessoal a terceiros, independente do motivo); (iii) reconhecimento de que serão consideradas confidenciais todas as informações, transmitidas por meios escritos, eletrônicos, verbais ou quaisquer outros e de qualquer natureza, incluindo, mas não se limitando a dados pessoais, dados sensíveis, técnicas, design, especificações, desenhos, cópias, modelos, fluxogramas, croquis, fotografias, software, mídias, contratos, planos de negócios, propostas comerciais, processos, tabelas, projetos, nomes de clientes, resultados de pesquisas, invenções e ideias, financeiras, comerciais, dentre outros; (iv) ter conhecimento de que a organização possui um programa de governança de dados pessoais e de segurança da informação, no qual o operador tem a obrigação de obedecer e auxiliar o cumprimento; (v) comprometimento do operador a não utilizar qualquer informação a qual tenha acesso, classificada como confidencial ou não, para fins diversos daqueles para os quais tive autorização de acesso; (vi) ciência por parte do operador de que é proibida a cópia de qualquer informação para dispositivos estranhos à estrutura da organização, bem como a divulgação e compartilhamento, exceto se a referida ação, seja estritamente necessária para a prestação dos serviços contratados, devendo ser realizada com a maior segurança possível e com expressa e prévia autorização do representante legal do controlador; (vii) reconhecimento

que os prejuízos causados pelo operador à organização, em razão da quebra de confidencialidade, disponibilidade ou integridade das informações às quais tenha acesso, poderão ser reclamados, judicial ou extrajudicialmente e, caso caracterizado qualquer infração penal, poderá o operador ser pessoalmente responsabilizado; (viii) reconhecimento pelo operador de que seus dados pessoais utilizados para acesso aos sistemas disponibilizados pelo controlador serão conservados durante o tempo que estiver vigente a relação contratual com a organização a qual esteja vinculado e após esta finalizar, durante os períodos de retenção de dados legalmente exigíveis, de forma estritamente necessária, tais como, mas não se limitando, pelos prazos prescricionais para ajuizamento de ação penal ou civil, assim como para o exercício do direito de defesa em processo judicial de qualquer natureza ou para outra finalidade por período não excessivo adotado pela organização, garantido a transparência, confidencialidade, integridade e disponibilidade das minhas informações pessoais, bem como o exercício dos direitos previstos na Lei Federal nº 13.709/2018 ("LGPD") na vigência da relação contratual assim como após o término da referida relação; (ix) reconhecimento do operador de que leu, compreendeu e sanou todas as dúvidas sobre o Termo.

5.3 Ativo LGPD: Artigo 48

O Artigo 48 da LGPD é focado na comunicação dos incidentes. O artigo diz que: "O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares" (BRASIL, 2018). Nessa primeira parte é descrito a obrigação do controlador em comunicar a todos os interessados no caso de incidente de segurança.

De acordo com o trabalho (DE SOUZA e OLIVEIRA, 2021) esse artigo é atendido pelos objetivos da competência: CM.8, CM.9, GQ.3 e GQ.7. A comunicação definida na primeira parte do artigo deve está estabelecida e mantida dentro das abordagens de relacionamentos com os clientes, conforme especificado no CM.8. Dos resultados esperados para o CM.8, destacam-se: estabelecimento e manutenção dos canais de relacionamento e comunicação com o mercado-foco; e realização de estudos para verificar a eficiência desses canais e, se caso for, realizar os ajustes necessários.

O artigo 48 (BRASIL, 2018) também traz no escopo da § 1º o que deve ser no mínimo mencionado nesta comunicação feita pelo controlador: 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.

A § 2º do Artigo 48 assevera que a depender da gravidade do incidente, a autoridade nacional poderá caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como: I - ampla divulgação do fato em meios de comunicação; e II - medidas para reverter ou mitigar os efeitos do incidente (BRASIL, 2018). As informações contidas nos itens I, II, III, IV, V e VI da § 1º e o item II da § 2º são obtidas por meio da implementação do objetivo CM.9.

Por fim, no que diz respeito a § 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los. As comprovações exigidas podem ser geradas a partir da implementação dos objetivos GQ.3. e GQ.7. A seguir, será apresentado como a implementação do Artigo 48 pode ser feita a partir dos objetivos elencados anteriormente.

5.3.1 CM.8 – Abordagens para o relacionamento com os clientes são estabelecidas e mantidas

Dos resultados esperados por ROUILLER (2018) para o objetivo da competência CM.8, destacam-se: estabelecimento e manutenção dos canais de relacionamento e comunicação com o mercado-foco; e realizar estudos para verificar a eficiência desses canais e, se caso for, realizar os ajustes necessários. Assim, para atender ao artigo 48 é necessário que os agentes de tratamentos estabeleçam canais de relacionamentos e comunicação com as partes interessadas no incidente de dados.

O canal de relacionamento é o meio pelo qual a organização irá comunicar a ANPD e aos titulares que tiveram seus dados envolvidos no incidente. Para tal, é necessário que o GT LGPD crie um modelo de documento chamado de Notificação de Violação de Dados. Este documento deve conter as seguintes informações: natureza dos dados afetados, os titulares afetados, quantitativo aproximado de titulares afetados, medidas técnicas e de segurança utilizadas para a proteção dos dados, riscos relacionados ao incidente, medidas que foram ou que serão adotadas para reverter ou mitigar o efeito dos prejuízos conforme estabelecido em (BRASIL, 2018).

A depender da gravidade do incidente, a organização pode ser obrigada a fazer a ampla divulgação dos fatos em meios de comunicação. Para isso, é necessário que a organização estabeleça um canal de comunicação padrão pelo o qual faz comunicações oficiais para o mercado-foco. Neste caso, esse canal deve ser o site oficial da organização, as redes sociais oficiais da organização e outros meios que a organização julgar necessário. Sugere-se criar dentro do site da organização, caso não tenha, uma página de notificação de incidentes de dados, para que desta forma, caso necessário, a organização possa ter um canal oficial que trata diretamente do assunto de proteção de dados. Esta padronização de canal de relacionamento fará com que a organização treine seus clientes a procurar informações verídicas no seu canal oficial, evitando assim a propagação de notícias falsas.

