UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE
CENTRO DE CIÊNCIAS EXATAS E DA TERRA
DEPARTAMENTO DE INFORMÁTICA E MATEMÁTICA APLICADA
PROGRAMA DE PÓS-GRADUAÇÃO EM SISTEMAS E COMPUTAÇÃO

Um Framework Fundamentado na Engenharia de Requisitos para Apoiar a Conformidade Legal e Regulatória em Sistemas Computacionais

Erica Esteves Cunha de Miranda

Natal/RN
2021

Um Framework Fundamentado na Engenharia de Requisitos para Apoiar a Conformidade Legal e Regulatória em Sistemas Computacionais

Erica Esteves Cunha de Miranda

Tese de Doutorado apresentada ao Programa de Pós-Graduação em Sistemas e Computação do Centro de Ciências Exatas e da Terra da Universidade Federal do Rio Grande do Norte como requisito parcial para a obtenção do título de Doutora em Ciência da Computação.

Área de concentração: Engenharia de Software.

Orientadora: Profa. Dra. Márcia Jacyntha Nunes Rodrigues Lucena

Natal/RN
2021

Universidade Federal do Rio Grande do Norte – UFRN
Sistema de Bibliotecas - SISBI
Catalogação de Publicação na Fonte. UFRN - Biblioteca Setorial Prof. Ronaldo Xavier de Arruda - CCET

Miranda, Erica Esteves Cunha de.
Um framework fundamentado na engenharia de requisitos para apoiar a conformidade legal e regulatória em sistemas computacionais / Erica Esteves Cunha de Miranda. - 2021.
232f.: il.

Tese (Doutorado) - Universidade Federal do Rio Grande do Norte, Centro de Ciências Exatas e da Terra, Departamento de Informática e Matemática Aplicada, Programa de Pós-Graduação em Sistemas e Computação. Natal, 2021.
Orientadora: Profa. Dra. Márcia Jacyntha Nunes Rodrigues Lucena.

1. Engenharia de software - Tese. 2. Requisito legal ou regulatório - Tese. 3. Conformidade legal e regulatória - Tese. 4. Fonte legal ou regulatória - Tese. 5. Ecossistema ágil - Tese. 6. Framework - Tese. I. Lucena, Márcia Jacyntha Nunes Rodrigues. II. Título.

RN/UF/CCET CDU 004.41

Elaborado por Joseneide Ferreira Dantas – CRB15/324

ÉRICA ESTEVES CUNHA DE MIRANDA

"***Um Framework Fundamentado na Engenharia de Requisitos para Apoiar a Conformidade Legal e Regulatória em Sistemas Computacionais***"

Esta Tese foi julgada adequada para a obtenção do título de Doutor em Ciência da Computação e aprovada em sua forma final pelo Programa de Pós-Graduação em Sistemas e Computação do Departamento de Informática e Matemática Aplicada da Universidade Federal do Rio Grande do Norte.

Prof.ª Dr.ª ANNE MAGALY DE PAULA CANUTO
Coordenadora do PPgSC

Banca Examinadora

(Assinado digitalmente em 05/08/2021 11:00)
APUENA VIEIRA GOMES
PROFESSOR DO MAGISTERIO SUPERIOR
IMD (11.00.05)
Matrícula: 3229319

(Assinado digitalmente em 04/08/2021 21:09)
EDUARDO HENRIQUE DA SILVA ARANHA
PROFESSOR DO MAGISTERIO SUPERIOR
DIMAP/CCET (12.05)
Matrícula: 1671962

(Assinado digitalmente em 03/08/2021 18:57)
JOSUÉ VITOR DE MEDEIROS JÚNIOR
PROFESSOR DO MAGISTERIO SUPERIOR
DEPAD/CCSA (16.14)
Matrícula: 1696802

(Assinado digitalmente em 03/08/2021 18:49)
MARCIA JACYNTHA NUNES RODRIGUES LUCENA
PROFESSOR DO MAGISTERIO SUPERIOR
DIMAP/CCET (12.05)
Matrícula: 2195240

(Assinado digitalmente em 03/08/2021 18:43)
MARÍLIA ARANHA FREIRE
ASSINANTE EXTERNO
CPF: 837.479.314-72

(Assinado digitalmente em 03/08/2021 17:53)
FERNANDA MARIA RIBEIRO DE ALENCAR
ASSINANTE EXTERNO
CPF: 349.895.954-91

(Assinado digitalmente em 04/08/2021 12:17)
ERICA ESTEVES CUNHA DE MIRANDA
DISCENTE
Matrícula: 20171007650

Para verificar a autenticidade deste documento entre em https://sipac.ufrn.br/documentos/ informando seu número: **1**, ano: **2021**, tipo: **FICHA DE AVALIAÇÃO**, data de emissão: **03/08/2021** e o código de verificação: **d0beb9c1e8**

Dedicatória

Dedico este trabalho à minha mãe Maria Edna Esteves Cunha, ao meu pai Elcio Lopes Cunha (*in memoriam*) e ao meu esposo Leonardo Cunha de Miranda pelo eterno e incondicional incentivo, amor e dedicação.

Agradecimentos

Tenho muito a agradecer!

Gostaria de começar agradecendo aos meus mentores da vida profissional e amigos de uma vida inteira: Dr. Gabriel Moraes Moysés, Profª. Anita Luiza Maciel Lopes, Prof. José Antonio dos Santos Borges, Prof. Gabriel Pereira da Silva, Profª. Ligia Alves Barros, Profª. Carmen Perrotta, Ana Malta.

Agradeço à pessoa que tornou a concretização desse sonho possível com sua experiência, sua atenção e suas orientações: Profª. Márcia Jacyntha Nunes Rodrigues Lucena.

Agradeço também aos Professores que aceitaram o convite para compor a banca examinadora desta tese de doutorado: Apuena Vieira Gomes, Eduardo Henrique da Silva Aranha, Fernanda Maria Ribeiro de Alencar, Josué Vitor de Medeiros Júnior, Marília Aranha Freire.

