Aprimoramento de Requisitos de Software da Área Financeira com Relação a Aspectos de Privacidade e Segurança: uma abordagem baseada na semiótica organizacional

Leonardo Manoel Mendes

15/04/2021

Dissertação de Mestrado em Ciência da Computação

Aprimoramento de Requisitos de Software da Área Financeira com Relação a Aspectos de Privacidade e Segurança: uma abordagem baseada na semiótica organizacional

Esse documento corresponde à dissertação apresentada à Banca Examinadora no curso de Mestrado em Ciência da Computação da UNIFACCAMP – Centro Universitário Campo Limpo Paulista.

Campo Limpo Paulista, 15 de abril de 2021.

Leonardo Manoel Mendes

Orientador: Prof. Dr. Rodrigo Bonacin

Coorientador: Prof. Dr. Ferrucio de Franco Rosa

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

Ficha catalográfica elaborada pela

Biblioteca Central da Unifaccamp

M491a

Mendes, Leonardo Manoel

Aprimoramento de requisitos de software da área financeira com relação a aspectos de privacidade e segurança: uma abordagem baseada na semiótica organizacional / Leonardo Manoel Mendes. Campo Limpo Paulista, SP: Unifaccamp, 2021.

Orientador: Prof°. Dr. Rodrigo Bonacin

Coorientador: Profº. Dr. Ferrucio de Franco Rosa

Dissertação (Programa de Mestrado Profissional em Ciência da Computação) – Centro Universitário Campo Limpo Paulista – Unifaccamp.

1. Engenharia de requisitos. 2. Sistemas de *software* financeiro. 3. Semiótica. 4. Privacidade de dados. 5. Segurança da informação. I. Bonacin, Rodrigo. II. Rosa, Ferrucio de Franco. III. Centro Universitário Campo Limpo Paulista. IV. Título.

CDD-005.43

Dedico este trabalho a minha querida mãe Josefa Olindina dos Santos e ao meu pai Manoel Mendes de Brito (*in memorian*) e a todos aqueles que estiveram comigo ao longo desta jornada, sempre me apoiando nos momentos difíceis assim como nos momentos de alegrias em cada uma das conquistas obtidas nesta jornada.

AGRADECIMENTOS

A Deus que esteve comigo em todas as fases deste programa de mestrado, concedendo todos os recursos que necessitei para que eu pudesse chegar até aqui. Aos meus queridos pais, Manoel Mendes de Brito (*in memorian*) e Josefa Olindina dos Santos, e aos meus irmãos e irmãs.

Ao meu orientador Dr. Rodrigo Bonacin e a meu coorientador Prof. Dr. Ferrucio de Franco Rosa, pelos conhecimentos, ensinamentos compartilhados durante todo o processo de construção do projeto do mestrado, sempre me apoiando nos momentos de incertezas e inseguranças que foram surgindo ao longo dessa caminhada. Grande parte dos créditos desta pesquisa devem ser atribuídos para ambos os Orientadores.

A todos os professores do Programa de Mestrado em Ciência da Computação da UNIFACCAMP.

Resumo

Com novas ameaças aos sistemas de informação, bem como a nova legislação sobre privacidade, se faz cada vez mais necessário desenvolver sistemas com elementos chaves para prover privacidade e segurança. Aprimorar requisitos da área financeira com relação a aspectos de segurança e privacidade requer dos profissionais conhecimento em técnicas de elicitação de requisitos, assim como em processos e métodos adequados. Para tanto, além dos conceitos e técnicas de engenharia de requisitos, são necessárias técnicas para análise multidimensional do problema, abrangendo aspectos informais, formais e técnicos, tais como as técnicas propostas pela Semiótica Organizacional. Ademais, múltiplas fontes de conhecimento e normas devem ser analisadas, tais como a Lei Geral de Proteção de Dados Pessoais, as normativas do BACEN e PCI DSS para as plataformas de *Internet Banking* e *Mobile Banking* das organizações financeiras. Diante dessas necessidades, esta dissertação apresenta o Método de Análise de Requisitos de Software para Privacidade e Segurança (MARSPS), que é baseado em conceitos e técnicas da Semiótica Organizacional e na análise de fontes de conhecimento e normas sobre segurança e privacidade. O MARSPS é composto de sete passos e demanda um conjunto inicial de requisitos de software da área financeira. O objetivo principal é sistematicamente analisar o conjunto inicial e propor requisitos enriquecidos com aspectos de segurança e privacidade. Neste trabalho, também é apresentado um estudo de caso para validar a proposta, onde MARSPS é instanciado em cenários onde faz-se necessário o enriquecimento de requisitos de um sistema da área financeira.

Palavras-chave: Engenharia de Requisitos, Sistemas de Software Financeiro, Semiótica Organizacional, Privacidade de Dados, Segurança da Informação.

Abstract

With new information systems threats, as well as new privacy legislation, it is increasingly necessary to develop systems with key elements to provide privacy and security. Enriching software requirements with key security and privacy aspects requires professionals to have knowledge of requirements elicitation techniques, based on systematic processes and methods. Therefore, in addition to the requirements engineering concepts and techniques, new techniques are needed for multidimensional analysis of the problem, covering informal, formal and technical aspects, such as those proposed by Organizational Semiotics. In addition, multiple sources of knowledge and standards must be analyzed, such as the General Law for the Protection of Personal Data, the BACEN and PCI DSS regulations for the Internet Banking and Mobile Banking platforms of financial organizations. In view of these needs, this dissertation presents the Software Requirements Analysis Method for Improvement of Privacy and Security (SRAM-PS), which is based on concepts and techniques of Organizational Semiotics as well as on the analysis of sources of knowledge and regulation on security and privacy. SRAM-PS is composed of seven steps and demands an initial set of financial software requirements. Its main objective is to systematically analyze an initial set of requirements and propose enriched ones, by considering aspects of security and privacy. This work also presents a case study to validate the proposal, where SRAM-PS is instantiated in scenarios where it is necessary to enrich the requirements of a financial software system.

Keywords*: Requirements Engineering, Financial Software Systems, Organizational Semiotics, Data Privacy, Information Security.*

Sumário

1. Introdução 1

1.1. Contexto e Motivação 2

1.2. Problemática e Justificativa 3

1.3. Objetivos, Contribuições e Métodos 4

1.4. Estrutura da Dissertação 6

2. Referencial Teórico e Metodológico 8

2.1. Conceitos de Privacidade, Segurança da Informação e Confiabilidade ... 8

2.2. Legislação para Tratamento de Dados Pessoais 11

2.3. Fontes de conhecimento de segurança para especificação e validação de requisitos de software da área financeira 12

2.4. Processos de Desenvolvimento de Software Seguro 16

2.4.1 Conceitos e processos de engenharia de requisitos 17

2.4.2 Técnicas de elicitação de requisitos 18

2.5. Semiótica Organizacional 20

2.5.1. Conceitos da Semiótica Organizacional 21

2.5.2. Métodos para Elicitação, Análise e Especificação de Requisitos de Usuário da Semiótica Organizacional. 22

3. Trabalhos Relacionados 27

3.1. Protocolo de Revisão 27

3.2. Resultados da Revisão sobre Trabalhos Relacionados 29

3.3. Discussão Sobre Trabalhos Relacionados 33

4. Elaboração e detalhamento do método MARSPS 35

4.1. Metodologia utilizada para concepção e validação do método 35

4.2. Descrição do Método MARSPS 37

4.2.1 Objetivos e Premissas do MARSPS 37

4.2.2 O Método MARSPS 38

5. Aplicação Preliminar do MARSPS 48

5.1. Execução do MARSPS para enriquecer requisitos de sistemas da área financeira 48

5.1.1. Execução do Passo 1: identificar fontes de requisitos de segurança e privacidade 48

5.1.2. Execução do Passo 2: identificar *stakeholders* 49

5.1.3. Execução do Passo 3: analisar *stakeholders* 49

5.1.4. Execução do Passo 4: listar interesses dos *stakeholders* 51

5.1.5. Execução do Passo 5: analisar problemas e ideias 51

5.1.6. Execução do passo 6: avaliar requisitos 54

5.1.7. Execução do passo 07: gerar artefatos de requisitos de segurança e privacidade de software 56

5.2. Considerações sobre a execução preliminar do MARSPS 57

6. Aplicação do MARSPS em Estudo de Caso com Especialistas 59

6.1. Objetivos, perfil dos participantes e método de avaliação 59

6.2. Resultados da Execução do MARSPS 61

6.2.1. Passo1: Identificar Fontes de Requisitos 61

6.2.2. Passo 2: Identificar *Stakeholders* 62

6.2.3. Passo 3: Analisar *Stakeholders* 63

6.2.4. Passo 4: Listar Interesses dos *Stakeholders* 63

6.2.5. Passo 5: Analisar Problemas e Soluções 64

6.2.6. Passo 6: Avaliar Requisitos 64

6.2.7. Passo 7: Gerar Artefato de Requisitos de Segurança e Privacidade de Software 65

6.3. Resultados do Formulário de Avaliação 66

6.4. Discussão sobre os Resultados Obtidos 72

7. Conclusão 73

7.1. Contribuições 73

7.2. Limitações e Trabalhos Futuros 75

7.3. Considerações Finais 76

8. Referências 77

APÊNDICE A – Lista de artefatos da execução do MARSPS para aprimoramento de requisitos de privacidade e segurança. 83

APÊNDICE B - Detalhamento do quadro de avaliação após o aprimoramento dos requisitos 84

APÊNDICE C – Questionário da validação do MARSPS pelos especialistas. ... 94

Lista de Tabelas

TABELA 1 – EXEMPLO DE QUADRO DE AVALIAÇÃO 25
TABELA 2- PARÂMETRO PARA REALIZAÇÃO DA REVISÃO 28
TABELA 3 - STRING DE BUSCA 29
TABELA 4 - CRITÉRIOS DE INCLUSÃO E EXCLUSÃO 29
TABELA 5 - ARTIGOS SELECIONADOS POR ETAPA 30
TABELA 6 - TRABALHOS SELECIONADOS NA REVISÃO 31
TABELA 7 - TRABALHOS RELACIONADOS 34
TABELA 8 - PERFIL PROFISSIONAL DOS PARTICIPANTES DO ESTUDO DE CASO 60
TABELA 9 - SÍNTESE DAS FONTES SUGERIDOS PELOS PARTICIPANTES NO PASSO 1 62
TABELA 10 - SÍNTESE DAS REPOSTAS DISSERTATIVAS DO FORMULÁRIO DE VALIDAÇÃO DO MARSPS 69
TABELA 11 - AVALIAÇÃO DOS STAKEHOLDERS A NÍVEL DE COMUNIDADE 84
TABELA 12 - AVALIAÇÃO DOS STAKEHOLDERS A NÍVEL DE MERCADO 85
TABELA 13 - AVALIAÇÃO DOS STAKEHOLDERS A NÍVEL DE FONTE 88
TABELA 14 - AVALIAÇÃO DOS STAKEHOLDERS A NÍVEL DE CONTRIBUIÇÃO 89
TABELA 15 - AVALIAÇÃO DOS STAKEHOLDERS A NÍVEL DE OPERAÇÃO 93

Lista de Figuras

FIGURA 1 - ESQUEMA DE RELAÇÃO ENTRE OS SISTEMAS EM UMA ORGANIZAÇÃO 22
FIGURA 2 - PARTES INTERESSADAS NO PROCESSO DE DESENVOLVIMENTO DE SISTEMAS DE SOFTWARE 24
FIGURA 3 - FRAMEWORK SEMIÓTICO 26
FIGURA 4- FASES E ATIVIDADES DO PROCESSO DE REVISÃO 27
FIGURA 5 - MÉTODO TRIANGULAÇÃO 36
FIGURA 6 - PROCESSO PARA EXECUÇÃO DO MÉTODO MARSPS 39
FIGURA 7 - IDENTIFICAÇÃO DE FONTES DE REQUISITOS DE SEGURANÇA E PRIVACIDADE. 40
FIGURA 8 - ANÁLISE DE STAKEHOLDERS 41
FIGURA 9 - CONSTRUÇÃO DO QUADRO DE AVALIAÇÃO 44
FIGURA 10 - CONSTRUÇÃO DA ESCADA SEMIÓTICA 46
FIGURA 11 - GERAÇÃO DE ARTEFATOS COM REQUISITOS DE SEGURANÇA E PRIVACIDADE DE SOFTWARE 47
FIGURA 12 - DIAGRAMA DE STAKEHOLDERS CONSTRUÍDO PARA APLICAÇÃO PRELIMINAR 50
FIGURA 13 - ESCADA SEMIÓTICA PARA O REQUISITO 1 55
FIGURA 14 – RESULTADOS DAS QUESTÕES DE MÚLTIPLA ESCOLHA SOBRE A PARTICIPAÇÃO DOS STAKEHOLDERS NO MARSPS 66
FIGURA 15 – RESULTADO DE QUESTÃO DE MÚLTIPLA ESCOLHA SOBRE A CONTRIBUIÇÃO DO QUADRO DE AVALIÇÃO. 67
FIGURA 16 – RESULTADOS DE QUESTÕES DE MÚLTIPLA ESCOLHA SOBRE A ESCADA SEMIÓTICA 67
FIGURA 17 – RESULTADO DE QUESTÃO DE MÚLTIPLA ESCOLHA SOBRE AS SAÍDAS DO MARSPS. 68
FIGURA 18 – RESULTADOS SOBRE QUESTÕES GERAIS DE MÚLTIPLA ESCOLHA SOBRE O MARSPS. 68

Glossário

Adquirente – Bancos comerciais e Processadoras de pagamentos.

Aplicativo – Programa de software (ou grupo de programas).

Autenticação – Método ou processo usado para acessar a aplicação por meio de um computador ou dispositivo móvel.

BACEN – Banco Central do Brasil.

COSIF – Plano Contábil das Instituições do Sistema Financeiro Nacional.

CVE – *Common Vulnerabilities and Exposures.*

DNS – *Domain Name Server.*

ER – Engenharia de Requisitos.

EU – União Europeia.

EUA – Estados Unidos da América.

Firewall – Hardware e/ou Software utilizado para proteger os recursos da rede de acesso não autorizado.

ID – Identificação.

LGPDP – Lei Geral de Proteção de Dados Pessoais.

OSVDB – *Open Source Vulnerability Database.*

OWASP – *Open Web Application Security Project.*

PCI – *Payment Card Industry.*

PCI DSS – *PCI Data Security Standard.*

RNF – Requisitos não Funcionais.

SO – Semiótica Organizacional.

Violação de Dados – Evento relacionado a apropriação indevida de dados de terceiros.

Vulnerabilidade – Fraqueza (ou falha) identificada em uma aplicação.

RSFN – Rede do Sistema Financeiro Nacional.

NVD – *National Vulnerability Database.*

1. Introdução

A privacidade é uma característica importante para vários *stakeholders* em projetos de desenvolvimento de sistemas de software. A necessidade por privacidade e segurança é eminente, no entanto, existem problemas na análise e especificação de diferentes dimensões e visões dos usuários e das organizações.

Para que elicitação e especificação de requisitos possam ser efetivas, o profissional da engenharia de requisitos deverá obter um entendimento do domínio da aplicação (*e.g.*, aplicações da área financeira), de modo que os requisitos legais relacionados a privacidade e segurança possam ser identificados. Tais requisitos podem estar presentes em diferentes fontes de informações, tais como leis de proteção de dados (*e.g.*, Lei 13709 – LGPDP - Lei Geral de Proteção de Dados Pessoais) (Brasil, 2018), decretos, emendas constitucionais, políticas internas de segurança de dados da organização, dentre outras fontes. Atualmente, existem diferentes alternativas para elicitar e especificar requisitos (*e.g.*, entrevistas com *stakeholders*, análise documental, prototipagem etc.), no entanto, elas ainda não são capazes de lidar por completo com tarefas de tal complexidade.

Neste trabalho adota-se uma abordagem baseada na Semiótica Organizacional (SO) (Liu, 2000; Liu & Li, 2014) que explora aspectos formais, informais e técnicos no entendimento e especificação de requisitos. Para tanto, é proposto um método de enriquecimento de requisitos de software financeiro com relação a aspectos de privacidade e segurança, visando que os requisitos não sejam negligenciados durante o ciclo de vida de desenvolvimento de software. Considera-se enriquecimento de requisitos o processo de avaliar e especificar adequadamente características relacionadas a privacidade e segurança da informação nos artefatos existentes ou gerados durante a engenharia de requisitos. Espera-se, nesse processo, que a SO proporcione um melhor entendimento do contexto no qual está inserido o software a ser elicitado, uma vez que a SO tem como base uma visão sociotécnica do processo de elicitação de requisitos de software (Baranauskas & Bonacin, 2008).

Neste contexto, esta dissertação tem por finalidade apresentar e avaliar o Método de Análise de Requisitos de Software para Privacidade e Segurança (MARSPS). MARSPS

é um método baseado em uma abordagem sistemática de sete passos para análise e especificação de requisitos de sistemas de software financeiro, que faz uso de técnicas oriundas da Semiótica Organizacional combinadas a fontes de requisitos de segurança e privacidade.

A Seção 1.1 apresenta o contexto e a motivação que levaram ao desenvolvimento desta dissertação. A Seção 1.2 detalha a problemática abordada neste trabalho e a justificativa para seu desenvolvimento. A Seção 1.3 apresenta o objetivo geral, objetivos específicos e a hipótese que norteiam o desenvolvimento deste trabalho, bem como uma visão geral dos métodos empregados. Ainda nesta seção, são apresentadas as contribuições científicas esperadas. Por fim, a Seção 1.4 apresenta a estrutura da dissertação contendo a descrição sucinta de cada capítulo.

1.1. Contexto e Motivação

Nos últimos anos, a tecnologia da informação ganhou importância no ambiente social e corporativo para auxiliar na tomada de decisão em diferentes situações nas organizações (Medeiros, 2019). A informação possui um valor significativo para organizações e partes interessadas (*stakeholders*), especialmente em instituições do sistema financeiro. Como a informação está armazenada em diferentes sistemas em uma organização, alguns usuários poderão não conhecer de fato o valor que a mesma possui e, com isso, em algumas situações chegam a compartilhar informações sensíveis sem nenhuma preocupação em ambiente *online* (*e.g.*, em redes sociais). Como em qualquer outra área de conhecimento, a tecnologia da informação carece de novos conceitos, práticas e vivências profissionais. À medida que o mercado cresce, surgem novas demandas e necessidades de utilização de sistemas computacionais para auxiliar os *stakeholders* no desenvolvimento das suas atividades cotidianas nas organizações. Essa evolução demanda sistemas mais robustos e confiáveis.

A privacidade de dados em ambiente *Web* é um tema sensível, uma vez que existe uma infinidade de aplicativos *online* que liberam acesso para seus usuários. No entanto, tais usuários não tem o conhecimento da forma como seus dados são armazenados e utilizados. A todo momento se faz necessária a realização de cadastros, onde os usuários fornecem um conjunto de informações que podem ser sensíveis ou de cunho pessoal. Isso

é ainda mais crítico em sistemas que lidam com dados sensíveis, tais como sistemas que lidam com dados de saúde e de finanças.

Um elemento de grande importância no desenvolvimento de software é a elicitação de requisitos (Sommerville, 2011, 2016). Ela é uma atividade essencial dentro da engenharia de requisitos, pois permite identificar as necessidades dos *stakeholders*, incluindo os requisitos não funcionais, tais como requisitos de privacidade e segurança.

Atualmente, para a elicitação de requisitos de sistemas de software financeiro, de modo que considere aspectos de privacidade, se faz necessário conhecer a Lei Geral de Proteção de Dados Pessoais (LGPDP), que segue basicamente os mesmos princípios da agência de direitos fundamentais da União Europeia (União Eutropéia, 2010). Isso é importante devido à grande quantidade de dados pessoais dos usuários disponíveis em aplicações. Isso evidencia a necessidade eminente de criar mecanismos de proteção de dados cada vez mais eficazes e, com isso, surge na necessidade de propor novos métodos de elicitação de requisitos, tais como o MARSPS.

1.2. Problemática e Justificativa

A dificuldade na identificação de necessidades de privacidade e segurança das informações muitas vezes se dá pela da falta de conhecimento ou experiência do profissional responsável pela atividade da elicitação de requisitos dos sistemas de software financeiro. Isso leva à necessidade de métodos e processos que possam apoiar os especialistas em privacidade e segurança em suas atividades na organização.

Com base na análise da literatura, por meio de consultas em diferentes bases de dados (*cf.*, Capítulo 3), foi possível identificar que existem diferentes técnicas para elicitação de requisitos. No entanto, percebe-se que existem lacunas em aberto no âmbito de técnicas que envolvem aspectos de privacidade e segurança das informações. Ou seja, são requisitos legais, organizacionais, sociais e subjetivos que devem constar em sistemas que prezam pela legalidade das informações, assim como a confiabilidade nos dados que são armazenados em diferentes sistemas computacionais. Especificamente, foram identificados trabalhos usando a semiótica no contexto organizacional para facilitar a comunicação entre os *stakeholders*, assim como trabalhos que propõem conjuntos de requisitos de segurança relacionados à privacidade (ou à confidencialidade). Porém, não

foram identificadas abordagens sistemáticas baseadas em semiótica voltadas a elicitar e especificar requisitos de sistemas de software financeiro considerando aspectos de privacidade e segurança da informação.

Baseado nesta problemática destaca-se a necessidade de criar novos métodos que visam sanar possíveis lacunas existentes nas abordagens atuais comumente utilizadas na elicitação e especificação de requisitos, em especial dos sistemas de software financeiro. Com isso, surge a proposta do MARSPS, que tem como base a SO, trazendo uma visão sociotécnica ao processo de elicitação desses requisitos. A elaboração do MARSPS foi um desafio multidisciplinar de pesquisa por envolver engenharia de requisitos, SO, privacidade de dados e segurança da informação. A junção dos conceitos e práticas das áreas resultou em um método voltado a mitigar lacunas importantes do processo de elicitação de requisitos, tais como falhas no mapeamento e na comunicação de *stakeholders*, falta de entendimento do domínio de aplicação (finanças) e falta de conhecimento das políticas de segurança da informação existentes na organização, de normas reguladoras do sistema financeiro e de leis proteção de dados pessoais. Estes problemas são abordados na concepção e na aplicação do MARSPS.

1.3. Objetivos, Contribuições e Métodos

A seguinte questão de pesquisa norteia este trabalho: *Como a Semiótica Organizacional poderá contribuir para a criação de um método para enriquecimento de requisitos de sistemas de software financeiro que considere aspectos de privacidade e segurança da informação?*

Portanto, o objetivo geral é propor um método para enriquecimento de requisitos de sistemas financeiros que considere aspectos de privacidade e segurança da informação, com base em conceitos e práticas da SO, a ser aplicado por engenheiros de segurança da informação e engenheiros de requisitos. Para tanto, se faz necessário deixar claro aos profissionais e organizações os passos a serem seguidos na execução do método, de modo a atender às reais necessidades de elicitação ou aprimoramento de requisitos.

Esta dissertação tem como foco principal atender às necessidades de instituições e usuários da área financeira, ao considerar suas especificidades e focar o estudo de caso nesta área. Embora, o método possa ser adaptado para outros domínios, está fora de o

escopo desta dissertação lidar com aspectos específicos de outros domínios, bem como requisitos não ligados a privacidade e segurança.

Para alcançar esse objetivo geral, faz-se necessário atingir objetivos específicos, detalhados a seguir:

1. Analisar e selecionar conceitos e técnicas de elicitação de requisitos e de SO que podem ser empregados para enriquecer requisitos de sistemas de software financeiro;
2. Mapear e analisar fontes de conhecimento sobre privacidade e segurança aplicáveis à área financeira, de modo a compreender o problema em questão e identificar possíveis itens de avaliação;
3. Propor a articulação de conceitos e técnicas de engenharia de requisitos, SO, privacidade de dados e segurança da informação para compor a abordagem;
4. Exercitar o método proposto em cenários da área financeira, de modo a avaliar seus pontos fortes e fracos, bem como apontar desafios de pesquisa futuros;
5. Validar o método proposto com especialistas do domínio financeiro; mais especificamente, com profissionais especialistas em engenharia de requisitos, privacidade de dados e segurança da informação que atuam no desenvolvimento de sistemas para a área financeira (*e.g.*, *Internet Banking* e Sistemas de Pagamentos).

A hipótese de pesquisa é que um método baseado em SO, técnicas de análise de requisitos e fontes de conhecimento em segurança e privacidade pode auxiliar no enriquecimento de requisitos de sistemas de software financeiro, de modo a considerar adequadamente aspectos críticos de privacidade de dados e segurança da informação. Para tanto, o método deverá proporcionar aos responsáveis pela elicitação e especificação, um conjunto de passos com informações relevantes ao exercício de cada atividade a ser realizada. Busca-se aprimorar o processo de elicitação de requisitos de software da área financeira para que engenheiros de requisitos e de segurança possam especificar novas necessidades. Espera-se que um método baseado em SO propicie uma visão sociotécnica do problema, contemplando diferentes perspectivas e necessidades dos *stakeholders*. Portanto, a proposta fará uso de etapas consolidadas na prática da elicitação e especificação de requisitos, adicionando a SO no processo com o objetivo de prover

melhor entendimento dos requisitos e melhor comunicação entre *stakeholders*. Um problema-chave a ser abordado é como destacar a real importância das características de privacidade e segurança para os principais *stakeholders* envolvidos no processo.

A principal contribuição da dissertação é um método baseado em conceitos e técnicas da SO para enriquecimento de requisitos de sistemas de software financeiro que considera aspectos de privacidade e segurança da informação, além de seu processo sistematizado de implementação. Como outras contribuições podem ser citadas: (1) identificação de lacunas existentes no processo de elicitação e especificação de requisitos de software financeiro, especialmente quanto a características de privacidade e segurança; (2) mapeamento de fontes de conhecimento sobre privacidade e segurança aplicáveis à área financeira, identificando possíveis itens de avaliação; (3) análise de conceitos e técnicas de elicitação de requisitos e de SO que podem ser empregados para enriquecer requisitos de software em outros domínios críticos em segurança e privacidade (*e.g.*, Saúde); e (4) como a proposta é validada por profissionais que estão diretamente ligados à prática da engenharia de requisitos de sistemas de software financeiro, os resultados desta avaliação poderão levar a novas demandas por aprimoramento no processo de desenvolvimento de sistemas críticos em outros domínios.

1.4. Estrutura da Dissertação

O restante da dissertação está organizado da seguinte maneira:

- No **Capítulo 2**, apresenta-se o referencial teórico e metodológico, incluindo elementos e conceitos que representam a segurança e a privacidade em ambiente computacional. Conceitos de engenharia de requisitos são descritos, em especial os requisitos não-funcionais e de privacidade, além de conceitos e técnicas da SO, com foco nos adotados pelo método proposto.
- No **Capítulo 3**, apresenta-se a revisão da literatura, envolvendo as três áreas abordadas na proposta, a saber: engenharia de requisitos, privacidade de dados e SO.
- No **Capítulo 4**, primeiramente apresenta-se a metodologia de pesquisa utilizada para concepção e validação do método. Em seguida, o MARSPS é apresentado e detalhado incluindo sua fundamentação, processo e atividades

do processo para utilização na elicitação de requisitos de sistemas de software financeiro.

- No **Capítulo 5**, são apresentados os resultados da execução do MARSPS em um projeto piloto, com cenários que incluem requisitos reais de sistemas de software da área financeira. Neste capítulo apresenta-se como foi realizada a execução do método em cada uma das atividades, incluindo subprocessos que compõem o método.
- No **Capítulo 6**, são apresentados os resultados da validação do MARSPS em conjunto com especialistas que atuam diretamente no domínio financeiro.
- No **Capítulo 7**, são apresentadas as considerações finais, incluindo contribuições, limitações e trabalhos futuros.
- No **Apêndice A**, apresenta-se a lista de artefatos gerados na execução do MARSPS nos cenários de aprimoramento de requisitos de um projeto piloto de sistema de software da área financeira.
- No **Apêndice B**, apresenta-se o detalhamento do quadro de avaliação durante o aprimoramento dos requisitos.
- No **Apêndice C**, apresenta-se o Questionário da validação do MARSPS pelos especialistas.

2. Referencial Teórico e Metodológico

Este capítulo tem por finalidade descrever a abordagem teórica e metodológica que fundamenta esta proposta. Os conceitos fundamentais englobam SO, engenharia de requisitos de software, além de privacidade e segurança em sistemas computacionais. A Seção 2.1 apresenta uma síntese de conceitos essenciais de privacidade, segurança da informação e confiabilidade. Na Seção 2.2 apresenta-se uma síntese da legislação para proteção de dados pessoais. Na Seção 2.3 são apresentadas as principais fontes de conhecimento de segurança da informação que podem ser usadas durante o processo de especificação e validação de requisitos de software da área financeira. A Seção 2.4 apresenta uma introdução sobre processos de desenvolvimento de software seguro, destacando conceitos e processos principais de engenharia de requisitos, além de técnicas de elicitação de requisitos. A Seção 2.5 descreve os conceitos e fundamentos da semiótica, assim como detalha as técnicas empregadas no método proposto nesta dissertação.

2.1. Conceitos de Privacidade, Segurança da Informação e Confiabilidade

O conceito de informação é fundamental para o entendimento de questões relacionadas à privacidade e segurança de informação. Informação é a "reunião dos conhecimentos, dos dados sobre um assunto ou pessoa" (Ferreira, 2015). Diferentes classes de informação são apresentadas por Côrte (2014), a saber:

- **Informação lixo:** esse tipo de informação é muito comum em diferentes ambientes da organização, podendo ser descartada a qualquer momento por não agregar valor.
- **Informação potencial:** são informações com potencial de gerar vantagem competitiva no mercado em que a empresa está inserida. Estes ganhos ocorrem por meio da utilização de sistemas de informação, que auxiliam no processo de apoio a tomada de decisões na organização.
- **Informação mínima***:* são informações essenciais, utilizadas pela gestão da organização em suas ações e tomadas de decisões.
- **Informação crítica:** este tipo de informações é de grande importância para que a empresa possa se manter em um nicho de mercado. São informações de cunho confidencial, ou seja, de grande valor estratégico e financeiro que faz

com que a empresa possa continuar exercendo suas funções e disponibilizando seus produtos e serviços para seus clientes.

A privacidade em sistemas computacionais vem se tornando cada dia mais importante para as empresas e para usuários de sistemas online. A privacidade de dados pode apresentar problemas decorrentes de diferentes aspectos, desde os aspectos técnicos, como a não criptografia dos dados e informações dos usuários, até aspectos humanos, como descuidos dos operadores do sistema. No entanto, devido à complexidade existente nas aplicações, a privacidade de dados pessoais dos usuários geralmente não é abordada corretamente. Isso comumente não está relacionado com escolhas do próprio usuário, mas com problemas e lacunas existentes nos sistemas computacionais, que são especificados por diferentes *stakeholders* oriundos de diferentes níveis e com diferentes visões.