5.3.2 CM.9 – Incidentes são registrados, analisados e ações preventivas são realizadas.

Para que a comunicação seja efetiva e atenda a proposta do artigo 48, é necessário que os incidentes sejam registrados, conforme tratado na implementação do artigo 46, para que desses registros sejam extraídas as informações do que se pede nos itens do artigo 48 (BRASIL, 2018): 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.

5.3.3 GQ.3 – Os bens e/ou serviços gerados pela unidade de negócio são verificados e GQ.7 Controles da qualidade dos bens e serviços são estabelecidos e mantidos.

A depender da gravidade do incidente, a Agência Nacional de Proteção de Dados pode solicitar e avaliar a eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis. Isto deve ser feito por meio da implementação do objetivo da competência GQ.3 que, segundo ROUILLER (2017), tem como resultado esperado a realização de verificações de qualidades dos bens e serviços entregues ao cliente, nesta dissertação isso é entendido como uma auditoria interna para validar se os dados estão sendo tratados em conformidades com a LGPD, isto

é, quanto a sua anonimização e inacessibilidade de acesso à pessoa ou sistema sem autorização. Por sua vez, objetivo da competência GQ.7 tem como resultado esperado a verificação da qualidade dos bens produzidos durante a sua produção. Em resumo, para ROUILLER (2017), "o objetivo GQ.3 verifica a qualidade final do bem ou serviço produzido enquanto GQ.7 estabelece esta verificação durante sua produção". Assim, é importante para esta dissertação a implementação de ambos os objetivos da competência, pois eles funcionam de maneira complementar um ao outro.

Desta forma, para implementação do § 3º do artigo 48, é necessário que seja mantido o registro de todas as práticas de tratamento de dados pessoais conduzidos pelos agentes de tratamento, incluindo o propósito de todas as atividades desenvolvidas para que a organização se resguarde em caso de incidentes e tenha provas de que realizou o tratamento de dados conforme previsto em lei.

Esses registros devem fazer parte de um processo ou rotina padrão dentro das organizações, isto é, desde a coleta dos dados até o seu descarte, todos os procedimentos inerentes ao processo de tratamento de dados deve ser registrado, contendo no mínimo as seguintes informações: responsáveis pelo tratamento de dados durante as fases de tratamento; necessidade do tratamento; titulares envolvidos; procedimentos e/ou tecnologias utilizadas para garantir a segurança da informação para tornar os dados pessoais afetados ininteligíveis; medidas, salvaguardas e mecanismos de mitigação de risco adotados pelo agente de tratamento.

Outro instrumento importante para o registro das atividades de tratamento de dados pelas unidades de negócio é o Registro de Operações de Tratamento de Dados Pessoais ou RoPA (*Record of Processing Activies*). Essa prática, a de registrar as operações de tratamento, é prevista no artigo 37. "O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse" (BRASIL, 2018). O RoPA ou Inventário dos Dados Pessoais vem descrito na NBR ISO/IEC 27001 (2013), que sugere que a organização mantenha os registros de tratamento do dado pessoal que pode incluir: tipo de tratamento; propósitos para o tratamento; uma descrição das categorias de dados pessoais e dos titulares dos dados (por exemplo, crianças); as categorias de destinatário para quem o dado pessoal tem sido ou será divulgado, incluindo os destinatários em outros países ou organizações internacionais; uma descrição geral das medidas de segurança técnica e organizacional; e um relatório de Avaliação de Impacto de Privacidade.

5.4 Ativo LGPD: Artigo 49

Este artigo trata diretamente dos sistemas de informações: "os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares." (BRASIL, 2018). Para implementação desse artigo, foram mapeados em (DE SOUZA e OLIVEIRA, 2021) os objetivos da competência GQ.6, CM.3 e CM.4 do MOSE Competence.

Deve-se usar o GQ.6 para incluir a definição de estruturas de sistemas de informações no tratamento de dados. Já os objetivos CM.3 e CM.4 são implementados de forma a estabelecer sistemas de informações na fase de coleta de dados e disponibilização de canal com os clientes para que estes estabeleçam seus direitos de petições e informação referentes aos seus dados (ROUILLER, 2017).

5.4.1 GQ.6 – Abordagens para a gestão da unidade de negócio são estabelecidas e mantidas, CM.3 Atendimentos aos clientes são realizados e CM.4 O Relacionamento com os clientes é realizado

Dentro da abordagem para a gestão da unidade de negócio, devem ser estabelecidos e mantidos sistemas de informações com soluções que contemplem engenharia de atendimento aos direitos de titulares, com segurança embarcada e mecanismos de controle de acesso e registro de atividades. Para complementar esse objetivo da competência, também é necessário verificar a implementação de sistemas de informações que realizem a coleta de dados no atendimento ao cliente, bem como na disponibilização de um canal para que o titular dos dados exerça os seus direitos e petição. Então é necessário realizar as seguintes fases para a implementação do artigo 49: (primeira fase) realizar o levantamento dos sistemas de informações ativos na instituição e que realizam tratamento de dados; (segunda 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; (terceira fase) executar a atualização e/ou compra de novos sistemas de informações; (quarta fase) monitorar, controlar e realizar melhorias continua nesses sistemas para que sempre fiquem aderentes às atualizações legislativas e normativas referentes à privacidade e proteção de dados dos titulares.

Caso a organização já tenha sistemas de informações, é necessário fazer o levantamento destes para verificar a viabilidade de atualização ou encerramento desse sistema para outro que ofereça o suporte necessário aos ditames da LGPD.

