Adequação da MOSE® Competence para a Implementação do Capítulo VII da LGPD: Um Mapeamento dos Ativos de Segurança e Boas Práticas

Maykon Araújo de Souza
Programa de Pós-Graduação em Ciência da Computação - Universidade Federal do Pará (UFPA)
Belém - Pará - Brasil
maykonaraujo23@gmail.com

Sandro Ronaldo Bezerra Oliveira
Programa de Pós-Graduação em Ciência da Computação - Universidade Federal do Pará (UFPA)
Belém - Pará - Brasil
srbo@ufpa.br

ABSTRACT

This study presents a mapping of the assets present in the Guiding Model for the Success of Public and Private Companies (MOSE) and the articles included in the General Data Protection Law (LGPD) of the Brazilian Government, with regard to Security and Good Practices in Chapter VII of this law. The theme becomes relevant, as more and more companies from different contexts need to implement the articles contained in this law in order to adhere to the standard of regulation of personal data processing activities defined by the Brazilian Federal Government. However, this law still needs guidelines for its proper implementation based on the adoption of good practices in models, methods and/or techniques available in the specialized literature. One of these instruments refers to the MOSE, which helps public and private companies to achieve levels of excellence in performance, governance and quality, in the production of goods and services, based on the use of practices and indicators specific to the area of knowledge or specialty. Thus, the research question guiding this work is: how to correspond/map the practices included in the MOSE to guide the implementation of the articles of the LGPD law? The methodology adopted was the asset mapping, described in a specific section of the paper, which included the following steps: definition of the LGPD chapter that focuses on data security management; definition of the model and law structures, and their inputs to be analyzed; identification of the description of each asset; analysis of correspondence between assets; evaluation of the mapping using the peer review technique with expert in the two target standards of this research. The result was the perception that 33% of the MOSE's competences goals, with the appropriate adjustments, have total adherence with 100% of the security and good pratices assets of LGPD. This mapping is intended to provide assistance in defining a roadmap containing activities, work products, tools, indicators and expected results to achieve the goals defined in the LGPD.

KEYWORDS

Mapping of Assets, Security and Good Practices, Recommendations, MOSE, LGPD.

1 INTRODUÇÃO

A Lei Geral de Proteção de Dados (LGPD) garante ao titular dos dados mais direitos e poderes sobre as suas informações [1]. A publicação e promulgação dessa Lei obrigou as organizações a adequarem seus processos de tratamento de dados, além de terem que criar mecanismos de transparência que possibilitem que o titular dos dados exerça o seu direito.

O problema é que não existe um roteiro ou um guia orientador para implementação da LGPD nas organizações, fazendo com que essas instituições tenham dificuldades em cumprir a Lei e, assim, ficando suscetíveis às penalidades previstas. Uma prova disso é que, mesmo após a sua publicação em 14 de agosto de 2018 [1] e a sua entrada em vigor em 18 de setembro de 2020 [2], 64% das empresas ainda não estão em conformidade com esta Lei [3].

Diante disso, a construção deste trabalho justifica-se e se faz necessária como uma forma de contribuição para a melhoria do cenário apresentado. Isso motivou um estudo aprofundado da LGPD e da Certificação MOSE Competence (Modelo Orientador para o Sucesso do Empreendimento) [4] com o objetivo de verificar a existência de uma correlação entre esses dois normativos.

Portanto, este trabalho tem o objetivo de estudar a LGPD e a MOSE a fim de construir um mapeamento que apresente a relação entre os ativos relacionados à segurança e às boas práticas da Lei, constantes em seu capítulo VII, com os objetivos da competência e resultados esperados presentes na certificação.

O resultado deste trabalho foi a percepção de que 33% dos objetivos da competência da MOSE, com as devidas adequações, tem aderência total com 100% dos ativos de segurança e boas práticas da LGPD.

Além desta seção introdutória, este artigo está organizado como segue: a Seção 2 apresenta a fundamentação teórica deste trabalho; a Seção 3 apreenta e discute alguns trabalhos relacionados; a Seção 4 apresenta a análise dos ativos da MOSE Competence para atendimento da LGPD; a Seção 5 apresenta a forma de avaliação dos resultados obtidos com este trabalho; e, por fim, a Seção 6 apresenta a conclusão deste estudo.

2 FUNDAMENTAÇÃO TEÓRICA

A seção de fundamentação teórica apresenta alguns conceitos para o melhor entendimento deste trabalho, tais como: a certificação MOSE Competence e a LGPD.

2.1 Certificação MOSE Competence

A certificação MOSE Competence foi criada pelo MOSE Competence Institute que é uma entidade de direito privado, com sede internacional na Suíça, e com atuação na Europa, na China e no Brasil [4]. Esta certificação foi desenvolvida para ser aplicada em diversos empreendimentos, quais sejam, empresas, órgãos públicos, grupo de pessoas, entre outros que desejam melhorar seu desempenho relacionado ao próprio negócio e à produção de bens

e serviços [5]. O MOSE Competence Institute criou essa certificação com a finalidade de apoiar o desenvolvimento de empreendimentos no mercado. O instituto percebeu, durante os seus 30 anos de experiência com empreendimentos, que existem problemas comuns que fazem com que essas organizações morram [5].