De acordo com Kuhn *et al.* (2017), a proteção de dados é um dos atributos que mais preservam a segurança de qualquer aplicativo móvel, especialmente para aplicativos financeiros, de assistência médica e de negócios. Segundo French *et al.* (2010), a confiabilidade se refere à confiança no ambiente eletrônico e é muito importante para as pessoas em ambientes colaborativos. Os autores exploram o conceito de "*e-trust*" ("*e*-confiança"). De acordo com Alhalafi (2015), ao prover privacidade deve-se incorporar a expectativa de privacidade do usuário do sistema de maneira interativa. O autor destaca a importância da privacidade em geral e incorpora no contexto a importância do envolvimento dos *stakeholders* no desenvolvimento.

A inclusão da preocupação com a privacidade no processo de desenvolvimento de sistemas envolve revisar as políticas adotadas pela organização para que não ocorram ambiguidades. Para Alhalafi (2015), a desambiguação no processo de desenvolvimento desempenha um papel muito importante na transformação da política de privacidade na organização. O autor também cita a transformação positiva decorrente da privacidade "estática" para a "interativa ou dinâmica". Assim, durante o processo de desenvolvimento de sistemas os desenvolvedores devem se atentar às expectativas de privacidade dos diversos perfis de *stakeholders*.

A cultura e a comunicação organizacional são de grande importância na condução do processo de engenharia de requisitos, de modo a levar em consideração aspectos relacionados à privacidade. Nem sempre a comunicação flui entre *stakeholders*

com a mesma clareza e objetividade. Rambo & Liu (2016) afirmam que é muito importante analisar o impacto cultural da inovação nos *stakeholders* envolvidos no processo para desenvolvimento de uma solução sistêmica que atenda às demandas da organização.

Com respeito à segurança das informações, podem-se identificar três pilares de grande importância para as organizações, a saber: confiabilidade, integridade e disponibilidade (Guaman et al., 2017).

A confidencialidade de uma informação está relacionada com a privacidade dos dados e informações das empresas e organizações. O objetivo é assegurar que os dados não sejam acessados por indivíduos não autorizados na organização (Nascimento, 2017).

A disponibilidade está relacionada ao tempo e à acessibilidade que se tem dos dados e sistemas da empresa, ou seja, se dados podem ser consultados a qualquer momento pelos colaboradores (Nascimento, 2017). A disponibilidade de uma informação diz respeito ao seu acesso quando necessário para consulta por usuários que possuam permissões, para que possam fazer uso dos dados e informações.

A integridade corresponde à salvaguarda da exatidão e completeza de ativos, ISO/IEC 27001 (ABNT, 2012). A integridade está relacionada ao armazenamento dos dados, ou seja, a precisão, a consistência e a confiabilidade dos dados e informações presentes no sistema.

Faz-se necessário enfatizar a importância das políticas de segurança de informação adotadas pelas organizações, buscando a mitigação de riscos. A ABNT NBR ISO/IEC 27002:2013 (ABNT, 2013), apresenta controles que visam a assegurar que a eficácia da segurança seja adequada em resposta às demandas solicitadas. Nesta norma, também é possível identificar, no contexto da segurança da informação, controles para assegurar as regras e normativas de segurança, que podem ser aplicadas a diferentes tipos de projetos que fazem uso de dados sensíveis.

Vulnerabilidades (fraquezas nos sistemas) podem ocorrer independentemente do tipo aplicação, *e.g.*, software *Web*, aplicativos móveis, etc. Aplicações financeiras devem possuir controles rígidos de acesso, de modo a restringir eventual exploração de vulnerabilidades e consequente acesso indevido a informações críticas. De maneira geral, busca-se garantir uma política de controle eficaz, com criptografia dos dados trafegados

pela rede, além de atuação na detecção, prevenção, recuperação e proteção de ataques. Outro ponto de grande importância, é que as vulnerabilidades técnicas conhecidas (e divulgadas) dos sistemas em operação devem ser identificadas e tratadas em tempo hábil, para que possam ser mitigados problemas com dados e informações dos *stakeholders* e da organização.

2.2. Legislação para Tratamento de Dados Pessoais

Esta seção tem por finalidade apresentar uma síntese da legislação para tratamento de dados pessoais.

De acordo com Miranda (2018), o direito à informação e o direito à privacidade de dados são reconhecidos como direitos fundamentais da pessoa, premissa confirmada pela literatura jurídica internacional. Tais direitos, depois de reconhecidos, passaram a sofrer mudanças decorrentes de evoluções sociais, políticas, econômicas e tecnológicas, sendo materializados em textos normativos. Nos últimos anos, com as constantes mudanças que ocorreram na sociedade, a demanda por proteção dos dados pessoais tem aumentado significativamente.

O Regulamento Geral sobre a Proteção de Dados (RGPD) (UE) 2016/679, por exemplo, é um regulamento do direito europeu sobre privacidade e proteção de dados pessoais, aplicável a todos os indivíduos na União Europeia (UE) e Espaço Econômico Europeu (EEE) (Adfue, 2014). Esta regulamentação tem a finalidade de regulamentar a exportação de dados pessoais para fora da UE e EEE. O objetivo do RGPD é possibilitar aos cidadãos europeus e residentes formais controlar seus dados pessoais, além de uniformizar a legislação na comunidade europeia.

Nos Estados Unidos da América (EUA), como cada estado possui leis próprias, até o presente momento não existe uma lei de proteção de dados única. No estado da Califórnia, por exemplo, o *California Consumer Privacy Act* de 2018 (CCPA) define os aspectos legais sobre proteção de dados.

Diferentes nações estão seguindo a regulamentação europeia como um modelo para criar suas leis de proteção de dados. Dentre estes países pode ser destacado o Brasil que seguiu o modelo europeu (GDPR) para criar a sua lei de abrangência nacional voltada à proteção de dados pessoais.

A LEI Nº 13.709 (LGPDP), de 14 de agosto de 2018 (Brasil, 2018) diz respeito ao 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. Segundo a LGPDP, a utilização de dados pessoais dos usuários só poderá ocorrer mediante consentimento. Esse consentimento poderá ser dado de diferentes maneiras na utilização de aplicações, por exemplo: (i) por meio de termos de consentimento de utilização dos dados, mas desde que as informações dos termos estejam bem definidas e seus objetivos de uso claros aos usuários; (ii) por meio da assinatura por escrito demostrando a vontade do titular. Ou seja, não basta apenas a utilização de um termo de consentimento em meio digital ou físico; o termo em si deve conter informações claras e objetivas quanto à utilização dos dados dos usuários.

2.3. Fontes de conhecimento de segurança para especificação e validação de requisitos de software da área financeira

Nesta Seção são apresentadas as principais fontes de conhecimento de segurança da informação que podem ser usadas durante o processo de especificação e validação de requisitos de software da área financeira.

Para que possam desenvolver seus sistemas em conformidade com os regulamentos, as instituições financeiras devem recorrer a normativas do Banco Central do Brasil (BACEN). O BACEN é uma instituição financeira (autarquia autônoma) ligada ao governo federal. Os demais emissores e credenciadores devem padronizar seus sistemas e homologar junto ao BACEN para que possam disponibilizar produtos e serviços bancários para seus clientes de forma segura, ou seja, garantido privacidade e segurança de dados existentes nas aplicações da organização.

Os requisitos de segurança são implementados para garantir a integridade, a confidencialidade, a disponibilidade e o não-repúdio das informações trafegadas pela rede BACEN (2020). Fornecedores, usuários da Rede do Sistema Financeiro Nacional – RSFN, assim como as pessoas ou empresas relacionadas, devem ser informados (ou ter meios para tomar ciência) sobre a existência e a extensão de medidas práticas, procedimentos e órgãos responsáveis para a segurança dos sistemas de informação na RSFN.

A Resolução n° 4.327 (BACEN, 2014), determina que as medidas e os procedimentos para a segurança de sistemas de software devem estar coordenados e integrados entre si. Além da determinação, esta resolução propõe que a coordenação e a integração com outros princípios das instituições participantes com o intuito de criar sistemas coesos e seguros que sejam passíveis de avaliações recorrentes (auditorias). É de fundamental importância para as organizações financeiras realizarem as validações dos componentes de *hardware* e software de acordo com essa resolução. A referida resolução também possui um conjunto de premissas técnicas importantes que devem ser seguidas pelas instituições, por exemplo: (i) todas as mensagens enviadas à RSFN serão obrigatoriamente autenticadas por meio de criptograma (assinadas digitalmente) pela instituição participante emissora, com exceção, caso julgado necessário, das relativas a testes de conectividade, das relativas a consulta de certificados digitais e das relativas a comunicação de erros de segurança; (ii) todas as instituições devem aderir às especificações de segurança do Sistema de Pagamentos Brasileiro - SPB, bem como ao protocolo de segurança para troca das mensagens. Além das premissas técnicas, existem diretrizes que determinam, por exemplo, que as instituições deverão criar e manter de maneira sistemática uma área de segurança da informação visando assegurar confidencialidade, integridade, autenticidade, não-repúdio e disponibilidade dos dados e das informações que são tratadas e classificadas como sensíveis.

Além das prerrogativas determinadas pelo BACEN, também devem ser observados os regimentos internos das instituições financeiras, ou seja, requisitos, políticas e outras regulações oriundas de departamentos de segurança da informação da própria instituição. É de grande importância que o desenvolvedor e o especialista em segurança da informação conheçam o regimento da instituição, para que possam obter um melhor entendimento do funcionamento das instituições. Além da fontes de informação elencadas, o especialista em segurança da informação de instituições da área financeira poderá recorrer ao Manual do COSIF[1] (COSIF, 1922).

PCI DSS (*Payment Card Industry Data Security Standard*) (PCI DSS, 2018) é um padrão de segurança de dados de cartões utilizados para pagamentos de compras físicas ou *online*. Os requisitos de segurança se aplicam a todos os componentes do sistema

[1] COSIF - Manual de Normas do Sistema Financeiro (https://www3.bcb.gov.br/aplica/cosif)

que estejam incluídos ou conectados no ambiente dos dados do titular do cartão. O ambiente de dados do titular do cartão compreende pessoas, processos e tecnologias que armazenam, processam, ou transmitem os dados do titular do cartão ou dados de autenticação confidenciais. No padrão também podem ser encontradas informações dos principais componentes do sistema, incluindo dispositivos de rede, servidores, dispositivos de computação e aplicativos (PCI DSS, 2018). Segundo Shihab *et al.* (2014), o PCI DSS consiste em um conjunto de requisitos mínimos para proteção de dados do titular do cartão. Esse conjunto mínimo é composto por 12 requisitos base que são combinados com procedimentos de teste, tornando-se uma ferramenta de avaliação da segurança de dados. Os seguintes requisitos base são propostos: 1. Instalar e manter uma configuração de firewall para proteger os dados do titular do cartão; 2. Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança; 3. Proteger os dados armazenados do titular do cartão; 4. Criptografar a transmissão dos dados do titular do cartão em redes abertas e públicas; 5. Proteger todos os sistemas contra malware e atualizar regularmente programas ou software antivírus; 6. Desenvolver e manter sistemas e aplicativos seguros; 7. Restringir o acesso aos dados do titular do cartão de acordo com a necessidade de conhecimento para o negócio; 8. Identificar e autenticar o acesso aos componentes do sistema; 9. Restringir o acesso físico aos dados do titular do cartão; 10. Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do titular do cartão; 11. Testar regularmente os sistemas e processos de segurança; 12. Manter uma política que aborde a segurança da informação para todas as equipes.

A *Open Web Application Security Project* (OWASP) é uma organização global sem fins lucrativos voltada a melhorar a segurança de sistemas de software (Leaders et al., 2013). Por exemplo, com o OWASP *Testing Guide,* é possível realizar os testes de forma mais rápida e precisa e eficiente (Leaders et al., 2013), buscando mitigar os problemas de segurança em projetos de sistemas de software na Internet. O OWASP vive em constante aprimoramento para atender as reais necessidades dos projetos de testes (Guaman et al., 2017). Segundo Leaders et al. (2013), o principal objetivo do OWASP é ajudar as pessoas a entenderem o que deve ser testado em um projeto de software, por que deve ser testado, quando testar as funcionalidades, onde e como testar os requisitos que foram implementados no aplicativos para a *Web*. Para Lukasiewicz & Cyganska (2019), o

OWASP possui dois objetivos: (i) ajudar a desenvolver e manter um software seguro; e (ii) ajudar na definição dos requisitos entre os provedores de serviços e seus respectivos clientes. Segundo Sohoel et al. (2018), os dez principais projetos do OWASP surgem de um consenso entre os especialistas da área da segurança; para isso, são levados em consideração a opinião dos especialistas sobre quais seriam as dez vulnerabilidades mais críticas existentes na *Web* no momento.

Como outras fontes importantes, incluem-se as bases de vulnerabilidades conhecidas. Segundo Qian et al. (2019), para elicitar requisitos de software, de modo a identificar necessidades de segurança, se faz necessário, por exemplo, conhecer as bases de vulnerabilidades, que podem levar a ataques de segurança ou vazamentos de dados confidenciais.

Open Source Vulnerability Database (OSVDB)[2], uma base de dados que atua de forma independente e aberta. O objetivo principal é fornecer informações técnicas precisas, detalhadas, atuais e imparciais sobre vulnerabilidades de segurança em sistemas de software. Atualmente, a OSVDB encontra-se disponível por meio do CVE[3]. Em novembro de 2013, o banco de dados catalogava mais de 100.000 vulnerabilidades.

A *National Vulnerability Database* (NVD) é um banco de dados nacional de vulnerabilidades do governo dos Estados Unidos (Kuhn et al., 2017). O NVD possui uma estrutura XML que inclui descrições de vulnerabilidades, entre outras informações (Baláž et al., 2019). Segundo Kuhn et al., (2017), o NVD conta com vulnerabilidades relatadas publicamente no dicionário *Common Vulnerabilities and Exposures* (CVE). Os bancos de dados de vulnerabilidades conhecidas desempenham um papel de grande importância na disponibilização e entrega de informações para os s*takeholders* (Mendes et al., 2011).

De acordo com Gallon (2010), mesmo com a existência de bases de dados de vulnerabilidades e dicionários disponíveis para consulta pública, estes ainda não são suficientes, pois se faz necessário criar *rankings* de fatores de riscos. Neste caso, surge a necessidade de elencar quais vulnerabilidades apresentam uma maior ou menor criticidade

[2] *Open Source Vulnerability Database* (OSVDB). Disponível em: (https://cve.mitre.org/data/refs/refmap/source-OSVDB.html)

[3] *Common Vulnerabilities and Exposures* (CVE). Disponível em: (https://cve.mitre.org/data/refs/refmap/source-OSVDB.html)

para o sistema e, após identificar o nível de criticidade, decidir qual ou quais vulnerabilidades devem ser postas em sua lista de prioridades. Para isso, segundo Ekstedt et al. (2018) e Gallon (2010), é proposto o *Common Vulnerability Scoring System* (CVSS), que é um padrão livre e aberto que propõe um sistema de pontuação confiável de criticidade das ameaças.

2.4. Processos de Desenvolvimento de Software Seguro

O desenvolvimento de software seguro requer a adoção de métodos e processos que têm por finalidade seguir passos bem definidos, que auxiliam a equipe de desenvolvimento em todas as etapas do projeto de software.

O Ciclo de Vida de Desenvolvimento de Segurança (SDL - *Security Development Lifecycle*) é composto por um conjunto de práticas que oferecem suporte à especificação de requisitos, visando a garantia e a conformidade de acordo com boas práticas de segurança. SDL apresenta 12 práticas[4] (recomendações), a saber: (1) fornecer treinamento; (2) definir requisitos de segurança; (3) definir relatórios de métricas e conformidade; (4) realizar modelagem de ameaças; (5) estabelecer requisitos de projeto; (6) definir e usar padrões de criptografia; (7) gerenciar o risco de segurança quando usar de componentes de terceiros; (8) usar ferramentas aprovadas; (9) executar teste de segurança de análise estática; (10) executar teste de segurança de análise dinâmica; (11) realizar testes de invasão; e (12) estabelecer um processo padrão de resposta a incidentes.

A utilização do SDL é importante para grandes projetos com grandes equipes de colaboradores; entretanto, é provável que as vulnerabilidades dos sistemas não desapareçam, pois as causas que as originam são muito difíceis de eliminar (Mendes et al., 2011). Segundo os autores, os componentes e sistemas de software disponíveis possuem vulnerabilidades, e neste caso, se faz necessário contar com meios eficazes para avaliar os riscos de segurança apresentados nos componentes e, com isso, selecionar aqueles que apresentam menor risco.

As subseções a seguir apresentam conceitos, processos e técnicas de engenharia de requisitos no ciclo de desenvolvimento de software.

[4] As 12 práticas de desenvolvimento de software seguro da Microsoft. Disponível em: <https://www.microsoft.com/en-us/securityengineering/sdl/practices#practice2>

2.4.1 Conceitos e processos de engenharia de requisitos

A engenharia de requisitos pode ser definida como o processo sistemático de desenvolvimento de requisitos, por meio de um processo interativo e cooperativo de análise do problema, resultantes em especificações em vários aspectos (Machado, 2015). Existem diferentes termos relacionados a “requisitos de software”, tais como análise de requisitos e gestão de requisitos. Segundo Machado (2015), ambos os termos são aplicados a projetos de software. Ainda em cada um destes termos, há subdivisões para que o professional responsável pela engenharia de requisitos possa fazer uso durante a identificação e coleta dos requisitos.

Os requisitos de um sistema são as descrições do que o sistema deve fazer, os serviços que oferecem e as restrições a seu funcionamento (Sommerville, 2016). Esses requisitos refletem as necessidades dos clientes para um sistema que serve a uma finalidade, como controlar um dispositivo, colocar um pedido ou encontrar informações. O autor destaca que o processo de descobrir, analisar, documentar e verificar esses serviços e restrições é chamado de engenharia de requisitos.

Segundo Sommerville (2016), o termo “requisito” não é usado de maneira consistente pela indústria de software. Em alguns casos, o requisito é apenas uma declaração abstrata em alto nível de um serviço que o sistema deve oferecer ou uma restrição a um sistema. No outro extremo, é uma definição detalhada e formal de uma função do sistema. Segundo o autor, os requisitos podem der divididos entre:

- **Requisitos funcionais:** São declarações de serviços que o sistema deve fornecer, de como o sistema deve reagir a entradas específicas e de como o sistema deve se comportar em determinadas situações. Em alguns casos, os requisitos funcionais também podem explicitar o que o sistema não deve fazer.
- **Requisitos não-funcionais:** São restrições aos serviços ou funções oferecidas pelo sistema. Incluem restrições de *timing*, restrições no processo de desenvolvimento e restrições impostas pelas normas. Ao contrário das características individuais ou serviços do sistema, os requisitos não-funcionais, muitas vezes, aplicam-se ao sistema como um todo, tais como: usabilidade, disponibilidade, interoperabilidade, segurança, privacidade, etc.

Sommerville (2016) apresenta um exemplo de modelo de processo de engenharia de requisitos. Cada organização tem sua própria versão ou instância desse modelo geral, dependendo de fatores locais, como o conhecimento do pessoal, o tipo de sistema a ser desenvolvido, as normas usadas etc. As atividades do processo são:

1. *Descoberta de requisitos*. Os requisitos de domínio dos s*takeholders* e da documentação são descobertos. Existem várias técnicas complementares que podem ser usadas para descoberta de requisitos.
2. *Classificação e organização de requisitos*. Requisitos não-estruturados são recebidos, requisitos relacionados são agrupados e organizados em grupos coerentes.
3. *Priorização e negociação de requisitos.* Inevitavelmente, quando vários *stakeholders* estão envolvidos os requisitos entram em conflito. Essa atividade está relacionada com a priorização de requisitos e em encontrar e resolver os conflitos por meio da negociação de requisitos.
4. *Especificação de requisitos.* Documentos formais ou informais de requisitos são produzidos.

2.4.2 Técnicas de elicitação de requisitos

A elicitação de requisitos de software é uma etapa do processo de desenvolvimento em que o profissional faz uso de diferentes técnicas para levantar (descobrir) os requisitos da aplicação. Existem diferentes técnicas que podem ser adotadas na etapa de elicitação para coletar os requisitos funcionais e não-funcionais.

Segundo Sommerville (2016), a entrevista com *Stakeholders* é uma técnica frequentemente utilizada para elicitação de requisitos. As entrevistas podem ser conduzidas de maneira formal ou informal. Durante a realização das entrevistas a equipe responsável pela engenharia de requisitos questiona os *stakeholders* sobre os sistemas da organização, assim como a solução sistêmica a ser desenvolvida. As respostas dos *stakeholders* fazem surgir os requisitos essenciais para o software a ser desenvolvido. O autor descreve dois tipos de entrevistas que podem ser adotadas durante a elicitação, a saber: (i) *entrevistas fechadas,* em que o *stakeholder* responde a um conjunto predefinido de perguntas; e (ii) *entrevistas abertas,* em que não existe uma agenda predefinida. A

equipe de engenharia de requisitos explora uma série de questões com os *stakeholders* do sistema e, assim, desenvolve uma melhor compreensão de suas necessidades.

O engenheiro de requisitos deverá ter conhecimento prévio do domínio da aplicação antes da elaboração do roteiro da entrevista. A escolha do tipo de pergunta a ser utilizada na realização das entrevistas com os *stakeholders* dependerá dos objetivos da equipe de engenharia de requisitos e da finalidade do projeto de software. Para Sommerville (2016), as entrevistas com os *stakeholders* costumam ser uma mistura de ambos os tipos. É importante que se tenha um roteiro, tanto para perguntas fechadas quanto para perguntas abertas. As respostas obtidas por meio de perguntas abertas proporcionam a criação de novas perguntas, buscando, assim, identificar a causa raiz do problema a ser resolvido com a solução sistêmica. As entrevistas podem apresentar dificuldades para um correto entendimento do domínio da aplicação. Estas dificuldades podem estar relacionadas à linguagem de comunicação, bem como ao entendimento do domínio.

Outra técnica bastante utilizada é a análise de documentos. Esta técnica tem por finalidade reutilizar soluções sistêmicas já existentes na organização, ou seja, usa-se como base sistemas legados, leituras baseadas em perspectiva, normas, legislação etc. A Arqueologia de Sistemas é uma técnica para extrair informações necessárias para construir um novo sistema a partir da documentação ou da implementação de código de um sistema legado ou de um sistema concorrente (Pohl, 2016). A Leitura baseada em Perspectiva é aplicada quando documentos precisam ser lidos a partir de uma perspectiva específica, tais como a perspectiva dos programadores e dos testadores. Aspectos contidos nos documentos que não dizem respeito à perspectiva atual são ignorados. Isso permite uma análise estritamente focada em partes específicas da documentação (Pohl, 2016). Segundo o autor, a análise de documentos deve ser combinada com outras técnicas de elicitação para requisitos para o novo sistema possam ser identificados. Pohl (2016) apresenta as seguintes perspectivas: (i) Na perspectiva do *conteúdo*, o auditor verifica o conteúdo dos requisitos documentado e certifica-se de sua qualidade; (ii) Na perspectiva da *documentação*, o auditor certifica-se de que todas as diretrizes de documentação para requisitos e para documentos de requisitos foram seguidas; (iii) Na perspectiva do *acordo*, o auditor verifica se todos os *stakeholders* estão de acordo com os requisitos e se existem conflitos com os requisitos que foram elicitados.

A utilização de questionários é outra técnica de elicitação de requisitos bastante utilizada. Essa técnica é comumente adotada quando há necessidade de se trabalhar com grandes grupos de *stakeholders*, visando a coleta de requisitos em larga escala. Segundo Machado (2015), os questionários são técnicas de elicitação de requisitos indicadas para quando os *stakeholders* estão alocados em regiões geograficamente diferentes. Na elaboração dos questionários, é necessário que o profissional da engenharia de requisitos possua conhecimento prévio do domínio da aplicação e conhecimentos elevados sobre o processo de negócio. Existem vários tipos de questionários que podem ser utilizados na prática da elicitação de requisitos (Machado, 2015), sendo seguintes os principais tipos: (i) Múltipla Escolha **(**usuário deve selecionar uma resposta dentre as respostas disponíveis); (ii) Lista de Verificação (questões com listas suspensas); e (iii) Questões com Espaços em Branco (resposta em texto livre). Os questionários devem ser acompanhados de uma carta ou qualquer outro tipo de documento que explique a real importância do seu correto preenchimento. Além disso, é importante que sejam criados controles para identificar os *stakeholders*, para que haja um *feedback* ou até mesmo a necessidade de esclarecimento.

2.5. Semiótica Organizacional

A semiótica é a ciência da significação e de todos os tipos de signos, podendo ser aplicada aos diferentes tipos de mídias e formatos de comunicação, ou seja, desde a comunicação interpessoal à comunicação mediada por dispositivos eletrônicos. A semiótica é uma das disciplinas que fazem parte do amplo arcabouço da filosofia de Pierce. A semiótica de Morris (1994) apresenta três relações existentes entre os signos, a saber: a "*Sintaxe*", a "*Semântica*" e a "*Pragmática*".

A *Sintaxe* aborda a concepção formal da linguagem. Estudos da sintaxe focam nas relações sintáticas entre os signos, ignorando o significado e a relação com quem os interpretam. O autor afirma que grande parte dos trabalhos desenvolvidos na linguística tem como foco a sintaxe; isso, de forma inconsciente, acaba gerando confusões no seu correto entendimento. A *Semântica* a foca na relação existente entre os signos e os objetos que são representados por esses signos, ou seja, o seu significado. Já a *Pragmática* se refere à relação dos signos com seus intérpretes (*e.g.*, organismos vivos), tais como suas

intenções e efeitos do uso dos signos incluindo, por exemplo, elementos psicológicos, biológicos e sociológicos.

2.5.1. Conceitos da Semiótica Organizacional

A SO trata as organizações como sistemas de informação, nos quais as informações são criadas, processadas, distribuídas, armazenadas e usadas, desenvolvendo uma teoria semiótica para entende-las com base no uso de signos (Jardim-Goncalves et al., 2010). Dessa maneira, a comunicação é entendida como instrumento base para o desenvolvimento na organização.

Segundo Rambo & Liu (2016), a SO baseia-se na observação de que todo comportamento organizado é afetado pela comunicação e interpretação dos signos, ou seja, a interpretação que as pessoas fazem de forma individual ou até mesmo em grupos. Para Jardim-Goncalves et al. (2010), a SO pode ser vista como uma disciplina que contribui para a compreensão das interações entre as pessoas dentro da sociedade, e entre elas com a tecnologia. De acordo com Arantes (2013), a SO busca mostrar as possíveis maneiras de se identificar e analisar organizações.

Neste contexto, cabe ressaltar o uso da SO na análise e elicitação de requisitos. A SO fornece uma fundamentação teórica sólida sobre como os signos são usados na comunicação e pode apoiar a integração dos sistemas de informação existentes na organização (Liu, 2000). O envolvimento de pessoas no processo de comunicação e a interação com outros *stakeholders* fazem da SO uma disciplina útil para o entendimento dessa comunicação, bem como para a coleta de requisitos do software a ser desenvolvido.

A perspectiva da SO pode acomodar em sua descrição o indivíduo e o social, humano, técnico, empresa e interações entre empresas, no nível de detalhe que é necessário para estudar, modelar, projetar organizações e sistemas técnicos (Li et al., 2015). A SO pode ser utilizada juntamente com outras técnicas e práticas para que os *stakeholders* possam melhor identificar suas necessidades para o desenvolvimento de um determinado sistema dentro da organização.

As organizações podem ser vistas como sistemas de informações com ligações interdependentes entre a organização, os processos de negócios e a tecnologia da informação (Liu, 2000; Liu & Li, 2014). Em SO as organizações como sistemas de

informações estão compreendidas em três níveis: (i) Sistema Informal, (ii) Sistema Formal, e (iii) Sistema Técnico. Um esquema de relação entre os sistemas em uma organização é apresentado na Figura 1.

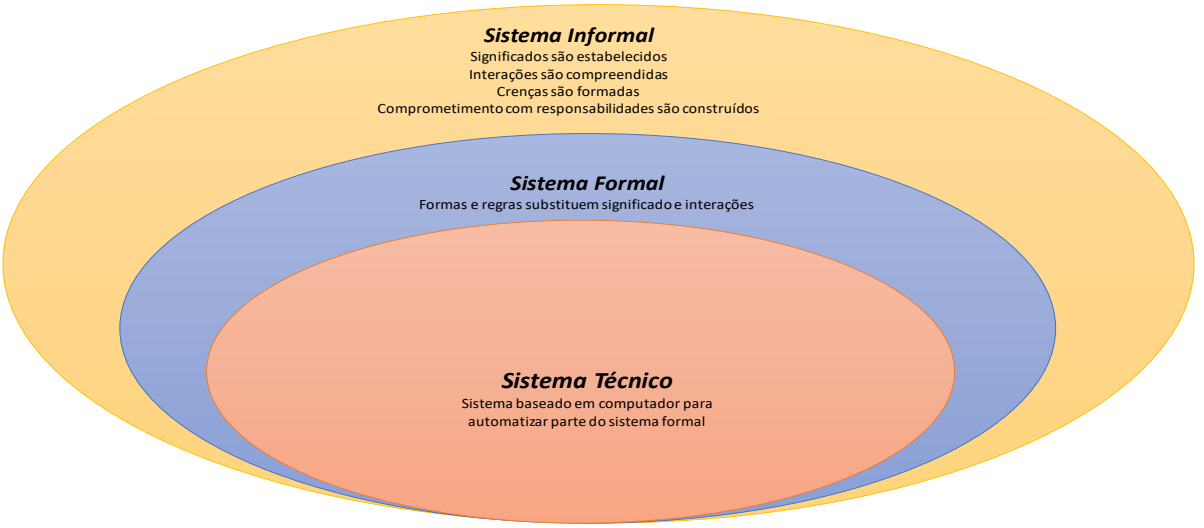


Figura 1 - Esquema de Relação entre os Sistemas em uma Organização

Adaptado de (Liu, 2000)

Com base na também chamada "Cebola Organizacional", ou "Cebola Semiótica" (Figura 1), é possível verificar que, no nível informal existe a subcultura que engloba os significados constituídos, onde as intenções são estabelecidas e compreendidas na organização. Neste momento são formadas as crenças e também surgem os comprometimentos e responsabilidades. De acordo com Simoni (2003), no nível formal, forma e autoridade substituem significado e intenção. No nível técnico parte do sistema formal é substituído por um sistema baseado em computador. Os níveis partem do mais geral (ou informal), engloba o nível formal, que por sua vez engloba o nível técnico. Alterações no nível informal ou formal, podem alterar o sistema de informação técnico. A introdução de um sistema computadorizado (nível técnico) também pode gerar alterações nos outros níveis. Para análise da organização nesses diferentes níveis, são utilizadas técnicas específicas da SO.