Reconheço, e por isto sou grata, as contribuições diretas ou indiretas na minha formação profissional e acadêmica de todos os professores do Departamento de Informática e Matemática Aplicada e da Pós-Graduação em Sistemas e Computação.

Assim como, faço uma homenagem por sua importância ao corpo técnico-administrativo e operacional do DIMAp pela disponibilidade em ajudar operacional e cotidianamente, em especial: Hélida Santos, Daniel Oliveira, Denis Medeiros, Sra. Rita de Cássia e Sr. Gaspar.

Sinto-me agraciada pela amizade, pelos momentos de descontração, pela força e pelo constante aprendizado junto aos amigos e aos colegas do Laboratório de Especificação e Teste de Software (LETS), em especial: Ilueny Santos, Gabriela Trindade, Fábio Penha, Hugo Melo, Eduardo Henrique, Rose Borges, Lucas Mariano, João Carlos, Renato Mesquita, Luana Souza, Rafael Jullian.

Sou muito grata ao meu esposo Leonardo Cunha de Miranda pelo amor, pela paciência, pelo companheirismo e pelo carinho ao longo desses últimos 20 anos e pelos próximos que virão.

Preciso dizer muito obrigada à minha mãe Maria Edna Esteves Cunha e ao meu pai (*in memoriam*) Elcio Lopes Cunha por todo amor, carinho, formação, incentivo e cuidados em toda a minha vida; aos meus irmãos Elcio e Eduardo e aos meus primos Janaina e Marcos Vinícius, que são companheiros de uma vida inteira.

Contemplo nesta homenagem igualmente aos meus sogros, às minhas cunhadas e aos meus cunhados pela amizade, pelo apoio e pelo carinho ao longo das nossas relações; às minhas sobrinhas e ao meu sobrinho pelo amor e por aceitarem minha ausência em alguns momentos tão importantes em suas vidas.

Enfim, sou muito agradecida a todos vocês que de modo direto ou indireto contribuíram para o alcance de um sonho e a ampliação dos meus horizontes.

“Aos que anseiam a bela visão do
desabrochar das flores, mostraria (de
bom grado) toda potência da
primavera nas bravas sementes que
repousam sob a neve das montanhas.”

Fujiwara no Ietaka

Um Framework Fundamentado na Engenharia de Requisitos para Apoiar a Conformidade Legal e Regulatória em Sistemas Computacionais

Autora: Erica Esteves Cunha de Miranda

Orientadora: Profª. Drª. Márcia Jacyntha Nunes Rodrigues Lucena

Resumo

O universo legal e regulatório permeia a tudo e a todos. Sendo assim, os sistemas computacionais necessitam estar desde sua concepção, evolução, ou até sua manutenção em conformidade legal e regulatória com as leis, normas, regulamentação, regimentos, estatutos, padrões, dentre outras mídias legais (nomeadas, nesta pesquisa, de fontes legais ou regulatórias - FLR), que regem o seu domínio, o seu contexto de aplicação. O objetivo desta pesquisa foi oferecer uma alternativa ao profissional da Computação (analistas de requisitos e gerentes de projeto, principalmente) de verificar e manter esta conformidade legal e regulatória em seus projetos, onde as fontes legais ou regulatórias não abrangem mais apenas pessoas físicas ou jurídicas, mas também pessoas digitais e, onde, essas FLR podem não ser mais somente nacionais. Identificar, definir e priorizar essas FLR passaram a ser problemas para esses profissionais da Computação em diferentes contextos, em especial nos ecossistemas ágeis de desenvolvimento de sistemas computacionais. Deste modo foram adotadas seguintes estratégias metodológicas: revisão sistemática da literatura; entrevistas presenciais e remotas; questionários; estudos de caso; pesquisa-ação; e etnografia organizacional. Como resultado desta pesquisa, foi formalizado e avaliado, junto a representantes do público-alvo de usuários, um framework visando auxiliar profissionais da Computação, no processo de implementação, implantação e verificação (auditoria) da conformidade legal e regulatória em sistemas computacionais em ecossistemas ágeis, não obstante facilmente adaptável a qualquer outra metodologia. Assim, além de criar facilidades em todo o ciclo de trabalho com os requisitos legais ou regulatórios, possibilita sistemas computacionais em conformidade legal e regulatória com FLR, as quais estiverem submetidos.

P*alavras-chave: requisito legal ou regulatório, conformidade legal e regulatória, fonte legal ou regulatória, ecossistema ágil, framework.*

A Framework Based on Requirements Engineering to Support Regulatory and Legal Compliance in Computer Systems

Author: Erica Esteves Cunha de Miranda
Advisor: Prof. Ph.D. Márcia Jacyntha Nunes Rodrigues Lucena

Abstract

The regulatory and legal universe permeates everything and everyone. Therefore, computer systems need to be from their conception, evolution, or even their maintenance in regulatory and legal compliance with the laws, rules, regulations, bylaws, statutes, standards, among other legal media (named, in this research, from regulatory or legal sources - RLS) that rule your domain, your application context. The objective of this research was to offer a alternative to the Computing professional (e.g., requirements analysts/engineers and project managers) ways to verify and maintain legal and regulatory compliance in their projects, where regulatory or legal sources no longer cover only individuals or legal entities, but also digital people and those RLS can not be only national. Identifying, defining, and prioritizing these RLS have become problems for these Computing professionals in different contexts, especially in agile ecosystems of computing systems development. Thus, the following methodological strategies were adopted: systematic literature review; face-to-face and remote interviews; questionnaires; case studies; action research; and organizational ethnography. As a result of this research, it was formalized and evaluated with representatives of the target user audience a framework aimed for assisting Computing professionals, in the deployment and implementation process, and verification (audit) of regulatory or legal compliance in computer systems in agile ecosystems, despite being easily adaptable to any other methodology. Thereby, in addition to creating facilities throughout the work cycle with regulatory or legal requirements, enable computer systems in regulatory and legal compliance with RLS.