A MOSE Competence é composta por 3 documentos principais: Base de Competências, Métodos de Avaliação e Guias de Medição. Estes documentos foram desenvolvidos respeitando as orientações da ISO (*International Organization for Standardization*) para a construção de modelos de capacidade e maturidade [5].

Este artigo utiliza o documento Base de Competências em seus estudos. A Base de Competências é composta por 5 dimensões: Talento Humano, Gestão e Qualidade, Inovação, Cliente e Mercado, e Sociedade e Sustentabilidade que, juntas, tratam aspectos relevantes para que um empreendimento evolua e tenha sucesso [5].

A dimensão de Talento Humano aborda os aspectos relacionados às responsabilidades de cada indivíduo no empreendimento, à sua contribuição para produção dos bens e serviços e ao desenvolvimento do negócio. Por sua vez, a dimensão de Gestão e Qualidade aborda aspectos relacionados à gestão da produção de bens e serviços e do próprio empreendimento. Enquanto que a dimensão de Inovação aborda temas relacionados a olhar o negócio (atual ou novo) sob uma nova perspectiva, potencializando as oportunidades observadas. Já a dimensão de Cliente e Mercado aborda temas como a estruturação do empreendimento para poder atender de forma satisfatória seus clientes, a análise constante do mercado (e/ou ambiente) e o impacto dos bens e serviços gerados nele. Por fim, a dimensão Sociedade e Sustentabilidade trata dos aspectos da inserção do empreendimento na sociedade a qual pertence, incluindo aspectos relacionados à responsabilidade social e ambiental [5].

Cada dimensão de competência é composta por objetivos da competência que resumem os objetivos que a unidade de negócio deve alcançar para o cumprimento do esperado pela certificação MOSE Competence [5]. Assim, cada objetivo de competência possui: um conjunto de resultados esperados, que são orientações de como os colaboradores de um empreendimento podem implementar em sua unidade/setor o que se recomenda pelo modelo; e um conjunto de indicadores obrigatórios e recomendados, que representam a maneira como deve se medir a performance de execução das atividades de um dado empreendimento, sendo adaptado de acordo com o contexto de negócio.

2.2 Lei Geral de Proteção de Dados

A Lei Geral de Proteção de Dados (LGPD) foi publicada em 14 de agosto de 2018 [1] e entrou em vigor em 18 de setembro de 2020 [2]. Ela 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 [1].

A LGPD (Lei No 13.709) [2] está estruturada nos seguintes capítulos: Capítulo I - Disposições Preliminares; Capítulo II – Do Tratamento de Dados Pessoais; Capitulo III – Dos Direitos do Titular; Capítulo IV – Do Tratamento de Dados Pessoais pelo Poder Público; Capítulo V – Da Transferência Internacional de Dados; Capítulo VI – Dos Agentes de Tratamento de Dados Pessoais; Capítulo VII – Da Segurança e Das Boas Práticas; Capítulo VIII – Da Fiscalização; Capítulo IX – Da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; e Capítulo X – Disposições Finais e Transitórias [1].

Para melhor entendimento da Lei, é necessário entender as definições presentes no artigo 5º, a saber: **dado pessoal**, informação relacionada à pessoa natural identificada ou identificável; **dado pessoal sensível**, dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; **dado anonimizado**, dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; **banco de dados**, conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico; **titular**, pessoa natural a quem se referem os dados pessoais que são objeto de tratamento; **controlador**, pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; **operador**, pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; **encarregado**, pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); **agentes de tratamento**, o controlador e o operador; **tratamento**, toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; **anonimização**, utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo; **consentimento**, manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada; **bloqueio**, suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados; **eliminação**, exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado; **transferência internacional de dados**, transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro; **uso compartilhado de dados**, comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados; **relatório de impacto à proteção de dados pessoais**, 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; **órgão**

de pesquisa, órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e **autoridade nacional,** órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional [1].

O artigo 6º trata dos princípios da LGPD, a saber: **finalidade**, realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; **adequação**, compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; **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; **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; **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; **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; **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; **prevenção**, adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; **não discriminação**, impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; **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 [1].

O objeto de estudo deste artigo é o Capítulo VII da LGPD que está dividido em duas seções: Seção I – Da Segurança e do Sigilo dos Dados; Seção II – Das Boas Práticas e da Governança. A **Seção I** traz os seguintes artigos:

- **46.** Os agentes de tratamento devem adotar 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. O seu parágrafo segundo complementa a informação ordenando que as medidas tratadas no caput do artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução;
- **47.** Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista na Lei em relação aos dados pessoais, mesmo após o seu término;
- **48.** 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. No contexto do artigo 48, segue-se os seguintes parágrafos que regimentam a comunicação entre o controlador e os demais interessados: a comunicação deverá ser feita em prazo razoável, conforme definido pela autoridade nacional. Esta comunicação deverá mencionar no mínimo: a descrição da natureza dos dados dos pessoais afetados; as informações sobre os titulares envolvidos; a indicação de medidas técnicas e de segurança utilizadas para a proteção de dados, observados os segredos comerciais e industriais; os riscos relacionados ao incidente; os motivos da demora, caso a comunicação não seja imediata; as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. O segundo parágrafo do artigo 48 indica que cabe à autoridade nacional verificar a gravidade do incidente e, a partir disso, determinar que o controlador tome as seguintes providências: ampla divulgação do fato em meios de comunicação; e medidas para reverter ou mitigar os efeitos do incidente. No terceiro parágrafo do artigo 48 é informado que no juízo da 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;
- **49.** 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 [1].