2.5.2. Métodos para Elicitação, Análise e Especificação de Requisitos de Usuário da Semiótica Organizacional.

Nesta subseção é apresentado um subconjunto dos métodos para elicitação, análise e especificação de requisitos de usuário da SO. O MEASUR (*Methods for Eliciting,*

Analysing and Specifying User Requirements) foi inicialmente proposto por Stamper (1973) com o objetivo de constituir um conjunto de métodos e técnicas para elicitação, análise e especificação de requisitos com base nos conceitos da semiótica. Liu (2000) utiliza um subconjunto de MEASUR, chamado de Métodos para Articulação de Problemas (PAM – *Problem Articulation Method*) para melhor definir (esclarecer) os problemas quando ainda estão vagos. Os métodos empregados nesta dissertação são baseados no PAM.

Dentre as ferramentas da SO, os seguintes artefatos e técnicas foram considerados adequados para uso neste trabalho: (A) *Diagrama de Stakeholders*, para análise das partes interessadas; (B) *Quadro de Avaliação*, para análise de problemas e soluções; e (C) *Framework Semiótico* (ou Escada Semiótica, pelo formato do diagrama), para identificação de requisitos. Versões adaptadas desses artefatos estão disponíveis para uso no sistema OpenDesign[5].

(a) Diagrama de Stakeholders

O Diagrama de *Stakeholders* é utilizado para analisar as partes interessadas de acordo com seu grau de envolvimento com o sistema em desenvolvimento. A Figura 2 apresenta um exemplo do referido diagrama, que inclui exemplos de *stakeholders* classificados em diferentes camadas, onde as mais internas significam maior envolvimento e as mais externas envolvimento indireto com o sistema ou projeto.

[5] Open Design (https://sandbox.opendesign.ml)

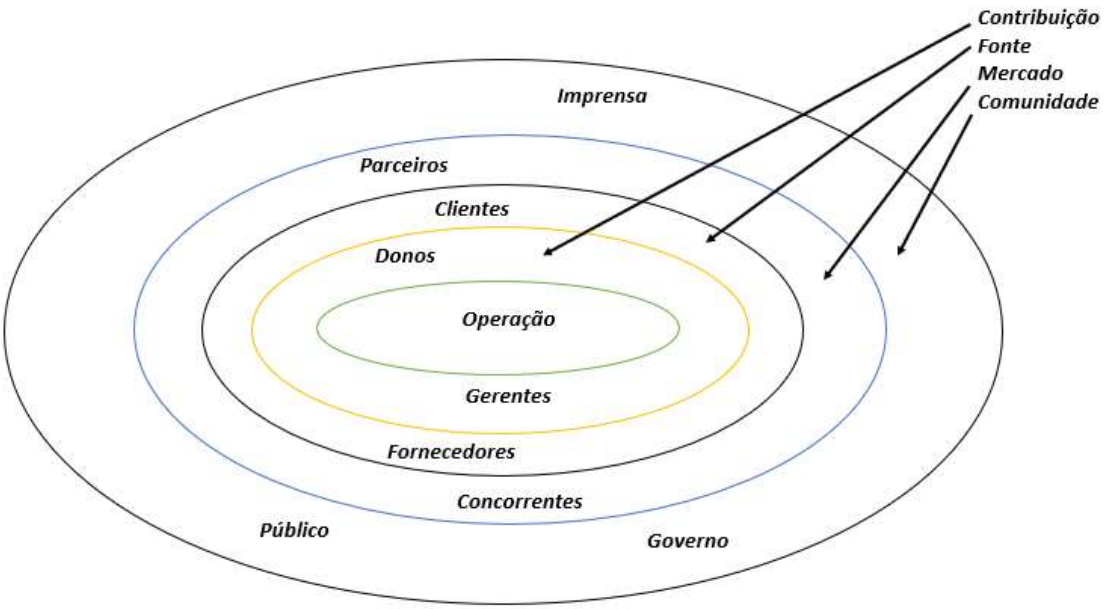


Figura 2 - Partes interessadas no processo de desenvolvimento de sistemas de Software
Adaptado de (Simoni, 2003)

Para a construção do Diagramada de *Stakeholders* deve-se primeiro identificar o sistema em questão (foco do projeto). Os analistas, clientes e usuários devem em consenso definir o foco da análise. No contexto desta dissertação, por exemplo, o foco deve remeter a questões de segurança e/ou privacidade. Tal definição é seguida por um *brainstorming* estruturado entre envolvidos com foco nos *stakeholders* relacionados a requisitos de segurança e privacidade. *Stakeholders* devem ser agrupados de acordo com as camadas do diagrama, conforme descrito a seguir:

- ***Operação:*** Nesta camada encontram-se *stakeholders* envolvidos na operação do sistema em questão.
- ***Contribuição*.** Nesta camada encontram-se *stakeholders* que estão diretamente envolvidos com o sistema de informação e com autoridade de tomada de decisão para o desenvolvimento do sistema. Por exemplo, nesta camada deverão ser identificados todos os atores e entidades que podem impactar diretamente na privacidade do sistema em uso.
- ***Fonte***. Nesta camada encontram-se os clientes e fornecedores que são afetados ou afetam a privacidade e/ou segurança do sistema.
- ***Mercado***. Nesta camada são listados todos os parceiros e colaboradores, assim como os concorrentes que impactam no curso da ação ou do sistema.

- ***Comunidade***. Nesta camada são listados diferentes agentes, tais como governo, imprensa, etc., que exercem influência ou são influenciados indiretamente pelo sistema.

(b) Quadro de Avaliação

O Quadro de Avaliação faz a correlação entre *stakeholder,* questões/problemas e possíveis soluções para o sistema em discussão. São formulados possíveis problemas existentes, ou que poderão surgir ao longo do ciclo de desenvolvimento do sistema, e posteriormente identificadas possíveis soluções para mitigar ou mesmo solucionar esses problemas. A Tabela 1 apresenta um exemplo de preenchimento do Quadro de Avaliação no contexto de privacidade e segurança de informação. O quadro é preenchido por meio de um processo de *brainstorming*.

Tabela 1 – Exemplo de Quadro de Avaliação

Stakeholders	Questões/Problemas	Possíveis Soluções
Gerência / Especialista em segurança e privacidade	Dificuldade em localização de documentos e falta de dados que permitam gerenciar todo o planejamento visualizando *feedbacks* para agir em situações críticas que envolvam privacidade e segurança.	Formalizar as dúvidas dos *stakeholders* envolvidos com o software a ser desenvolvido, levando em consideração o papel e função que cada um assume no projeto, ou seja, respeito as hierarquias existentes nos projetos, assim como a hierarquia organizacional.
Coordenação de Segurança e Privacidade	Grande número de *stakeholders* precisando garantir que a privacidade de seus dados seja realizada de maneira eficaz.	Registrar todas as necessidades dos *stakeholders* em relação ao software a ser desenvolvido; fornecer insumos base para uma correta elicitação de novos requisitos para um novo sistema de software ou aprimorar requisitos de software para que o projeto possa atender as normas e leis vigentes.
Coordenação de Segurança e Privacidade	Falta de apresentação para os *stakeholders* dos resultados dos trabalhos realizados de forma a atingir a meta determinada para o projeto de software, mostrando a falta de envolvimento da equipe com o tema abordado.	Reuniões com os *stakeholders* para a integração e uniformização do trabalho a ser desenvolvido.
Protocolo / Expediente	Falta de padronização na comunicação adotada.	Documentação de todas as partes do processo.

(c) Framework Semiótico

O *framework* semiótico, ou escada semiótica, tem por objetivo auxiliar engenheiros, analistas de requisitos e *stakeholders* nas atividades de elicitação e especificação de requisitos em diversos níveis de estudo da semiótica (Liu, 2000; Liu & Li, 2014). Conforme apresentado na Figura 3, o *framework* é dividido em dois grupos: Funções do Sistema de Informação Humano (mundo social, pragmático e semântico), e Plataforma de

Tecnologias da Informação (elementos sintáticos, empíricos e mundo físico) (Liu, 2000; Liu & Li, 2014). Os grupos têm relação com os requisitos que são elicitados e aprimorados no projeto de desenvolvimento de software para a organização.

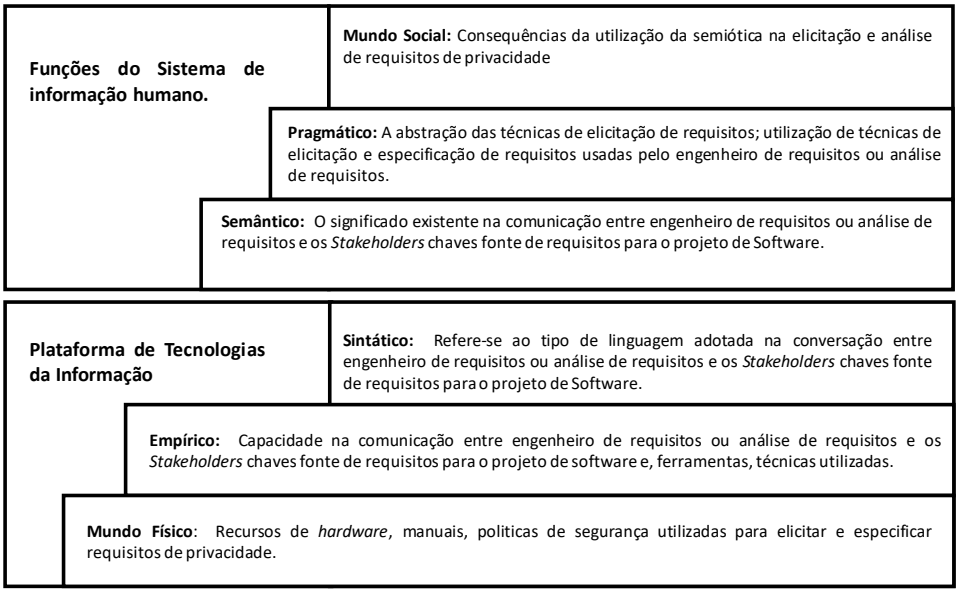


Figura 3 - Framework Semiótico
Adaptado de (Liu, 2000)

Em cada nível do *framework* podem ser identificados requisitos de software para o sistema em questão, ou mesmo, um requisito pode ter reflexo em todas as camadas do *framework* semiótico. Por exemplo, no mundo físico são elicitados requisitos relacionados a recursos de *hardware*, ao passo que no mundo social o foco está em requisitos relacionados às demandas e consequências do uso do sistema na sociedade. Problemas e soluções listadas no Quadro de Avaliação devem ser traduzidas em requisitos nos diversos níveis do *framework* semiótico. Tal especificação é realizada por meio da análise sistemática dos requisitos presentes em cada nível, percorrendo cada proposta de solução e visualizando como estas se refletem em requisitos no *framework* semiótico.

3. Trabalhos Relacionados

Este capítulo tem por finalidade apresentar uma síntese da revisão de literatura. Nesta síntese são elencados os trabalhos que possuem relação com as áreas da segurança da informação, privacidade de dados, engenharia de requisitos e a SO. Primeiramente, apresenta-se o protocolo de revisão (Seção 3.1), na sequência, são apresentados os resultados da revisão (Seção 3.2) e, por fim, é apresentada uma discussão sobre os trabalhos relacionados (Seção 3.3).

3.1. Protocolo de Revisão

Para um melhor entendimento sobre elicitação de requisitos de software financeiro com respeito aos aspectos de privacidade, busca-se identificar lacunas que dificultam a prática da elicitação de requisitos, além de identificar trabalhos que fazem uso de técnicas da SO. A revisão foi realizada em três fases: Planejamento, Condução e Publicação dos Resultados. Cada fase possui um conjunto de atividades (Figura 4).

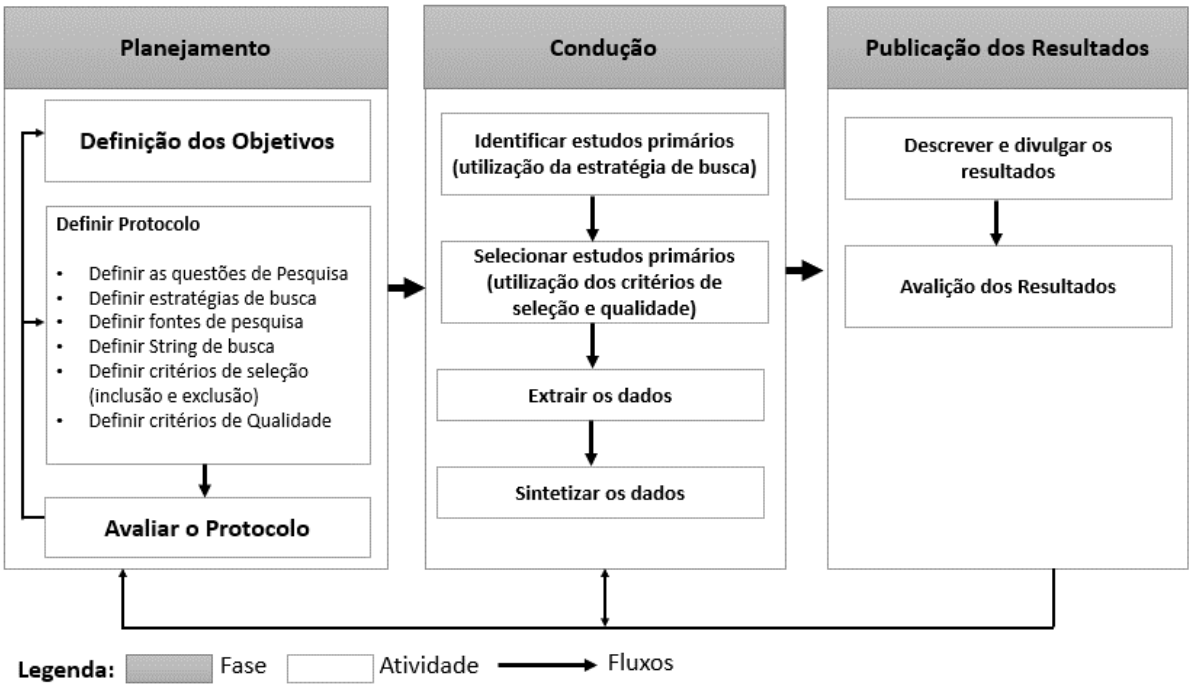


Figura 4- Fases e Atividades do Processo de Revisão

Adaptado de (Romero Felizardo Scannavino et al., 2017)

A primeira fase teve por finalidade a definição dos objetivos relevantes para a realização da revisão. Após a definição dos objetivos, foi estabelecido o protocolo da revisão. Durante a elaboração do protocolo foram definidos os seguintes elementos: questão de pesquisa, estratégias de busca em cada uma das bases de artigos, fontes de pesquisa, *string* de busca e critérios de inclusão e exclusão.

Os passos desta revisão incluem: (1) estabelecimento da hipótese ou questão de pesquisa; (2) amostragem ou busca na literatura (critérios de inclusão e exclusão de artigos); (3) categorização dos estudos (extração/organização das informações e formação do banco de dados); (4) avaliação dos estudos incluídos na revisão das publicações selecionadas (análise dos resultados); (5) interpretação e descrição dos resultados (discussão dos resultados); e (6) síntese do conhecimento ou apresentação da revisão (resumo das evidências disponíveis).

A questão norteadora desta revisão é: "*Como a Semiótica Organizacional poderá contribuir para a criação de um método para enriquecimento de requisitos de sistemas de software financeiro que considere aspectos de privacidade e segurança da informação? "*

Foram adotadas bases de dados científicas que fornecem publicações relevantes no contexto da dissertação. A Tabela 2 apresenta os parâmetros utilizados na realização da revisão, assim como as palavras-chave utilizadas na busca.

Tabela 2- Parâmetro para realização da revisão

Parâmetros da Busca	
Estratégia de busca	Artigos publicados de 2010 a 2019, nos idiomas inglês e português.
Bases de dados científicas	IEEE Xplore[6], ACM Digital Library[7], Scholar Google[8], Science Direct[9] e Springer Link[10]
Palavras-chave	semiotics, requirements, trust, security, privacy

[6] https://ieeexplore.ieee.org/Xplore/home.jsp
[7] https://dl.acm.org/dl.cfm
[8] https://scholar.google.com.br/
[9] https://www.sciencedirect.com/
[10] https://link.springer.com/

Como estratégia de busca foram adotados os idiomas inglês e português, com publicações entre os anos de 2010 e 2019. As bases de dados científicas foram selecionadas devido a sua importância para a área da Ciência da Computação. Para a seleção das palavras-chave, foi realizado um refinamento até encontrar um conjunto de termos que melhor representasse os objetivos da revisão como um todo. A Tabela 3 apresenta a *string* de busca adotada.

Tabela 3 - String de busca

String de busca
(semiotics AND requirements AND (trust OR security OR privacy)).
(semiótica AND requisitos AND (confiança OR segurança OR privacidade)).

A Tabela 4 apresenta os critérios de Inclusão (I) e Exclusão (E). A inclusão de artigos levou em consideração a sua relevância em relação ao tema desta dissertação, de modo que constem apenas estudos que retratam o estado da arte sobre análise e especificação de requisitos de software financeiro baseadas em semiótica.

Tabela 4 - Critérios de Inclusão e Exclusão

Critério	**ID**	**Descrição**
Inclusão	I1	Estudos envolvendo semiótica e semiótica organizacional.
	I2	Estudos envolvendo privacidade em software.
	I3	Estudos envolvendo elicitação e especificação de requisitos.
	I4	Publicações entre 2010 e 2019.
Exclusão	E1	Estudos repetidos em diferentes bases de dados selecionadas para a revisão.
	E2	Artigos publicados em idiomas diferentes de inglês e português.
	E3	Artigos publicados antes de 2010.
	E4	Dissertações de mestrado e teses de doutorado.
	E5	Resumos de artigos.

3.2. Resultados da Revisão sobre Trabalhos Relacionados

Inicialmente (Etapa 1), os artigos foram obtidos nas bases de dados científicas, por meio da *string* de busca. Posteriormente (Etapa 2), foram aplicados os critérios de inclusão e exclusão. Neste momento, foi realizada a leitura do título e do resumo para selecionar artigos relacionados com o tema da pesquisa, resultando em um conjunto de artigos menor.

Na Etapa 3, já com um conjunto de artigos mais reduzido, foi realizada uma análise com mais profundidade para que a revisão apresentasse artigos relacionados diretamente com o tema da dissertação. Por fim (Etapa 4), um conjunto de artigos primários foi lido por completo.

A Tabela 5 apresenta os resultados brutos obtidos das bases de dados científicas, em cada uma das etapas da revisão. Em todas as bases de dados foi aplicada a *string* de busca, assim como os critérios de inclusão e exclusão. Com relação à base de dados *Google Scholar*, após a aplicação da *string* de busca obteve-se 17.400 títulos, mas apenas os 100 primeiros foram considerados na análise.

Tabela 5 - Artigos selecionados por etapa

Base de dados	**Etapa 1**	**Etapa 2**	**Etapa 3**	**Etapa 4**
IEEE Xplore	104	65	40	11
Springer Link	1029	120	20	5
ACM Digital Library	1	0	0	0
Google Scholar	17400	100	25	5
Science Direct	963	150	13	2
Total	**19.497**	**425**	**98**	**23**

A Tabela 6 apresenta os 23 trabalhos selecionados. Nessa tabela, além da referência, são apresentados um resumo do objetivo e o respectivo papel da semiótica nos estudos descritos nos artigos. Na última linha da tabela, destaca-se o objetivo e o papel da semiótica nesta dissertação, apresentando uma comparação com os outros trabalhos.

Tabela 6 - Trabalhos selecionados na Revisão

Referência	Objetivo	Papel da Semiótica
(Arantes, 2013)	Criar de um método baseado na SO considerando questões sociais, políticas, culturais e éticas envolvidas na compreensão do problema do *design* para elicitação e especificação de requisitos.	Auxiliar os *stakeholders* na compreensão do domínio da aplicação, envolvendo questões relacionadas ao ambiente em que os usuários estão envolvidos no contexto do projeto de software a ser desenvolvido.
(Alhalafi, 2015)	Transformar a cultura da privacidade em projetos de desenvolvimento de sistemas na organização.	Destacar a importância da privacidade em projetos de desenvolvimento de sistemas de software, assim como o papel que a privacidade desempenha no processo de transformação de uma política organizacional.
(Alkubaisy, 2017)	Apresentar um *framework* para gerenciar conflitos entre os requisitos de segurança e privacidade em projetos de desenvolvimento de software.	Auxiliar no entendimento do contexto da aplicação, assim como na interação entre os *stakeholders* no projeto de desenvolvimento de software na organização.
(Arantes, 2011)	Utilizar a semiótica na representação de signos para elicitação de requisitos.	Contribuir para a elicitação de requisitos em diferentes níveis, buscando identificar as necessidades desde o mais baixo até o nível mais elevado, visando a representação dos signos na comunicação e na organização para elicitação de requisitos.
(Barn et al., 2015)	Identificar e preservar os requisitos de privacidade com a teoria ontológica da privacidade informativa de Luciano Floridi.	Preservação da abordagem na utilização de diferentes áreas de conhecimento e, visando identificar e preservar os requisitos de privacidade no suporte e análise de informações.
(Breaux & Rao, 2013)	Identificar requisitos e políticas de privacidade em ambiente *Web*.	Compreender as reais necessidades, limitações dos projetos de sistemas de software em ambiente *Web*.
(Cabitza & Mattozzi, 2017)	Utilizar a semiótica na construção de artefatos interativos no desenvolvimento de aplicações.	Contribuir na construção de artefatos interativos para o desenvolvimento de aplicações por meio do estudo dos signos, com base no entendimento e na aplicação dos conceitos e práticas da semiótica na organização.
(French et al., 2010)	Adotar práticas de políticas de segurança e confiabilidade em modelos computacionais.	Auxiliar na conscientização dos *stakeholders* com relação à confiabilidade em modelos computacionais da organização.
(Jardim-Goncalves et al., 2010)	Utilizar a semiótica para facilitar a compreensão dos signos pelos seres humanos.	Utilizar a semiótica social e organizacional como uma teoria para descrever práticas de trabalho relacionados a padrões de comunicação humana.
(Karlsson et al., 2017)	Utilizar políticas de segurança da informação em projetos de sistemas de software.	Auxiliar na abordagem prática de utilização de políticas de segurança da informação, por meio de etapas que devem ser seguidas na implementação de uma política de segurança dentro da organização.
(Lee & Wong, 2017)	Envolver os *Stakeholders* no processo de desenvolvimento de software.	Maior envolvimento das partes interessadas no sistema, para que estes possam colaborar de forma efetiva e integrada visando a construção do todo.

Referência	Objetivo	Papel da Semiótica
(Levy & Hadar, 2018)	Utilizar a técnica *Design Thinking* na elicitação de requisitos com diferentes técnicas e métodos.	Auxiliar na utilização *Design Thinking* como uma técnica para trabalhar com *stakeholders* na etapa de análise e especificações de requisitos.
(Li et al., 2015)	Estudar a comunicação por meio dos signos no âmbito organizacional.	Fornece comunicação no âmbito organizacional de forma que os *stakeholders* possam melhor compreender o contexto e a significação da representação de um signo.
(Oliveira et al., 2016)	Utilizar a semiótica computacional na modelagem de sistemas artificiais.	Utilizar a semiótica para monitoramento médico e para descoberta de conhecimento, realizando monitoramento para aprendizagem de máquina.
(Omoronyia et al., 2013)	Possibilitar proteção de dados dos usuários na utilização de aplicativos.	Apresentar aos *stakeholders* a importância da comunicação e conscientização na proteção de dados em ambientes com aplicativos móveis.
(Rambo & Liu, 2016)	Tratar a engenharia de requisitos por meio de uma abordagem sociológica do sistema a ser desenvolvido.	Prover compreensão dos requisitos a *stakeholders* com diferentes formações culturais.
(Shah & Patel, 2012)	Propiciar correto entendimento dos requisitos para mitigar retrabalho em projetos de software.	Auxiliar no processo de análise e especificação de requisitos de software, para diminuir retrabalho durante e após o desenvolvimento.
(Souza et al., 2010)	Gerar conhecimento por meio da inspeção semiótica em diferentes interfaces de sistemas.	Facilitar a compreensão e comunicação entre os usuários e entre as diferentes interfaces e seus signos na aplicação.
(Tejas & Patel, 2012)	Modelar requisitos de privacidade em projetos de software por meio do entendimento para evitar retrabalho no processo de desenvolvimento.	Auxiliar no processo de entendimento das necessidades de requisitos de privacidade para evitar retrabalho durante o desenvolvimento de software.
(Tran & Wei, 2011)	Identificar e aplicar os conceitos de privacidade e segurança em requisitos de ambientes virtuais.	Auxiliar no entendimento dos conceitos aplicados a privacidade e segurança em ambiente virtual, especialmente em sistemas de comercio eletrônico.
(Whiskerd et al., 2018)	Aprimorar a proteção de dados em sistemas que fazem uso de biometria.	Auxiliar no correto entendimento do domínio da aplicação evitando ambiguidade dos requisitos elicitados, ou seja, focando na segurança e confiabilidade dos dados a serem capturados e utilizados por meio da biometria em sistemas computacionais.
(Yang & Li, 2009)	Utilizar os requisitos para modelagem de arquitetura de sistemas da área de saúde, com base na semiótica.	Auxiliar no entendimento do domínio da aplicação, para que sejam mitigados os problemas de comunicação na utilização dos requisitos.
Esta Dissertação	***Aprimoramento de Requisitos de software da Área Financeira com Relação a Aspectos de Privacidade e Segurança: uma abordagem baseada na semiótica organizacional***	***Prover conceitos, artefatos e técnicas para propiciar uma melhor elicitação e especificação dos requisitos de software financeiros com uma visão sociotécnica.***

3.3. Discussão Sobre Trabalhos Relacionados

A partir da análise dos trabalhos, identificou-se a necessidade de propor métodos apropriados à elicitação de requisitos de software. Alguns trabalhos utilizam a semiótica como um instrumento para levantamento e especificação de requisitos. No entanto, não foram identificados trabalhos que utilizam a semiótica para a elicitação de requisitos de software financeiro considerando aspectos de privacidade e segurança de informação.

Os trabalhos abordam aspectos mais genéricos ligados aos requisitos funcionais. Foi possível identificar também que abordar aspectos de privacidade requer um amplo entendimento do domínio da aplicação. No contexto de software financeiro, devido a sua criticidade, faz-se necessária a combinação de diferentes técnicas para elicitação de requisitos, itens de avaliação de segurança e conhecimentos da regulamentação vigente.

Os estudos apontam que a comunicação com (e entre) *stakeholders* no processo de elicitação de requisitos de sistemas críticos é um aspecto-chave, ou seja, emissores e receptores de mensagens devem ter uma linguagem comum. Modelos e artefatos baseados em semiótica podem ajudar a aprimorar a comunicação.

A proposta desta dissertação (MARSPS) inclui um processo de aprimoramento de requisitos de software financeiro. A abordagem é uma sequência de passos a serem realizados de forma sistemática por desenvolvedores e *stakeholders*. MARSPS se diferencia dos demais trabalhos por fazer uso de técnicas da SO para enriquecimento de requisitos de software financeiro com relação a aspectos de privacidade e segurança da informação. Espera-se melhorar a compreensão do escopo do projeto a ser aprimorado em relação aos aspectos de privacidade e segurança.

Dessa forma, MARSPS proporciona aos desenvolvedores e *stakeholders* um instrumento formal composto por sete passos, onde cada passo contém atividades que devem ser seguidas para que um requisito possa ser aprimorado de forma a atender as reais necessidades de privacidade e segurança das soluções sistêmicas.

Na Tabela 7, são detalhados os trabalhos que apresentam uma maior relação com o MARSPS.

Tabela 7 - Trabalhos Relacionados

Referência	Título Traduzido	Contribuição
(Pan et al., 2018)	Estendendo o modelo de aceitação de tecnologia para pagamento móvel por proximidade via semiótica organizacional.	*Modelo de aceitação de tecnologia para pagamento móvel por aproximação.* Os autores usaram a Escada Semiótica para avaliar a aceitação em dois grupos (sistema de informação humano e plataforma de tecnologia), identificando os requisitos para adoção do pagamento móvel nas funções de informação humana e na plataforma de tecnologias da informação. Em comparação, MARSPS utiliza outras técnicas da SO (Cebola Organizacional e Quadro de Avaliação), além da Escada da Semiótica.
(Alkubaisy, 2017)	Um *framework* para gerenciar conflitos entre requisitos de segurança e privacidade.	*Framework para mitigar os riscos à segurança em três dimensões (gerenciamento de riscos, segurança e privacidade)*. Em comparação, MARSPS utiliza técnicas da SO para identificar e analisar *stakeholders* e suas respectivas necessidades de privacidade e segurança, além de gerir eventuais conflitos antes da implementação dos requisitos da área financeira.
(Tejas & Patel, 2012)	Modelagem de Requisitos orientada a Segurança do Sistema, Privacidade e Confiança para Sistema de Exame.	*Framework RE para modelagem de requisitos orientada a segurança, privacidade e confiança da área da saúde*. Em comparação, MARSPS utiliza técnicas da SO para identificar e analisar *stakeholders* e suas respectivas necessidades de privacidade e segurança, além de gerir eventuais conflitos antes da implementação dos requisitos da área financeira.
(de Oliveira et al., 2016)	Proposta para aplicação do método de inspeção semiótica na atividade de pesquisa de requisitos de artefatos futuros.	*Abordagem para aplicação do método de inspeção semiótica na atividade de pesquisa de requisitos.* A semiótica foi usada para facilitar a comunicação e a interação entre os *stakeholders* em um experimento com alunos de engenharia de software usando o método de inspeção semiótica em artefato proveniente da atividade de levantamento de requisitos. Em comparação, MARSPS utiliza técnicas da SO para aprimorar requisitos de software financeiro. Os *stakeholders* são analisados em diferentes camadas da Cebola Semiótica, mitigando possíveis problemas de comunicação no projeto.
(Breaux & Rao, 2013)	Análise formal das especificações de requisitos de privacidade para aplicativos de várias camadas.	*Abordagem para análise formal das especificações de requisitos de privacidade para aplicativos de várias camadas.* Dentre as contribuições foram apresentadas: (i) identificação sistemática de subconjuntos de requisitos relevantes para políticas de privacidade no estudo de caso; (ii) implementação de subconjunto de requisitos de dados em uma linguagem de descrição lógica (DL) para especificação de requisitos de privacidade; (iii) modelagem e verificação de conflitos de requisitos usando DL; e (iv) modelagem dos fluxos de dados para políticas de privacidade. Em comparação, MARSPS utiliza técnicas da SO para aprimorar requisitos de software financeiro. Os *stakeholders* são analisados em diferentes camadas da Cebola Semiótica, mitigando possíveis problemas de comunicação no projeto. Com respeito a aspectos de segurança e privacidade, propõe-se utilizar fontes de conhecimento de segurança para apoiar o processo de enriquecimento dos requisitos de software financeiro.
Esta dissertação	**Aprimoramento de Requisitos de Software da Área Financeira com Relação a Aspectos de Privacidade e Segurança: uma abordagem baseada na semiótica organizacional**	***Uma abordagem baseada na SO para aprimoramento de requisitos de software da área financeira com relação a aspectos de privacidade e segurança.* A abordagem é explicitada por meio de um método, juntamente com seu processo de implementação. Um estudo de caso é conduzido para validar a proposta conceitual.**

4. Elaboração e detalhamento do método MARSPS

Este capítulo apresenta a metodologia adotada para o desenvolvimento do método MARSPS (Seção 4.1). Na sequência, o capítulo descreve o método em detalhes (Seção 4.2), incluindo: os objetivos e premissas, bem como cada passo, atividade e artefato proposto pelo método. O MARSPS parte de um conjunto de requisitos de um sistema da área financeira, e gera especificações (*user stories*, casos de uso e critérios de aceite) com o objetivo de tornar robusto o sistema com relação a aspectos de segurança e privacidade.