1ª fase – levantamento de sistemas ativos: o levantamento deve ter o acompanhamento do DPO e do responsável pelo sistema. Esse levantamento pode seguir estes passos: primeiramente, faz-se o levantamento de todos os sistemas de informações; após isso, verifica-se quais desses sistemas realizam tratamento de dados, excluindo os que não fazem; por fim, deve-se levantar as seguintes informações (i) nome do sistema, (ii) unidade de negócio responsável pelo sistema, (iii) natureza dos dados transacionados no sistema, (iv) tipos de dados transacionados, se são dados sensíveis ou não, (v) operações de dados realizadas no sistema, (vi) verificar se o sistema dispõe de mecanismos de segurança da informação para tornar os dados pessoais ininteligíveis, (vii) verificar se o sistema dispõe de mecanismos de segurança da informação que permitam que somente usuários com permissão ao dado possa acessá-lo.

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: por meio do levantamento dos sistemas e das informações preenchidas, é possível verificar se o sistema em questão atende ou não a LGPD. A partir disso, caso não atenda, devem-se levantar com o responsável pelo sistema os custos para atualização do sistema e, paralelo a isso, deve-se verificar se no mercado existem sistemas semelhantes e mais atuais que estão adeptos a LGPD e verificar o custo de aquisição e migração de dados entre sistemas.

Após isso, o DPO, com todas essas informações em mãos, deve emitir um Parecer Técnico informando o que é mais benéfico para a organização: atualização do sistema atual ou investimento em um novo sistema. Anexo a esse parecer devem ir todas as informações que foram levantadas dos sistemas para dar embasamento e justificativa para a decisão final do parecer.

3ª fase - executar a atualização e/ou compra de novos sistemas de informações: caso o parecer do DPO seja pela atualização do sistema, o responsável pelo sistema deve gerar o Plano de Projeto que deve conter o cronograma, os custos, os requisitos e os impactos da nova atualização do sistema. Esse Plano deve ser revisado pelo DPO quanto

ao seu requisito para validar se essa atualização irá fazer com que o sistema se torne aderente a LGPD. Todo o Plano de Projeto deve ser aprovado pela alta administração ou imediato responsável por aprovar esse tipo de projeto. Sugere-se, caso necessário, que esse Plano de Projeto seja discutido com todas as áreas da organização que fazem uso do sistema para que todos estejam cientes e se sintam inclusos no processo de atualização.

Por outro lado, se o parecer do DPO for favorável à aquisição de um novo sistema, deve-se realizar os procedimentos padrões da organização para aquisição de novo sistema, bem como realizar o encerramento do sistema atual e realizar o processo de migração de um sistema para o outro.

4ª fase - monitorar, controlar e realizar melhorias continua nesses sistemas para que sempre fiquem aderentes às atualizações legislativas e normativas referentes à privacidade e proteção de dados dos titulares: o DPO é responsável por coletar as informações relacionadas aos sistemas de informações que realizam tratamento de dados, seja por meio do RoPA, explicado anteriormente, seja por meio de um processo proativo de mitigação de risco ou até mesmo uma necessidade reativa a um incidente. Dessa forma, a depender do caso, deve-se tornar rotina o monitoramento, o controle e a melhoria contínua nos sistemas de informações da organização. Apesar da responsabilidade do DPO, toda a organização deve estar ciente da sua responsabilidade colaborativa e manter informado o GT LGDP sobre possíveis inconsistências sistêmicas ou comportamentos inesperados dos sistemas para que a área responsável seja acionada, de forma a prevenir e mitigar os riscos de vazamento de dados.

Desta forma, cabe ao DPO manter-se atualizado em relação às atualizações da LGPD para que essas atualizações sejam imediatamente implementadas nos sistemas de informações. Outro fator importante são as atualizações tecnológicas, onde deve-se verificar se os mecanismos de segurança da informação para tornar os dados pessoais ininteligíveis estão atualizados e são seguros. Esse tipo de informação pode ter responsabilidade compartilhada com a área de Segurança de Informação, a qual pode emitir relatórios trimestrais sobre a segurança dos sistemas de informação da organização.

5.5 Ativo LGPD: Artigo 50

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

Fica claro no artigo que a organização poderá optar por definir suas regras de boas práticas e de governança. Entretanto, mesmo que a lei deixe como opcional essa implementação, para o processo de amadurecimento da empresa para atendimento da LGPD, é essencial que seja estabelecida uma política de governança e boas práticas nos tratamentos dos dados na organização.

De acordo com DE SOUZA e OLIVEIRA (2021), esse artigo é atendido pelos objetivos da competência GQ.1, GQ.2, GQ.3, GQ.4, GQ.6, GQ.7, GQ.9, TH.1, TH.6, IN.1, CM.4 e CM.9 do MOSE. Pode-se observar que são necessárias quatro dimensões da MOSE Competence, quais sejam Gestão e Qualidade, Talento Humano, Inovação e Cliente e Mercado, para atendimento deste artigo. Isso se deve ao fato de que a governança e as

boas práticas contemplam a organização como um todo, estando presentes em todos os níveis organizacionais: estratégico, tático e operacional.

Para atendimento do artigo 50 no que diz respeito à implementação de um programa de governança em privacidade e boas práticas, faz-se necessário iniciar esse processo pela alta administração da organização que deve definir as diretrizes para implantação do programa de governança em privacidade e boas práticas, bem como verificar se os bens produzidos pela organização estão aderentes a LGPD. Além disso, a governança deve ser estabelecida e mantida e contemplar a gestão de riscos.

Para isso, deve-se criar o Programa de Governança em Privacidade – PGP que, segundo a (BRASIL, 2020), "consiste na captura e consolidação dos requisitos de privacidade e segurança com o intuito de ditar e influenciar como os dados pessoais são manuseados no seu ciclo de vida como um todo".

Para a criação do PGP e, consequentemente, a adequação com o artigo 50 da LGPD, deve-se estabelecer as fases desse processo. O Quadro 3 tem como referência o Programa de Boas Práticas do Ministério de Economia que detalha as fases dessa implementação.