Da **Seção II**, que trata das boas práticas e da governança, será utilizado somente o artigo **50**. Nesse artigo está descrito que 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. Essas regras devem estabelecer 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 [1].

O primeiro parágrafo do artigo 50 diz que ao estabelecer regras de boas práticas, o controlador e o operador levarão 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 [1].

Já o segundo parágrafo do artigo 50 faz referência aos princípios da segurança e da prevenção. Enfatizando que na aplicação desses princípios, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá implementar um 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; e demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento da LGPD [1].

3 TRABALHOS RELACIONADOS

Guarda *et al.* [6] 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 busca em sites de discussão sobre a implementação da GDPR pela ISO 27001. Este trabalho conseguiu comprovar que apesar da ISO 27001 não atender completamente a GDPR, uma organização que tenha implementado esta ISO pode simplificar o processo de adequação [6].

Essa implementação da Lei de proteção de dados européia assemelha-se, em um nível geral, ao que se propõe neste trabalho, entretanto eles não utilizaram a revisão por pares e nem obtiveram uma avaliação direta de um especialista. Outro ponto é que diferente da ISO 27001, a certificação MOSE se preocupa com a performance da Instituição que implementa o Modelo [5]. Isso significa que, além da MOSE atender aos ativos LGPD indicados, a certificação também garante manter e/ou melhorar o desempenho da organização, assim, é possível implementar a MOSE de modo que não onere a produtividade da instituição [5].

Truong *et al.* [7] objetivam prover o gerenciamento de dados pessoais em conformidade da GDPR por meio de uma solução baseada em *blockchain* (conjunto de técnicas diversificadas incluindo sistemas distribuídos, redes de computadores, bancos de dados, e a criptografia que faz o papel de um livro-razão distribuído). 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 [7].

A proposta acima, que trata da adequação à GDPR por meio de uma plataforma que garanta o rastreio e a integridade da informação, atende ao propósito de implementação da LGPD no nível de ferramentas e software. Embora a solução apresentada tenha resultados satisfatórios, ela atende somente no nível operacional. Assim, algumas questões, que não são o propósito do trabalho de Truong *et al.* [7], ficam em aberto, tais como: Qual o nível de maturidade que uma organização precisa ter para fazer uso dessa ferramenta? Quais são os pré-requisitos a nível de gestão e governança que uma organização deve ter para alcançar um resultado satisfatório com o uso da plataforma? Dito isso, nota-se que o diferencial da implementação da LGPD por meio da MOSE é que ela cobre organizações de pequeno, médio e grande portes, quer seja pública ou privada [5]. A MOSE trabalha na organização como um todo, e a partir do momento que a organização vai entendendo seus processos e ganhando maturidade, a atualização ou aquisição de software serão apenas reflexo do processo de obtenção da certificação. Desta forma, é possível perceber que para uma organização que amadureceu por meio do processo de certificação da MOSE, a aquisição de um software que atende a uma lei de proteção de dados representa apenas uma das opções a serem seguidas.

4 ANÁLISE DOS ATIVOS DA MOSE COMPETENCE PARA ATENDIMENTO DA LGPD

Nesta seção é aprofundado o estudo e a construção do mapeamento. Serão apresentados os seus objetivos, a metodologia utilizada, o relacionamento entre os normativos e, por fim, o resultado do mapeamento.

4.1 Objetivos

O objetivo geral deste trabalho é oferecer um instrumento para auxiliar na implementação da LGPD nas organizações. Desta forma, um dos meios para se atingir esse objetivo é a construção de um mapeamento que visa encontrar uma correlação entre os objetivos da competência da MOSE e Lei Geral de Proteção de Dados a partir do estudo de seus ativos. Por fim, pretende-se com esse mapeamento possibilitar um instrumento de apoio para uma futura definição de um roteiro contendo atividades, artefatos, ferramentas, indicadores e resultados esperados para o alcance das metas definidas na LGPD.

4.2 Metodologia

A metodologia adotada para a construção do mapemanto foi o método comparativo, no qual a investigação é feita por meio da análise de dois ou mais ativos dos normativos previamente definidos, analisando as diferenças e similaridades existentes entre eles. O método comparativo utilizado teve os seguintes passos: estudos gerais e detalhados dos normativos envolvidos, definição do capítulo da LGPD que foca na gestão da segurança dos dados; definição das estruturas do modelo e da Lei, e seus devidos insumos a serem analisados; identificação da descrição de cada ativo; análise da correspondência entre os ativos; avaliação do mapeamento usando a técnica de revisão por pares com especialista nos dois padrões-alvo desta pesquisa.