4.1. Metodologia utilizada para concepção e validação do método

Este trabalho tem como escopo a aplicação de fontes de conhecimento e políticas de segurança, técnicas de análise e elicitação de requisitos, e conceitos da Semiótica Organizacional para aprimorar requisitos de software financeiro incorporando características de segurança e privacidade. Para tanto, propõe-se um método para auxiliar analistas de requisitos nesta tarefa. Esta seção destaca as etapas para concepção e validação deste método. A metodologia adotada para a realização deste projeto de pesquisa é baseada na Triangulação, conforme descrita por Lehtola e Kauppinen (2006). De acordo com os autores, este modelo faz uso de diferentes métodos de pesquisa para a obtenção de dados e para comparação de resultados. Este tipo de metodologia tem por finalidade certificar a qualidade, confiabilidade e a veracidade das informações geradas nos estudos. De acordo com Bruning *et al.* (2018), a Triangulação é constituída da investigação em torno de um mesmo tema central do projeto que está sendo desenvolvido, onde os dados e as análises de cada aspecto procuram criar uma coincidência, abordando a pesquisa da totalidade do fato. A Figura 5 ilustra a adoção da Triangulação. De acordo com Triviños (1987), a Triangulação é uma técnica que está apresentada sob três aspectos diferentes em si, sendo eles: (i) processos de produtos centrados no sujeito; (ii) elementos produzidos por meio do sujeito; e (iii) processos e produtos ocasionados pela estrutura socioeconômica e cultural do micro-organismo social do sujeito. A descrição do autor remete a pesquisa sociais, no entanto, os conceitos e técnicas podem ser aplicados em diferentes áreas de estudos com o objetivo de realizar uma análise voltada para a abordagem qualitativa dos dados obtidos com o cruzamento dos dados.

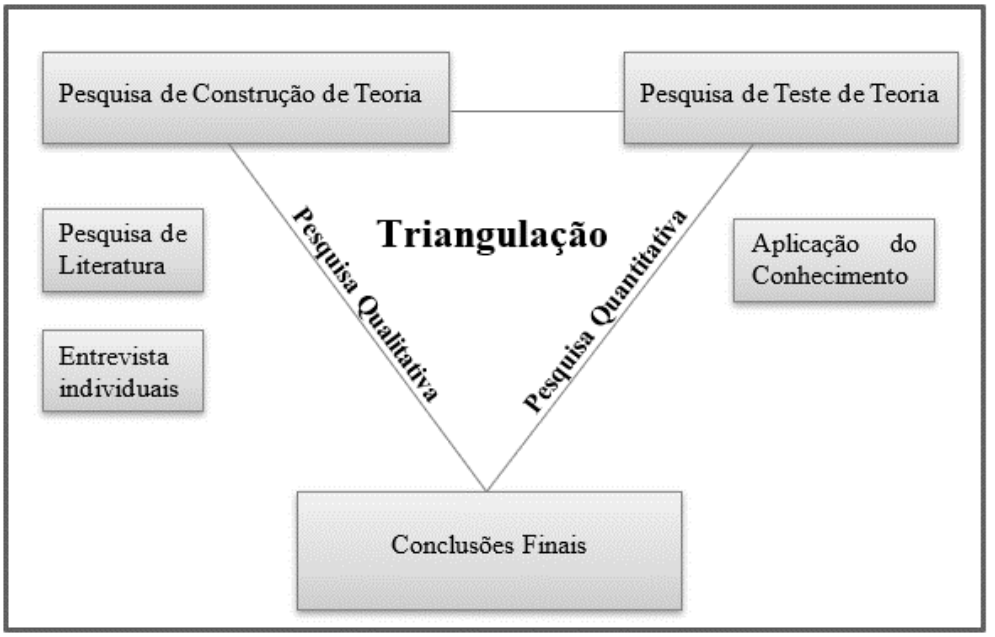


Figura 5 - Método Triangulação

Adaptado de (Manteli et al., 2010)

O método Triangulação (Figura 5) segue duas abordagens diferentes, sendo elas: (i) a pesquisa de construção de teoria, que é baseada na revisão da literatura, buscando efetuar uma análise exploratória; e (ii) a pesquisa de teste de teoria. Inspirado na pesquisa de triangulação, a abordagem adotada para concepção e validação do método é composta das seguintes etapas:

1. *Pesquisa Teórica* (canto superior da Figura 5). A pesquisa teórica inicial foi realizada com o objetivo de fundamentar o método MARSPS. Os resultados desta pesquisa são apresentados nos capítulos 2 e 3 desta dissertação. Estes dados serão confrontados com a pesquisa prática, bem como a análise de dados quantitativos e qualitativos.
2. *Análise Preliminar.* Em uma etapa preliminar, no que diz respeito à obtenção de dados qualitativos (lado esquerdo da Figura 5), foi aplicado um questionário para profissionais de engenharia de requisitos de uma empresa do sistema financeiro. O objetivo foi conhecer o atual formato utilizado para levantar aspectos de segurança e privacidade para os projetos de software.
3. *Formalização do Método.* Análise preliminar (item 2) bem como a pesquisa teórica (item 1) foram as bases para elaborar o método MARSPS. (Detalhado na próxima seção).

4. *Aplicação Inicial do Método* (lado direito da Figura 5). Uma vez especificada a versão inicial do MARSPS, ele foi instanciado em cenários de aplicação, todos os passos e atividades foram realizadas, bem como todos os artefatos foram produzidos. O Capítulo 5 detalha esta etapa da metodologia.
5. *Avaliação do Método* (lado direito da Figura 5). O método foi então avaliado por um conjunto de profissionais com experiência em especificação de requisitos de software da área financeira e em segurança da informação. O Capítulo 6 detalha esta etapa da metodologia.
6. *Triangulação dos Resultados e Proposta de Melhorias*. A combinação de resultados da pesquisa teórica, entrevistas e coleta de dados da aplicação do método resultará na triangulação de dados contendo diferentes fontes de informação. A Seção 6.3 apresenta uma discussão que contrapõe os resultados obtidos.

4.2. Descrição do Método MARSPS

Esta seção ressalta os objetivos principais e premissas do método (Subseção 4.2.1) e apresenta uma visão geral do método e suas fases (Subseção 4.2.2).

4.2.1 Objetivos e Premissas do MARSPS

O método MARSPS visa aprimorar a prática da elicitação, análise e especificação de requisitos de software financeiro com o auxílio da SO; ou seja, busca elucidar necessidades e requisitos não-funcionais ligados à privacidade nos projetos de desenvolvimento de software financeiro. O método deve auxiliar profissionais na busca de soluções sistemáticas, em uma visão sociotécnica, para atender as reais necessidades das empresas, assim como satisfazer as necessidades dos usuários. No método proposto, a segurança e a privacidade de dados dos usuários são pontos que devem ser elencados no início do processo e seguir no ciclo de vida do projeto de software como um todo. Considera-se a engenharia de requisitos um fator-chave de sucesso em um processo de desenvolvimento e também se destaca a liberdade de escolha da melhor técnica no projeto do software. Poderão ser adotadas uma ou mais técnicas propostas pelo método para melhor elicitar os requisitos do software. O processo adota como premissa que as partes interessadas têm diferentes visões, interesses e necessidades a serem elencadas e discutidas durante a execução do método.

4.2.2 O Método MARSPS

O Método de Análise de Requisitos de Software para Privacidade e Segurança (MARSPS) é voltado a auxiliar engenheiros de requisitos e especialistas em privacidade e segurança na missão de aprimorar características de segurança e privacidade, resultando em uma maior qualidade dos requisitos de um sistema financeiro. O método proposto pode ser utilizado em sistemas existentes ou em desenvolvimento.

Conforme apresentado na Figura 6, em um cenário macro, há dois *stakeholders* que possuem papéis e responsabilidades no processo de elicitação de requisitos de privacidade e segurança, a saber: o "Engenheiro de Requisitos – ER" e o "Engenheiro de Segurança da Informação – ESI". As atividades atribuídas para cada um são listadas na Figura 6, conforme *swimlanes* do processo. O ER disponibiliza o "Conjunto de Requisitos do Sistema" (item A1 da Figura 6), que contém os requisitos de software, assim como requisitos básicos de segurança e privacidade, caso tenham sido modelados. Este é o documento inicial para o ESI iniciar o processo. O ESI é o responsável pela execução do MARSPS, devendo conhecer cada um dos passos que compõem o método. Após gerar os artefatos, o ESI os enviará ao ER que receberá e analisará os requisitos aprimorados (parte superior direita da Figura 6).

O método proposto é composto por 7 passos, que abrangem desde o recebimento (a partir do ER) de um conjunto de requisitos do sistema (item A1 da Figura 6) até o aprimoramento (robustecimento) desses requisitos com um conjunto de requisitos de segurança e privacidade de software (item A8 da Figura 6). Os passos devem ser adotados (ou adaptados) por um ESI durante a especificação dos requisitos de software. Cada passo contém um conjunto de atividades a serem realizadas para gerar artefatos intermediários (itens A2-A7 da Figura 6). Os artefatos resultantes (item A8 da Figura 6) podem variar de acordo com as necessidades, características e metodologias a serem utilizadas para o software em desenvolvimento (por exemplo, *user stories*, critérios de aceite ou casos de uso).

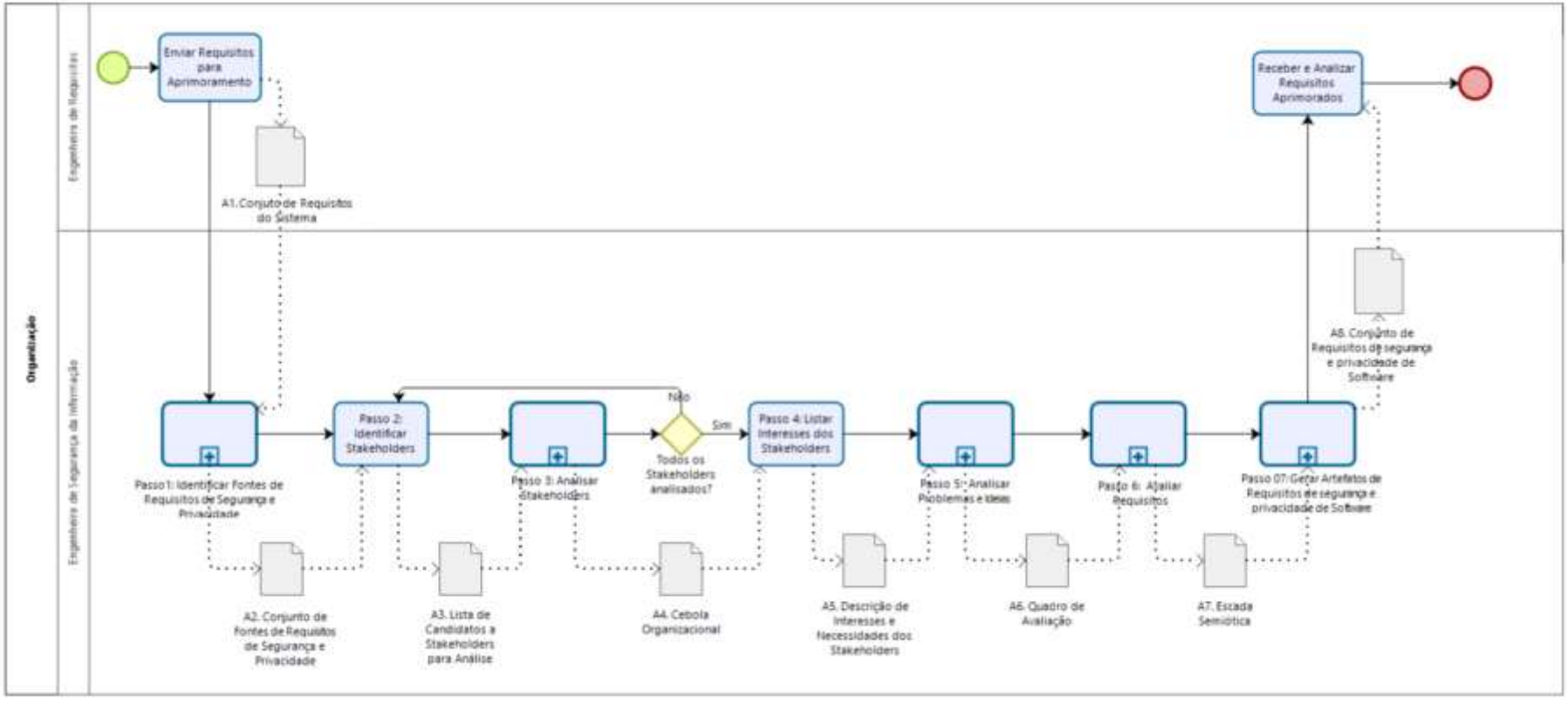


Figura 6 - Processo para Execução do Método MARSPS

A seguir apresenta-se uma síntese dos passos para execução do MARSPS.

Passo 1: Identificar Fontes de Requisitos de Segurança e Privacidade

Neste passo (Figura 7), são identificadas as fontes de conhecimento de requisitos de segurança e privacidade que podem (ou devem) ser usadas no processo de obtenção ou melhoria dos requisitos do sistema financeiro em desenvolvimento. Requisitos importantes podem ser identificados em diferentes fontes sendo, portanto, necessária uma pesquisa ampla para identificar todas as fontes a serem utilizadas no processo. A utilização de cada uma das fontes citadas dependerá das reais necessidades de privacidade e segurança a serem consideradas no projeto de software.

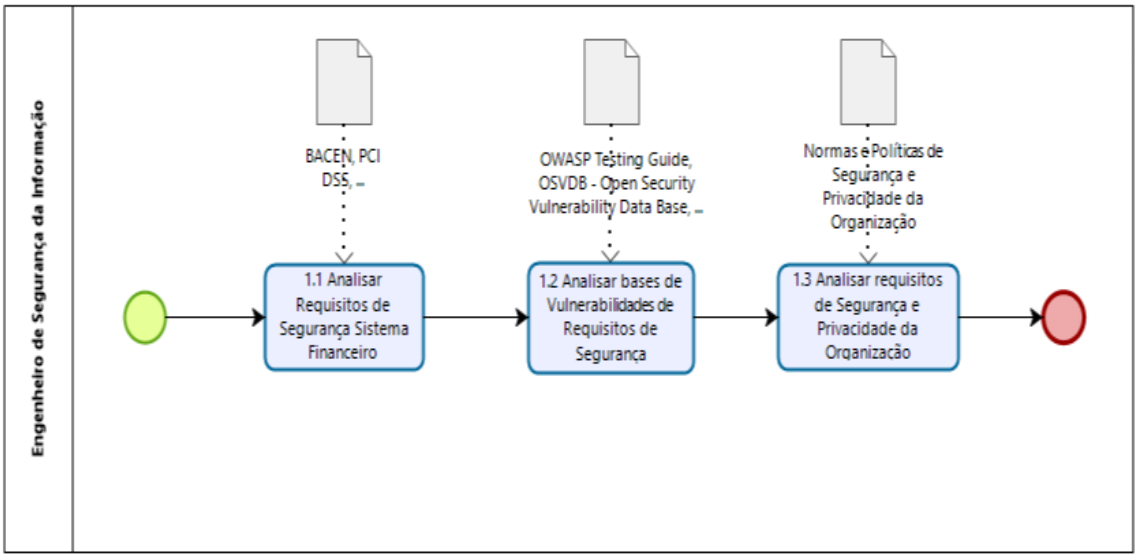


Figura 7 - Identificação de Fontes de Requisitos de Segurança e Privacidade

Após a identificar fontes de requisitos de segurança e privacidade, deve-se listar as fontes e analisá-las. Neste passo é proposto analisar requisitos de segurança do sistema financeiro (Item 1.1 da Figura 7) (*e.g.*, BACEN, PCI-DSS, entre outras), analisar as bases de vulnerabilidades de segurança (Item 1.2 da Figura 7) (*e.g.*, OWASP *Testing Guide*, OSVDB, entre outras), bem como adicionalmente analisar requisitos de segurança e privacidade da organização (Item 1.3 da Figura 7) (*e.g.*, normas e políticas de segurança e privacidade da organização). O método é flexível e outras fontes podem ser incluídas. As fontes inicialmente propostas foram definidas a partir de um mapeamento de fontes de conhecimento de segurança (Rosa, 2018). A saída do passo é um conjunto de fontes selecionadas com seus respectivos requisitos que serão potencialmente considerados na implementação do sistema (Item A2 da Figura 6).

Passo 2: Identificar Stakeholders

Neste passo, são identificados os *stakeholders* candidatos que podem influenciar ou serem influenciados diretamente ou indiretamente por aspectos de privacidade e segurança relacionados ao projeto em questão. Estes *stakeholders* serão analisados por uma adaptação do Diagrama de *Stakeholders* (*cf.*, Capítulo 2). O engenheiro de requisitos deverá considerar na identificação diferentes tipos de *stakeholders*, tais como:

- Pessoas que farão parte do sistema ou do contexto do sistema a ser melhorado ou desenvolvido. Usuários, bem como pessoas envolvidas ou afetadas indiretamente por questões de privacidade e segurança;
- Organizações, sendo estas partes interessadas em requisitos de privacidade e segurança do projeto em questão;
- Sistemas (compostos por pessoas e dispositivos computacionais) que poderão ser partes interessadas em requisitos de privacidade e segurança do projeto em questão.

A saída deste passo é uma lista de candidatos a *stakeholders* para análise (Item A3 da Figura 6).

Passo 3: Analisar Stakeholders

O terceiro passo (Figura 8) tem como finalidade analisar os *stakeholders* identificados em cada uma das camadas do Diagrama de *Stakeholders* (*cf.*, Capítulo 2).

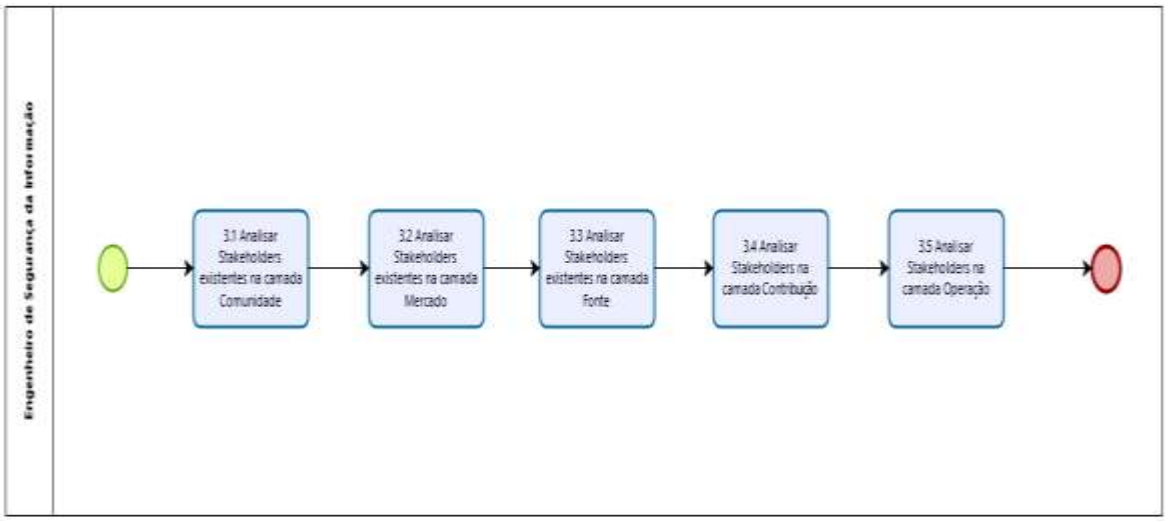


Figura 8 - Análise de Stakeholders

Neste passo, as seguintes atividades são realizadas:

- Analisar *stakeholders* existentes na camada *Comunidade* (Item 3.1 da Figura 8): na camada mais externa devem ser listados espectadores e legisladores que exerçam influência indireta ou são indiretamente influenciados pela privacidade e segurança do sistema em questão.
- Analisar *stakeholders* existentes na camada *Mercado* (Item 3.2 da Figura 8): nesta camada são adicionados os *stakeholders* provenientes do mercado, incluindo parceiros e concorrentes que possuem interesses relacionados com a privacidade e segurança do sistema em questão.
- Analisar *stakeholders* existentes na camada *Fonte* (Item 3.3 da Figura 8): esta camada inclui as "fontes do sistema", tais como os clientes e fornecedores de tecnologia, infraestrutura, etc., que possuem interesses relacionados com a privacidade e segurança do sistema em questão.
- Analisar *stakeholders* na camada *Contribuição* (Item 3.4 da Figura 8): esta camada inclui *stakeholders* que contribuem diretamente com o sistema, incluindo atores e responsáveis, tais como usuários diretos do sistema, administradores do sistema, técnicos, entre outros, que influenciam ou são influenciados diretamente por aspectos relacionados a privacidade e segurança do sistema em questão.
- Analisar *stakeholders* na camada *Operação* (Item 3.5 da Figura 8): na camada mais interna está o sistema (e/ou projeto) desenvolvido ou em desenvolvimento. As partes interessadas internas relacionadas a privacidade e segurança do sistema em questão fazem parte desta camada.

Conforme apresentado na Figura 6, os passos 2 e 3 de MARSPS devem ser repetidos até que todos os *stakeholders* sejam identificados e analisados. Após esses passos temos como saída o Diagrama de *Stakeholders* preenchido (Item A4 da Figura 6).

Passo 4: Listar Interesses dos Stakeholders

Neste passo, deve-se listar os interesses e necessidades de privacidade e segurança de cada um dos *stakeholders* que foram identificados e analisados nos passos anteriores. Diferentes tipos de *stakeholders*, possuem diferentes necessidades de privacidade e segurança; assim, deve-se lidar com interesses conflitantes e desenvolver estratégias para conciliar estes interesses, tais como oficinas, entrevistas e análise

documental para discutir conflitos identificados. Para tanto, deve-se listar as necessidades e apresentá-las de maneira clara.

Propõe-se listar as necessidades dos stakeholders e requisitos dos sistemas existentes de acordo com as seguintes atividades:

- *Listar as necessidades de segurança e privacidade dos usuários*: esta atividade tem por finalidade identificar e listar os requisitos de privacidade e segurança para o sistema sob o ponto de vista dos usuários. Os interesses devem ser listados de acordo com as necessidades de cada um dos envolvidos;
- *Listar as necessidades de segurança e privacidade das organizações*: esta atividade tem por finalidade identificar e listar as necessidades de privacidade e segurança referentes às organizações. Tais necessidades podem ser identificadas, por exemplo, nas normas e políticas de segurança existentes das organizações envolvidas.
- *Listar os requisitos de segurança e privacidade nos sistemas existentes*: esta atividade tem por finalidade identificar e listar os requisitos de privacidade e segurança existentes nos sistemas (computacionais, humanos ou híbridos) em operação. Para tanto, deve-se analisar sistemas legados, entrevistar participantes e realizar oficinas.

A saída deste passo inclui a descrição de interesses e necessidades de cada um dos stakeholders identificados anteriormente (Item A5 da Figura 6).

Passo 5: Analisar Problemas e Ideias

Neste passo (Figura 9), a construção do Quadro de Avaliação (*cf.*, Capítulo 2) tem como objetivo analisar possíveis problemas (ou questões) existentes, assim como propor ideias (ou soluções) relacionadas com a privacidade e segurança a serem adotadas pelo sistema a ser desenvolvido ou aprimorado. Deve-se identificar os problemas e propor soluções aos problemas relacionados a cada necessidade dos *stakeholders.*

O quadro pode ser organizado em níveis, de acordo o diagrama de *stakeholders*. Neste caso, cada problema ou ideia relacionada a privacidade e segurança é atribuída em um dos níveis (comunidade, mercado, fonte, contribuição e operação) e ligados aos *stakeholders* do diagrama de *stakeholders* (Itens 5.1-5.5 da Figura 9). O sistema

OpenDesign[11], por exemplo, disponibiliza funcionalidades para fazer esta ligação entre os problemas e ideias do quadro de avaliação, com os *stakeholders* e respectivos níveis utilizados na análise de *stakeholders* (Cebola Semiótica).

Como resultado deste passo, obtém-se o Quadro de Avaliação preenchido em todos os níveis com problemas e ideias (item A6 da Figura 6).

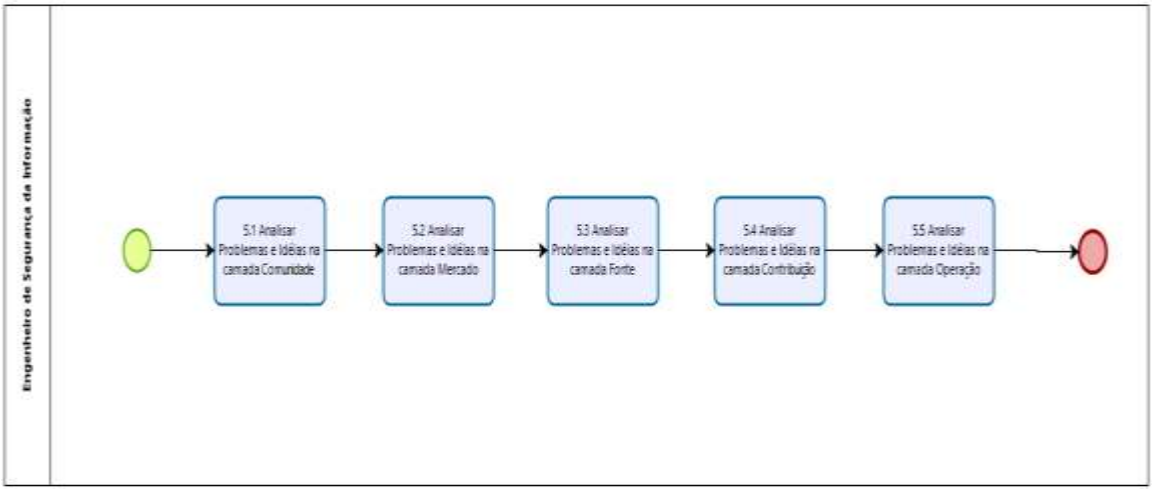


Figura 9 - Construção do Quadro de Avaliação

Passo 6: Avaliar Requisitos

Neste passo (Figura 10), é desenvolvido o *Framework* Semiótico (ou Escada Semiótica) (*cf.*, Capítulo 2), onde os 6 níveis do *framework* são preenchidos com potenciais requisitos ligados a privacidade e segurança. Isso inclui posicionar e elencar requisitos nos níveis referentes às funções do sistema de informação humano (social, pragmática e semântica) (Itens 6.1 a 6.3 da Figura 10), bem como nos níveis referentes à plataforma de tecnologia da informação (sintática, empírica e física) (Itens 6.4 a 6.6 da Figura 10).

A seguir são descritas em detalhe as atividades previstas para os níveis do *Framework* Semiótico e exemplos de ligações com a privacidade e segurança de informação:

- ***Função do Sistema de Informação Humano***. (i) *Descrever Requisitos do Mundo social* (Item 6.1 da Figura 10)*:* são elencados requisitos relacionados à sociedade, tais como aspectos legais e a percepção da sociedade sobre aspectos de privacidade e segurança de informação; (ii) *Descrever Requisitos*

[11] https://sandbox.opendesign.ml/

relacionados à Pragmática (Item 6.2 da Figura 10)*:* são elencados requisitos relacionados à pragmática, tais como a intenção e o comprometimento do usuário no uso do sistema no que se refere aos aspectos de privacidade e segurança de informação; e (iii) *Descrever Requisitos Relacionados à Semântica* (Item 6.3 da Figura 10)*:* são elencados requisitos relacionados à semântica do sistema, tais como se os usuários entendem os termos utilizados, se a linguagem da interface é adequada e suficientemente clara, entre outros aspectos ligados ao entendimento do usuário sobre conceitos de privacidade e segurança de informação.

- ***Plataforma de Tecnologia da Informação***. (i) *Descrever Requisitos Relacionados à Sintaxe* (Item 6.4 da Figura 10)*:* são elencados requisitos relacionados aos aspectos sintáticos do sistema, tais como linguagens de programação, protocolos e modelos de dados utilizados e suas relações com privacidade e segurança de informação; (ii) *Descrever Requisitos Relacionados à Capacidade Empírica* (Item 6.5 da Figura 10)*:* são elencados requisitos relacionados aos aspectos empíricos do sistema, tais como banda de comunicação, velocidade e capacidade de processamento e suas relações com privacidade e segurança de informação; e (iii) *Descrever Requisitos Relacionados aos Aspectos Físicos* (Item 6.6 da Figura 10)*:* são elencados requisitos relacionados com o *hardware* do sistema, tais como computadores, processadores, redes físicas, entre outros. O foco está na relação do *hardware* com aspectos de privacidade e segurança de informação.

A saída deste passo é a Escada Semiótica preenchida, com seu respectivo conjunto de potenciais requisitos em cada nível (Item A7 da Figura 6).