Keywords: regulatory or legal requirement, regulatory and legal compliance, regulatory or legal source, agile ecosystem, framework.

Lista de Figuras

Figura 1: Tríade da fundamentação teórica. 24
Figura 2: Visão da divisão dos requisitos funcionais e não funcionais. 26
Figura 3: Decomposição ou refinamento de requisito. 28
Figura 4: Demonstração do processo de tornar-se um requisito testável. 28
Figura 5: Estrutura de Risco Operacional segundo Basiléia II. 33
Figura 6: Demonstra o processo entre o protocolo implementado e sua execução. 44
Figura 7: Representa o processo de “filtragem” 51
Figura 8: Gráfico com a distribuição dos estudos selecionados por ano. 54
Figura 9: Gráfico dos assuntos mais encontrados nos estudos selecionados. 55
Figura 10: Gráfico sobre a qualidade atribuída a cada estudo. 56
Figura 11: Gráfico do perfil dos participantes das entrevistas. 76
Figura 12: Gráfico apresentando o tempo de experiência no cargo dos respondentes. 77
Figura 13: Gráfico da distribuição dos respondentes por sexo. 77
Figura 14: O *template* de requisitos completos, com especificações de condições temporais e lógicas. 87
Figura 15: Visão Geral do Framework. 88
Figura 16: Modelo de rastreabilidade para requisitos legais. 90
Figura 17: Diagrama de transição de estados da vigência da norma. 93
Figura 18: Diagrama da transformação de fonte(s) legal(is) ou regulatória(s) - FLR - em requisito(s) legal(is) ou regulatório(s) testável(is) - RLRT. 100
Figura 19: Diagrama sobre fundamentação de requisito(s) legal(is) ou regulatório(s) testável(is) - RLRT - a partir de fonte(s) legal(is) ou regulatória(s) - FLR. 101
Figura 20: Gráfico dos Cargos/Funções dos respondentes da pesquisa. 109
Figura 21: Gráfico da distribuição dos respondentes por sexo. 109
Figura 22: Gráfico da formação acadêmica dos respondentes. 109
Figura 23: Gráfico com os tipos de rastreabilidade realizadas. 116

Lista de Tabelas

Tabela 1: Matriz de sinônimos para termos para string de busca. 46
Tabela 2: Método PICOC (population, intervention, control, outcome, context).....47
Tabela 3: Artigos selecionados na revisão sistemática da literatura.....51
Tabela 4: Sumarização dos projetos feitos em colaboração.....68
Tabela 5: Caracterização dos participantes das entrevistas.....78
Tabela 6: Exemplo de história de usuário com requisito legal. 85

Lista de Abreviaturas e Siglas

CCET – Centro de Ciências Exatas e da Terra
DIMAp – Departamento de Informática e Matemática Aplicada
FLR – fonte(s) legal(is) ou regulatória(s)
GDPR – General Data Protection Regulation
JSON – JavaScript Object Notation
LGPD – Lei Geral de Proteção de Dados Pessoais
PPgSC – Programa de Pós-Graduação em Sistemas e Computação
RLR – requisito(s) legal(is) ou regulatório(s)
RLRT – requisito(s) legal(is) ou regulatório(s) testável(is)
UFRN – Universidade Federal do Rio Grande do Norte
Web – World Wide Web
XML – Extensible Markup Language

Sumário

1 Introdução 15
1.1 Contexto da pesquisa 16
1.2 Problema e relevância 19
1.3 Objetivos 20
1.4 Justificativa 20
1.5 Metodologia 21
1.6 Organização dos capítulos 22
2 Fundamentação Teórica 24
2.1 Fontes legais e regulatórias 25
2.1 Requisitos legais e regulatórios 26
2.2 Visualização da informação 30
2.4 Direito Digital 31
2.5 Conformidade legal e regulatória 32
2.6 Políticas, planos e processos 34
2.7 Cultura e profissionais generalistas *versus* especialistas 36
2.8 Requisitos legais e regulatórios em metodologias ágeis 37
2.9 Trabalhos relacionados 38
2.10 Considerações 39
3 Revisão Sistemática da Literatura 40
3.1 Conformidade legal e regulatória em ecossistemas ágeis de desenvolvimento de sistemas computacionais 41
3.2 Metodologia para realização da revisão sistemática 42
3.3 Resultados por questão de pesquisa 56
3.4 Discussão 65
3.5 Considerações 66
4 Estudos Exploratórios 67
4.1 Caracterização dos projetos em colaboração 70
4.2 Projeto com foco em conformidade legal e regulatória 73
4.3 Discussões e considerações 81
5 Framework 83
5.1 Solução Proposta 83
5.2 A transformação de uma fonte legal ou regulatória em requisito legal ou regulatório 85
5.3 Componentes do *Framework* 87
5.4 Fluxos de atividades 99

5.5 Auditoria de tecnologias da informação e da comunicação 102
5.6 Discussões e considerações 103
6 Avaliação do *Framework*..... 105
6.1 Planejamento e desenho da avaliação..... 105
6.2 Análise das respostas ao questionário e as entrevistas 113
6.4 Limitações e ameaças à validade..... 133
6.5 Discussão e considerações..... 134
7 Considerações Finais..... 136
7.1 Contribuições a serem destacadas 137
7.2 Publicações decorrentes do processo de doutoramento..... 138
7.3 Trabalhos futuros..... 140
7.4 Conclusões finais..... 140
Referências..... 142
Apêndices 157
Apêndice A - Instrumentos de Apoio aos Estudos Exploratórios 158
Apêndice B – *Template* para criação de documentação de um requisito 204
Apêndice C – Exemplos da transformação de história de usuário em requisito legal ou regulatório e sua relação com a legislação aplicável 207
Apêndice D – Instrumentos de Apoio à Avaliação do *Framework* Proposto..... 214

1 Introdução

A área Engenharia de Requisitos é inter e multidisciplinar dada a sua natureza de tratar com diferentes domínios, pessoas, interesses e intenções. Quando opera no domínio legal ou regulatório, encontra diversos desafios, que por um momento, podem parecer intransponíveis. Visto que a lei pode ser entendida, como foi defendida por Kelsen (1949): "a lei é a norma primária, que estipula sanção". Sem a sanção, tudo passa a ser apenas uma recomendação, um conselho, uma lição, por exemplo. Desse modo, é necessário maior atenção ao fato de, em diferentes momentos, ser o fiel da balança, um juiz, por exemplo, ser o responsável por decidir por aquilo que é mais justo aos olhos da Lei e dos homens para um jurista, o que para um engenheiro de requisitos pode parecer até arbitrário.