4.2.1 Fluxo da Metodologia. O fluxo do processo da metodologia deste trabalho iniciou-se com o estudo da base de competências da certificação MOSE [5]. Primeiro foi realizado um estudo da metodologia como um todo: arquitetura da MOSE, níveis de excelência, categorias de um empreendimento, elementos bases da competência e a avaliação da organização [5].

Após o estudo geral, o próximo passo foi estudar e entender a base de competências da MOSE que é formada por: dimensões da competência que, por sua vez, é composta por objetivos da competência e objetivos da excelência, e estes compostos por resultados esperados e indicadores, como já definido na Seção 2.

Com o entendimento da certificação, passou-se para o estudo e compreensão da LGPD. Então, o objetivo desse passo foi estudar os artigos da Lei e entender a sua proposta.

Com o entendimento geral sobre a LGPD e com o conhecimento da certificação, o próximo passo foi escolher o capitulo da Lei que mais se alinhasse com a proposta da

certificação MOSE. Desta forma, foi escolhido o Capítulo VII da LGDP que trata da segurança e das boas práticas.

Diante dos estudos dos normativos e escolha dos ativos da LGPD a serem trabalhados, partiu-se para a construção do mapeamento. Para a realização do mapeamento, utilizou-se a técnica de "dividir para conquistar", isto é, o Capítulo VII foi separado em 5 artigos e esses artigos foram separados em 23 ativos. Após isso, a próxima etapa foi fazer o mapeamento dos objetivos da competência da MOSE que tinham aderência total ou parcial com os 23 ativos da LGPD. Depois desse mapeamento, foi a vez de realizar a soma das partes, então os 23 ativos voltaram a se tornar 5 artigos, mas desta vez eles vieram com os seus respectivos objetivos da competência definidos.

Cada etapa desses estudos foi apresentada e avaliada quanto a sua coerência por um orientador com experiência em: mais de 10 pesquisas sobre o uso da certificação MOSE; 20 anos de experiência com melhoria de processo; implementação da certificação MOSE Competence em mais de 30 empresas de Tecnologia da Informação (TI); e condução em mais de 30 trabalhos científicos sobre mapeamento entre normativos.

Com o mapeamento pronto, a próxima etapa foi planejar a revisão por pares, encontrar por meio de um questionário um especialista com o perfil adequado para avaliar o mapeamento, executar a revisão por pares e executar as correções propostas pelo especialista.

Por fim, com o mapeamento revisado e aprovado pelo especialista, foi feito uma análise para chegar à conclusão final deste trabalho.

4.3 Relacionamentos entre os Ativos

A partir dos ativos envolvidos, conforme descritos na Seção 2, foi possível gerar o mapa de correspondência entre os ativos da MOSE para atendimento dos ativos de segurança e boas práticas contidos no Capítulo VII da LGPD. Na Figura 1 é possível observar o relacionamento direto ou de equivalência pela igualdade de cores, por exemplo, os objetivos de competência da MOSE e os artigos do Capítulo VII da LGPD possuem correspondência. De modo geral, destaca-se que os ativos sem cor (fundo branco) não foram correlacionados porque este estudo não direciona a análise para atendimento de capítulo e/ou seções da LGPD, mas somente para os artigos, que garante o atendimento da Lei. Observa-se também que nem todos ativos da MOSE tiveram correspondência com os artigos da LGPD.

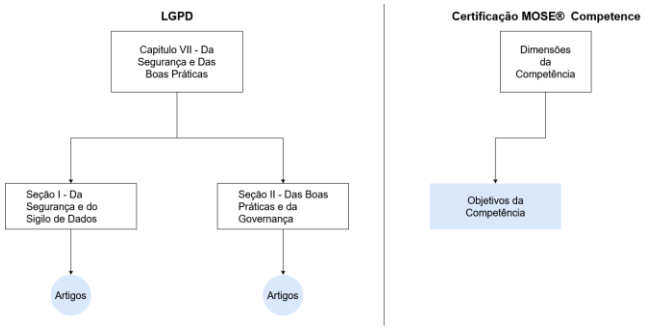

Figura 1: Diagrama de relacionamento entre os ativos da MOSE Competence com os ativos do Capítulo VII da LGPD.