Quadro 3 – Fases de Implantação de um Programa de Boas Práticas

Fase	Descrição	Etapas
Iniciação e Planejamento	Compreensão de quais são as primeiras informações e dados importantes que devem ser conhecidos	1. Nomeação do Encarregado; 2. Alinhamento de Expectativas com a Alta Administração; 3. Maturidade da Organização; 4. Medidas de Segurança; 5. Estrutura Organizacional; Proteção de Dados Pessoais; 6. Inventário de Dados Pessoais; 7. Levantamento de Contratos fechados com clientes, bem como com terceiros ou parceiras que fazem tratamento de dados.
Construção e Execução	Construção e Execução de marcos que protegem os direitos do cidadão em relação à privacidade da informação	1. Políticas e práticas para proteção da privacidade; 2. Cultura de segurança e proteção de dados e Privacy by Design; 3. Relatório de Impacto à Proteção de Dados Pessoais (RIPD); 4. Política de Privacidade 5. Adequação de cláusulas contratuais 6. Termo de uso
Monitoramento e Controle	Acompanhamento e Correções referentes às conformidades com a LGPD	1. Gestão de Incidentes; 2. Inovação

Fonte: (BRASIL, 2020).

Além do exposto no Quadro 3, a LGPD (BRASIL, 2018) elenca alguns pontos básicos na implantação de programa de governança e boas práticas: (i) levar em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular; (ii) observar a boa fé e aplicar os seguintes princípios: I - Finalidade, realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - Adequação, compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - Necessidade, limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV - Livre acesso, garantia, aos titulares, de consulta facilitada e gratuita sobre a

forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - Qualidade dos dados, garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI - Transparência, garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII - Segurança, utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - Prevenção, adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - Não discriminação, impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - Responsabilização e prestação de contas, demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas; (iii) implementar programa de governança em privacidade que, no mínimo: demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais; seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta; seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados; estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade; tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular; esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos; conte com planos de resposta a incidentes e remediação; e seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

5.5.1 Iniciação e Planejamento

Esta é a primeira fase da implantação da Governança e boas práticas em proteção de dados. Nesta etapa inicial, devem-se levantar as informações pertinentes em relação à LGPD na organização. De modo que seja possível definir a base para implantação da governança. Este início deve incluir, além da nomeação do encarregado, uma estrutura organizacional para planejar, executar, monitorar e controlar por tempo indeterminado a implantação, atualização e melhorias na proteção de dados pessoais na organização. Adiante será tratada cada etapa definida para essa fase conforme quadro anterior.

Nomeação do Encarregado: a primeira etapa da fase da implantação da Governança é boas práticas é a nomeação do encarregado. Para isso, devem-se utilizar os preceitos da dimensão Talento Humano da MOSE. Mais especificamente os objetivos da competência TH.1 que trata da definição dos papéis e responsabilidades dos colaboradores na organização, além do que já está definido pela própria LGPD. Dentro do programa de governança e boas práticas é ideal destacar: as atividades do encarregado, os requisitos que um colaborador ou terceiro externo à organização deve ter para exercer a função e como deve ser o relacionamento entre o colaborador, a organização e público externo.

De maneira geral, o encarregado dos dados atuará como um patrocinador e articulador no que diz respeito à Lei Geral de Proteção de Dados dentro da Organização. Além disso, deve ser o responsável por fomentar a cultura de proteção de dados na organização e deve estar sempre alerta em relação à conformidade da organização com a LGPD. O programa de governança deve definir as atividades do encarregado dos dados

igualmente ao que se é definido na LGPD e já fora apresentado nesta dissertação na implementação do artigo 46.

Um dos objetivos do Encarregado, que é citado pela própria LGPD, é ser o responsável pela comunicação entre a organização e a ANPD e a organização com os titulares dos dados. Para que essa comunicação seja efetiva, faz-se necessário implementar o objetivo da competência CM.4 no qual traz diretrizes para do relacionamento com os clientes e/ou pessoas interessadas, neste caso ANPD e titulares dos dados. Então, um dos primeiros passos é a divulgação pela organização do nome e contato do encarregado de dados para o público. Essas informações podem ser divulgadas no sítio eletrônico da organização.

A organização deve ter definido em sua governança os requisitos necessários para que um colaborador ou um terceiro externo à organização assuma o papel de Encarregado. BRASIL (2020) sugere os seguintes requisitos para a escolha do encarregado, levando sempre em conta o porte, o tipo da organização: experiência na análise e elaboração de respostas de pedido(s) de acesso à informação demandado(s) pelos canais de atendimento da organização, como SAC e Ouvidorias; conhecimentos multidisciplinares, incluindo as áreas de gestão, segurança da informação, gestão de riscos, tecnologia da informação, proteção da privacidade e governança de dados; caso a empresa tenha um programa de cursos obrigatórios, o encarregado deve tê-los concluídos antes de assumir o cargo.

Levando em consideração o nível organizacional e por meio da implementação da dimensão de competência Gestão e Qualidade, o encarregado deve ter liberdades para exercer sua função, tais como orientado por (BRASIL, 2020): definição de orçamento e recursos que poderão ser aplicados em ações necessárias; acesso a informações sobre as estruturas organizacionais; apoio das unidades de negócios; apoio da alta administração; autonomia e independência funcional para tratar de assuntos referentes à proteção de dados com todos os cargos e níveis hierárquicos na organização para, assim, poder investigar pró-ativamente os níveis de conformidade e instruir os responsáveis pelos riscos a corrigir as lacunas encontradas.

Observa-se que o Encarregado é a figura central na implantação e manutenção do Programa de Privacidade e Melhores Práticas. Para que seu trabalho seja cumprido, é necessário que a organização seja transparente para com o seu encarregado no que diz respeito ao tratamento de dados pessoais. Nesta linha de raciocínio, BRASIL (2020) diz que para o sucesso da implantação de um programa de governança é essencial que o trabalho executado pelo encarregado seja apoiado pela alta administração, nisso inclui-se o seu envolvimento nas decisões e recursos suficientes para pessoa, treinamentos, entre outros. O encarregado também deve ter assegurado uma estrutura organizacional suficiente para governança e gestão de proteção de dados, a depender do porte da instituição. É importante também que o encarregado tenha autonomia e independência funcional para avaliar as atividades de tratamento de dados pessoais realizadas pela organização. Por fim, a organização, a depender do seu porte, deve primar pela capacitação do seu encarregado para que este mantenha um continuo aperfeiçoamento por meio de treinamentos e capacitações.