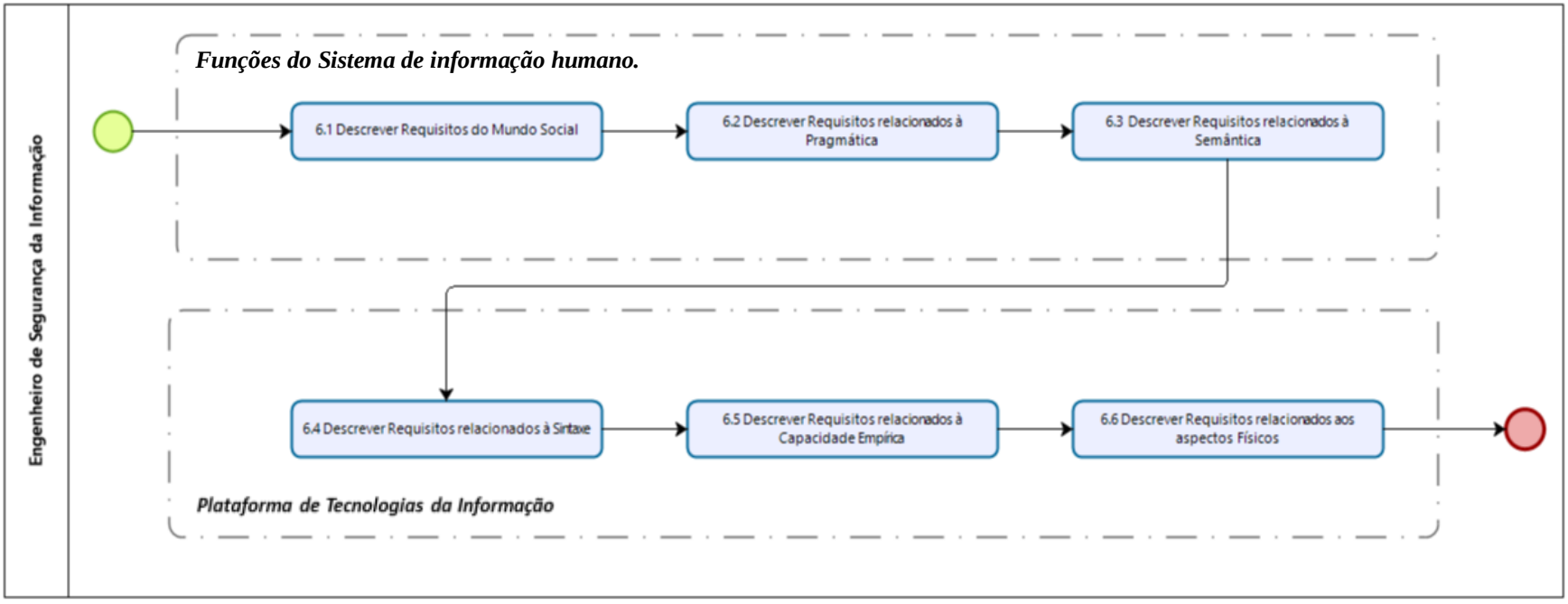


Figura 10 - Construção da Escada Semiótica

Passo 7: Gerar Artefatos de Requisitos de Segurança e Privacidade de Software

Ao final da execução do método, o Passo 7 do MARSPS (Figura 11) tem por finalidade gerar saídas de diferentes formatos, de acordo com as características e necessidades do projeto.

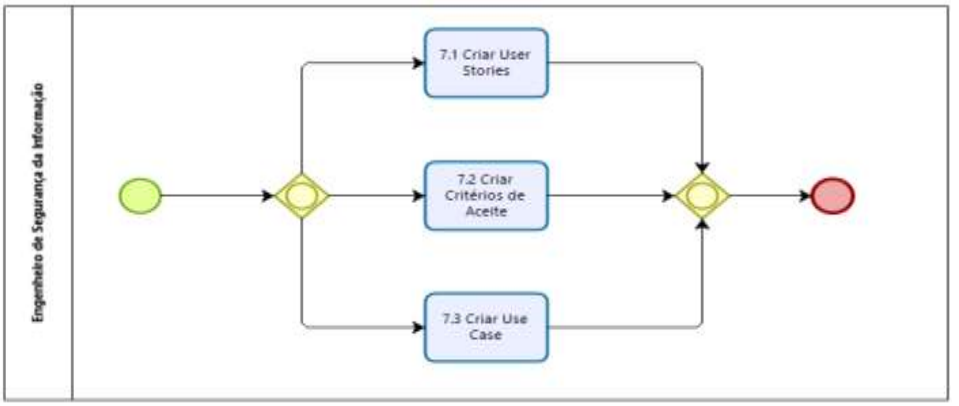


Figura 11 - Geração de Artefatos com Requisitos de Segurança e Privacidade de Software

Para gerar artefatos com requisitos de segurança e privacidade, as seguintes atividades são executadas:

- *Criar User Stories* (Item 7.1 da Figura 11)*: User Stories* (ou Estórias de usuário) são criadas ou adaptadas com base em necessidades, requisitos, ideias, problemas e soluções elencadas nos passos anteriores. As *User Stories* são utilizadas em metodologias ágeis.
- *Criar Critérios de Aceite* (Item 7.2 da Figura 11)*:* são elaborados critérios de aceite que devem contemplar necessidades, requisitos, ideias, problemas e soluções elencadas nos passos anteriores; estes critérios podem ser utilizados em projetos de sistemas de software que trabalham com uma abordagem hibrida, ou seja, a junção de métodos ágeis com metodologias tradicionais.
- *Criar Use Cases* (Item 7.3 da Figura 11)*: Use Cases* (Casos de uso) devem ser elaborados ou adaptados de acordo com necessidades, requisitos, ideias, problemas e soluções elencadas nos passos anteriores; os Casos de Uso podem ser utilizados em projetos de sistemas de software que requerem documentação mais rígida, ou seja, projetos que adotam metodologias tradicionais de desenvolvimento.

5. Aplicação Preliminar do MARSPS

Este capítulo apresenta resultados obtidos a partir da execução do MARSPS para aprimoramento de dois requisitos de sistemas da área financeira. Apresenta-se a execução do MARSPS (Seção 5.1) e considerações sobre os resultados desta execução (Seção 5.2).

5.1. Execução do MARSPS para enriquecer requisitos de sistemas da área financeira

Todos os passos e atividades do MARSPS foram executados, resultando em pelo menos uma instância de cada tipo de artefato descrito no capítulo anterior. O Apêndice A descreve os artefatos produzidos durante a execução preliminar do MARSPS, além de um *link* para os artefatos contendo todos os detalhes. As Seções 5.1.1 a 5.1.7 apresentam resultados da execução dos passos 1 a 7 (*c.f.*, Capítulo 4) respectivamente.

Os seguintes requisitos foram elencados para ilustrar a aplicação do método:

> **Requisito 1** – "*Enviar dados da fatura digital do titular do cartão por canais digitais*"; e
>
> **Requisito 2** – "*Enviar comprovantes de operações de transferência e pagamento de boletos bancários por meio de Mobile Banking e Internet Banking".*

5.1.1. Execução do Passo 1: identificar fontes de requisitos de segurança e privacidade

O pesquisador, no papel de engenheiro de segurança da informação, identificou as fontes de requisitos de segurança e privacidade. Houve a necessidade de recorrer a fontes de conhecimento de segurança confiáveis, tais como BACEN (2020), PCI (PCI-DSS, 2010), e também consultas às bases de vulnerabilidades conhecidas tais como CVE/OSVDB, visando aumentar a cobertura na identificação e correção de vulnerabilidades. Maiores detalhes podem ser encontrados no artefato A2 do Apêndice A.

5.1.2. Execução do Passo 2: identificar *stakeholders*

O pesquisador, no papel de engenheiro de segurança da informação, identificou os *stakeholders* principais para colaboração. Após a execução do Passo 2 do MARSPS, foi criado um artefato contendo todos os *stakeholders* candidatos para análise. Maiores detalhes podem ser encontrados no artefato A3 do Apêndice A. Os seguintes *stakeholders* foram inicialmente identificados: cliente, gerência de negócios, organizações legisladoras, governo, administradoras de cartões de crédito, bancos emissores, bancos credenciadores, engenheiro de requisitos, engenheiro de segurança da informação, engenheiro de software, arquiteto de softwares, arquiteto de testes, analistas de testes e cliente da aplicação (contratante).

5.1.3. Execução do Passo 3: analisar *stakeholders*

Os *stakeholders* principais, que foram identificados e listados no passo anterior, foram analisados. O processo de analisar *stakeholders* resultou no diagrama de stakeholders (Figura 12) detalhada no artefato A4 do Apêndice A. Pode-se observar que nesse artefato existem *stakeholders* em todos os níveis, com diferentes papéis e ligações com o sistema. Isso aponta para a demanda por uma análise aprofundada dos interesses e necessidades dos *stakeholders* em todos os níveis nos próximos passos do MARSPS.

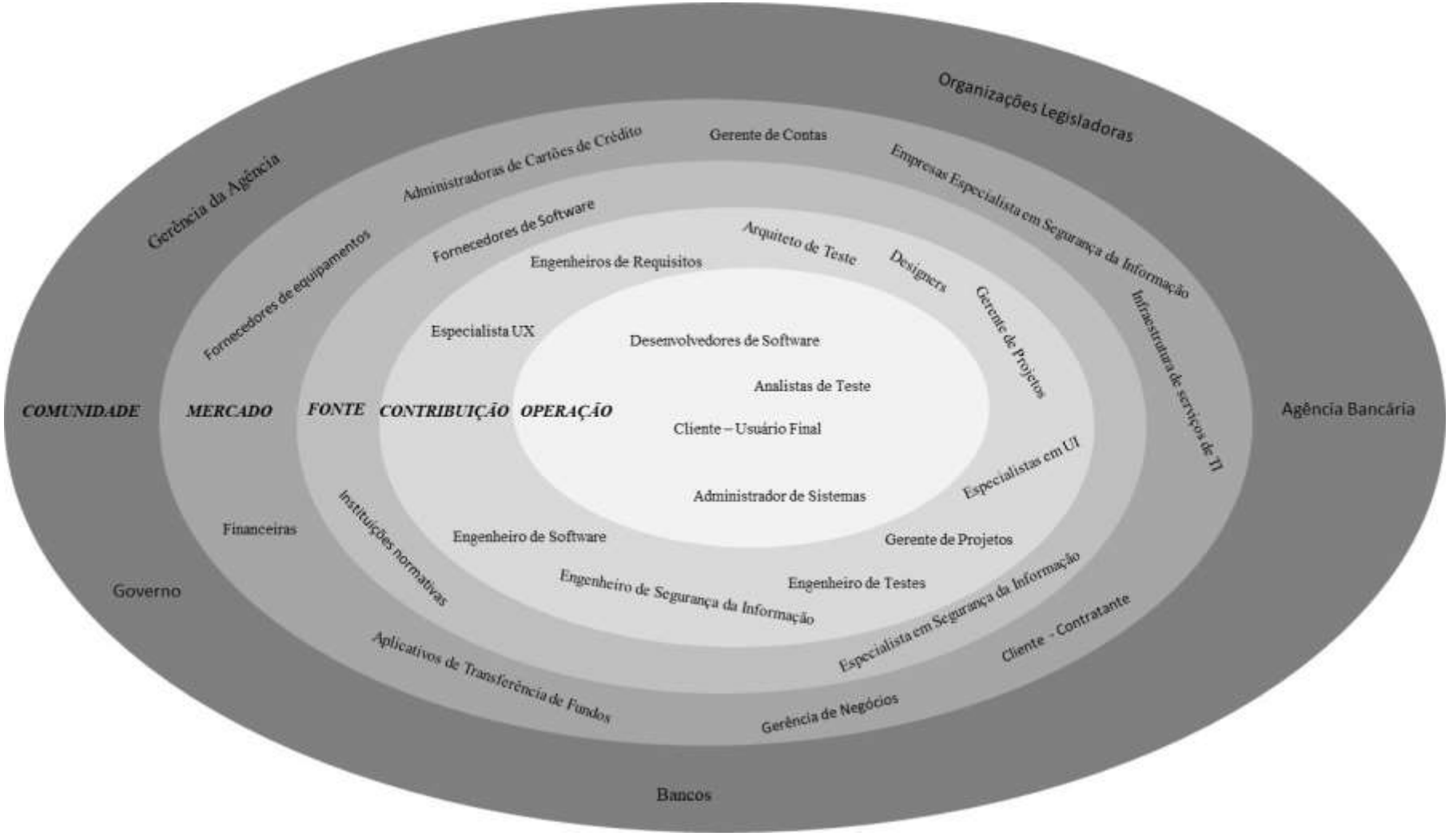


Figura 12 - Diagrama de Stakeholders construído para aplicação preliminar

5.1.4. Execução do Passo 4: listar interesses dos *stakeholders*

O pesquisador, no papel de engenheiro de segurança da informação, executou a atividade para listar os interesses dos *stakeholders*, após a execução deste passo foi gerado o artefato A5 do Apêndice A. Os itens seguintes são exemplos que ilustram necessidades dos *stakeholders* modeladas para o Requisito 1:

- *Stakeholder Cliente*: possuir mecanismos de segurança e privacidade que assegurem que seus dados e informações do seu histórico de compras não sejam interceptados e visualizados sem autorização.
- *Stakeholder Gerente de Projetos*: garantir que toda a equipe esteja envolvida com os objetivos de privacidade e segurança do projeto, além de considerar aspectos de produtividade e reduzir tempo de entrega.

5.1.5. Execução do Passo 5: analisar problemas e ideias

Neste passo foram analisados problemas e perguntas, bem como propostas de soluções e de ideias relacionadas a cada um dos *stakeholders*, identificados em cada um dos 5 níveis do Diagrama de *Stakeholders*: Comunidade, Mercado, Fonte, Contribuição e Operação. Os problemas apontados para cada um dos *stakeholders* estão detalhados nas Tabelas 11 a 15 do Apêndice B. A seguir são apresentados exemplos do nível *Comunidade*.

Stakeholder: **Agência Bancária**

Problemas e Questões: A proteção de dados e informações sensíveis nas organizações é uma atividade de fundamental importância e essa necessidade torna-se cada vez maior nas instituições financeiras como é o caso das agências bancárias. Diante de tais necessidades surge a necessidade de aprimorar os mecanismos de privacidade e segurança das informações. Com isso, como garantir a privacidade de dados e informações em sistemas existentes na agência bancária?

Soluções e Ideias: A necessidade de privacidade e segurança é algo que deve envolver todos na organização e com isso surge a necessidade de propor treinamentos e conscientização dos colaboradores para que a privacidade e segurança de dados e informações possam ser asseguradas na organização.

***Stakeholder:* Gerência da Agência**

Problemas e Questões: prover segurança e privacidade de dados e informações de utilizadores de aplicações sistêmica em ambientes de *Mobile Banking* e *Internet Banking* é um ponto crucial para as instituições financeiras. Para isso, a gerência das agências busca colaborar para garantir que a proteção de dados de clientes em aplicativos e sistemas bancários seja assegurada na utilização de canais digitais por seus clientes. Qual a necessidade da gerência da agência em relação a segurança e privacidade de informações em aplicações bancárias?

Soluções e Ideias: o problema da exposição de dados e informações dos *stakeholders* pode estar relacionada com a falta da cultura da proteção de dados e informações e com o desconhecimento do valor da informação que está sendo manipulada. Mediante as necessidades de privacidade e segurança, se faz necessário testar todas as aplicações simulando as necessidades dos clientes em suas agências bancárias de maneira a garantir que a proteção dos dados dos clientes possa ser assegurada durante a sua utilização.

***Stakeholder:* Governo**

Problemas e Questões: o governo publica normas e fiscaliza os sistemas utilizados por instituições da área financeira, buscando assegurar que instituições bancárias e outras instituições financeiras sigam todas as instruções determinadas pelo BACEN no que diz respeito a segurança e privacidade de dados. Como assegurar que as instituições financeiras estão seguindo as normas e determinações do governo em relação a privacidade de dados e informações de usuários em suas aplicações e sistemas?

Soluções e Ideias: mediante a necessidade de desenvolver sistemas que atendam às exigências das instituições financeiras e as normativas existentes no mercado financeiro, se faz necessário que as instituições sigam as determinações explicitas nas regulamentações do BACEN no desenvolvimento dos sistemas e aplicativos, proporcionando a seus clientes segurança e privacidade nas suas transações bancárias e no compartilhamento das informações resultantes dessas transações.

***Stakeholder:* Bancos**

Problemas e Questões: diferentes tipos de serviços são oferecidos para os usuários de aplicações bancárias e é necessário garantir que os produtos e serviços oferecidos possam cumprir os requisitos de segurança e privacidade dos seus clientes nos diversos canais digitais disponíveis. Como a instituição bancária poderá melhorar a segurança e privacidade das operações realizadas por seus clientes durante a utilização dos canais digitais?

Soluções e Ideias: para mitigar possíveis riscos relacionados ao ambiente bancário na utilização de sistemas e aplicativos, é de fundamental importância que sejam realizadas revisões nos serviços disponíveis. Isso é necessário para assegurar que a segurança e privacidade dos clientes está sendo mantida mediante às novas necessidades de aprimoramento das ferramentas disponíveis na Internet e aplicativos em dispositivos móveis. Dessa forma, o banco poderá garantir que os clientes farão uso seguro em todos os canais digitais da organização bancária.

***Stakeholder:* Organizações Legisladoras**

Problemas e Questões: as organizações legisladoras possuem um papel de grande destaque no cenário das instituições financeiras, pois criam determinações para que as instituições financeiras possam desenvolver seus sistemas de forma segura e respeitando a concorrência de mercado. Como assegurar que as organizações desenvolvam aplicações que garantam segurança e privacidade aos usuários?

Soluções e Ideias: as instituições financeiras precisam criar planos de desenvolvimento que busquem mitigar problemas de privacidade e segurança em transações por meio digital; por exemplo, no compartilhamento de comprovantes de transações efetuadas entre usuários de aplicações bancárias.

5.1.6. Execução do passo 6: avaliar requisitos

Após a construção do Quadro de Avaliação, os requisitos foram analisados em dois grupos de acordo com o *Framework* Semiótico. Conforme especificado pelo processo, no primeiro grupo buscou-se analisar os requisitos do ponto de vista das funções do sistema de informação humano, ou seja, neste grupo houve a necessidade de o engenheiro analisar os aspectos pragmáticos, semânticos e os relacionados ao mundo social, ligados às ideias e soluções levantadas no Quadro de Avaliação. No segundo grupo, que é relacionado à Plataforma de Tecnologias da Informação, foram analisados os aspectos sintáticos, empíricos e físicos.

A Figura 13 apresenta a Escada Semiótica construída para o requisito 1. Apresenta-se a análise em cada nível, contendo aspectos que podem levar a novos requisitos funcionais e não-funcionais do sistema, por exemplo: no nível social é indicada a necessidade de preservar a confiança subjetiva do sistema (não-funcional), já no nível sintático é destacada a necessidade de ter funcionalidades para escolher o formato da fatura a ser utilizado (funcional).

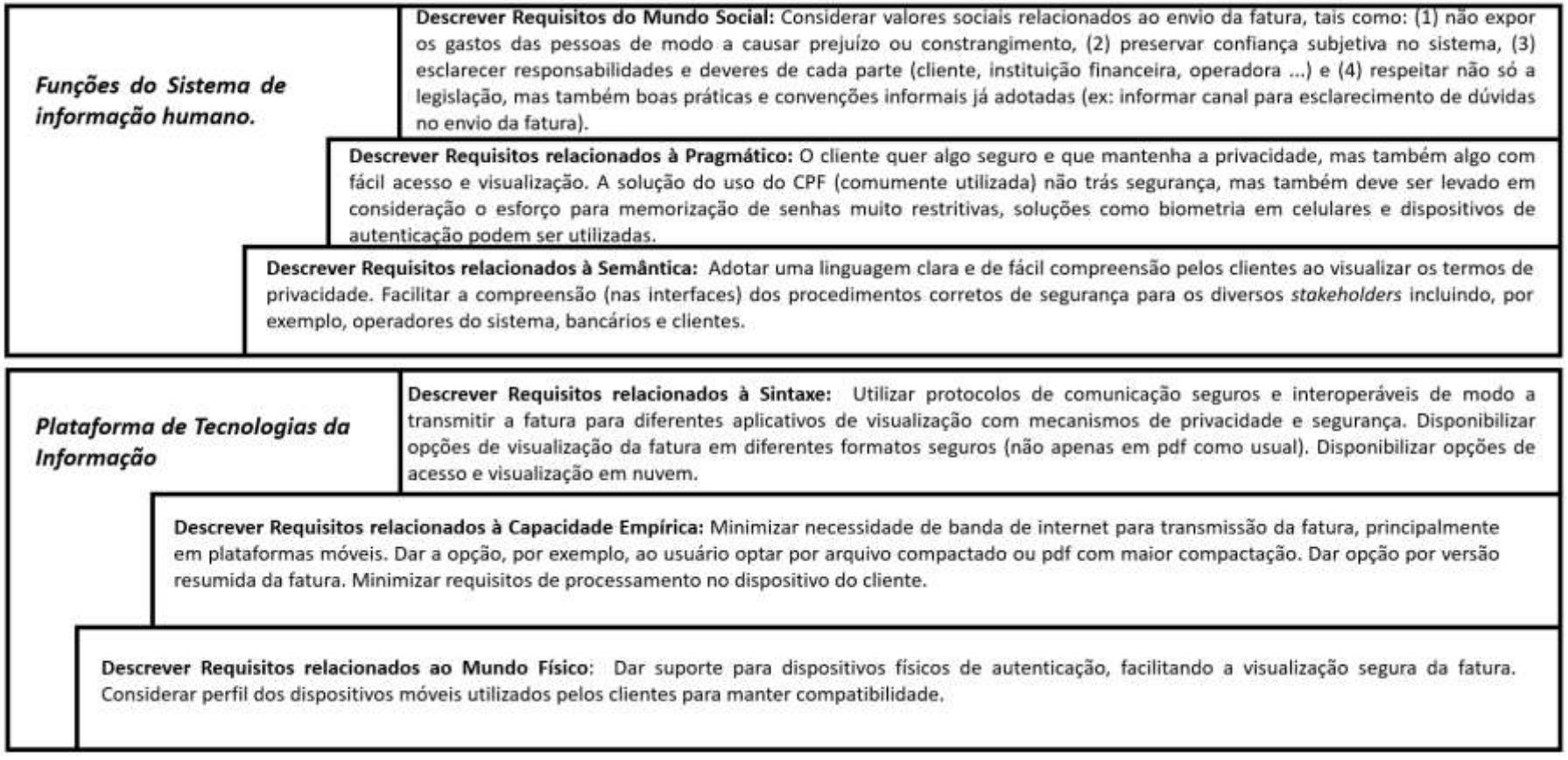


Figura 13 - Escada Semiótica para o Requisito 1

5.1.7. Execução do passo 07: gerar artefatos de requisitos de segurança e privacidade de software

Após ter executado todas as etapas do MARSPS, foram gerados artefatos de saída do método. Dentre os modelos de artefatos pospostos, optou-se por gerar *User Stories* e suas respectivas tabelas com critérios de aceite.

Este passo resultou na confecção de 2 *User Stories* (REQ_001 e REQ_002), que são detalhadas no Artefato 8 do Apêndice A. A seguir é apresentada uma narrativa de negócio (resumida) construída para o REQ_002, exemplos de regras de negócio e exemplos de critérios de aceites:

- REQ_002 – Narrativa de Negócio Resumida: *Atualmente os comprovantes gerados mediante transações bancárias podem ser compartilhados em qualquer veículo de comunicação digital sem que exista qualquer tipo de verificação sobre o dado que está sendo transmitido para um usuário ou mesmo grupos de usuários. O compartilhamento de comprovantes de transações bancárias pode expor a privacidade de clientes. Apesar disso, nos sistemas atuais não existem mecanismos que certifiquem que o cliente está ciente do risco alto de exposição de seus dados pessoais e financeiros. O sistema deveria, por exemplo, perguntar para o cliente se ele está de acordo em compartilhar o comprovante, e informar o conjunto de dados sensíveis e de interesse apenas do correntista ou destinatário da transação. Após o compartilhamento do comprovante, o cliente não terá mais controle dos dados compartilhados, e por isso também deve estar ciente dos ricos que envolve o compartilhamento.*
- Exemplos de Regras de Negócio para REQ_002:
    - Garantir que o cliente seja informado dos riscos do compartilhamento do comprovante gerado, quando utilizar *Mobile Banking* e *Internet Banking*;
    - Antes de enviar o comprovante para outro contato, o cliente deverá confirmar que o contato está correto e que assume a responsabilidade da exposição dos dados fora do domínio da aplicação.

- Exemplos de Critérios de Aceite para REQ_002:
    - Dado que foi gerado no comprovante de transações (transferência ou pagamento). Quando for gerado comprovante da transação bancária nas plataformas *Mobile Banking* e o *Internet Banking*. Então, o sistema deverá informar o cliente dos riscos do compartilhamento do comprovante gerado por meio da utilização de *Mobile Banking* e *Internet Banking*. Resultado: notificação gerada e o cliente está ciente dos riscos do compartilhamento do comprovante.
    - Dado que foi gerado no comprovante de transações (transferência ou pagamento). Quando for gerado comprovante da transação bancária nas plataformas *Mobile Banking* e o *Internet Banking*. Então antes de enviar o comprovante para um destinatário, o cliente deverá confirmar se o destinatário está correto e assumir a responsabilidade da exposição dos dados fora do domínio da aplicação. Resultado: o destinatário é confirmado pelo cliente.

5.2. Considerações sobre a execução preliminar do MARSPS

A execução preliminar do método mostrou sua viabilidade, bem como propiciou levantar ajustes que foram incorporados à versão atual. No Passo 1, foi possível selecionar 5 fontes de conhecimento, que foram úteis para o entendimento de problemas, bem como para gerar ideias e especificar requisitos nos passos posteriores. Isso reforça a necessidade do Passo 1, bem como aprofundar na busca por requisitos.

Nos passos 2 a 4 foram identificados, analisados e listados os interesses de 33 *stakeholders*. Isso propiciou uma visão ampla de quem são os *stakeholders* e quais são suas necessidades, influenciando para ter um conjunto maior de requisitos elicitados durantes os próximos passos. Esses passos foram trabalhosos, pois enquanto houver *stakeholders* a serem envolvidos no projeto, o Diagrama de *Stakeholders* deve passar por reformulação.

O Passo 5 foi essencial, ao proporcionar uma maneira organizada de levantar problemas e soluções relacionados a privacidade e segurança da informação. Entretanto,

foi o passo que demandou mais esforços, uma vez que além de identificar problemas e soluções é necessário relacionar ao nível e *stakeholders* envolvidos.

O passo 6, por meio da Escada Semiótica, fez com que os problemas fossem analisados em diversos níveis (do físico ao social) de maneira integrada em um mesmo diagrama. Isso ajudou a identificar as relações dos requisitos com diversos aspectos, tais com o equipamento utilizado, o entendimento do cliente e suas intenções. A execução do Passo 7 mostrou que os artefatos escolhidos foram capazes de representar os requisitos levantados.

Por fim, é importante destacar a necessidade de experimentação do método por especialistas no domínio, e não somente pelo pesquisador. Para tanto, foi realizado o estudo descrito no próximo capítulo.

6. Aplicação do MARSPS em Estudo de Caso com Especialistas

Este capítulo apresenta o estudo de caso da aplicação do MARSPS em cenário real com especialistas do domínio. Na Seção 6.1 são descritos os objetivos, o perfil dos participantes e o método de avaliação. A Seção 6.2 detalha os resultados (e artefatos) obtidos com a execução do método. Na Seção 6.3 é apresentada uma síntese dos resultados obtidos com as respostas do formulário de avaliação. Por fim, na Seção 6.4 apresenta-se uma discussão sobre os resultados do estudo de caso.

6.1. Objetivos, perfil dos participantes e método de avaliação

O MARSPS foi aplicado em um cenário do mundo real na área financeira, com objetivo principal de verificar sua viabilidade. Para tanto, foi realizado *Workshop* com a participação de especialistas em especificação de requisitos e segurança da informação que atuam na área financeira.

Participaram do *Workshop* 4 especialistas recrutados de maneira voluntária por meio de convites realizados pelo pesquisador em sua rede de contato pessoal. A Tabela 8 apresenta o perfil dos especialistas, sendo 2 da área de segurança da informação (Especialistas A e C) e 2 de áreas relacionadas à engenharia de requisitos (Especialistas B e D). Todos trabalham em empresas financeiras, sendo 3 de São Paulo, SP, Brasil, e 1 de Miami, Flórida, Estados Unidos. Todos os participantes têm graduação e especialização em áreas relacionadas à computação. Conforme detalha a Tabela 8, os participantes têm de 4 a 10 anos de experiência em suas respectivas áreas, e exercem atualmente as funções de: Engenheiro de Segurança, Analista Funcional, Analista de Segurança da Informação e Coordenador Comercial. Todos os especialistas, independentemente de suas experiências, executaram todas as etapas do método.

Os especialistas analisaram a utilização do MARSPS para enriquecimento de requisitos no seguinte cenário: *compartilhamento de recibos de transações bancárias realizadas em ambientes de Internet Banking e Mobile Banking*. Esses recibos contêm informações confidenciais que podem ser compartilhadas sem qualquer verificação pelos usuários e instituições, levando a riscos relacionados à privacidade e segurança. Neste

caso, é necessária uma análise rigorosa dos dados pessoais e dos requisitos, o que justifica a aplicação do método.

Tabela 8 - Perfil profissional dos participantes do estudo de caso

Nome	Formação Acadêmica	Função	Experiência Profissional
Especialista A	Graduação em Tecnologia em Processamento de Dados; MBA em Segurança da Informação.	Engenheiro de Segurança da Informação – área bancária.	10 anos
Especialista B	Graduação em Sistemas de Informação; Mestrado em Sistemas de Informação.	Analista Funcional – área financeira (Bandeira de Cartões).	5 anos
Especialista C	Graduação em Tecnologia em Sistemas para Internet; Especialização em Gestão de Tecnologia da Informação.	Analista de Segurança da Informação.	4 anos
Especialista D	Graduação em Sistemas de Informação; Especialização em Sistemas de Informação.	Coordenador Comercial – área financeira.	5 anos

As seguintes atividades foram adotadas durante o *Workshop*:

- *Atividade 1:* O pesquisador realizou uma apresentação do MARSPS, detalhando cada passo que compõe o método, as atividades a serem realizadas e exemplos dos artefatos a serem produzidos. Após a apresentação os participantes puderam discutir e tirar dúvidas sobre o MARSPS.
- *Atividade 2:* O cenário real supracitado foi apresentado aos participantes, destacando principalmente os aspectos de segurança e privacidade. O procedimento de avaliação foi apresentado e os participantes puderam sanar suas dúvidas antes do início da avaliação.
- *Atividade 3:* Os participantes executaram o MARSPS com foco em atender demandas de privacidade e segurança para o cenário de compartilhamento de recibos de transações bancárias. A execução incluiu todas as atividades do MARSPS, desde o recebimento dos requisitos até a geração dos artefatos necessários para o enriquecimento/robustecimento destes requisitos.
- *Atividade 4:* Por fim, os participantes responderam um questionário online no aplicativo Google Forms. O Apêndice C apresenta este questionário, que inclui questões de múltipla escolha utilizando a escala *Likert* e questões dissertativas onde puderam opinar livremente sobre as características e passos do MARSPS.