Por outro lado, como esperado, estar inserida neste universo de leis, normas, regulamentação, regimentos, estatutos, padrões, dentre outros não é surpreendente, todavia deverasmente desafiador, quando se observa a instabilidade, a fragilidade, a parcialidade e a pessoalidade nos textos e nas ações que, por via de regra, não deveriam ter. Foi cunhado um termo para facilitar a referência a estes textos e suas características compartilhadas por essa variedade de "consciências", que, de alguma forma, tentam traduzir o que é cultural, moral ou tecnicamente aceito pela sociedade. Isto, considerando que, atualmente, podem ser utilizadas diferentes mídias para informar, ou melhor, formalizar um "texto legal", a opção foi nesta tese empregar o termo "fonte legal ou regulatória" (FLR) ou, em inglês, "regulatory or legal source" (RLS). Assim, não importaria em qual tipo de mídia a fonte dos requisitos do sistema apresentar-se-ia e, também possibilitaria melhor adequação à constante e crescente criação de novos formatos de divulgação destes tipos de documentos.

Do mesmo modo, isto torna o termo mais abrangente por considerar uma variedade de documentos, que necessariamente não são de origem da área de Direito, mas também aqueles oriundos de órgão normativos ou regulatórios de um domínio ou contexto, por exemplo. Ainda, é preciso observar que a globalização da sociedade trouxe elementos para além da cultura, como o que é tido como intercultural (BAUMAN, 1998). Isto muda, o que é aceito por aqueles que vivem neste mundo intercultural e multicultural. É mais uma preocupação dos que vivem dos negócios e no mundo digital (BECK, 2018): pessoas físicas, pessoas jurídicas e pessoas simplesmente digitais (PECK, 2013).

Neste mundo "digital", embora seja regulado pelo novíssimo Direito Digital, que é precedido e fundamentado por todos os outros tipos de direito, defende, de certa forma, a

autorregulação baseada em contratos firmados em as partes, visto as particularidades relacionadas ao tempo (a urgência por conta de segundo, que pode gerar um malefício maior do que, por exemplo, um serviço oferecido pelos meios tradicionais) e a geolocalização (fontes legais ou regulatórias próprias ou serviços ainda não legalizados/formalizados no local em questão), que podem atingir as partes de forma oposta, inclusive. Assim, as principais áreas do Direito, como Civil, Autoral, Comercial, Contratual, Econômico, Financeiro, Tributário, Penal, Internacional, dentre outros (PECK, 2013) precisam ser considerados, quando do projeto, manutenção e evolução dos sistemas. Além disso, ainda precisam ser consideradas todas e quaisquer fontes legais ou regulatórias relacionadas com o contexto, domínio do sistema e localização do usuário, do serviço oferecido ou do armazenamento das informações (GARG et al., 2015).

O conhecimento da legislação ou normas não é facultativo ao indivíduo na sociedade brasileira, embora pareça ser cultural alegar o desconhecimento (BRASIL, 2019). Igualmente, acontece com o proprietário ou desenvolvedor de um sistema computacional, que precisa estar ciente de toda e qualquer legislação ou norma aplicável ao contexto, domínio e localidade de armazenamento, instalação ou uso do sistema propriamente dito (BRASIL, 2014; GORDON e BREAUX, 2011). Cliente e desenvolvedor são solidários com relação à responsabilidade ao sistema implementado, mantido e gerenciado desde o ano 2014, quando da promulgação da Lei nº 12.965, de 23 de abril de 2014, considerada o Marco Civil da Internet (BRASIL, 2014). Ademais, provedores e toda cadeia de fornecimento e produção do bem ou do serviço também podem ser solidárias, quando não observados os diferentes tipos de contratos estabelecidos (GONÇALVES, 2017). Na Era Digital, o instrumento de poder é a informação, não só recebida, mas refletida (PECK, 2013).

1.1 Contexto da pesquisa

Considerando as novas tecnologias, a velocidade de transformação da informação e da sociedade, a evolução das fontes legais ou regulatórias, e a difícil preservação e continuidade no mundo dos negócios, os sistemas computacionais estão em constante expansão. Assim, estes sistemas sofrem frequentes correções, manutenções e evoluções para garantir sua sustentação ao longo dos anos. Por conta disso, os sistemas computacionais estão cada vez mais complexos, abarcando novos e diferentes conceitos, públicos (clientes e usuários), intenções operacionais (sociais - por exemplo, interacionais, comunicações, mobilizações; negócios - como, comércio,

parcerias e transações financeiras; “hacking” - por exemplo, utilização para a finalidade não previamente estabelecida, obtenção de informações de forma incorreta, identificação de falhas e modificações de seus artefatos) e possibilidades de intervenções (por exemplo - política em virtude de alguma anomalia ou exceção, realização de auditoria, supressão de módulos). Assim, qualquer sistema computacional pode ser visto e tratado como um produto ou um serviço e, compulsoriamente, deve estar em conformidade legal e regulatória à luz de seu contexto, domínio, tempo e geolocalização.