4.4 Mapeamentos dos Ativos do MOSE Competence para as Orientação da LGPD

Nesta seção é apresentado o resultado do mapeamento que mostra a correspondência dos objetivos da competência da MOSE que atendem os ativos de segurança e boas práticas da Lei. Para melhor entendimento do mapeamento, são apresentados os rótulos e seus respectivos significados no mapeamento:

- **Ativo LGPD**, refere-se aos artigos extraídos da LGPD, aqui será mostrado somente o nome do artigo que está melhor descrito na Seção 2 deste artigo;
- **Dimensão da Competência**, refere-se às dimensões de competência da MOSE Competence;
- **Objetivos da Competência**, refere-se aos objetivos da competência que fazem parte da dimensão da competência;
- **Grau de Aderência**, refere-se ao grau de aderência e/ou adequabilidade que o objetivo da competência tem com o respectivo ativo da LGPD. Para definição do Grau de Aderência a pergunta que deve ser feita é: este objetivo ou grupo de objetivos da competência atende de forma parcial ou total ao respectivo ativo da LGPD? Atender de forma **Parcial** significa que o referido objetivo ou grupo de objetivos da competência atende ao respectivo item da LGPD em partes. Por outro lado, atender de forma **Total** siginifca que o referido objetivo da competência ou o grupo de objetivos da competência atende ao respectivo ativo da LGPD de forma total e integral, não deixando espaço para dúvidas quanto ao seu completo atendimento;
- **Justificativa**, refere-se ao entendimento que se teve para escolha de determinado objetivo da competência ou grupo de objetivos da competência para atender aquele ativo da Lei e o motivo da escolha do grau de aderência.

Assim, a seguir os mapeamentos serão apresentados de acordo com cada artigo constante no Capítulo VII da Lei e seguindo as orientações dos rótulos previamente definidos.

4.4.1 ***Ativo LGPD: Artigo 46***. **Dimensões da Competência da MOSE:** Gestão e Qualidade, Talento Humano, e Cliente e Mercado. **Objetivo da Competência da MOSE:** GQ.1. Estruturas básicas para a gestão da unidade de negócio são estabelecidos e mantidos; GQ.2 Abordagens para gestão de equipes da Unidade de Negócio são estabelecidas e mantidas; GQ.4. Melhorias são identificadas e implementadas; TH.2. Necessidades de capacitação são identificadas e tratadas; TH.6. Programas (e/ou ações) de capacitação são estabelecidos e mantidos; TH.8. Análises do impacto dos programas (e/ou ações) de capacitação são realizadas; CM.9. Incidentes são registrados, analisados e ações preventivas são estabelecidas. **Grau de Aderência:** Total. **Justificativa:** os objetivos da competência GQ.1, GQ.2, GQ.4, TH.2, TH.6, TH.8 e CM.9 implementados em conjunto atendem ao respectivo ativo LGPD de maneira total. Para atendimento das medidas administrativas propostas pelo ativo foram selecionados da dimensão Gestão e Qualidade da MOSE os seguintes objetivos da competência: GQ.1 que aborda que o controlador deve estabelecer e manter uma estrutura de gestão de negócio para evitar trabalhar de forma caótica; GQ.2 que, por sua vez, justifica-se pelo fato dos operadores desempenharem um papel importante no processo de tratamento de dados, então, por isso o controlador deve estabelecer e manter abordagens para gestão de equipes para que tenha os recursos disponíveis quando necessário; GQ.4 sob a justificativa de que a

melhoria contínua é um processo indispensável para que o controlador mantenha-se atualizado e aderente a LGPD. Para atender a implementação de medidas técnicas na organização, foram adotados da dimensão Talento Humano os seguintes objetivos da competência: TH.2 com a implementação deste objetivo da competência espera-se que o controlador, em um primeiro momento, identifique as áreas do seu negócio que terão impacto com a aderência da LGPD, levantando a necessidade de capacitação e treinamentos dos operadores para que, desta forma, em um próxima etapa sejam iniciados programas de treinamentos que permitam com que o operador trabalhe em conformidade à LGPD; TH.6 que visa atender e concretizar as necessidades de capacitação que foram identificadas no objetivo da competência TH.2. Por fim, para atendimento das medidas de segurança, foi selecionado da dimensão Cliente e Mercado o objetivo da competência CM.9**,** do qual se espera que incidentes durante o tratamento dos dados para produção de bens e/ou serviços sejam tratados em tempo de não gerar desgastes com o titular dos dados [5]. Outro ponto importante desse objetivo é que os incidentes resolvidos devem ser registrados e análises periódicas devem ser realizadas com a intenção de preveni-los.

4.4.2 Ativo LGPD: Artigo 47. **Dimensão da Competência da MOSE:** Talento Humano. **Objetivo da Competência da MOSE:** TH.1**.** Papéis e responsabilidades dos colaboradores são definidos, comunicados e aprovados. **Grau de Aderência:** Total. **Justificativa:** O objetivo da competência TH.1 atende de forma total o respectivo ativo da LGPD, pois com a implementação deste objetivo espera-se que todos os papéis e as responsabilidades dos colaboradores da controladora estejam definidos, tenham sido comunicados para esses colaboradores e que eles tenham aprovadas as responsabilidades a eles atribuídas. Entende-se como colaborador toda pessoa e/ou agente de tratamento que participou de alguma forma do tratamento de dados.