Cada participante demorou por volta de 3h:30m para executar todos as atividades do método e responder o formulário (Atividades 3 e 4). O método foi executado individualmente, sem comunicação entre os participantes.

Os resultados da avaliação com especialistas foram obtidos de forma individual, ou seja, o processo foi inteiramente executado em paralelo pelos quatro participantes. Ao final, o pesquisador realizou uma síntese e consolidou os dados individuais em uma narrativa coletiva. Tal narrativa, apresentada na próxima seção, expressa o consenso e a divergência do grupo em relação aos passos do MARSPS.

6.2. Resultados da Execução do MARSPS

Esta seção detalha os resultados e artefatos obtidos em cada passo durante a execução do MARSPS, estruturados em subseções apresentadas a seguir. Esses resultados foram obtidos por meio de relatos dos participantes e observações do pesquisador durante a execução do método. Tais resultados são complementados por respostas ao formulário de avaliação analisadas na Seção 6.3.

6.2.1. Passo1: Identificar Fontes de Requisitos

No Passo 1, os especialistas sugeriram fontes de requisitos ligados ao sistema financeiro (*e.g.*, BACEN e PCI-DSS), bem como bases de dados de vulnerabilidades conhecidas (*e.g.*, CVE/OSVBD) e fontes de requisitos de segurança e privacidade (*e.g.*, OWASP *Testing Guide*). Os especialistas avaliaram se as fontes eram suficientes para realizar o aprimoramento dos requisitos.

Para um maior aprofundamento nas fontes de segurança da informação foi sugerido usar tecnologias de priorização de risco de vulnerabilidades, tais como Kenna Security[12] e Tenable.io (ou Tenable.sc)[13] (sistemas de gestão de vulnerabilidades baseada em risco); estas ferramentas gerenciam vulnerabilidades, priorizando as mais críticas, *i.e.*, as que representam risco iminente de exploração por possuírem *exploit* (software de exploração da vulnerabilidade) disponível publicamente.

Um dos especialistas considerou as fontes suficientes para o cenário, mas também recomendou considerar outros *frameworks* (*e.g.*, NIST Cybersecurity[14] e

[12] https://www.kennasecurity.com/
[13] https://www.tenable.com/
[14] https://www.nist.gov/cyberframework

COBIT[15]). Outro especialista sugeriu GDPR[16], CCPA[17], LGPD, e ISO 27001. A Tabela 9 apresenta uma síntese das fontes sugeridas, incluindo uma breve descrição.

Tabela 9 - Síntese das Fontes Sugeridos pelos Participantes no Passo 1

Fontes	***Descrição***
CVE/OSVBD	Listas de vulnerabilidades de softwares conhecidas.
OWASP *Testing Guide*	Guia para testar a segurança de aplicativos e serviços da web.
BACEN	Normas e resoluções de segurança emitidas pelo BACEN, aplicadas ao sistema financeiro brasileiro.
Kenna Security	Sistema de gestão de vulnerabilidades baseada em risco.
Tenable.io/ Tenable.sc	Conjunto de ferramentas para gestão de vulnerabilidades baseada em risco.
NIST Cybersecurity	*Framework* para avaliar capacidades de prevenção, detecção e resposta a ataques cibernéticos.
COBIT	*Framework* de boas práticas para a governança de TI.
GDPR	Regulamento europeu sobre privacidade e proteção de dados.
CCPA	Estatuto sobre direitos de privacidade e proteção do consumidor do estado da Califórnia - EUA.
LGPD	Legislação brasileira de proteção de dados pessoais.
ISSO/IEC 27001	Padrão para gestão da segurança da informação.

6.2.2. Passo 2: Identificar *Stakeholders*

No Passo 2, todos os especialistas sugeriram que a atividade de identificar os *stakeholders* foi fácil, uma vez que foram auxiliados pela descrição deste passo no MARSPS, que sugere diferentes tipos de *stakeholders*.

Neste passo foi possível identificar os *stakeholders* que poderiam contribuir ou que teriam interesse no projeto de aprimoramento de requisitos do cenário em questão, totalizando 8 perfis de *stakeholders*. A identificação de *stakeholders* é uma atividade que apresenta vantagens para o projeto, pois uma vez identificados de maneira correta, estes podem explicitar suas necessidades e contribuir para o projeto. Entretanto, os especialistas apontaram a dificuldade de conseguir disponibilidade na agenda dos *stakeholders* experts de domínio para que possam participar de forma ativa do projeto. No total, 8 perfis de *stakeholders* foram levantados pelos participantes (*e.g.*, clientes e administradora de cartões de crédito).

[15] https://www.isaca.org/bookstore/cobit-5/wcb5b
[16] https://gdpr-info.eu/
[17] https://oag.ca.gov/privacy/ccpa

6.2.3. Passo 3: Analisar *Stakeholders*

No Passo 3, todos os especialistas indicaram que o Diagrama de *Stakeholders* proporciona para a organização uma visão ampla/holística dos papéis e responsabilidades de todos os *stakeholders* do projeto de aprimoramento de requisitos da área financeira. Os especialistas relataram que não tiveram dificuldades no entendimento dos níveis do Diagrama de *Stakeholders*, bem como no posicionamento correto dos *stakeholders* no Diagrama de *Stakeholders*.

Os participantes consideraram uma vantagem poder delimitar bem as percepções de cada *stakeholde*r em cada camada do diagrama. Segundo os participantes, um ponto que deve ser levado em consideração é que quanto maior for o conjunto de requisitos maior será a quantidade de *stakeholders* a serem identificados e analisados, aumentando assim a complexidade para construir o Diagrama de *Stakeholders* e representá-los todos em um único diagrama.

Ao final, os participantes analisaram todos os *stakeholders* identificados na etapa anterior. Entretanto, cabe ressaltar que na proposta do MARSPS existe uma condição no final do Passo 3, que diz que somente pode seguir para o próximo passo se todos os *stakeholders* foram identificados e analisados. Por motivo de simplicidade e tempo de execução, os participantes não retornaram ao Passo 2 para identificar novos *stakeholders*.

6.2.4. Passo 4: Listar Interesses dos *Stakeholders*

Neste passo, os participantes descreveram as necessidades de privacidade e de segurança dos *stakeholders* previamente listados com foco no cenário proposto. No total, 18 necessidades de privacidade e segurança foram identificadas, o que mostra a viabilidade da atividade. Entretanto, os especialistas destacaram dificuldades para atender às demandas dos *stakeholders*.

Três especialistas concordaram que os *stakeholders* poderiam ter dificuldades para expressar suas próprias necessidades, pois poderiam não entender requisitos, aspectos de segurança, problemas com custo e tempo, etc. Dentre as dificuldades apontadas estão o atendimento dos requisitos considerando custo, tempo e tecnologia de forma equilibrada.

Adicionalmente, foi apontada a falta da cultura de segurança e privacidade entre os *stakeholders*.

6.2.5. Passo 5: Analisar Problemas e Soluções

Neste passo, os especialistas apontaram vantagens e desvantagens no uso do Quadro de Avaliação.

Como vantagens os especialistas identificaram que o Quadro de Avaliação é útil para definir e priorizar os requisitos, assim como identificar as vulnerabilidades pré-existentes que podem ser tratadas. Também foi apontada a visibilidade e organização que o Quadro de Avaliação proporciona sobre os requisitos de cada *stakeholder*, nos permitindo analisar e discutir o real impacto de cada requisito e propor melhorias para cada cenário. Como desvantagens, os especialistas apontam que a elaboração do quadro de avaliação pode demandar muito tempo, principalmente elencando soluções que não podem ser aplicadas, além de que o número de ideias e soluções pode ser muito grande, aumentando muito o tamanho do projeto.

Foram definidos e priorizados 10 problemas (*e.g.*, problemas de infraestrutura, problemas de contratação, dificuldades no entendimento por parte dos usuários, etc.), assim como foram identificadas 3 vulnerabilidades pré-existentes. Ao final da execução deste passo, com a análise de problemas e soluções identificadas, os especialistas foram capazes de gerar um artefato contendo o Quadro de Avaliação para o requisito compartilhamento do comprovante de transação bancária em ambientes *Internet Banking e Mobile Banking*.

6.2.6. Passo 6: Avaliar Requisitos

Neste passo, de maneira geral, os especialistas apontaram que o *Framework* Semiótico (Escada Semiótica) é adequado para identificar e gerir requisitos de segurança e privacidade de forma dinâmica nos diversos níveis. Segundo os especialistas, isso nos permite envolver os *stakeholders* e fornecer visões geral e personalizada dos processos da organização. Todos os participantes concordaram que os níveis do *Framework* Semiótico que trata das funções do sistema de informação humano são muito importantes para que

se possa entender o impacto do requisito a ser aprimorado em diferentes setores das organizações, assim como para os *stakeholders* que fazem uso de aplicações no dia a dia. Um especialista apontou que o *Framework* Semiótico pode ser útil para análise da maturidade de segurança da empresa.

Como desvantagem, foi apontado que o uso da Escada demanda tempo e é um pouco burocrático, tornando o processo menos ágil. Por outro lado, ressalta-se que mesmo que seja um processo ágil de desenvolvimento, aspectos de privacidade e segurança não podem ser negligenciados, pois poderia resultar em possíveis vulnerabilidades quando o sistema estiver em operação. Foram definidos e priorizados 10 requisitos potenciais, entre requisitos não-funcionais (*e.g.*, adotar uma linguagem de fácil compreensão) e funcionais (*e.g.*, usar outra chave de bloqueio de visualização da fatura no lugar do CPF).

6.2.7. Passo 7: Gerar Artefato de Requisitos de Segurança e Privacidade de Software

No último passo, os especialistas não relataram dificuldades para escolher o modelo de artefato adequado à abordagem metodológica adotada em suas respectivas empresas. Todos os especialistas optaram pelo artefato *User Stories*, com o objetivo de conciliar a construção do artefato com a prática de desenvolvimento ágil (existente em suas respectivas organizações). Esta preferência foi decorrente do fato de todos atuarem em organizações que utilizam metodologias ágeis. Além disso, destacaram que este artefato pode gerar vantagens ao projeto e consequentemente para todas as equipes envolvidas (incluindo a equipe que irá atuar na implementação do requisito) devido à sua facilidade de leitura.

Os participantes também destacaram que os artefatos sugeridos são capazes de representar adequadamente os requisitos aprimorados e seus respectivos detalhes. Um especialista sugeriu que mudasse na descrição do método o nome “artefato” pois é um termo comum na área de forense computacional. No total, 2 requisitos iniciais foram aprimorados (envio da fatura digital de cartão de crédito; e recibos de operações de transferência bancária e de pagamento de boletos) e 8 requisitos de privacidade e segurança foram propostos (*e.g.*, elaboração de senha exclusiva para acesso da fatura

digital com a utilização de caracteres maiúsculos e minúsculos, números e caracteres especiais; e informar ao cliente os riscos do compartilhamento do comprovante gerado).

6.3. Resultados do Formulário de Avaliação

No final do *Workshop*, após utilizar o MARSPS, os participantes responderam a um questionário com questões dissertativas e de múltipla escolha (escala *Likert*). Primeiramente, serão apresentados os resultados das questões de múltipla escolha. O Apêndice C apresenta o formulário de avaliação completo.

Na Figura 14 são apresentados os resultados das duas questões de múltipla escolha relacionadas aos *stakeholders* do projeto, a saber: *Q 4.2* (*Os stakeholders descrevem suas necessidades de segurança e privacidade de forma clara e objetiva?*) E *Q 4.3* (*Como avalia a importância do envolvimento dos stakeholders durante a atividade de identificação dos requisitos?*). Com relação a Q 4.2, *75%* dos participantes apontaram que os *stakeholders* são capazes de descreverem suas necessidades (1 concordou totalmente e 2 concordaram parcialmente). Já em relação a Q 4.3, todos concordaram que o envolvimento dos *stakeholders* no projeto é importante.

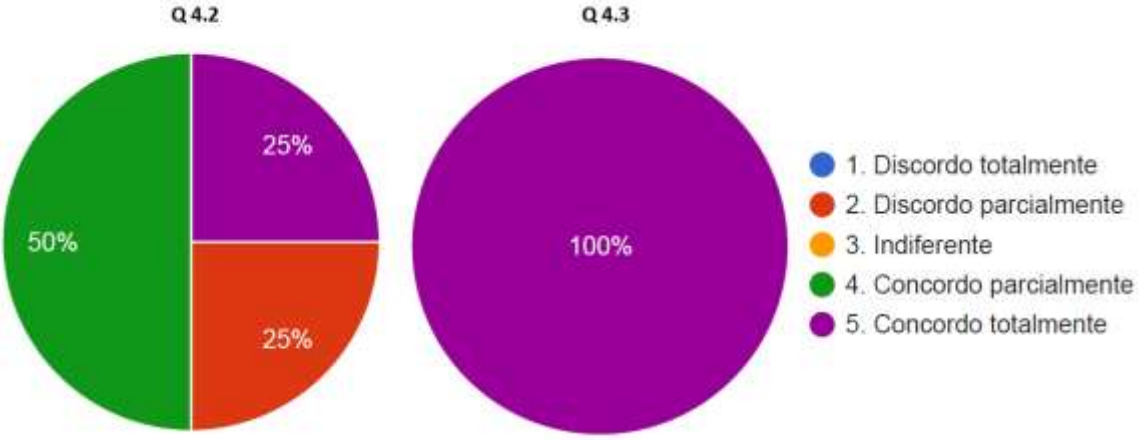


Figura 14 – Resultados das questões de múltipla escolha sobre a participação dos Stakeholders no MARSPS

A Figura 15 apresenta o resultado da questão de múltipla escolha sobre a importância do Quadro de Avaliação (*Q 5.2*): *A construção do Quadro de Avaliação contribuiu para um melhor entendimento na resolução dos problemas relacionados com*

as necessidades de privacidade e segurança dos requisitos identificados? Após o uso do método, todos os participantes concordaram totalmente que o Quadro de Avaliação contribui para um melhor entendimento do problema.

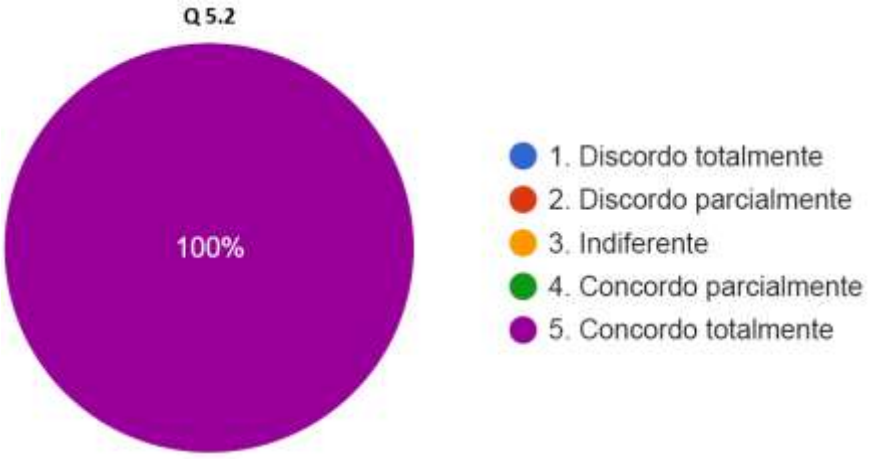


Figura 15 – Resultado de questão de múltipla escolha sobre a contribuição do Quadro de Avalição.

A Figura 16 destaca os resultados das duas questões de múltipla escolha relacionadas ao artefato Escada Semiótica, a saber: *Q 6.1* (*Como você avalia as "Funções do Sistema de Informação Humano" na construção da Escada da Semiótica para o aprimoramento de requisitos da área financeira?*) e *Q 6.2* (*Como você avalia a "Plataforma de Tecnologia da Informação" na construção da Escada Semiótica para o aprimoramento de requisitos da área financeira?*). Todos os participantes concordaram totalmente, tanto para as funções do sistema de informação humano, quanto para a plataforma de tecnologia da informação.

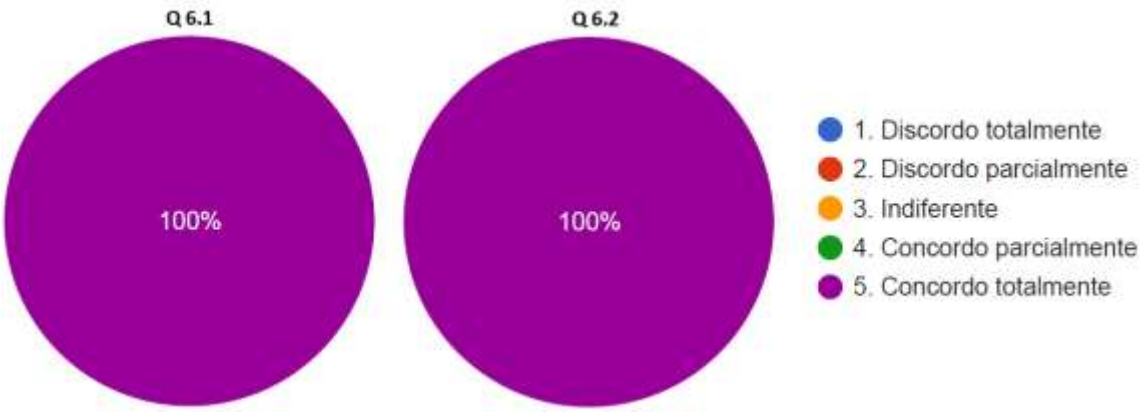


Figura 16 – Resultados de questões de múltipla escolha sobre a Escada Semiótica.

A Figura 17 apresenta o resultado da questão de múltipla escolha sobre resultados MARSPS (*Q 7.1*): *Você considera que saídas apresentadas na execução do MARSPS são*

suficientes para gerar artefatos de requisitos? Todos os participantes concordaram que as saídas são suficientes, sendo que 3 concordaram totalmente e 1 concordou parcialmente.

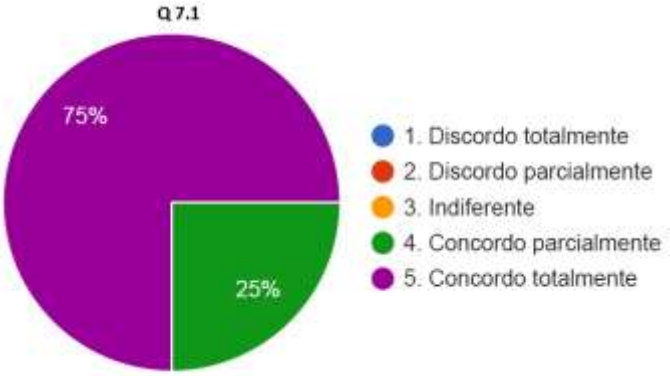


Figura 17 – Resultado de questão de múltipla escolha sobre as saídas do MARSPS.

A Figura 18 apresenta os resultados das duas questões "gerais" de múltipla escolha relacionadas ao MARSPS, a saber: *Q.Geral 1* (*Na execução do MARSPS para aprimorar requisitos da área financeira a sequência de passos foi suficiente?*) E *Q.Geral 2* (*Você consideraria o MARSPS como um instrumento para apoiar no aprimoramento dos requisitos da área financeira?* Todos os participantes concordaram totalmente que os passos foram suficientes, bem como concordam totalmente que o MARSPS é um instrumento adequado para aprimorar requisitos com respeito a aspectos de segurança e privacidade.

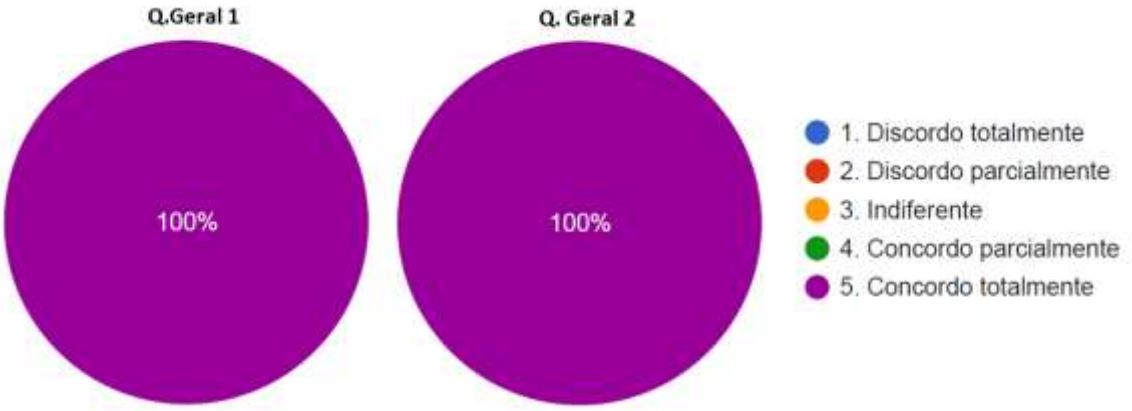


Figura 18 – Resultados sobre questões gerais de múltipla escolha sobre o MARSPS.

As questões dissertativas buscavam avaliar cada passo do MAPSPS, bem como levantar sugestões de melhorias para o método. A Tabela 10 apresenta uma síntese das vantagens e facilidades de cada passo do método, bem como as respectivas desvantagens

e dificuldades encontradas. Esta tabela foi construída pela síntese e interpretação das respostas obtidas nas questões dissertativas.

Para explicar a construção e conteúdo da Tabela 10, pode-se considerar o primeiro item apontado como vantagens e facilidades: "*Ajuda a identificar fontes corretas para obter a informação necessária para o projeto de aprimoramento de requisitos*". Esta é uma síntese de um conjunto de repostas às questões abertas para o Passo 1 (ver Apêndice C), que inclui várias respostas dos participantes, como (para citar algumas): "*Em um primeiro momento, sim, pois abrange as perspectivas de vulnerabilidades de uma forma que consigam ser explanados e aprimorados os diferentes aspectos relacionados à segurança e privacidade*"; *e "Sim, as fontes de privacidade e segurança são suficientes, porém, devem ser utilizadas as suas últimas versões disponibilizadas. São fontes suficientes por se tratar de fontes seguras, especializadas e as mais utilizadas pelo mercado como parâmetros de segurança para a área financeira."*. Os demais itens da tabela, seguem a mesma lógica, ou seja, cada item da tabela corresponde à síntese de um conjunto de respostas longas que foram interpretadas e revisadas pelo pesquisador.

Tabela 10 - Síntese das repostas dissertativas do formulário de validação do MARSPS

	Vantagens e Facilidades	**Desvantagens e Dificuldades**
Passo 1	- Ajuda a identificar fontes corretas para obter a informação necessária ao aprimoramento de requisitos. - Detalha as atividades para identificar as fontes de requisitos.	- Não foram identificadas desvantagens ou dificuldades.
Passo 2	- Proporciona identificar e envolver os possíveis *stakeholders* logo no início do projeto de aprimoramento de requisitos. - Proporciona maior clareza no entendimento dos *stakeholders*. - Ajuda a identificar quais *stakeholders* poderão participar do projeto.	- É difícil manter todos os *stakeholders* envolvidos e principalmente alinhados com a discussão do projeto de aprimoramento de requisitos. - Pode faltar comprometimento por parte de alguns s*takeholders*.
Passo 3	- Ajuda a analisar o envolvimento dos *stakeholders* com o objetivo do projeto. - Delimita a percepção e grau de envolvimento de cada uma das partes interessadas.	- É difícil saber qual *stakeholder* deverá ficar em cada um dos níveis da Cebola Organizacional/ Diagrama de *Stakeholders*.
Passo 4	- Proporciona clareza e objetividade na identificação das necessidades de privacidade e segurança da informação. - Garante o correto entendimento da necessidade do requisito a ser aprimorado. - Proporciona a organização da estrutura do projeto de aprimoramento com todos os envolvidos.	- É difícil listar todas as necessidades dos *stakeholders* mediante escopo e custo do projeto. - Dificuldade em visualizar como atender as necessidades dos *stakeholders* de forma equilibrada, levando em consideração escopo e custos do projeto de aprimoramento de requisitos.

Passo 5	- Ajuda a priorizar os requisitos a serem aprimorados. - Facilita a identificação de vulnerabilidades existentes. - Estrutura as necessidades de privacidade e segurança em cada nível apontado no Diagrama de *Stakeholders*. - Organiza os pontos importantes a serem executados pelos especialistas do domínio da aplicação. - Foca nas reais necessidades relacionadas ao sistema a ser aprimorado.	- Consome muito tempo para analisar problemas e propor soluções para cada necessidade de privacidade e segurança apontada por cada um dos *stakeholders*.
Passo 6	- Ajuda a avaliar o impacto que o requisito irá causar em cada um dos grupos da Escada Semiótica. - Proporciona uma avaliação que inclui tanto fatores humanos como tecnológicos. - Proporciona clareza e objetividade no detalhamento das necessidades dos *stakeholders* em cada um dos dois grupos da Escada Semiótica. - Pode de ser utilizado para análise de maturidade. - Propicia visão dos impactos que o aprimoramento dos requisitos irá causar nos sistemas da organização. - Propicia mapeamento e detalhamento claros das necessidades dos *stakeholders* em cada nível.	- A quantidade de etapas a serem seguidas para construir a Escada Semiótica é muito grande, podendo engessar o processo na organização. - Dificuldade em associar as necessidades de privacidade e segurança de maneira correta em cada um dos dois grupos que compõe a Escada Semiótica.
Passo 7	- Permite gerar artefatos de acordo com a metodologia de desenvolvimento de sistemas adotada na organização. - Permite gerar documentos de fácil atualização.	- Não foram apontadas desvantagens ou dificuldades na execução desse passo.

Quando questionados sobre sugestões de alterações e melhorias nos passos descritos no MARSPS (ver questões no Apêndice C), as seguintes respostas forma obtidas:

- Um participante relatou que a proposta atual é suficiente: "*Acredito que a proposta está suficiente.* "
- Outro participante destacou a necessidade de estudos constantes sobre o tema e que sejam utilizadas sempre as fontes de requisitos mais atuais: "*Gostaria apenas de mais uma vez reforçar que o tema exige muita atenção e estudos constantes para um levantamento de requisitos corretos e reais. Desta forma, como melhoria proponho que na fase 1 sejam observados nas fontes de requisitos de privacidade e segurança as versões mais atualizadas disponíveis. É um item de extrema importância e que pode impactar diretamente no risco ao negócio.* "
- Outro participante sugeriu utilizar técnicas de visualização para melhor entendimento dos requisitos elencados: "*Talvez sugeriria utilizar gráficos e tabelas visuais utilizando o Power BI, por ser um APP que gera views personalizáveis e que possam atender diferentes demandas.* "
- Também foi destacado que o método poderia ser mais flexível, bem como a necessidade de um estudo em uma empresa. "*Sugiro a mudança de alguns termos e avaliar a possibilidade de ser bem flexível para a aplicabilidade em*

qualquer organização. Sugiro também fazer um experimento com alguma empresa de médio porte que precisa estar em conformidade com a LGPD. ”

A última questão do formulário busca coletar as diferenças do MARSPS em relação a outros métodos existentes (ver questões no Apêndice C). As seguintes respostas foram obtidas:

- Um participante relatou como diferencial a capacidade de adaptação do MARSPS a diferentes metodologias de desenvolvimento: “*Uma vantagem é a possibilidade de se adequar a diferentes metodologias de desenvolvimento. É fortemente adaptável, sob minha visão.* ”
- Outro participante destacou a contribuição do MAPSPS para o levantamento de requisitos de privacidade e segurança, uma vez que segundo ele esta é uma área negligenciada e o MAPSPS pode contribuir para gerar uma cultura de segurança: “*Pela minha experiência profissional, as fases de levantamento de requisitos de privacidade e segurança para aprimoramento de softwares da área financeira é extremamente negligenciada. Principalmente quando pensamos que o cenário real hoje, mesmo em grandes corporações, é de se pensar nestes requisitos depois que as soluções estão prontas, ou seja, onde o custo de tempo e investimento para as melhorias e correções é muito maior. Com o MARSPS, que na minha visão apresenta uma proposta bastante interessante, clara, objetiva e seria de se tratar o tema de privacidade e segurança em projetos de melhoria de sistemas de software da área financeira, o ganho em tempo, maturidade, segurança e privacidade se torna algo real e justificável. São fases bem desenhadas e de fácil implementação. Mostra seu valor garantindo uma menor exposição a riscos para estes sistemas e cria a cultura de segurança que tanto se almeja. ”*
- Outro participante destacou um aspecto relacionado às licenças, uma vez que o MARSPS é público e não está atrelado a consultorias: “*A diferença principal pode estar relacionada a custos de software como licenças.* ”
- Também foi destacado que o método poderia ser utilizado para avaliação de software: “*Para avaliação de software, se o framework estiver cobrindo o OWASP, não me lembro desta parte, acho neste caso eficaz.* ”

6.4. Discussão sobre os Resultados Obtidos

Esta seção detalha os resultados obtidos dos formulários. Os resultados estão alinhados com os relatos dos participantes e observações do pesquisador durante a execução do método (Seção 6.3). De maneira geral, esses resultados apontam que o MAPSPS apresentou vantagens, tais como proporcionar para a organização e colaboradores um processo sistemático e uma visão ampla do que precisa ser feito para garantir a segurança e privacidade. Segundo os especialistas, também é possível evitar retrabalho e mitigar riscos com o aprimoramento de requisitos.

Os participantes também apontaram para desvantagens relacionadas ao tempo necessário para execução dos passos propostos, bem como para dificuldades para envolver os *stakeholders* no processo. Entretanto, é importante salientar que existem questões complexas ligadas à privacidade e segurança que devem ser minuciosamente e sistematicamente analisadas, o que dificulta a elaboração de métodos mais leves. Uma maior integração do MAPSPS com metodologias ágeis já existentes nas respectivas organizações pode ser um caminho de pesquisas focadas em tornar o método mais ágil.

Aspectos relacionados com a atualização constante do método foram destacados como sugestões, por exemplo, levar em consideração novas versões das fontes trabalhadas e até mesmo novas fontes de requisitos. Além disso, se faz necessária a execução das atividades por um período maior. Por exemplo, durante a avalição não foi possível retornar do passo 3 ao passo 2 devido a limitação de tempo, impossibilitando assim identificar todos os *stakeholders*. Os participantes também destacaram a necessidade de um estudo em uma empresa, em ambiente real, para uma maior abrangência da utilização do método. Isso aponta para necessidade de estudos de longo prazo para analisar possíveis evoluções e adaptações do método e torná-lo um produto pronto para o mercado (o que está fora do escopo desta dissertação).