Observou-se que o emprego de metodologias ágeis, além de promissor, estava arraigado no contexto dos ambientes aos quais havia interesse em realizar esta pesquisa. Assim, mostrou-se como caminho natural, conhecer formas, meios, instrumentos, e artefatos utilizados, bem como as estratégias e as dificuldades enfrentadas por aqueles profissionais imersos nesse mundo ágil. Para a área de Engenharia de Requisitos, esse mundo ágil traz em essência desafios e práticas distintas do emprego das metodologias tradicionais no ciclo de vida dos sistemas computacionais.

Para Ramesh, Cao e Baskerville (2010), Inayat *et al.* (2015) e Kasauli *et al.* (2021) os principais desafios são, por exemplo: a exigência de documentação mínima; lidar com a disponibilidade do cliente; a possibilidade de planejamento de uma arquitetura e de uma infraestrutura inadequadas; a falta de estimativa de orçamento e tempo; o fato de, geralmente, se negligenciar requisitos não funcionais; a necessidade de concordância e a incapacidade do cliente de lidar com questões técnicas; a obrigação de construir e manter uma compreensão compartilhada do valor do cliente e do sistema; as limitações contratuais; as constantes mudanças de requisitos e verificação inadequada de requisitos; a priorização em uma única dimensão; a criação e a manutenção de rastros; a dificuldade de manutenção da compatibilidade com versões anteriores; o esforço da aprendizagem e conhecimento serem de longo prazo; a dificuldade de gerenciar níveis e decomposições; a falta de apoiar diferentes representações; o esforço de gerenciar integridade; a falta de processos de engenharia de requisitos consistentes; a relação de qualidade *versus* tempo de colocação no mercado; o plano de verificação e validação com base apenas nas necessidades.

Dessa forma, dada a complexidade e a velocidade imposta para manutenção e evolução dos sistemas computacionais e da sociedade, associadas às metodologias de desenvolvimento/manutenção/evolução de sistemas computacionais, talvez, o mais difícil seja a identificação e a manutenção dos relacionamentos entre os artefatos, sua visualização e sua documentação com evidência legal. Há pouca ou nenhuma preocupação em promover a rastreabilidade, visualização e documentação entre esses artefatos, instrumentos que poderiam

ser utilizados de diferentes formas no ciclo de um sistema. Exemplos disso seriam: a identificação de artefatos, que serão impactados por uma alteração; responsáveis pela implementação e solicitação de um artefato; evidenciação da conformidade legal e regulatória de um sistema computacional.

A rastreabilidade, entendida como a oportunidade de rastrear artefato durante todo o ciclo de vida de um sistema, parafraseando o que foi dito por Pohl (2010) com relação a um requisito, possibilitaria, por exemplo, a relação de uma lei com os requisitos legais ou regulatórios decorrentes. Esses por sua vez com as funcionalidades ou regras do sistema computacional, além de todo e qualquer artefato derivado e relacionado, que for considerado importante pela equipe de desenvolvimento, manutenção, sustentação e evolução de um sistema computacional. Ressalta-se que os artefatos produzidos e rastreados podem ser diferentes para cada equipe, visto que isto envolve custos, manutenção e importância atribuída pelos interessados.

Desafios que podem se tornar maiores, quando contemplada, então, a obrigatoriedade de atendimento às leis e à regulação, e sua constante evolução, como reflexo da sociedade e de sua cultura, a rastreabilidade também poderia facilitar a gestão de mudanças. Esta gestão pode ser decisiva em diferentes aspectos na busca pela conformidade de um sistema, por exemplo: manutenibilidade, sustentabilidade, promoção e verificação da qualidade e da legalidade, derivação de novos produtos. Todavia, apenas a rastreabilidade pode não ser suficiente para a conformidade e a sustentabilidade dos projetos de sistemas computacionais. Por isso podem ser vistas outras estratégias sendo utilizadas com a intenção de dar maior robustez a esses projetos, como diferentes formas de visualização dos artefatos (SPENCER, 2014), uso de ferramentas ou metodologias para apoio a gestão da informação e da documentação (CONSELHO NACIONAL DE ARQUIVOS - BRASIL, 2011), identificação e tradução de requisitos (SIENA et al., 2008).

A liquidez observada na sociedade moderna (BAUMAN, 2013) e na cultura decorrente pode ser dita como a pedra angular da complexidade dos sistemas computacionais utilizados por essa mesma sociedade; mais ainda quando considerada a imposição da conformidade legal e regulatória desses sistemas. Isto é perene. A indústria 4.0 não vende mais o produto, e sim o projeto, os serviços associados (BETTIOL, 2020). Por esta razão, esforços para adequação podem ser observados quando há uma preocupação na garantia de privacidade e segurança dos dados privados (BARROSO, 2017a; PINHEIRO, 2020), na transformação digital (MILANI, 2019), na transparência dos dados dos serviços públicos (BARROSO, 2017), na redução de

riscos relacionados à sustentabilidade de um sistema (PASQUALINO, 2021), na curadoria das informações de uma instituição (SABHARWAL, 2015), por exemplo.

1.2 Problema e relevância

A falta da observação de leis, normas, regulamentação, regimentos, estatutos, em suma "fontes legais ou regulatórias", presentes na sociedade moderna, resulta na inconformidade legal ou regulatória em todos e quaisquer sistemas, independentemente de sua natureza, seu propósito, ou sua classificação. A conformidade legal e regulatória não é algo, simplesmente, a ser atingida, e sim regularmente a ser verificada e mantida.

Entende-se que, além desta temática, outras temáticas das gerações 4.0 ou 5.0 trazem em seu cerne, naturalmente a necessidade de conformidade legal e regulatória, como, por exemplo: *Smart Cities* (Cidades Inteligentes), *Business* 5.0 (Negócios 5.0), *Society* 5.0 (Sociedade 5.0), *Industry* 4.0/5.0 (Indústria 4.0/5.0), *Digital Governance* 4.0 (Governança Digital 4.0), *Supply Chain* 4.0 (Cadeia/Rede/Gestão da Cadeia de Mantimentos), *Services* 4.0 (Serviços 4.0), *Brain* 4.0 (Cérebro 4.0), *Health* 4.0 (Saúde 4.0).