4.4.3 Ativo LGPD: Artigo 48. **Dimensões da Competência da MOSE:** Cliente e Mercado, e Gestão e Qualidade. **Objetivo da Competência da MOSE:** CM.8. Abordagens de relacionamento com os clientes são estabelecidas e mantidas; CM.9 Incidentes são registrados, analisados e ações preventivas são realizadas; GQ.3. Os bens e/ou serviços gerados são verificados; GQ.7. Controles de qualidade e dos bens e serviços são estabelecidos e mantidos. **Grau de Aderência:** Total. **Justificativa:** os objetivos da competência CM.8, CM.9, GQ.3 e GQ.7 implementados em conjunto atendem ao respectivo ativo da LGPD de maneira total, pois por meio do objetivo CM.8 o controlador tem estabelecido e mantido os canais de relacionamento e comunicação com os clientes e todos as partes interessadas no tratamento de dados. Com o atendimento do objetivo CM.9 o controlador terá condições de comunicar os acontecimentos de incidentes em tempo de não gerar desgastes com o titular dos dados, atendendo o prazo razoável do ativo LGPD. Além disso, o CM.9 prevê o registro e a análise dos incidentes, desta forma, será possível contemplar as informações exigidas na comunicação do incidente. Com o atendimento do objetivo GQ.3, o controlador pode comprovar, por meio dos relatórios de auditoria, que adotou medidas técnicas adequadas no tratamento dos dados. Por fim, o GQ.7 permite que o controlador verifique a qualidade durante a produção do bem e/ou serviço, isto é, realiza a aferição da qualidade do processo em relação aos protocolos definidos, tais como: identificação de itens relevantes, armazenamento desses itens, situação do andamento do item na esteira do processo de produção, restrição de acesso ao item. Da mesma forma, existe a preocupação de gerenciamento de defeitos identificados, indicando que estes devem ser tratados e comunicados, em tempo hábil.

4.4.4 Ativo LGPD: Artigo 49. **Dimensões da Competência da MOSE:** Gestão e Qualidade, e Cliente e Mercado. **Objetivo da Competência da MOSE:** GQ.6. As abordagens para a gestão da unidade de negócio são estabelecidas e mantidas; CM.3. Atendimento aos clientes é realizado; CM.4. O relacionamento com os clientes é realizado. **Grau de Aderência:** Total. **Justificativa:** os objetivos da competência GQ.6, CM.3 e CM.4 implementados em conjunto atendem ao respectivo ativo da LGPD de maneira total, pois por meio do objetivo GQ.6 o controlador deve definir e manter abordagens para a gestão da organização, entre elas estão a aquisição ou a adequação de sistemas que suportem a gestão do negócio e que estejam alinhados e aderentes a LGPD e demais normas regulamentadoras. Com o atendimento do objetivo CM.3 a organização proporcionará o atendimento ao cliente por meio de sistemas de atendimentos que, por sua vez, estarão aderentes a LGPD e que seguirão protocolos para a coleta de dados, o processamento de informações e os canais de atendimento para tratar de dúvidas do titular, além de disponibilização de informação de interesse deste. Por fim, o objetivo CM.4 tem por objetivo manter o relacionamento com o cliente por meio de diversos canais de comunicação, incluindo sistemas online que permitam que o cliente solicite informações, faça reclamações, tire suas dúvidas, entre outras situações na qual o cliente precise entrar em contato com a organização.

4.4.5 Ativo LGPD: Artigo 50. **Dimensões da Competência da MOSE:** Gestão e Qualidade, Cliente e Mercado, Talento Humano e Inovação. **Objetivo da Competência da MOSE:** GQ.1. Estruturas básicas para a gestão das metas de negócio são estabelecidas e mantidas; GQ.2. Abordagens para gestão de equipe são estabelecidas e mantidas; GQ.3. Os bens e/ou serviços gerados são verificados; GQ.4. Melhorias são identificadas e implementadas; GQ.6. Abordagens para a gestão da unidade de negócio são estabelecidas e mantidas; GQ.7. Controles da qualidade e dos bens e serviços são estabelecidos e mantidos; GQ.9. Gerenciar riscos relacionados ao negócio e à gestão e produção de bens e serviços; TH.1. Papéis e responsabilidades dos colaboradores são definidos comunicados e aprovados; TH.6. Programas e/ou ações motivacionais são estabelecidos e mantidos; IN.1. Oportunidades e/ou problemas são identificados e registrados; CM.4. O relacionamento com o cliente é realizado; CM.9. Incidentes são registrados, analisados e ações preventivas são realizadas. **Grau de Aderência:** Total. **Justificativa:** os 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 implementados em conjunto atendem ao respectivo ativo da LGPD de forma total, pois com a implementação do GQ.6 espera-se que o controlador tenha definido abordagens de gestão, considerando aspectos como: estrutura, escala, volume e sensibilidade dos dados tratados. Espera-se também que o controlador estabeleça acordos de nível operacional (entre as equipes) e os níveis de acordos com os clientes. Assim, o controlador compromete-se em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais. Com a implementação do GQ.9 o controlador é