Por fim, os participantes reportaram que o MAPSPS é um método flexível, que pode trazer contribuições para criar uma cultura de segurança nas organizações, destacando que este é um método gratuito. Eles também vislumbram a possiblidade de aplicação futura do método na avaliação de software, destacando, assim, o potencial de aprimoramento e uso do MAPSPS em projetos futuros.

7. Conclusão

Com a expansão do uso da computação no dia a dia surgiram novas preocupações e desafios relacionados com questões ligadas à segurança da informação e privacidade. Isso fez surgir novos requisitos de software que possuem caráter interdisciplinar. A complexidade e abrangência de tais requisitos apontam para a necessidade de novos métodos e processos de levantamento e enriquecimento de requisitos de sistemas da área financeira ligados a privacidade e segurança da informação. Para tanto, esta dissertação se aprofunda no tema e propõe o método MARSPS. A Seção 7.1 apresenta as principais contribuições desta pesquisa; a Seção 7.2 destaca as limitações e aponta trabalhos futuros; e, por fim, a Seção 7.3 apresenta as considerações finais desta dissertação.

7.1. Contribuições

Esta dissertação apresenta contribuição para as áreas de Engenharia de Software e Segurança da Informação, mais especificamente para o levantamento e especificação de requisitos de privacidade e segurança da informação de software financeiro.

Com o objetivo de responder à questão de pesquisa que norteia este trabalho "*Como a Semiótica Organizacional poderá contribuir para a criação de um método para enriquecimento de requisitos de sistemas financeiros que considere aspectos de privacidade e segurança da informação?* ", foram realizados estudos que resultaram na especificação do método MARSPS, que consiste na principal contribuição desta pesquisa. A seguir são destacadas as contribuições obtidas nesta dissertação.

- ***Revisão Sistemática*** *(Artigo)*. A revisão sistemática sobre a aplicação da semiótica no contexto da elicitação de requisitos de privacidade de dados, permitiu identificar trabalhos e soluções que utilizam a semiótica como um instrumento para identificação e modelagem de requisitos. Esta revisão clarificou como os métodos foram utilizados por esses trabalhos, bem como as possíveis contribuições da semiótica para o problema em questão. Os estudos selecionados pela revisão destacam que a comunicação com os *stakeholders* no processo de elicitação de requisitos é um aspecto chave, bem como propõem modelos e artefatos baseados em semiótica que podem ajudar a aprimorar a comunicação.

Entretanto, não forram identificados estudos que utilizam a semiótica para a elicitação de requisitos não-funcionais de privacidade e segurança, sendo esta uma contribuição única desta dissertação. Esta revisão resultou na publicação do artigo científico intitulado "Uma Revisão Sobre o Uso da Semiótica na Análise e Especificação de Requisitos de Privacidade" publicado no XV Workshop de Computação da UNIFACCAMP, 2019.

- ***MARSPS*** (*Especificação do método e Artigo*). A especificação completa do método MARSPS visa apoiar engenheiros de requisitos e engenheiros de segurança da informação no enriquecimento de requisitos de sistemas da área financeira ao considerar aspectos de privacidade e segurança. Este método possui abordagem única na literatura científica baseada na semiótica organizacional e uma extensa análise de padrões de segurança da informação e privacidade de dados. Assim, o MARSPS provê uma visão ampla das partes interessadas, suas necessidades, bem como analisa os requisitos considerando aspectos físicos, empíricos, sintáticos, semânticos, pragmáticos e sociais. A sistematização de todos os passos, técnicas empregadas, fontes de conhecimento e tarefas a serem desenvolvidas permitem aos analistas executarem o enriquecimento dos requisitos de maneira clara e direta. A proposta do MARSPS está descrita no artigo intitulado "*Enriching Financial Software Requirements Concerning Privacy and Security Aspects: a semiotics based approach*" aceito para a *18th International Conference on Information Technology-New Generations* (ITNG 2021).
- ***Análise Empírica dos Resultados*** (Artigo). A análise da aplicação do MARSPS em workshop com quatro especialistas no domínio contribui não só para versões futuras do método, como também para o direcionamento de outras pesquisas em temas relacionados. São contribuições únicas da análise apresentada a experimentação dos artefatos da semiótica organizacional para o enriquecimento de requisitos com base em aspectos de privacidade e segurança. Resultados parciais do estudo realizado estão descritos no artigo aceito para publicação na ITNG 2021 (ver item anterior). Uma versão estendida deste artigo para publicação em revista está planejada.

7.2. Limitações e Trabalhos Futuros

Nesta seção são apresentadas as limitações e como estas direcionam os principais trabalhos futuros propostos por esta dissertação.

Primeiramente, é importante destacar que o MARSPS não faz uso da metodologia completa da semiótica organizacional, sendo, portanto, capaz de ser aprimorado por meio do uso de novas técnicas disponíveis. Com a análise de normas, por exemplo, é possível modelar padrões comportamentais do usuário, intenções, preferências e responsabilidades nos níveis pragmático e social. Como o comportamento humano perante as questões de privacidade é diverso, a análise de normas pode ajudar no entendimento e na especificação das necessidades dos diferentes *stakeholders* envolvidos em um projeto. Portanto, trabalhos futuros podem ser realizados no sentido de aprimorar o MARSPS com outras técnicas da semiótica organizacional, bem como técnicas de outras áreas relacionadas à análise dos aspectos humanos e sociais no uso de sistemas computacionais.

Atualmente, a integração do MARSPS com a metodologia de desenvolvimento de software existente nas organizações se dá principalmente por meio da escolha do tipo de artefato produzido (*e.g.*, *user stories*, critérios de aceite ou casos de uso). Tal integração pode não ser suficiente, principalmente quando se pretende considerar aspectos de segurança e privacidade desde as etapas iniciais de levantamento de requisitos. Portanto, espera-se futuramente integrar as atividades do MARSPS em metodologias de desenvolvimento de software já empregadas nas organizações (*e.g.*, metodologias ágeis).

A construção de ferramentas para apoio ao MARSPS também pode agregar valor aos resultados desta pesquisa. Ferramentas que facilitem a classificação, armazenamento, recuperação e pesquisa por fontes de conhecimento em privacidade e segurança da área financeira podem auxiliar na execução do método. A integração das ferramentas para modelagem dos artefatos da SO com demais artefatos da engenharia de requisitos também ajudaria a deixar a execução mais ágil e menos custosa. Portanto, vislumbra-se como trabalho futuro a pesquisa, design e desenvolvimento de ferramentas de apoio à aplicação do método.

No que se refere à avaliação e uso do MARSPS, é importante salientar que ele foi avaliado com um número pequeno de requisitos e por um número reduzido de

profissionais, dentro das limitações de tempo e escopo de uma dissertação de mestrado. O uso em larga escala na especificação de requisitos por diferentes profissionais e organizações, bem como aprimoramentos decorrentes da prática nas organizações, deve ser realizado em investigações de longo prazo. Como próximos passos desta pesquisa, pretende-se expandir o número de requisitos avaliados, bem como o número de avaliadores.

7.3. Considerações Finais

Considerando os estudos realizados, os resultados obtidos da avaliação do método sugerem que o uso de técnicas da semiótica organizacional no aprimoramento de requisitos de sistemas da área financeira, no que diz respeito aos aspectos de privacidade e segurança, se mostrou um instrumento viável para os profissionais.

O MARSPS permitiu aos especialistas do domínio da aplicação uma melhor compreensão do escopo do projeto de aprimoramento de requisitos de aplicações em ambientes *Internet Banking* e *Mobile Banking*. Com a utilização do MARSPS foi possível identificar as principais fontes de requisitos de privacidade do domínio da aplicação, identificar os *stakeholders* que podem colaborar com o projeto, analisar os *stakeholders* por meio do Diagrama de *Stakeholders*, identificar suas necessidades, bem como levantar os problemas que estão relacionados com estas necessidades e, com base nos problemas, propor soluções. Dessa maneira, é importante ressaltar que foi possível avançar no conhecimento de como elicitar e aprimorar requisitos com o objetivo de melhorar a segurança e a privacidade de dados dos *stakeholders* que fazem uso ou são afetados por aplicações da área financeira.

8. Referências

ABNT. (2012). *ISO/IEC 27001 - Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos*. https://www.abntcatalogo.com.br/norma.aspx?ID=306580

ABNT. (2013). *ABNT NBR ISO/IEC 27002 - Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação*. https://www.abntcatalogo.com.br/norma.aspx?ID=306582

Adfue. (2014). *Manual da Legislação Europeia Sobre Proteção de Dados*. https://doi.org/10.2811/73790

Alhalafi, D. (2015). A new methodology to disambiguate privacy. *Acta Physica Polonica A*, *128*(2), 319–323. https://doi.org/10.12693/APhysPolA.128.B-319

Alkubaisy, D. (2017). A framework managing conflicts between security and privacy requirements. *Proceedings - International Conference on Research Challenges in Information Science*, 427–432. https://doi.org/10.1109/RCIS.2017.7956571

Arantes, F. L. (2011). Organizational Semiotics and Participatory Design to Requirements Elicitation – A Case Study. *VII Brazilian Symposium on Information Systems*, 322–333.

Arantes, F. L. (2013). Requirements Engineering of a Web Portal Using Organizational Semiotics Artifacts and Participatory Practices. *International Journal of Computer Science and Information Technology*, *5*(2), 131–146. https://doi.org/10.5121/ijcsit.2013.5212

BACEN. (2014). *RESOLUÇÃO Nº 4.327, DE 25 DE ABRIL DE 2014*. https://www.bcb.gov.br/pre/normativos/res/2014/pdf/res_4327_v1_O.pdf

BACEN. (2020). *Manual de Segurança do SFN Versão 4.03*. https://www.bcb.gov.br/content/estabilidadefinanceira/cedsfn/Manual_Segurança_SFN-v4_03.pdf

Baláž, A., Hulie, M., Kurilec, M., & Štancel, M. (2019). Classification of Security for System Vulnerabilities 1. *2019 IEEE 17th International Symposium on Intelligent Systems and Informatics (SISY)*, 29–34. https://doi.org/10.1109/SISY47553.2019.9111624

Baranauskas, M. C. C., & Bonacin, R. (2008). Design - Indicating through signs. *Design Issues*, *24*(3). https://doi.org/10.1162/desi.2008.24.3.30

Barn, B. S., Primiero, G., & Barn, R. (2015). *An approach to early evaluation of informational privacy requirements*. 1370–1375. https://doi.org/10.1145/2695664.2695788

Brasil. (2018). *Lei Geral de Proteção de Dados Pessoais (LGPD)*. LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

Breaux, T. D. ., & Rao, A. (2013). Formal analysis of privacy requirements specifications for multi-tier applications. *2013 21st IEEE International Requirements Engineering Conference (RE)*, 14–23. https://doi.org/10.1109/RE.2013.6636701

Bruning, C., Godri, L., & Takahashi, A. R. W. (2018). Triangulação em Estudos de Caso: incidência, apropriações e mal-entendidos em pesquisas da área de Administração. *Administração: Ensino e Pesquisa*, *19*(2), 277–307. https://doi.org/10.13058/raep.2018.v19n2.889

Cabitza, F., & Mattozzi, A. (2017). The semiotics of configurations for the immanent design of interactive computational systems. *Journal of Visual Languages and Computing*, *40*, 65–90. https://doi.org/10.1016/j.jvlc.2017.01.003

Côrte, K. (2014). *Segurança da Informação Baseada no Valor Da Informação e nos Pilares Tecnologia, Pessoas e Processos*. Universidade de Brasília.

COSIF. (1922). *PLANO CONTÁBIL DAS INSTITUIÇÕES DO SISTEMA FINANCEIRO NACIONAIS -COSIF*. *Circ 1273*.

de Oliveira, S. F., Martinez, P. V, Fabri, J. A., L'Erario, A., Duarte, A. S., & Gonçalves, J. A. (2016). Proposal for semiotics inspection method application in coming artifacts requirements survey activity. *2016 11th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–7.

Ekstedt, M., Franke, U., Johnson, P., & Lagerstr, R. (2018). *Can the Common Vulnerability Scoring System be Trusted ? A Bayesian Analysis*. *15*(6), 1002–1015. https://doi.org/10.1109/TDSC.2016.2644614

Ferreira, A. B. de H. (2015). *Dicionario Aurelio da Lingua Portuguesa*. Positivo.

French, T., Bessis, N., & Maple, C. (2010). A High-level semiotic trust agent scoring model for collaborative virtual organisations. *24th IEEE International Conference on Advanced Information Networking and Applications Workshops, WAINA 2010*, 1114–1120. https://doi.org/10.1109/WAINA.2010.173

Gallon, L. (2010). On the Impact of Environmental Metrics on CVSS Scores. *Conference, Ieee International Computing, Social Conference, Ieee International*. https://doi.org/10.1109/SocialCom.2010.146

Guaman, D., Guaman, F., Jaramillo, D., & Sucunuta, M. (2017). Implementación de técnicas y recomendaciones de seguridad OWASP para evitar ataques de tipo inyección SQL, XSS utilizando J2EE y WS-Security. *Iberian Conference on Information Systems and Technologies, CISTI*. https://doi.org/10.23919/CISTI.2017.7975981

Jardim-Goncalves, R., Grilo, A., Hassan, T., & Steiger-Garcao, A. (2010). Semiotics-based manufacturing systems integration in the advent of a single electronic market. *International*

Journal of Computer Integrated Manufacturing, *23*(8–9), 832–851. https://doi.org/10.1080/0951192X.2010.490274

Karlsson, F., Hedström, K., & Goldkuhl, G. (2017). Practice-based discourse analysis of information security policies. *Computers and Security*, *67*, 267–279. https://doi.org/10.1016/j.cose.2016.12.012

Kuhn, D. R., Raunak, M. S., & Kacker, R. (2017). An Analysis of Vulnerability Trends, 2008-2016. *Proceedings - 2017 IEEE International Conference on Software Quality, Reliability and Security Companion, QRS-C 2017*, 587–588. https://doi.org/10.1109/QRS-C.2017.106

Leaders, P., Meucci, M., & Muller, A. (2013). *Papers from III World Congress on Water Resources, held at Mexico City, Mexico, on April 23-27, 1979. Volume 3. Cc*.

Lee, C.-S., & Wong, K. D. (2017). Design thinking and semiotics to increase socio-cognitive-affective engagement: An inclusive design human factors case study. *2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, *2017-Decem*(2015), 264–268. https://doi.org/10.1109/IEEM.2017.8289893

Lehtola, L., & Kauppinen, M. (2006). Suitability of requirements prioritization methods for market-driven software product development. *Software Process: Improvement and Practice*, *11*(1), 7–19. https://doi.org/https://doi.org/10.1002/spip.249

Levy, M., & Hadar, I. (2018). The Importance of Empathy for Analyzing Privacy Requirements. *2018 IEEE 5th International Workshop on Evolving Security & Privacy Requirements Engineering (ESPRE)*, 9–13. https://doi.org/10.1109/ESPRE.2018.00008

Li, W., Liu, K., & Liu, S. (2015). Semiotics in Interoperation for Information Systems Working Collaboratively. In *Communications in Computer and Information Science* (Vol. 348, pp. 370–386). https://doi.org/10.1007/978-3-662-46549-3_24

Liu, K. (2000). Semiotics in Information Systems Engineering. In *Cambridge University Press* (Vol. 232, Issue 1).

Liu, K., & Li, W. (2014). *Organisational semiotics for business informatics*. Routledge.

Lukasiewicz, K., & Cyganska, S. (2019). Security-oriented agile approach with AgileSafe and OWASP ASVS. *Proceedings of the 2019 Federated Conference on Computer Science and Information Systems, FedCSIS 2019*, *18*, 875–878. https://doi.org/10.15439/2019F213

Machado, F. N. R. (2015). *Análise e gestão de requisitos de software: Onde nascem os sistemas*. Editora Érica.

Manteli, C., van de Weerd, I., & Brinkkemper, S. (2010). Bridging the Gap between Software Product Management and Software Project Management. *Proceedings of the 11th International Conference on Product Focused Software*, 32–34. https://doi.org/10.1145/1961258.1961266

Medeiros, D. R. I. de. (2019). *A Influência da Governança de TI no ambiente corporativo : Um estudo deste fator como uma vantagem competitiva*. Universidade Federal do Rio de Janeiro.

Mendes, N., Duraes, J., & Madeira, H. (2011). *Benchmarking the Security of Web Serving Systems Based on Known Vulnerabilities*. https://doi.org/10.1109/LADC.2011.14

Miranda, L. A. (2018). *A proteção de dados pessoais e o paradigma da privacidade*. https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:livro:2018;001154477

Morris, C. (1994). *v*. 50.

Nascimento, E. F. do. (2017). Segurança da Informação. *Revista Interface Tecnológica*, *2018*(1), 9. https://doi.org/10.1111/jse.12269

Oliveira, S. F., Martinez, P. V, Fabri, J. A., Erario, A. L., Duarte, A. S., & Goncalves, J. A. (2016). Proposal for semiotics inspection method application in coming artifacts requirements survey activity | Proposta de Aplicação do Método de Inspeção Semiótica em Artefatos Provenientes da Atividade de Levantamento de Requisitos. *Iberian Conference on Information Systems and Technologies, CISTI*, *2016-July*. https://doi.org/10.1109/CISTI.2016.7521399

Omoronyia, I., Cavallaro, L., Salehie, M., Pasquale, L., & Nuseibeh, B. (2013). Engineering adaptive privacy: On the role of privacy awareness requirements. *Proceedings - International Conference on Software Engineering*, 632–641. https://doi.org/10.1109/ICSE.2013.6606609

Pan, Y.-C., Jacobs, A., Tan, C., & Askool, S. (2018). Extending Technology Acceptance Model for Proximity Mobile Payment via Organisational Semiotics. In K. Liu, K. Nakata, W. Li, & C. Baranauskas (Eds.), *Digitalisation, Innovation, and Transformation* (pp. 43–52). Springer International Publishing.

PCI-DSS. (2010). *Padrão de segurança de dados Requisitos e procedimentos de avaliação da segurança*.

PCI DSS. (2018). PCI DSS Quick Reference Guide 3.2.1. *PCI Security Standard Documents*, 1–40.

Pohl, K. (2016). *Requirements engineering fundamentals: a study guide for the certified professional for requirements engineering exam-foundation level-IREB compliant*. Rocky Nook, Inc.

Qian, K., Parizi, R. M., & Lo, D. (2019). OWASP Risk Analysis Driven Security Requirements Specification for Secure Android Mobile Software Development. *DSC 2018 - 2018 IEEE Conference on Dependable and Secure Computing*, 4–5. https://doi.org/10.1109/DESEC.2018.8625114

Rambo, K., & Liu, K. (2016). An Organisational Semiotics Approach to Multicultural

Requirements Engineering: Stakeholder's Analysis of Online Shopping for Saudi Arabian Female Consumers. *International Journal for Infonomics*, *4*(1/2), 473–483. https://doi.org/10.20533/iji.1742.4712.2011.0053

Romero Felizardo Scannavino, K., Nakagawa, E. Y., Camargo Pinto Ferraz Fabbri, S., & Cutigi Ferrari, F. (2017). Revisão Sistemática da Literatura em Engenharia de Software. In *Revisão Sistemática da Literatura em Engenharia de Software*.

Rosa, F. F. (2018). *HCAPP-SEC : seleção e análise de itens de avaliação de segurança baseadas em heurísticas e critérios* [FEEC- Universidade Estadual de Campinas]. http://repositorio.unicamp.br/handle/REPOSIP/332221

Shah, T. R., & Patel, S. V. (2012). *SystemSecurity, Privacy and Trust Oriented Requirements Modeling for Examination System*. 6–8. https://doi.org/10.1109/NUICONE.2012.6493189

Shihab, M. R., Misdianti, F., & Indonesia, U. (2014). Moving Towards PCI DSS 3.0 Compliance: A Case Study of Credit Card Data Security Audit in an Online Payment Company. *2014 International Conference on Advanced Computer Science and Information System*, 151–156.

Simoni, C. A. C. (2003). A Prática de Desenvolvimento de Software e a Abordagem da Semiótica Organizacional. In *Dissertação de Mestrado: Unicamp*.

Sohoel, H., Jaatun, M. G., & Boyd, C. (2018). OWASP Top 10 - Do Startups Care? *2018 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2018*, *0102*. https://doi.org/10.1109/CyberSecPODS.2018.8560666

Sommerville, I. (2011). *Engenharia de Software*. Pearson Universidades.

Sommerville, I. (2016). Software engineering (10th edition). In *Pearson Education Limited*. Pearson.

Souza, C. S. de;, Leitão, C. F., Prates, R. O., Amélia Bim, S., & da Silva, E. J. (2010). Can inspection methods generate valid new knowledge in HCI? The case of semiotic inspection. *International Journal of Human-Computer Studies*, *68*(1–2), 22–40. https://doi.org/10.1016/j.ijhcs.2009.08.006

Stamper, R. (1973). *Information in Business and Administrative Systems*. Wiley.

Tejas, R. S., & Patel, S. V. (2012). Security, privacy and trust oriented requirements modeling for examination system. *2012 Nirma University International Conference on Engineering (NUiCONE)*, 1–6. https://doi.org/10.1109/NUICONE.2012.6493189

Tran, H., & Wei, J. (2011). Impact of privacy and security on users' trust in ubiquitous commerce. *BMEI 2011 - Proceedings 2011 International Conference on Business Management and Electronic Information*, *5*, 7–10. https://doi.org/10.1109/ICBMEI.2011.5914418

Triviños, A. N. S. (1987). Introdução à Pesquisa em Ciências Sociais: a Pesquisa Qualitativa em Educação – O Positivismo, A Fenomenologia, O Marxismo. In *TRIVIÑOS, Augusto Nibaldo*

Silva. (Vol. 1, Issues 1–1750). https://doi.org/10.33081/formação.v1i20.2335

União Eutropéia. (2010). Tratados Consolidados Carta Dos Direitos Fundamentais. *Luxemburgo, Serviço Das Publicações Da União Europeia*.

Whiskerd, N., Dittmann, J., & Vielhauer, C. (2018). A Requirement Analysis for Privacy Preserving Biometrics in View of Universal Human Rights and Data Protection Regulation. *2018 26th European Signal Processing Conference (EUSIPCO)*, 553–557. https://doi.org/10.23919/EUSIPCO.2018.8553045

Yang, H., & Li, W. (2009). Modeling requirement driven architecture of adaptive healthcare system based on semiotics. *Proceedings - 2009 International Forum on Information Technology and Applications, IFITA 2009*, *2*, 723–727. https://doi.org/10.1109/IFITA.2009.277

APÊNDICE A – Lista de artefatos da execução do MARSPS para aprimoramento de requisitos de privacidade e segurança.

Lista dos artefatos gerados na execução do MARSPS para aprimorar requisitos de privacidade e segurança em aplicações da área financeira.

A1. Conjunto de Requisitos do Sistema - v_1.0

A2. Conjunto de Fontes de Requisitos de Segurança e Privacidade v_1.0

A3. Lista de Candidatos a Stakeholders para Análise - REQ_001 - v_1.0

A3. Lista de Candidatos a Stakeholders para Análise - REQ_002 - v_1.0

A4. Cebola Organizacional - v_1.0

A5. Descrição de Interesses e Necessidades dos *stakeholders* - REQ_001 - v_1.0

A5. Descrição de Interesses e Necessidades dos *stakeholders* - REQ_002 - v_1.0

A6. Quadro de Avaliação v_1.0

A7. Escada Semiótica - REQ_001 v_1.0

A7. Escada Semiótica - REQ_002 - v_1.0

A8. Conjunto de Requisitos de segurança e privacidade de software - REQ_001 - v_1.0

A8. Conjunto de Requisitos de segurança e privacidade de software - REQ_002 - v_1.0

Disponível em:
https://www.dropbox.com/sh/f523mpuq3dun0d7/AADExa7DPCkQIMeQPuQK3wGTa?dl=0

APÊNDICE B - Detalhamento do quadro de avaliação após o aprimoramento dos requisitos

Tabela 11 - Avaliação dos Stakeholders a nível de Comunidade

Stakeholder	Problemas e perguntas	Soluções e Ideias
Agência bancária	A proteção de dados e informações sensíveis nas organizações é uma atividade de fundamental importância e essa necessidade torna-se cada vez maior nas instituições financeiras como é o caso das agências bancárias. Diante de tais necessidades surge a necessidade de aprimorar os mecanismos de privacidade e segurança das informações. • Como garantir a privacidade de dados e informações em sistemas existentes na agência bancária?	A necessidade de proteção e segurança é algo que deve evolver todos na organização e com isso surge a necessidade de propor treinamentos e conscientização dos colaboradores para que a proteção e privacidade de dados e informações possam ser asseguradas na organização.
Gerência da agência	A segurança e privacidade de dados e informações de utilizadores de aplicações sistêmica em ambientes de *mobile Banking* e *Internet Banking* é um ponto crucial para as instituições financeiras, para isso, a gerência das agências buscam colaborar para garantir que a proteção de dados de clientes em aplicativos e sistemas bancários sejam assegurados na utilização de canais digitais por seus clientes. • Qual a necessidade da gerência da agência em relação a proteção e privacidade de informações em aplicações bancárias?	O problema da exposição de dados e informações dos *stakeholders* poderá estar relacionada com a falta da cultura da proteção de dados e informações e, em grande parte por desconhecer o valore relacionado ao tipo de informação que está sendo exposta. Mediante a tais necessidades cabe recomentar que possam testar todas as aplicações simulando as necessidades dos clientes em suas operações bancárias de forma a garantir que a proteção dos dados dos clientes possa ser assegurada durante a sua utilização.
Governo	O governo no contexto de desenvolvimento de sistemas para serem utilizados por instituições da área financeira. Dessa forma, para assegurar que as instituições bancárias, assim como as instituições financeiras sigam todas as instruções determinadas pelo BACEN – Banco Central do Brasil no que diz respeito à segurança e privacidade de dados em sistema a serem desenvolvidos pelas instituições da área financeira. • Como assegurar que as instituições bancárias e financeiras estão seguindo as normas e determinações do governo em relação a privacidade de dados e informações de usuários em aplicações e sistemas da área financeira?	Mediante a necessidade de desenvolver sistemas que atenda às necessidades da instituição financeiras e as normativas existentes no mercado financeiro, se faz necessário propor para as instituições seguir as determinações explicitas nas regulamentações do BACEN para que possam desenvolver sistemas de software e aplicativos que proporcione a seus clientes segurança e privacidade da dados e informações nas suas transações assim como no compartilhamento das informações resultantes das transações bancárias na utilização de recursos dos canais digitais como é o caso dos aplicativos e sistemas *Web*.
Bancos	Diferentes tipos de serviços são oferecidos para os usuários de aplicações bancárias e, garantir que os produtos e serviços oferecidos pela instituição bancária possa cumprir com os quesitos	Para mitigar possíveis riscos relacionados ao ambiente bancário na utilização de sistemas de software , é de fundamental importância que sejam realizadas revisões nos serviços

	de segurança e privacidades de seus clientes durante as operações e transações realizadas por meio da utilização dos canais digitais disponíveis na organização para seus clientes. • Como que a instituição bancária poderá melhorar a segurança e privacidade das operações realizadas por seus clientes durante a utilização dos canais digitais para realizar suas transações?	disponíveis parar os clientes por meio de diferentes canais digitais, isso para assegurar que a segurança e privacidade dos clientes está sendo mantida mediantes as novas necessidades de aprimoramento das requisições na utilização das ferramentas disponíveis na *Internet* e por meio da utilização de aplicativos em dispositivos móveis. Dessa forma o banco poderá garantir que os clientes farão uso dos canais digitais da organização bancária.
Organizações legisladoras	As organizações legisladoras possuem um papel de grande destaque no cenário das instituições financeiras, isso devido ao seu papel em criar determinações para que as instituições financeiras possam desenvolver seus produtos de sistemas de software de forma segura e respeitando a concorrência de mercado. • Dessa forma, como garantir que as organizações desenvolvam aplicações sistêmica que garantam a segurança e privacidade de dados e informações de usuários?	As organizações legisladoras com todo o seu poder de determinar as diretrizes a serem seguidas pelas instituições financeiras no desenvolvimento de suas soluções sistêmicas, para isto, há a necessidade de propor para as instituições financeiras criar planos de desenvolvimento que visem atender as necessidades de privacidade e segurança em ambientes sistêmicos para que os usuários dos canais digitais das organizações possam realizar suas operações de forma segura e sem riscos ao compartilhamento comprovantes das transações efetuadas entre usuários de aplicações bancárias.