Assim, a problemática tratada nesta tese pode ser dividida em duas partes, que estão diretamente relacionadas à:

- Como melhor realizar a engenharia dos requisitos legais ou regulatórios relacionados ao contexto dos sistemas computacionais em diferentes domínios?
- Como implementar e rastrear os artefatos destes sistemas, de forma a manter a conformidade legal e regulatória do sistema em questão e, ainda, oferecendo evidências legais aos auditores e agências reguladoras ou fiscalizadoras?

A principal relevância atribuída a esta pesquisa está associada à diligência e aos artefatos produzidos para minimizar os esforços dos interessados no processo de desenvolvimento, manutenção e evolução dos sistemas computacionais. Sendo que os interessados, que terão, principalmente, o enfoque da pesquisa serão os gerentes de projetos e os analistas/engenheiros de requisitos, enquanto, com relação ao processo, o maior ponto de interesse será a manutenção da conformidade legal e regulatória dos sistemas computacionais.

1.3 Objetivos

O objetivo geral desta pesquisa é propor uma sistemática para melhorar a manutenção da conformidade legal e regulatória dos sistemas computacionais a partir da evolução do sistema, das fontes legais ou regulatórias aplicáveis ao contexto do sistema e dos requisitos legais ou regulatórios elicitados ou atualizados. Para melhor conduzir esta pesquisa foram traçados objetivos específicos e representativos para o processo definido:

1. Realizar levantamento do estado da arte e da indústria da engenharia de requisitos legais ou regulatórios;
2. Identificar quais são os principais desafios na engenharia de requisitos legais ou regulatórios;
3. Verificar quais são as estratégias adotadas para engenharia de requisitos legais ou regulatórios por analistas ou engenheiros de requisitos em equipes de desenvolvimento;
4. Observar a forma de realizar a rastreabilidade dos requisitos legais ou regulatórios pelas equipes de desenvolvimento;
5. Investigar quais são os artefatos que podem atuar na documentação e no gerenciamento dos requisitos legais ou regulatórios;
6. Especificar formas alternativas que auxiliem a recuperação dos artefatos relacionados com os requisitos legais ou regulatórios;
7. Oferecer alternativas que facilitem as equipes de desenvolvimento evidenciar a conformidade legal e regulatória dos sistemas;
8. Promover facilidades na manutenção e evolução dos sistemas sem que isto leve a inconformidade legal ou regulatória;
9. Avaliar a solução proposta (*framework*) junto ao público-alvo.

1.4 Justificativa

Em um país, onde é tão nova a forma de lidar com as leis, não seria diferente lidar com a conformidade legal ou regulatória. A constituição em vigor é muito recente (BRASIL, 2019), e com muitas emendas, muitas mudanças a cada troca de parlamentares e presidentes, se contraposta, por exemplo, com a dos Estados Unidos da América de 1787. Com diferentes formas de armazenamento e acesso à informação, a transparência e o acesso às leis em vigor

também são dificultados, principalmente, para os não juristas. As leis são ambíguas, não claras, não verificáveis, por exemplo.

Em áreas novas, quando comparadas, como a própria Engenharia de Software e Engenharia de Requisitos, é possível perceber que, quando o sistema computacional não é de um domínio crítico ou, altamente, regulado, as fontes legais e regulatórias muitas das vezes não são vistas, ou assim o são apenas observadas quando "cai em exigência" em um processo de auditoria ou fiscalização. Isto acontece, como foi possível observar na prática, independentemente do tamanho, do domínio ou da esfera de atuação da instituição (fábrica de *software*). No Brasil, as equipes dessas instituições, dificilmente, contam com profissionais da área de direito ou com algum apoio jurídico. Muitos dos profissionais de tecnologias da computação ou da informação e da comunicação desconhecem a necessidade ou os termos ligados à conformidade legal e regulatória.

Em sendo assim, esta pesquisa pode ser o início, logicamente, somado a outros esforços de vanguarda nacionais e internacionais para melhorar a visão nacional, minimamente, que é possível construir sistemas computacionais em conformidade legal e regulatória; é possível atender o que fontes legais e regulatórias buscam para melhoramento das relações, das organizações, das pessoas, dos animais, do meio ambiente. Visto que é cultural, social, e precisa ser vivenciado pelo povo brasileiro.

1.5 Metodologia

Para a realização desta pesquisa, inicialmente, fez-se uma Revisão Sistemática da Literatura seguindo parâmetros preconizados por Kitchenham et al. (2009), por entender a necessidade de conhecer o estado da arte como defendido por Creswell e Creswell (2017). Em seguida, em posse dos resultados do extrato obtido do material bibliográfico lido, avançou-se para o próximo passo que era conhecer a indústria (o verdadeiro "chão de fábrica"). Com este intuito diferentes estratégias foram empregadas, como: entrevistas nos moldes defendidos por Denzin e Lincoln (2006; 2017), Preece, Sharp e Rogers (2015) e Weiss (1995). Foram diferentes etapas de entrevistas, onde variaram entrevistados e duplas entrevistadores, artefatos, meios e objetivos, o que exigiu diversas técnicas e perícias para planejamento, estudo e análise dos materiais.

Houve um momento de aplicação de um estudo de caso, seguindo as metodologias de Yin (2017) e Runeson et al. (2012), com profissionais da área de Engenharia de Requisitos de

uma fábrica de *software* de grande porte - hoje, chamadas de alto desempenho - (IBGE, 2020). Foi observado, neste estudo, que havia diferentes dificuldades no uso dos artefatos e ferramentas da área, falta de entendimento dos mesmos e de suas atribuições profissionais, além da falta padronização e documentação das atividades e integração entre as equipes. Assim, em outro momento, foi realizada uma etnografia organizacional baseada nos estudos de Ybema et al. (2009) e Angrosino (2007), nesta mesma fábrica de *software*, com duas equipes de desenvolvimento diferentes. A opção pela etnografia organizacional foi feita com a intenção de entender a organização, que naquele momento passava por um processo de transformação ágil (DIKERT, PAASIVAARA e LASSENIUS, 2016).