BRASIL (2020) também apresenta tópicos que podem ser abordados, analisados e tratados pelo encarregado: alinhamento de expectativas entre o encarregado e a alta administração da organização. Isto pode ser feito a cada inicio de projeto dentro do programa de governança; apresentação para as unidades de negócio e seus colaboradores sobre a importância do papel de encarregado com o objetivo de criar uma atmosfera de cooperação com o encarregado para que este consiga exercer seu papel de maneira mais fluida e com menos entraves; priorização e foco em melhorias, tendo consciência da

estrutura, dos requisitos de dados pessoais, bem como da maturidade de compliance do órgão; instituição e coordenação do Grupo de Trabalho da LGPD ou de unidade de negócio semelhante que trate da implantação e acompanhamento da LGPD na organização; criação e apresentação da politica de privacidade, bem como fazer a sua revisão, melhorias e atualizações conforme proposições da alta administração; realização do mapeamento do cenário atual referente à privacidade e proteção de dados para posterior levantamento da necessidade de modificação da política atual. O mapeamento deve ser realizado a cada 12 meses e deve conter um parecer com os pontos mapeamentos e o orçamento de custo das mudanças necessárias para posterior aprovação da alta administração.

Alinhamento de Expectativas com a Alta Administração: alta administração é o maior patrocinador do programa de governança em uma organização. Então, na fase de iniciação e planejamento, o alinhamento das expectativas com a alta administração é crucial para o sucesso da implantação da governança em privacidade e boas práticas. Ao definir as diretrizes do programa, deve-se apresentar o planejamento para avaliação da alta administração, essa por sua vez deverá: analisar e priorizar as ações mais urgentes; avaliar e, caso necessário, propor melhorias e refinamentos para as estratégias de privacidade; autorizar o Plano de Governança em Privacidade e Boas práticas; comprometer-se a realizar ações que promovam a cultura de proteção de dados na Instituição.

Diagnóstico de Maturidade da Organização: nesta etapa de iniciação e planejamento, faz-se necessário realizar um diagnóstico da empresa para saber em que nível de maturidade a organização está em relação à proteção e privacidade dos dados. Esse diagnóstico é importante, pois enquadra a organização em determinado nível de maturidade, de forma que é possível cortar custos e mão de obra na implantação de processos que a organização já tem. Outra motivação para o diagnóstico é de que a organização conheça suas forças e fraquezas para que, assim, seja implantada uma governança mais alinhada e mais focada em resolver os gaps organizacionais.

As sugestões para realização do diagnóstico estão no Quadro 2 na seção de implementação do artigo 46.

Medidas de Segurança: na etapa de Iniciação e Planejamento, deve-se analisar e adotar medidas de segurança, bem como realizar revisões periódicas e propor melhorias nas diretrizes antes definidas. Para implementação dessa etapa faz-se necessário o uso do objetivo da competência CM.9 da MOSE Competence, no qual trata das ações preventivas, corretivas em caso de incidentes.

Na definição da Política de Segurança e Privacidade dos Dados Pessoais, é necessário que se implemente o conceito de Privacidade desde a Concepção e por Padrão (Privacy by Design e by Default), ficando, desta forma, aderente ao proposto no artigo 46 da LGPD que diz que os agentes de tratamento devem garantir a privacidade e segurança dos dados desde a fase de concepção (BRASIL, 2018). O conceito de privacidade desde a Concepção significa que a privacidade dos dados deve ser considerada desde o início e durante todo o ciclo de vida dos projetos, sistemas, serviços, produtos ou processos. Essa privacidade pode ser alcançada fazendo uso do objetivo da competência CM.9 do MOSE, conforme descrito a seguir.

Seja pró-ativo, ao invés de reativo - foco na prevenção, ao invés da correção: ROUILLER (2017), por meio do Objetivo da Competência CM.7, diz que devem ser feitas análises periódicas com a intenção de prevenir os incidentes. Ela assevera que se deve mapear os incidentes ao longo do ciclo de vida dos serviços e produtos oferecidos pela organização, tendo assim uma atitude proativa em relação à segurança e à privacidade dos dados pessoais. Desta forma, fica evidente que a preocupação com a segurança e a

privacidade deve nascer com o projeto, sistema, serviço, produto ou processos que farão tratamento de dados.

A privacidade deve ser o padrão dos sistemas de TI ou práticas de negócio: o correto atendimento a essa diretiva está relacionado à minimização dos riscos, custos e problemas referente à proteção dos dados. A organização terá certeza da eficácia da implementação da privacidade a partir do momento em que o titular dos dados não realizar nenhuma ação quando ocorrer algum incidente de vazamento de dados (BRASIL, 2020).

Privacidade incorporada ao projeto (design): a privacidade deve ser sempre um pré-requisito explicito de todo projeto de sistema ou prática de negócio. Desta forma, na construção de um novo sistema durante a fase de levantamento de requisitos é preciso que a organização faça uso de um documento padrão de levantamento de requisitos que já traga o requisito de privacidade de maneira explicita. Indo além, é necessário que a organização defina critério funcionais que abranja a privacidade para que a privacidade deixe de ser apenar um requisito não funcional que muitas vezes é deixado em segundo plano. Por exemplo, pode-se definir um requisito que diz: toda informação salva em banco de dados deve ser anonimizada por meio da criptografia RSA. Como se pode observar, ficou claro que os dados serão anonimizados com alguma técnica conhecida de anonimização. Assim, não restará dúvida para quem for desenvolver o sistema que a privacidade é um item importante e que deverá ser implementado. Com base nesse exemplo, a organização pode definir outras formas de anonimização para se tornar padrão não somente de sistemas, mas de projetos e esteja presente na cultura da empresa de maneira geral.

Segurança e proteção de dados pessoais do início ao fim do ciclo de tratamento de dados: tão importante quanto à privacidade por padrão nos projetos, é o monitoramento e o controle da segurança e da privacidade dos dados dos titulares durante todo o ciclo de vida do tratamento de dados. Deve ser implementado padrões em segurança que garantam a confidencialidade, integridade e disponibilidade dos dados pessoais durante o ciclo de tratamento. Outro ponto importante é a definição do prazo em que esses dados ficaram em posse da organização e, consequentemente, quais são os gatilhos e processos que serão acionados para a eliminação desses dados.