Tabela 12 - Avaliação dos Stakeholders a nível de Mercado

Stakeholder	***Problemas e perguntas***	***Soluções e Ideias***
Fornecedores de equipamentos	O fornecimento de equipamentos para as organizações financeiras é essencial para que as estas possam desenvolver suas atividades, no entanto, o fornecimento de tais equipamentos trazer para a organizações problemas, caso os equipamentos não estejam dentro das normas e padrões estabelecidos que correspondam as especificações do produto em contratos entres as instituições. • Como garantir que o fornecimento de equipamentos suprirá a necessidade da organização para a sua operação?	Mediante as necessidades, solucionar possíveis problemas de compatibilidade na aquisição de equipamentos, a organização deverá possuir em seu quadro de colaboradores especialistas em *hardware* para que os equipamentos a serem adquiridos não apresentem incompatibilidade com o padrão estabelecido para a organização, para isso, se faz necessário a realização de mapeamento dos equipamentos existentes, ou seja, o inventário de tudo que existe na organização, dessa forma podendo evitar que novas aquisições de equipamentos não acarrete em grandes impactos operacionais na organização.
Infraestrutura de serviços de TI	A infraestrutura de serviços de tecnologias da informação disponíveis para as organizações, na oferta dos serviços disponíveis em nuvem podem acarretar em problemas de	A aquisição de serviços de infraestrutura a ser adotada pelas organizações deverá seguir os princípios e requisitos de privacidade e segurança existentes nas normativas do BACEN

	privacidade e de segurança de dados e informações de usuários em aplicações sistêmicas das organizações. • Como garantir que o os serviços de tecnologias das organizações financeiras disponíveis por meio dos serviços em nuvem estarão protegidos de usuários mal intencionados?	para aplicações bancárias como no caso das operações de transferências de fundos e para as operações com cartões de crédito fazer uso do PCI DSS. Tais normativas são compostas de requisitos de privacidade para garantir que o trafego de dados por meio da utilização da Internet seja seguro para as organizações e consecutivamente para seus clientes. Além das políticas de segurança da informação existentes na organização.
Cliente - Contratante	Na contratação de serviços de relacionados à segurança e privacidade de dados e informações as organizações financeiras possuem diferentes tipos de necessidades que precisam serem levadas em consideração, antes da contratação de serviços oferecidos por empresas terceiras. No entanto, tais necessidades poderão ser transformarem em problemas, caso as contratações ocorram de forma inadequada. • Qual a necessidade da organização em relação a contratação de serviços relacionados a privacidade e segurança de dados da área financeira?	As organizações em geral possuem diferentes tipos de necessidade em relação a privacidade e segurança de dados de seus ativos, assim como a segurança e privacidade de seus clientes na utilização de diferentes tipos de serviços disponíveis em seus canais digitais. E, para que os serviços possam ser disponibilizados de forma segura em seus canais digitais, a organização financeira poderá investir no aperfeiçoamento de suas normas e políticas de segurança e exigir das empresas contratadas que elas entreguem serviços seguros para a organização e seus clientes.
Administradoras de Cartões de Crédito	A administração de cartões é uma atividade muito importante para as administradoras que fornecem este tipo de serviço e os ofertam para seus clientes e, na utilização do cartão de crédito, problemas poderão ocorrer, desde uma compra até a entrega da fatura em formato digital para o cliente. • Como garantir que o cliente será o único usuário a conseguir visualizar o conteúdo existente no arquivo disponibilizado contendo a fatura digital do cartão de crédito?	A visualização de dados e informações dos dados de uma fatura de cartão de crédito devem ser de acesso restrito ao titular do documento, portanto, para mitigar possíveis problemas de vulnerabilidades existentes, as administradoras poderão investir no aprimoramento de requisitos que visem aumentar a segurança e a privacidade de usuários que fazem uso dos serviços disponíveis por meio da utilização de canais digitais na organização, como é o caso da fatura digital e a sua entrega par o cliente. Esse aprimoramento requer na adoção de mecanismos mais seguros na criação de senhas que permitam a visualização do conteúdo existente na fatura digital.
Financeiras	A concorrência de mercado entre as instituições financeira é alta, no entanto, estas devem ofertar cada vez mais serviços que a torne atraentes para seus correntistas • Como se tornar atrativo e atrair novos clientes para usufruir do produtos e serviços disponibilizados pelas organizações que atuam no mercado financeiro?	A priorização da segurança e a privacidade de seus serviços para os clientes durante a realização de operações e envio e ou recebimento de documentos em formato digital, tais como comprovantes de transações *online*, onde o documento possui um conjunto de informações sensíveis e dados de grande importância para os titulares da documentação para que o documento não seja acessado por quem não é de direito.

Empresas especialista em segurança da informação	Uma das dificuldades enfrentadas pelas empresas especializadas em serviços de segurança da informação é garantir a segurança e a privacidade de usuários que fazem uso de recursos da tecnologia da informação para acessar serviços disponibilizados perlas organizações dos mais diferentes tipos e ramos de atuação no mercado. • Tendo em vista que a segurança e privacidade de dados e informações é um problema eminente da área da segurança da informação, quais seriam as ações a serem tomadas para mitigar os problemas causados pela exposição de dados e informações usuários de canais digitais da área financeira?	Investir no aprimoramento das tecnologias existentes para que possam mitigar ou mesmo erradicar os problemas pontuais da exposição de dados e informações de usuários de canais digitais das organizações financeira na utilização dos serviços disponibilizados por estas empresas como melhorar a segurança e privacidade para obter acesso ao conteúdo de uma fatura digital, assim como no compartilhamento de dados sensíveis em comprovantes de operações bancarias na *Internet* e por meio da utilização de aplicativos em dispositivos móveis.
Aplicativo de transferência de fundos	Atualmente, clientes de diferentes instituições bancárias contam com a facilidade e praticidade para obter acesso e visualizar dados da sua conta bancária, além de fazer diferentes tipos de operações como a transferência de fundos para outros clientes da mesma rede bancária ou de uma rede diferente, isso graças aos recursos da tecnologia da informação disponível na palma das mãos dos usuários, ou seja, o uso de dispositivos móveis conectados à *Internet*. O *mobile Banking e Internet Banking* proporcionam para os clientes das agências a comodidade dos serviços disponíveis a qualquer momento e lugar sem ter que enfrentar filas em posto físico para atendimento, no entanto toda essa praticidade poderá acarretar em problemas para os usuários quando não treinados e conscientizados a fazer uso dos recursos de maneira correta e segura. • Como assegurar que as operações de transferência de fundos entre indivíduos que usam o *mobile Banking e Internet Banking* sejam seguras e sem danos para os clientes que realizam as operações de transferência usando estes canais?	Em relação aos problemas elencados, a organização deverá realizar melhorias em seus sistemas, sejam estes, *mobile Banking* ou *Internet Banking* de forma a garantir que os clientes farão uso de aplicações seguras. Essa segurança pode ser garantida na aplicação de Legislações vigente, assim como consultar as bases de vulnerabilidades para que problemas possam ser identificados e corrigidos mesmo antes que as aplicações possam ser disponibilizadas para os clientes das instituições financeiras possam realizar suas transações por meio do *mobile Banking e Internet Banking*. Todo esse cuidado se faz necessários, pois a proteção das transações bancárias é uma necessidade cada vez maior, isso devido à grande aceitação dos canais digitais disponíveis pela organização para os seus clientes.
Gerente de contas	Assegurar que a privacidade de informações seja garantida na utilização de sistemas, assim como na utilização de aplicativos bancários nas atividades da instituição financeira. • Como garantir que as aplicações bancárias possam ser acessadas de forma que a segurança e privacidade de dados e informações não sejam expostos por clientes e colaboradores das organizações?	Propor um plano de treinamento e conscientização no uso das aplicações bancária e o compartilhamento de informações geradas por meio da utilização das aplicações, assim como o seu compartilhamento em diferentes canais digitais. Assegurar que os clientes poderão contar com aplicações seguras, onde a segurança e a privacidade de dados é um fator primordial para que o cliente possa a cada dia confiar na organização e nos

		diferentes tipos de serviços que são disponibilizados em ambiente *online* como é o caso do *mobile Banking e Internet Banking*.
Gerência da Negócios	Assegurar que a privacidade de informações e dados dos clientes nas aplicações *Web* e na utilização de aplicativos sejam prioridade, visando garantir que o cliente passe a confiar nos serviços disponibilizados por meios dos canais digitais da organização. • Como a gerencia de negócios irá garantir que a privacidade de dados e informações não impacte na utilização das aplicações pelos clientes da organização?	A gerência de negócios possui um papel de grande importância no entendimento dos requisitos, dessa forma é importante que este possa entender as necessidades de privacidade para que os serviços disponibilizados pela organização não sejam impactados com a adoção de norma, política de segurança, assim como a legislação para garantir que a privacidade de dados e informações dos clientes possa ser assegurada durante a utilização dos canais digitais para realizar suas transações financeiras.

Tabela 13 - Avaliação dos Stakeholders a nível de Fonte

Stakeholder	**Problemas e perguntas**	**Soluções e Ideias**
Fornecedores de software	Atualmente no mercado de tecnologia da informação existem incontáveis empresas que fornecem soluções sistêmicas para diferentes tipos de organizações. E, para a área financeiras, o fornecimento de sistemas de software devem seguir regras e normas determinas por instituições regulamentadoras e, quando existem falhas em seus processos de desenvolvimento, os produtos de softwares desenvolvidos poderão não atender as reais necessidades de privacidade e segurança esperado para o produto de software. • Como garantir que a organização financeira está recebendo de seus fornecedores soluções sistêmicas que presam pela segurança e a privacidade de seus usuários na utilização dos serviços disponíveis em suas aplicações?	Para que a organização possa assegurar que as aplicações sistêmicas atendam às suas necessidades, se faz necessário que a organização exija de seus fornecedores a documentação das especificações das necessidades de segurança e privacidade para que estejam em conformidade no aceite da aplicação. Dessa forma, a organização garante que a aplicação estará dentro do escopo e atendendo a todas as requisições iniciais do projeto, seguindo com foco na privacidade e segurança de dados de seus clientes na utilização dos canais digitais para recebimento e compartilhamento de informações.
Instituições normativas	As normas e resoluções determinam como as instituições da área financeira devem fazer para que possam atuar no mercado. Cada tipo de negócios possui conjunto de requisitos que as instituições devem seguir, ou melhor, implementá-los em seus sistemas. Dentre as instituições normativas estão o BACEN, PCI DSS que possuem conjuntos de requisitos com foco em segurança e privacidade.	As instituições normatizadoras possuem papéis de grande importância. Tenha a função de criar normas que determinam as diretrizes para que as instituições financeiras possam atuar no mercado. Dessa forma, determinam que as organizações revisem os requisitos de segurança e privacidade de forma que possam encontrar possíveis vulnerabilidades antes da implementação dos requisitos, com isso assegurar que caso seja encontrada vulnerabilidades, estas deverão ser corrigidas antes do início das

	• Como fazer com que as instituições financeiras adotem todas as normativas e resoluções para garantir a segurança e a privacidade na utilização de sistemas para receber ou compartilhar informações por meio dos serviços digitais das organizações financeiras?	aplicações de sistemas de software *mobile Banking e Internet Banking.*
Especialista em Segurança da Informação	O especialista em segurança da informação na organização é um *stakeholder* de grande destaque no âmbito sistêmico da organização, no entanto, este stakeholder se depara com diferentes necessidades de privacidade para diferentes *stakeholders*, e na maioria das vezes atender as estas requisições não é uma tarefa tão simples em projetos de desenvolvimento de sistemas de software para diferentes plataformas, como é o caso do ambiente *Web* e o desenvolvimento para dispositivos móveis. • Como assegurar que as necessidades de privacidades elencadas por diferentes *stakeholders* envolvidos diretamente com o projeto de desenvolvimento de software ou mesmo o aprimoramento de funcionalidades ou componentes de software s existentes na organização?	A privacidade de dados e informações das organizações é por sua vez uma necessidade que cresce a cada dia, assim como as necessidades dos usuários na utilização de soluções sistêmicas. E garantir que as necessidades de privacidade sejam atendidas para cada usuário ou grupos de usuários se faz necessário que o engenheiro de segurança da informação recorra a diferentes fontes de informações e bases de vulnerabilidades sistêmicas para que as necessidades elencadas por cada *stakeholder* possam ser atendidas de forma a não impactar na segurança da aplicação disponibilizada para operação. Dentre as fontes de vulnerabilidades, o especialista em segurança da informação poderá consultar a OWASP, assim como a OSVDB para certificar que o requisito a ser implementado não acarretará na operação do sistema.

Tabela 14 - Avaliação dos Stakeholders a nível de Contribuição

Stakeholder	**Problemas e perguntas**	**Soluções e Ideias**
Engenheiro de requisitos	A atividade da engenharia de requisitos no processo de desenvolvimento de sistemas de software é essencial para as organizações e, um dos problemas eminente que circunda a vida de um engenheiro de requisitos em projetos de desenvolvimento de sistemas de software é a falta de entendimento das reais necessidades dos *stakeholders* para atender as demandas da organização. Problemas oriundos de falhas existentes na comunicação. • Como é que o engenheiro de requisitos poderá contribuir com as necessidades de segurança e privacidade das solicitadas pela organização?	Sendo o engenheiro de requisitos, um dos principais *stakeholders* no processo de desenvolvimento ou aprimoramento de um sistema de software , a sua principal contribuição em relação a demanda para melhorar a segurança e a privacidade de utilização e compartilhamento de dados e informação nos sistemas *mobile Banking e Internet Banking* e no acesso a fatura digital é entender as necessidades dos *stakeholders* e recorrer as fontes essenciais para que as necessidades sejam atendidas de forma que possíveis vulnerabilidades possam ser identificadas e eliminadas do projeto, com isso gerando ganhos significativos para a organização e seus clientes.

Engenheiro de segurança da Informação	Diante do cenário existente nas organizações, o engenheiro de segurança da informação na organização se depara com diferentes necessidades de privacidade para diferentes *stakeholders*, e com base nessas necessidades, visa atender as requisições para o desenvolvimento de aplicações *mobile Banking e Internet Banking* para atender as demandas solicitadas. • Qual a principal contribuição do engenheiro de segurança da informação para com as necessidades de segurança e privacidade com o aprimoramento de sistemas para *mobile Banking e Internet Banking* na organização?	Sendo o engenheiro de segurança da informação um Stakeholders de grande destaque no aprimoramento de requisitos de privacidade, a principal contribuição é assegurar que a privacidade de dados e informações das organizações, assim como a de seus clientes possa ser assegurada. Dessa forma, tem por finalidade garantir que as necessidades de privacidade sejam atendidas para cada usuário ou grupos existentes na organização. Além destes fatores, o engenheiro de segurança da informação trará contribuições por meio de pesquisas em bases de vulnerabilidade para que as necessidades de privacidade para atualização da solução sistêmica possam proporcionar confiança para a organização e consequentemente para seus clientes.
Designers	No processo de desenvolvimento de sistemas de software o design de um produto de software quando elaborado de forma que o projeto de interface não atende as expectativas dos *stakeholders*, isso acarreta impactando a sua aceitação e utilização da aplicação. • Como garantir que o design de um produto de software seja algo favorável para a organização e aceitação do cliente?	A aceitação do projeto de interface pela construção e disponibilização de um produto de software que atenda as reais necessidades da organização e de seus clientes está relacionada pela forma que as informações do produto de software são elencadas e encaminhadas para a elaboração do projeto de interface. Outo ponto e envolver o *design* de produto para entender as necessidades da organização elencadas pelo engenheiro de requisitos antes da criação do projeto de interface.
Especialista *UX*	As organizações cada vez mais dependem de sistemas de software que atendam as reais necessidades da organização, assim como as necessidades de seus clientes. Com isso, os especialistas em *UX* quando não estão envolvidos neste contexto, as aplicações desenvolvidas tendem a não atender as necessidades para as quais as aplicações sistêmicas *em mobile Banking e Internet Banking* foram desenvolvidas. • Como contribuir para que os projetos de *interface* atendam às necessidades dos usuários e da organização?	Dentre os agentes que contribuem par garantir a qualidade de um produto de sistemas de software desenvolvido e disponibilizado para a organização financeira e consequentemente para seus clientes, o especialista *UX* contribui para que o design do produto atendas as necessidades do aprimoramento seja realizado de forma eficaz pela equipe responsável pelo projeto na organização.
Especialista UI	Falhas no entendimento do produto de software é uma das causas que ocorrem com especialistas de *UI* em projetos de aprimoramento ou desenvolvimento de software na organização. • Qual a principal contribuição do especialista UI para como projeto de aprimoramento de requisitos de privacidade e segurança em projetos *mobile Banking e Internet Banking* na organização?	O seu papel é de grande importância, uma vez que, o especialista *UI* deve se envolver no processo para que possa entender as necessidades apontadas pelo engenheiro de requisitos e o engenheiro de segurança da informação resolver problemas de entendimento das necessidades do produto de software a ser aprimorado pela organização, o especialista *UI* deverá se inserir

		no contexto da aplicação, de forma que as melhorias possam refletir na proposta para o projeto de software .
Engenheiro de Teste	O engenheiro de testes possui um papel de fundamental importância no processo de desenvolvimento de sistemas de software e a sua ausência em projeto de desenvolvimento de sistemas irá impactar diretamente na qualidade, consequência dessa ausência é percebida na má elaboração do projeto de teste, logo é uma das grandes causas de fracasso em projeto de software em diferentes áreas do conhecimento. • Qual a principal contribuição do engenheiro de teste para o projeto de aprimoramento de requisitos de segurança e privacidade de software da área financeira para a organização?	O engenheiro de teste possui um papel de grande importância no contexto do desenvolvimento de aplicações sistêmicas e, dessa forma, este profissional fará grande diferença nos resultados a serem entregues para a organização financeira. Para isso, o engenheiro de teste deve ser inserido no projeto desde a fase inicial para que o mesmo possa entender as necessidades da demanda solicitada e com isso prepara juntamente com os arquitetos e analistas de testes os detalhes do projeto a ser testado de acordo com o tipo de requisito a ser implementado para cada tipo de *stakeholders*. Dessa forma, elaborando o projeto e o plano de execução dos testes visando a garantia de que as novas requisições de privacidade não impactem nas funcionalidades e módulos existentes nas soluções sistêmicas.
Arquiteto de Testes	O arquiteto de testes em suas atividades poderá se deparar com diferentes dificuldades, no entanto, quando não há o envolvimento do arquiteto no projeto de testes, isso faz com que o tipo de teste a ser arquitetado para o projeto de software fique em segundo plano ou até mesmo inexistente nas organizações. • Qual a principal contribuição do arquiteto de teste no projeto de aprimoramento de requisitos de segurança e privacidade para a área financeira em projetos de testagem de software?	O Arquiteto de testes traz para o projeto de teste a importância de entender os requisitos a serem aprimorados para que com base nestes requisitos possa elaborar o projeto de teste a ser executado. Seu papel e mitigar os problemas no momento da execução, criando e disponibilizando para a equipe de analistas de testes toda a estrutura contendo os cenários a serem testas, assim como o passo a passo a ser seguido durante a execução de cada caso de teste do projeto de aprimoramento.
Engenheiro de software	A engenharia de software possui um papel de extrema importância no contexto de um sistema de software a ser desenvolvimento ou mesmo em fase aprimoramento. Quando não há envolvimento de engenheiros de software em projetos de desenvolvimento ou aprimoramento de requisitos, as necessidades quando implementadas poderão não atender as reais necessidades para as quais foram planejadas e implementadas para satisfazer as necessidades da organização em suas aplicações em ambientes *mobile Banking e Internet Banking.* • Pensando na importância do engenheiro de software em projetos de desenvolvimento de sistemas de software, qual seria a sua contribuição para o projeto de aprimoramento de requisitos de segurança e privacidade para a área financeira?	A engenharia de software traz para o projeto de aprimoramento de requisitos de segurança e privacidade para a área financeira grandes contribuições, dentre elas a estruturação do processo de desenvolvimento que deve ser seguido pela equipe de desenvolvimento, escolha das tecnologias a serem adotadas, metodologias para desenvolvimento de forma que as necessidades de aprimoramento nas aplicações sistêmicas se enquadre nas reais necessidades da equipe de desenvolvimento e na cultura da organização.

Gerente de Projetos	O gerenciamento de projetos de sistemas de software é uma atividade de grande importância, para isso, requer o papel de um *stakeholder* com conhecimentos e práticas para que possa gerenciar todas as etapas e atividades a serem desenvolvidas no projeto. Em projetos de desenvolvimento de sistemas de software poderão surgir diferentes tipos de problemas que deverão ser contornados pela gestão do projeto. Para aprimorar requisitos em sistemas de software existentes na organização se não houver planejamento de gestão das demandas poderão surgir atrasos nas entregas, não seguir o escopo e o cronograma adotado para o projeto de aprimoramento. • Como a gestão de projetos poderá contribuir para um gerenciamento eficaz das demandas de aprimoramento de requisitos de privacidade e segurança para a organização financeira?	A gestão de projeto possui um papel de grande destaque em projetos de desenvolvimento ou aprimoramento de sistemas de software, a gestão eficaz proporciona a organização produtos de software com qualidade que atenda as reais necessidades da organização, assim como as necessidades dos clientes ao utilizarem os serviços disponíveis em *mobile Banking e Internet Banking*, e em arquivos disponibilizados em canis digitais como é o caso das faturas *online*. Desse modo, a gestão proporciona grande contribuição para o projeto de aprimoramento de requisitos de privacidade e segurança na organização.

Tabela 15 - Avaliação dos Stakeholders a nível de Operação

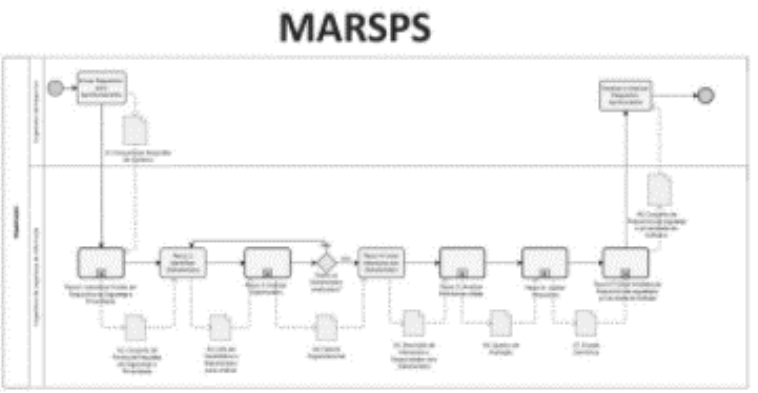
Stakeholder	Problemas e perguntas	Soluções e Ideias
Desenvolvedores de software	O desenvolvimento de sistema de software é primordial para que as necessidades elencadas para cada *stakeholders* envolvido com o projeto de aprimoramento do sistema sejam implementadas. Um dos grandes problemas encarados pela equipe de desenvolvimento de *software* é a falta de entendimento dos requisitos por incompletude ou ambiguidade dos requisitos. • Como garantir a contribuição dos desenvolvedores de *software* para o projeto de aprimoramento de requisitos de segurança e privacidade da área financeira na organização?	A equipe de desenvolvimento traz grandes contribuições para o projeto de aprimoramento, contribuição essa que se reflete na aceitação das implementações realizadas pelos desenvolvedores de *software* envolvido com o projeto de aprimoramento.
Cliente – Usuário final	O usuário final de uma aplicação sistêmica é um *stakeholders* que possui um envolvimento de destaque com o requisito que está sendo disponibilizado de forma aprimorada. No entanto, este *stakeholders* possui diferentes necessidades de privacidade e segurança que devem ser levadas em consideração na utilização das aplicações para realizar diferentes tipos de operações. As operações geram comprovantes e, tais comprovantes podem ser compartilhados em diferentes canis digitais. • Como garantir a proteção de dados pessoais dos clientes bancários durante o compartilhamento de comprovantes de transações bancarias em ambientes *Web* e dispositivos móveis?	Visando garantir que o usuário final da aplicação possa cada vez mais confiar nos serviços disponibilizados pelas instituições financeiras. Estas devem criar mecanismo para que usuários de aplicações bancárias possam confirmar o compartilhamento de informações das transações realizadas por meio de aplicações *Web* ou por meio da utilização de aplicativos utilizados por dispositivos móveis quando disponibilizados para produção pela organização.
Administrador de Sistemas	A administração de sistemas é uma atividade de grande importância dentro das organizações, no entanto, está atividade não é tão simples, pois gerenciar sistemas e seus *stakeholders* por meios de acessos, dessa forma visando garantir a autenticidade dos usuários na utilização da aplicação. A proteção dos dados dos sistemas também se torna problemas quando os responsáveis por esta não possuem expertise para tal responsabilidade. • Como garantir que a administração de sistemas esteja seguindo as determinações atribuídas pela organização para a demanda de gerenciar os sistemas?	O administrador de sistema deverá ser um *stakeholder* com bastante expertise na área de administração de sistemas, além de conhecimentos em outras áreas como banco de dados, políticas de segurança, redes etc. para que possa cumprir com excelência a função de administrar sistemas na organização. Essa administração deverá estar alinhada as necessidades da organização e a proteção e privacidade dos dados e informações dos *stakeholders* da organização na utilização da solução sistêmica que foi aprimorada para as plataformas *mobile Banking e Internet Banking*.

APÊNDICE C – Questionário da validação do MARSPS pelos especialistas.

Passo:1 Identificar Fontes de Requisitos

Requer listar conjunto de fontes de requisitos de segurança e privacidade - A2

MARSPS



1.1 - Na execução do passo 1, identificação das fontes de requisitos de privacidade e segurança você considera que as fontes elencadas para aprimoramento de requisitos de privacidade e segurança da área financeira são suficientes? Por que? *

Sua resposta

1.2. Você teve dificuldade para identificar e acessar as fontes de requisitos de privacidade e segurança? *

Sua resposta

1.3 - Você considera que as fontes de requisitos de privacidade utilizadas são suficientes para o aprimoramento de requisitos de privacidade e segurança? Se sim quais outras fontes poderiam ser utilizadas? *

Sua resposta

Voltar Próxima

Passo 2 - Identificar Stakeholders

Requer listar os candidatos a Stakeholders para Análise - A3

2.1 - Na execução do passo 2, foi fácil identificar os stakeholders que estão relacionados com os requisitos a serem aprimorados? *

Sua resposta

2.2 - Cite as vantagens, desvantagens e dificuldades para identificar os stakeholders. *

Sua resposta

Voltar Próxima

Passo 3 - Analisar Stakeholders

Requer a construção da Cebola Organizacional - A4

3.1 - Na execução do passo 3, analisar Stakeholders, você teve alguma dificuldade para analisar os stakeholders correspondentes a cada uma das camadas da cebola organizacional? *

Sua resposta

3.2 - Quais dificuldades você identificou para construir a cebola organizacional? Poderias descrever as dificuldades? *

Sua resposta

3.3 - Quais vantagens e desvantagens que considera ao construir a cebola organizacional para analisar stakeholders na organização? *

Sua resposta

Voltar Próxima

Passo 4 - Listar Interesses dos Stakeholders

Requer a construção da descrição de interesses e necessidades dos Stakeholders - A5

4.1 -Na execução do passo 4, identificar interesses dos Stakeholders, quais foram as dificuldades encontradas para listar os interesses de privacidade e segurança de cada stakeholders relacionado com os requisitos a serem aprimorados? *

Sua resposta

4.2 - Numa escala de 1 a 5, onde 1 você discorda totalmente e 5 você concorda totalmente. Os stakeholders descrevem suas necessidades de segurança e privacidade de forma clara e objetiva? *

- ◯ 1. Discordo totalmente
- ◯ 2. Discordo parcialmente
- ◯ 3. Indiferente
- ◯ 4. Concordo parcialmente
- ◯ 5. Concordo totalmente

4.3 - Numa escala de 1 a 5, onde 1 você discorda totalmente e 5 você concorda totalmente, como avalia importância do envolvimento dos Stakeholderes durante a atividade de identificação dos requisitos? *

- ◯ 1. Discordo totalmente
- ◯ 2. Discordo parcialmente
- ◯ 3. Indiferente
- ◯ 4. Concordo parcialmente
- ◯ 5. Concordo totalmente

Voltar Próxima

Passo 5 - Analisar Problemas e Soluções

Requer a construção do Quadro de Avaliação - A6

5.1 - Na execução do passo 5, para a construção do Quadro de Avaliação quais são as vantagens e desvantagens de se utilizar este passo no aprimoramento de requisitos de privacidade e segurança em sistemas da área financeira? *

Sua resposta

5.2- Numa escala de 1 a 5, onde 1 você discorda totalmente e 5 você concorda totalmente, a construção do quadro de avaliação contribuiu para um melhor entendimento para resolução dos problemas relacionados com as necessidades de privacidade e segurança dos requisitos identificados? *

- ◯ 1. Discordo totalmente
- ◯ 2. Discordo parcialmente
- ◯ 3. Indiferente
- ◯ 4. Concordo parcialmente
- ◯ 5. Concordo totalmente

Voltar Próxima

Passo 6 - Avaliar Requisitos

Requer a construção a Escada da Semiótica

6.1 – Numa escala de 1 a 5, onde 1 você discorda totalmente e 5 você concorda totalmente, como você avalia as "Funções do Sistema de informação humano" na construção da escada da semiótica para o aprimoramento de requisitos de privacidade e segurança da área financeira? *

- ◯ 1. Discordo totalmente
- ◯ 2. Discordo parcialmente
- ◯ 3. Indiferente
- ◯ 4. Concordo parcialmente
- ◯ 5. Concordo totalmente

6.2 – Numa escala de 1 a 5, onde 1 você discorda totalmente e 5 você concorda totalmente, como você avalia as "Plataforma de Tecnologia da Informação" na construção da escada da semiótica para o aprimoramento de requisitos de privacidade e segurança da área financeira? *

- ◯ 1. Discordo totalmente
- ◯ 2. Discordo parcialmente
- ◯ 3. Indiferente
- ◯ 4. Concordo parcialmente
- ◯ 5. Concordo totalmente

6.3 - Você teve dificuldade para construir a escada de semiótica para avaliar os requisitos de privacidade e segurança nos grupos: "Funções do Sistema de informação humano" e "Funções do Sistema de informação humano"? *

Sua resposta

Quais foram as vantagens e desvantagens encontradas na construção da escada da semiótica? *

Sua resposta

Voltar Próxima

Passo 7 - Gerar artefato de Requisitos de e segurança e privacidade de software

7.1 - Durante a execução do MARSPS para aprimorar requisitos de privacidade e segurança houve alguma dificuldade para escolher a saída do método e gerar o artefato contendo o requisito aprimorado? *

Sua resposta

7.2 - Numa escala de 1 a 5, onde 1 discorda totalmente e 5 concorda totalmente, você considera que saídas apresentadas na execução do MARSPS são suficientes para gerar artefatos de requisitos? *

- ◯ 1. Discordo totalmente
- ◯ 2. Discordo parcialmente
- ◯ 3. Indiferente
- ◯ 4. Concordo parcialmente
- ◯ 5. Concordo totalmente

Voltar Próxima

Ponto de Vista do Profissional em relação ao MARSPS

Numa escala de 1 a 5, onde 1 discorda totalmente e 5 concorda totalmente, a execução do MARSPS para aprimorar requisitos de privacidade e segurança da área financeira a sequência de passos foram suficientes? *

- ◯ 1. Discordo totalmente
- ◯ 2. Discordo parcialmente
- ◯ 3. Indiferente
- ◯ 4. Concordo parcialmente
- ◯ 5. Concordo totalmente

Você recomendaria alguma alteração ou melhorias nos passos descritos no MARSPS para o aprimoramento dos requisitos de privacidade e segurança para organização? *

Sua resposta

Numa escala de 1 a 5, onde 1 discorda totalmente e 5 concorda totalmente, você consideraria o MARSPS como um instrumento para apoiar no aprimoramento dos requisitos de privacidade e segurança da área financeira? *

- ◯ 1. Discordo totalmente
- ◯ 2. Discordo parcialmente
- ◯ 3. Indiferente
- ◯ 4. Concordo parcialmente
- ◯ 5. Concordo totalmente

Na sua opinião o que diferencia o MARSPS de outros métodos existentes para aprimoramento de requisitos de privacidade e segurança em projetos de melhoria de sistemas de software da área financeira? *

Sua resposta

Voltar Próxima

Obrigado pela Colaboração

Eu, Leonardo Mendes, agradeço imensamente pela sua colaboração nesta etapa de validação do instrumento de pesquisa que foi apresentado como uma proposta de Projeto de Pesquisa no mestrado em Ciência da Computação.