capaz de identificar, avaliar, quantificar e priorizar os riscos relacionados ao tratamento de dados; identificar ações para o contingenciamento e mitigação dos riscos, monitorando-as frente a sua efetividade, e modificá-las caso não estejam surtindo resultados. Desenvolver uma base de conhecimento em relação aos riscos identificados ao longo do tempo e às ações que foram realizadas, com o intuito de amadurecer continuamente a gestão de riscos. Desta forma, é possível definir políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade. Com a implementação do CM.4 o controlador estabelece formas de se relacionar com o titular que visa garantir uma boa imagem da organização com o objetivo de fidelização do titular. Implementando o GQ.3 o controlador garante que o seu serviço e/ou produto cumpram todos os protocolos antes definidos com base na LGPD e que, desta forma, consiga realizar a supervisão do programa de governança em privacidade. Para resposta a incidentes, deve-se implementar o CM.3 para que o controlador tenha os potenciais riscos de incidentes mapeados ao longo do ciclo de vida dos seus produtos e/ou serviços para que, desta forma, consiga gerenciar ações proativas e reativas. Para manter-se sempre atualizado em relação à Lei, o controlador por meio do GQ.4 tem um processo de melhoria contínua implementada, no qual o programa de governança em privacidade seja atualizado continuamente por meio do monitoramento e controle, além de promover práticas de auditorias que consiga identificar problemas e/ou gerar possíveis melhorias no programa. Finalmente, para demonstrar a efetividade dos programas de governança, deve-se implementar o GQ.6 para que o controlador consiga demonstrar o percentual de metas, acordos operacionais cumpridos ou não cumpridos para que, desta forma, demonstre a efetividade de seus programas, entre eles o programa de governança e privacidade.

5 AVALIAÇÃO

O mapeamento, resultado deste trabalho, foi submetido a uma revisão por pares na qual um especialista avaliou o trabalho e propôs ajustes que foram prontamente atendidos. O especialista possui alto nível de conhecimento em normativos como a MOSE e a LGPD. Além disso, possui certificação e tem mais de 5 anos de experiência com a implantação de normativos, como: MOSE, CMMI, MPS.Br, CERTICS, ISO (25000, 9126, 12207, 15504, 9001). Por fim, este especialista já implementou e fez *gap analysis* usando a LGPD em pelo menos 10 empresas da área de TI.

5.1 Objetivos

Os objetivos principais para a realização da avaliação foi: avaliar o mapeamento da Lei Geral de Proteção de Dados com a certificação MOSE Competence; verificar o relacionamento definido entre os ativos constantes entre os dois normativos; analisar o percentual de aderência definido para este relacionamento; e analisar a justificativa do percentual de aderência.

5.2 Metodologia

Por meio de vídeo conferência pelo software Skype, o autor deste trabalho entrevistou o especialista para identificar e avaliar se ele tinha o perfil adequado para a avaliação do trabalho. Após a constatação de que o especialista detinha a experiência necessária para avaliar o trabalho, o próximo passo foi enviar o mapeamento para o especialista avaliar.

Em seguida, o especialista avaliou o mapeamento e sugeriu correções. Essas correções foram apresentadas em uma estrutura de tabela que contém as seguintes colunas com seus respectivos significados: **ID**, identificador único da correção; **Categoria**, caracteriza o tipo da correção, podendo ser TA (Técnico Alto), indicando que foi encontrado um problema em um item que, se não for alterado, comprometerá as considerações, TB (Técnico Baixo), indicando que foi encontrado um problema em um item que seria conveniente alterar, E (Editorial), indicando que foi encontrado um erro de português ou que o texto pode ser melhorado, Q (Questionamento), indicando que houve dúvidas quanto ao conteúdo das considerações, e G (Geral), indicando que o comentário é geral em relação às considerações; **Item**, é o item do mapeamento a ser corrigido; **Comentário com a Justificativa**, é o comentário do especialista sobre o item solicitado para modificação; **Novo Texto Proposto**, é a proposta do especialista para resolução do item; e **Resolução**, é o que o autor fez para resolver o item de correção.

Por fim, o autor teve um período para apresentar a resolução das modificações apontadas pelo especialista, de forma que ficassem explícitas as que foram corrigidas como proposto pelo especialista e as que foram corrigidas de forma diferente do que foi proposto. Cada item de modificação enviado pelo especialista foi analisado individualmente, focando naqueles que tratam diretamente do conteúdo e da estrutura do trabalho, isto é, adição e organização de novas seções e ajustes no próprio conteúdo do mapeamento. Itens relacionados à indicação explícita de modelo de documento para o mapeamento não foi atendido, pois foi escolhido um modelo diferente do indicado por se adequar melhor a proposta do trabalho.

5.3 Planejamento

Para a execução da revisão por pares foi necessário procurar por um especialista com experiência comprovada em implantação da MOSE e/ou outros normativos similares. Após isso, foi criado um documento para ser enviado para esse especialista, contendo o objetivo da revisão por pares, instruções da execução da revisão, identificação do revisor, questionário para traçar o perfil do especialista, definição e descrição da tabela de mapeamento e, finalmente, a tabela a ser preenchida pelo especialista. O próximo passo foi criar um cronograma para realizar a efetiva revisão por pares e a data para cumprimento das proposições de correções. Por fim, ficou definido que a reunião seria realizada de forma remota por meio de uma ligação no software Skype.