Visibilidade e transparência: a Privacidade desde a Concepção tem por objetivo dar visibilidade e transparência às pessoas interessadas nos processos de tratamento de dados. Isso força com que a organização atenda aspectos importantes como: responsabilização, prestação de contas e conformidade. A responsabilização diz respeito a designar quem será o responsável por determinada etapa de processamento de dados. Isto já fora discutido no atendimento do artigo 47. Entretanto, vale ressaltar a importância de um processo transparente no qual toda a organização sabe quem é o responsável pela respectiva etapa do processamento de dados. Já a prestação de contas diz respeito às formas como os titulares poderão fazer petição referente aos seus dados, petições de acesso, alteração, exclusão e remoção de autorização de uso dos dados. Por fim, a conformidade está relacionada às etapas necessárias para monitorar, avaliar e verificar a conformidade com as políticas e procedimentos estabelecidos. Essa conformidade pode ser averiguada por uma auditoria interna para que a organização não seja surpreendida por uma auditoria externa.

Respeito pela privacidade do usuário: a Privacidade desde a Concepção exige que a organização defina padrões de privacidade, avisos em interfaces sistêmicas ou na própria área de atendimento ao cliente sobre como a organização faz a coleta e o uso dos dados. Diversas abordagens podem ser escolhidas, como: avisos em sites, publicidade em meios de comunicação, avisos em balcão de atendimento, entre outros. A ideia aqui é deixar o usuário confortável e ciente de que a empresa segue os procedimentos previstos

na LGPD. Além disso, a nível concreto, a organização deve definir artefatos padrões para coleta de consentimento do titular dos dados, lembrando que esse consentimento deve seguir a letra da lei no que diz respeito que o consentimento deve ser específico. Os dados coletados também devem ser precisos, isto é, deve-se somente coletar os dados que realmente serão usados no tratamento. Além disso, conforme mencionado anteriormente, a empresa deverá deixar canais de atendimento abertos, conforme mencionados na implementação do CM.4, para que o titular exerça seus direitos previstos em lei.

Estrutura Organizacional para Governança e Gestão de Proteção de Dados Pessoais: a definição da estrutura organizacional é bastante abordada na implementação do artigo 46. Então, para implementação dessa estrutura com base no trabalho de DE SOUZA e OLIVEIRA (2020) é citado os objetivos da competência GQ.1, GQ.2, GQ.4, GQ.6. Essas dimensões fazem parte da dimensão de Gestão e Qualidade que, segundo ROUILLER (2017), serve como base para a construção de uma estrutura organizacional. No contexto dessa etapa, é essencial que a organização faça o planejamento necessário para que seja definida essa estrutura organizacional que irá suportar o Programa de Governança e Boas Práticas em Privacidade. O planejamento e a implementação dessa estrutura podem ser encontrados na implementação do artigo 46 descrito em seção anterior.

Inventário de Dados Pessoais: nesta fase é importante que a organização defina como irá realizar o inventário de dados pessoais. Para criação e manutenção desse inventário, pode usar sistemas ou planilhas eletrônicas centralizadas, no qual é possível identificar por meio dos processos, isto é, em uma abordagem *top/down*, como a organização coleta e trata esses dados durante determinados ciclos de tratamentos. Aqui pode ser usado tanto o RIPD – Relatório de Impacto à Proteção de Dados que já fora mencionado.

Levantamento de modelos de contratos com clientes, bem como com terceiros ou parceiras que fazem tratamento de dados: na etapa de planejamento, faz-se necessário também fazer o levantamento de todos os modelos de contratos com clientes, parceiros e terceiros. Para isso, deve ser aplicado o objetivo da competência CM.1 que trata da gestão de contratos pela unidade de negócio. Esse levantamento será necessário para que a organização analise e verifique a necessidade de atualização das suas cláusulas, adicionando àquelas que têm relação direta com a Lei Geral de Proteção de Dados. Assim, novos modelos deverão ser gerados para condizerem com a realidade atual da organização no que diz respeito ao complice com a LGPD.

5.5.2 Construção e execução

Findo a etapa de início e planejamento para a criação do Programa de Governança e Boas Práticas em Privacidade. Chega-se à etapa de construção e execução. Esta etapa deve seguir o planejado e caso seja verificado durante o processo a necessidade de ajustes, esses ajustes devem ser documentados nos artefatos produzidos na etapa de planejamento. Dito isso, os próximos tópicos trataram dos marcos a serem alcançados na construção do Programa de Governança e Boas Práticas em Privacidade (PGBPP).

Políticas e práticas para proteção da privacidade: na construção do PGBPP devem ser especificadas e criadas as políticas e práticas para proteger a privacidade do cliente da organização. As políticas devem ser normatizadas internamente e fazer parte do dia a dia da organização. As políticas devem garantir que: o s dados pessoais estão sendo tratados em conformidade com a LGPD; os dados pessoais estão protegidos contra mau uso e compartilhamento indevido; os processos de tratamento de dados realizando as anonimizações necessárias (BRASIL, 2020).

Para o melhor gerenciamento e controle das políticas e práticas, é necessário que a organização, por meio da dimensão da competência TH.1, defina os papéis os papeis e responsabilidades dos colaboradores, parceiras e terceirizadas que realizam o tratamento de dados. Esses papéis devem ser definidos em nível de unidades de negócios, bem como colaboradores que tratam de processos específicos de tratamento de dados dentro dessas unidades. Para isso, é necessário definir o papel e as responsabilidades dos envolvidos na coleta, retenção, processamento, compartilhamento e eliminação dos dados.

Para que esses agentes de tratamento cumpram com seu papel e com suas responsabilidades, faz necessário que a organização, por meio do objetivo da competência TH.6, estabeleçam e mantenham programas de capacitação com a temática da LGPD e da proteção de dados. Indo além, é importante também nesse momento a participação da alta administração para reforçar a importância dos treinamentos para organização.