Foi enriquecedor passar por esse momento junto aos profissionais, poder participar e, ainda, propor soluções em conjunto, ao mesmo tempo em que se estruturava o produto desta pesquisa. Assim, a metodologia escolhida foi a pesquisa-ação (WHITEHEAD e MCNIFF, 2000; MCNIFF e WHITEHEAD, 2006). Por fim, com a concretização do framework, partiu-se para o processo de validação com uma nova bateria de entrevistas e o emprego de um questionário no gerenciamento de processos e de projetos com manutenção da conformidade legal e regulatória.

1.6 Organização dos capítulos

Para sistematização e satisfatória apreciação dos resultados de cada etapa planejada para a realização desta pesquisa, o restante do texto foi organizado da seguinte forma:

Capítulo 2 – Fundamentação Teórica, onde são apresentados os principais termos e fundamentos, que serviram de alicerces para esta pesquisa;

Capítulo 3 – Revisão Sistemática da Literatura, revisão baseada nos conceitos-chave iniciais para conhecimento do estado da arte e da exploração das principais lacunas de interesse envolvidas pesquisa;

Capítulo 4 – Pesquisa Exploratória, neste capítulo foram empenhados diferentes esforços através de metodologias e projetos para conhecimento do público-alvo, suas necessidades, seus interesses, suas maiores dificuldades, onde e de que forma poderiam acontecer as contribuições desta pesquisa;

Capítulo 5 – Framework para promoção e manutenção da conformidade legal e regulatória, neste capítulo são apresentados os principais elementos que compõem o framework proposto e os principais fluxos de uso;

Capítulo 6 – Avaliação do F*ramework* visando entender se os objetivos foram alcançados e quais seriam as possíveis melhorias. A avaliação foi realizada junto ao público-alvo; definido para esta pesquisa,

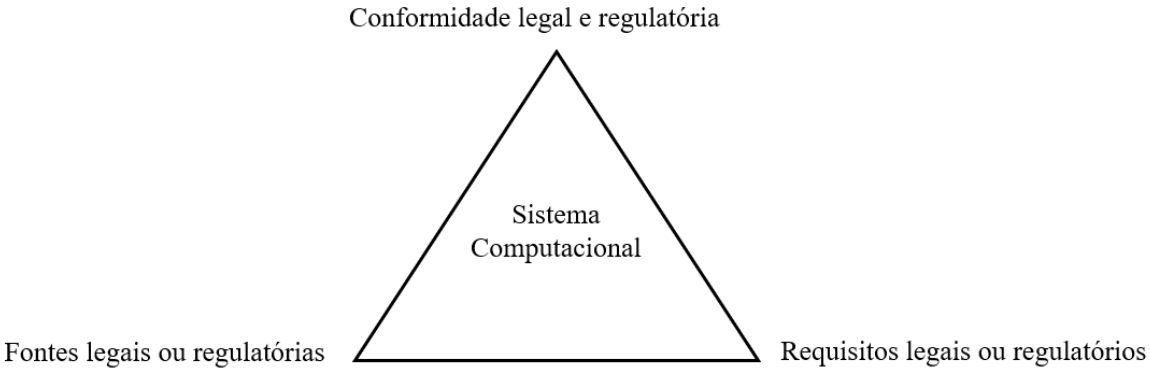
Capítulo 7 – Considerações Finais, momento em que há o resgate dos objetivos alcançados e contribuições, além de sugestões de trabalhos futuros e conclusões desta pesquisa de doutoramento.

2 Fundamentação Teórica

Para maior abrangência, aqui, o Direito foi tratado a partir da Constituição Brasileira 1988 e suas emendas até o ano de 2019 (BRASIL, 2019). Esta é a carta magna do país, onde esta tese foi concebida, por ser um ramo do Direito Público e, também ser o início para outras inserções e interações ao longo deste e dos próximos capítulos. Além disso, a ótica desta tese está voltada para o Neoconstitucionalismo e o Neoprocessualismo, que buscam trazer caminhos e mais efetividade dos direitos fundamentais. De alguma forma, estas ideias, como uma cultura pós-positivista, a aplicabilidade das normas constitucionais, passam a serem horizontais, diretas e imediatas, sem a obrigatoriedade de manifestação legislativa. Altera-se a ordem de postura (JALES, 2012; LENZA, 2019).

Assim, a efetividade da constituição deve-se a sua interpretação positiva e genérica dos valores liberais e sociais (COHEN-KOPLIN, 2011), e o julgador deve aplicar a "lei com equidade, o que não significa substituí-la pela equidade" (DE OLIVEIRA, 2004). O objetivo é também não se perder ao longo do processo, que deve ser justo, mesmo havendo inúmeros recursos apensados. Por mais inconcebível que possa parecer, esta ação pode tornar-se mais árdua pelo fato de poucos das partes interessadas (*stakeholders*) estarem preparadas, serem especializadas ou interessadas, no que tange ao Direito. Isto acontece mesmo sendo cada vez mais evidente, que todo e qualquer domínio de um sistema computacional há leis aplicáveis e, que logicamente, precisam ser cumpridas, estarem em conformidade legal. Desta forma, neste capítulo, constam conceitos, propostas de encaminhamento para a tríade proposta como fundamentação teórica desta pesquisa, presente na Figura 1.

Figura 1: Tríade da fundamentação teórica.



Fonte: a autora.