5.4 Execução

A execução deu-se conforme o planejado. Encontrou-se o especialista, o documento foi produzido e a reunião ocorreu de maneira satisfatória pela plataforma escolhida. Após isso, foram feitas as devidas correções que culminaram em um mapeamento revisado e avaliado pelo especialista.

5.5 Análises dos Resultados

O mapeamento mostrou-se satisfatório. Em relação à coerência do mapeamento, o especialista aprovou a metodologia e o relacionamento apresentado da MOSE com a LGPD.

As modificações solicitadas pelo especialista, 4 do tipo Técnico Baixo, foram em relação ao conteúdo pré-textual do

mapeamento, ou seja, ele sugeriu que fossem criadas as seções: contexto, objetivos, metodologia e mapeamentos. Na seção contexto, o especialista sugeriu que fosse apresentado em qual contexto o mapeamento estava inserido. Na seção objetivos, ele sugeriu que fosse explicitado o motivo do mapeamento. Na seção metodologia, foi solicitado explicar a metodologia utilizada para chegar no mapeamento. Para finalizar, na seção de mapeamento, o especialista solicitou que fosse explicado o que cada rótulo do mapeamento significava.

Todas as solicitações foram atendidas. Isso resultou em um melhor entendimento sobre o mapeamento e o seu motivo de existir.

6. CONCLUSÕES E TRABALHOS FUTUROS

Este trabalho apresentou um mapeamento de ativos do Capítulo VII da LGPD com a Certificação MOSE Competence. A partir de estudos dos dois normativos, seguidos de apresentações, validação do entendimento com o orientador, construção do mapeamento e avaliação do mapeamento por um especialista, foi possível concluir que existe uma relação entre os normativos e, assim, contribuir para a melhoria do problema apresentado no início deste artigo. O mapeamento também se mostrou útil para que a partir dele seja criado um roteiro contendo atividades, artefatos, ferramentas, indicadores e resultados esperados para o alcance das metas definidas na LGPD.

Espera-se que este trabalho motive a adequação da certificação MOSE para atendimento da LGPD, pois se verificou que isto é possível, uma vez que o resultado deste trabalho foi a percepção de que dos 45 objetivos da competência da MOSE 15 deles (33%), com as devidas adequações, tem aderência total aos 4 artigos (100%) do Capítulo VII da LGPD, ou seja, apenas 15 objetivos de competência constantes na MOSE são necessários para implementar na sua totalidade os itens constantes no Capítulo VII da LGPD.

Por outro lado, os outros 35 (67%) objetivos de competência não possuem alinhamento a partir de seus resultados esperados e práticas para o alcance dos itens constantes na LGPD, uma vez que não focam nas metas definidas para a implementação do Capítulo VII, porém é possível que sejam usadas para implementar os demais Capítulos constantes nesta Lei por haver um alinhamento com as finalidades dos itens constantes nestes demais capítulos.

Para trabalhos futuros tem-se: criar um guia que oriente como implementar os objetivos de competência selecionados da MOSE para contemplar os ativos da LGPD; definir um conjunto de indicadores da certificação para a mensuração da performance da estratégia de implementação da LGPD; e validar esses trabalhos por meio de uma avaliação da estratégia de implementação da MOSE para a LGPD a partir da condução de um estudo de caso participativo ou de uma prova de conceito.

AGRADECIMENTOS

Os autores querem agradecer ao MOSE Institute pelos treinamentos oficiais fornecidos de maneira gratuita ao autor-pesquisador deste trabalho, bem como ao especialista participante da revisão por pares pelos *feedbacks* relevantes que nortearam a fase de avaliação do mapeamento aqui apresentado.

REFERÊNCIAS

[1] Presidência da República do Brasil. 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Retrieved from http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Accessed: 07/09/2020.

[2] Agência Brasil. 2020. *Entra em vigor Lei de Proteção de Dados*. Retrieved from https://agenciabrasil.ebc.com.br/geral/noticia/2020-09/entenda-o-que-muda-com-a-lei-geral-de-protecao-de-dados. Accessed: 07/09/2020.

[3] Akami. 2020. *Segurança, entrega na nuvem, desempenho*. Retrieved from https://www.akami.com. Accessed: 07/09/2020.

[4] MOSE Competence Institute, 2020. *Sobre a Certificação MOSE Competence*. Retrieved from https://www.mosecompetence.org/sobre. Accessed: 07/09/2020.

[5] Ana Cristina Rouiller. 2017. *MOSE: base de competências (2nd. ed.)*. Editora Pé Livre Ltda, Recife, Pernambuco.

[6] Isabel Maria Lopes, Teresa Guarda and Pedro Oliveira. 2019. How ISO 27001 Can Help Achieve GDPR Compliance. In *14th Iberian Conference on Information Systems and Technologies (CISTI)*, Coimbra, Portugal, 2019, pp. 1-6, doi: 10.23919/CISTI.2019.8760937.

[7] Nguyen Binh Truong, Kai Sun, Gyu Myoung Lee and Yike Guo. 2019. GDPR-Compliant Personal Data Management: A Blockchain-Based Solution. In *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1746-1761, doi: 10.1109/TIFS.2019.2948287.