Por fim, a organização deve definir de maneira geral em suas políticas e boas práticas qual é a finalidade e a base legal que a organização utiliza para fazer o tratamento de dados. Isso deve estar internalizado na cultura organizacional de maneira que os colaboradores não tenham dúvidas durante a contratação de tecnologias, serviços, treinamentos entre outros aspectos em que essa informação seja relevante.

Cultura de segurança e proteção de dados e Privacidade Por Padrão (Privacy by Design): na etapa de construção, deve-se promover a cultura de segurança e proteção de dados seguindo o que foi definido na fase de planejamento. Vale ressaltar que a Privacidade por Padrão deve atender todas as características mencionadas anteriormente como cobrir a empresa de ponta a ponta, privacidade incorporada ao projeto, privacidade desde a concepção, dentre outras.

Relatório de Impacto à Proteção de Dados Pessoais (RIPD): nesta etapa deve ser elaborado o RIPD. Esse artefato é um instrumento que visa à verificação e a demonstração da conformidade do tratamento de dados pessoais realizados pela organização. O RIPD deve descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas de salvaguardas e mecanismos de mitigação de risco (BRASIL, 2020). Esse relatório é definido pela LGPD como "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco" (BRASIL, 2018).

O RIPD deve ser elaborado por meio do atendimento ao objetivo da competência GQ.9 que tem por objetivo estabelecer e manter uma estratégia para o gerenciamento de riscos na organização. ROUILLER (2017) elenca resultados esperados para o objetivo GQ.9 que podem ser incluídos no RIPD, como identificar, avaliar, quantificar, priorizar os riscos relacionados ao negócio, identificar ações para o contingenciamento e mitigação dos riscos, desenvolver uma base de conhecimento em relação aos riscos mitigados. Essas informações devem compor o Relatório para, caso seja necessário, ser apresentado para a ANPD quando solicitado.

Para reforçar o exposto acima, o controlador deve observar a Lei que trata das informações mínimas que devem estar presente neste relatório: "o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação" (BRASIL, 2018).

Política de Privacidade: a Política de Privacidade da organização deve ser construída nessa etapa. Por meio do CM.4, no qual é estabelecido o relacionamento com o cliente, é possível atender ao princípio da transparência em que o controlador, por meio do

documento da Política de Privacidade, irá transparecer ao usuário a forma como a organização faz o tratamento dos dados e quais são os meios pelo qual a organização fornece privacidade ao usuário.

Esta politica deve estar presente nos meios de comunicação da organização com o cliente e com o mercado, de forma que seja de fácil acesso ao público. O documento de Política de Privacidade deve abordar os seguintes temas, conforme (BRASIL, 2020): controlador; operador; encarregado; como os dados são coletados; quais dados são tratados; quais dados são necessários por tipo de atendimento; quais as tecnologias empregadas na coleta dos dados; como os dados são compartilhados; como os dados são utilizados; como os dados são armazenados; qual o tratamento de dados realizados e qual finalidade; transferência Internacional dos dados; quais dados sensíveis são coletados; segurança dos dados; políticas de cookies; tratamento posterior dos dados para outras finalidades; a validade dos dados; os procedimentos de exclusão; quais procedimentos são utilizados para proteção dos dados; quais são os direitos dos titulares dos dados; quais são os canais de atendimento ao cliente; nome e informações de contato do DPO.

Adequação de cláusulas contratuais: após o levantamento inicial dos contratos vigentes e válidos da organização. Nesta etapa, faz necessário realizar as adequações contratuais dos contratos vigentes, bem como a atualização do modelo de contratos para os novos contratos. As novas atualizações contratuais devem estar aderentes a LGPD, desta forma, sugere-se analisar e abordar os seguintes pontos definidos em (BRASIL, 2020) para atualização dos contratos com clientes, empresas parceiras ou terceiras que realizam tratamento de dados em nome do controlador: delimitações claras e objetivas das responsabilidades do controlador e operador; a forma que é realizada a coleta e o tratamento de dados; a existência da possibilidade de o titular acessar os seus dados coletados; a forma que é realizada a correção, bloqueio ou eliminação de dados mediante solicitação do titular; a existência da possibilidade de revogação do consentimento dado pelo titular; o detalhamento de quem tem acesso aos dados, o responsável por seu uso e tratamento, a forma de armazenamento e as particularidades de possíveis auditorias; as medidas de proteção e segurança dos dados coletados e armazenados pela contratada.

Termo de Uso: o Termo de Uso é outro documento que deve ser atualizado conforme a preconização da LGPD. Esse termo é um documento que fornece uma descrição detalhada do serviço, das condições e das regras aplicáveis a ele (BRASIL, 2020). Na atualização, melhoria ou criação de um termo de uso, a organização deve analisar e descrever os seguintes tópicos na construção desse documento: 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.

Encarregado: para finalizar essa fase de execução, segundo BRASIL (2020), o Encarregado deve realizar os seguintes procedimentos para o adequado fechamento desta fase: implementação das ações identificadas na fase de Iniciação e Planejamento; demonstração, para a alta administração, do progresso e dos resultados obtidos com as atividades envolvendo o inventário dos dados e a divulgação e conscientização da LGPD junto aos colaboradores e pessoas interessadas; se necessário, redefinição de prioridades, baseando-se nos resultados alcançados e no retorno dos dirigentes e secretarias do órgão; estabelecimento e manutenção de documentação relacionada à LGPD e aos dados pessoais tratados na organização, com informações sobre: atividades em andamento e planejadas; responsáveis pelos serviços e sistemas que utilizam dados pessoais; e incidentes e vazamento de dados pessoais; definição de mecanismos de reportes internos, assegurando transparência e rapidez na troca de informação, além de reafirmar o papel como facilitador.

5.5.3 Monitoramento

A LGPD é uma lei recente e deverá passar por muitas atualizações, então é crucial que a organização mantenha a estrutura organizacional que vise o monitoramento e controle das ações condizentes com as atualizações da Lei. Assim, a etapa de monitoramento tem por objetivo de fornecer os feedbacks por meio de relatórios e apresentação dos resultados. Acima de tudo, a organização deve manter uma gestão de monitoramento de incidentes no qual consiga amadurecer e aprender com os erros, por meio de uma base de conhecimento de incidentes.

Gestão de Incidentes: por meio do Objetivo da Competência CM.9 é possível estabelecer na organização um programa de gestão de incidentes no qual seja obtidos os resultados esperados por ROUILLER (2017), que sejam: definir estratégia para resolução de incidentes (ex.: o que é um incidente, equipe que deve estar apta a resolvê-lo e analisá-lo, onde registrá-lo, categorização por tipo de cliente, periodicidade de análise, entre outros); identificar incidentes; resolver incidentes ocorridos; registrar os incidentes; mapear potenciais incidentes ao longo do ciclo de vida do dado; mapear potenciais incidentes no tratamento de dados; definir método para análise de impacto de incidentes; analisar periodicamente os incidentes e realizar ações para sua prevenção; gerenciar ações de prevenção até a sua conclusão; catalogar os incidentes em uma base de conhecimento de incidentes. Por fim, BRASIL (2020) recomenda que a Gestão de Incidentes possua um Plano de Comunicação orientando a forma que os incidentes de segurança, que acarretem risco ou dano, sejam informados aos órgãos fiscalizatórios e à imprensa.

Inovação: como mencionado anteriormente, a LGPD deverá passar por várias atualizações no decorrer de sua existência. Para isso a organização deve manter em sua organização uma estrutura organizacional que seja responsável por manter a instituição atualizada em relação à LGPD. Para isso, é necessário implementar uma gestão de inovação por meio da dimensão de competência Inovação da MOSE. Pode usar ainda, o objetivo da competência IN.1 para verificar de tempos em tempos o mercado para coletar novidades sobre a LGPD de maneira que possa ser implantada na organização.

4. CONCLUSÕES

Os relatórios AKAMAI (2020) e CODEBY (2020) apontaram que a maioria das empresas brasileiras não estão em conformidade com a LGPD ou, em um cenário mais alarmante, os profissionais dessas empresas desconhecem a existência da Lei de proteção de dados. A falta de informação sobre a LGPD foi um dos motivos apontados no relatório da CODEBY para a formação do cenário apresentado.

Assim, este trabalho propõe-se a fornecer um conjunto de orientações para a implementação da LGPD a partir das práticas presentes no MOSE. Desta forma, este guia deve contribuir como material de referência para implementação da LGPD em organizações de todo porte e por consequência melhorar o cenário atual, fazendo com que mais empresas se adequem à LGPD e, assim, evitem multas que venha a prejudicar a sua existência, além de manter a empresa em igualdade com a concorrência que venha a usar a aderência com a LGPD como diferencial competitivo. Espera-se também beneficiar as pessoas naturais, pois com mais organizações aderentes à LGPD, esse trabalho estará promovendo uma sociedade mais transparente e preocupada com a privacidade dos dados.

Como trabalhos futuros, espera-se mostrar a aplicação deste trabalho em um cenário simulado. Outro ponto importante também seria a utilização do guia proposto em mais organizações, além da avaliação do guia por mais profissionais especialistas na área para a coleta de *feedbacks* e evolução do trabalho proposto.

REFERÊNCIAS BIBLIOGRÁFICAS

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

ABNT. NBR ISO/IEC 27001. (2013). "Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação – Requisitos". Brasil.

ABNT. NBR ISO/IEC 27002. (2013). "Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação". Brasil.

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.

BRASIL. Ministério da Economia. (2020). "Guia de Elaboração de Programa de Governança em Privacidade". V.1. Brasília, Brasil.

CODEBY (2020). "Pesquisa sobre LGPDY". São Paulo, SP, Brasil.

LOPES, M., GUARDA, T., Oliveira P. (2019), "How ISO 27001 Can Help Achieve GDPR Compliance". 14th CISTI. Coimbra, Portugal.

PROCEMPA (2020). "LGPD - PROCEMPA Plano de Resposta a Incidentes de Segurança e Privacidade". Porto Alegre, RS, Brasil.

RIBEIRO, R. C., CANEDO, E. D. (2020). "Using MCDA for Selecting Criteria of LGPD Compliant Personal Data Security". In The 21st DGO. ACM, USA.

ROUILLER, A. C. (2017) "MOSE: base de competências (2nd. ed.)". Editora Pé Livre Ltda. Recife, PE, Brasil.

ROUILLER, A. C. (2020). "MOSE.LGPD: Sistema para evolução progressiva da maturidade da governança em gestão, tratamento e proteção dos dados". 1ªedição. Editora Pé livre: MOSE Competence Institute, Recife, PE, Brasil.

SILVA, J., CALEGARI, N., GOMES, E. (2019). "After Brazil's General Data Protection Law: Authorization in Decentralized Web Applications". In 2019 WWW '19. ACM, USA.

SILVA, D. C. (2020). "Manual da Lei Geral de Proteção de Dados para Instituições de Ensino". 1. Ed. Brasília, Brasil.

DE SOUZA, M. A., OLIVEIRA, S. R. B. (2021). "Adequação da MOSE® Competence para a Implementação do Capítulo VII da LGPD: Um Mapeamento dos Ativos de Segurança e Boas Práticas". In COTB'21. Brasil.

TORRE, D., ABUALHAIJA, S., SABETZADEH, M., BRIAND, L., BAETENS, K., GOES, P., FORASTIER, S. (2020), "An AI-assisted Approach for Checking the Completeness of Privacy Policies Against GDPR". IEEE 28th RE. Zurich, Switzerland.

TRUONG, N. B., SUN, K., LEE, G. M., GUO, Y. (2020). "GDPR-Compliant Personal Data Management: A Blockchain-Based Solution". in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 1746-1761.

UE - União Europeia. (2016). "Regulamento Geral de Proteção de Dados". Jornal Oficial da União Europeia. Disponível em *https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679* Acesso em Julho/2021.