2.1 Fontes legais e regulatórias

Compreender as diferenças entre Justiça e Direito é importante para o entendimento desta pesquisa. Na perspectiva de Platão (JOWETT, 1888), a justiça traz em seu cerne o belo, o justo e o verdadeiro de um tempo, de uma cultura, de uma sociedade. Entretanto, tem por intenção de ser atemporal, para além da moral e dos bons costumes de uma nação e de suas relações, ou de um período atual na ocasião, pode ser útil ao analisar e pôr em prática os direitos e as obrigações. Enquanto o Direito é temporal, traduz uma sociedade em movimento, em constante mudança. Segundo Reale, "O Direito é um fato ou fenômeno social; não existe senão na sociedade e não pode ser concebido fora dela" (REALE, 2012). Então, fundamentalmente, só existe por haver pessoas, sociedade e cultura. A imperfeição imposta a todo e qualquer humano, e mais ainda dito, humano social, também pode ser percebida na "fonte legal ou regulatória". Intencional ou não, isto é um fato por inúmeras razões, que neste momento não seria oportuno listá-las, e até mesmo propor possíveis caminhos a minimizá-la. Cabe ao cidadão cumprir a lei.

A fonte legal ou regulatória é sempre um código, e como todo bom código segue padrões; logo extrair informações não deveria ser algo tão difícil, como afirmaram Kiyavitskaya, Krausová e Zannone (2008). Antes de tudo, são textos produzidos na língua nativa ou, até traduzidos para facilitar os não nativos! Todavia, é uma tarefa difícil! Em sua grande maioria, são produzidas, por exemplo, por legisladores, muitos sem formação em direito, por técnicos, por gerentes de equipe. Assim, os códigos "perfeitos" em forma/formato são imperfeitos, imprecisos, dinâmicos (prontamente desatualizados), ambíguos na língua, no contexto, no tempo.

Há formas como ambiente, *templates* e ferramentas amigáveis para extrações das informações das fontes legais e regulatórias (KIYAVITSKAYA, KRAUSOVÁ e ZANNONE, 2008), entretanto a mais conhecida no Brasil não chegou ao conhecimento da população, deste modo não foi amplamente alimentada e, consequentemente, não é totalmente funcional. O nome deste sistema SILEX (LexML, 2018), que tinha por intenção oferecer, inicialmente, um modelo gestão da informação jurídica através de sistemas informatizados, onde as informações pudessem estar distribuídas e ao mesmo tempo uniformizadas e unificando fontes legais ou regulatórias nas esferas municipais, estaduais, distritais ou federais, seja da administração direta ou indireta. O piloto foi implantado na Biblioteca do Senado Federal. Essa iniciativa foi similar, por exemplo, a utilizada pela União Europeia com EUR-Lex e N-Lex (CORDIS, 2018), As

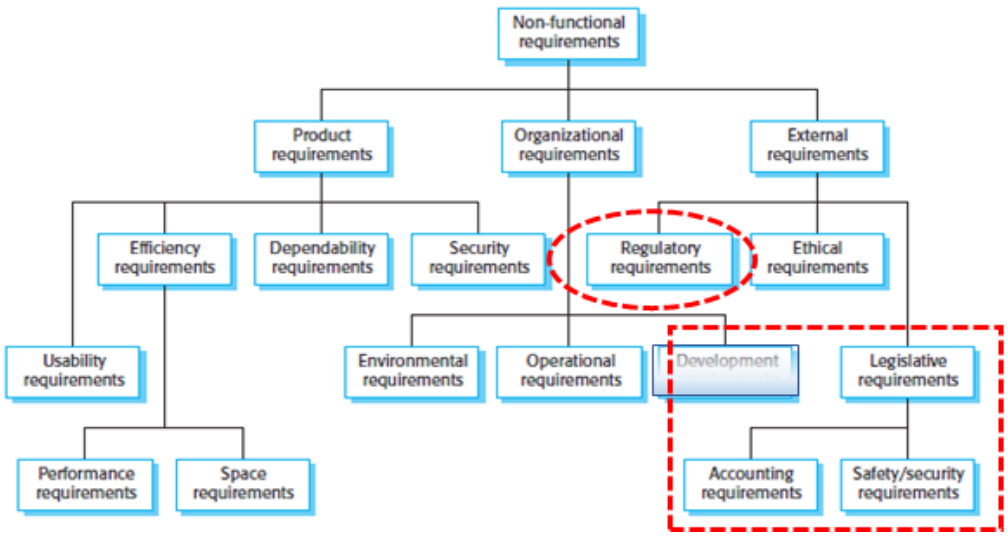
Nações Unidas (FAO, 2020) para, dentre outras questões, leis relacionadas a alimentos e à agricultura.

Mesmo havendo essas iniciativas e modelos, muitos deles abertos e passíveis de serem estendidos, no Brasil, a maioria das fontes legais ou regulatórias encontram-se nos melhores casos em páginas HTML, quando não em diários oficiais digitais, fotos ou impressos para consulta. Sendo assim, os requisitos legais ou regulatórios, que terão como fontes legais ou regulatórias essas mídias com tantos vícios, necessitam de um cuidado especial em sua extração e refinamento.

2.1 Requisitos legais e regulatórios

Sommerville (2016), divide os requisitos em funcionais e não-funcionais (Figura 2), sendo os não-funcionais subdivididos em três: requisitos do produto, requisitos organizacionais e requisitos externos. O foco desta pesquisa está voltado para diretamente os requisitos regulatórios (*regulatory requirements*) e os requisitos legais (*legislative requirements*), entretanto permeia os requisitos não funcionais, que não os externos, quando trata do produto ou da organização para melhor garantir resultados satisfatórios para a fábrica de *software*. Outro ponto de vista defendido por Sommerville (2016) e corroborado por BHATIA e BREAUX (2015) é que devem ser definidos por uma autoridade, e devem ser cumpridos. Não são negociáveis! Isso visa garantir que o sistema esteja dentro da Lei, e é aceitável para uso.

Figura 2: Visão da divisão dos requisitos funcionais e não funcionais.



Fonte: Sommerville (2016)

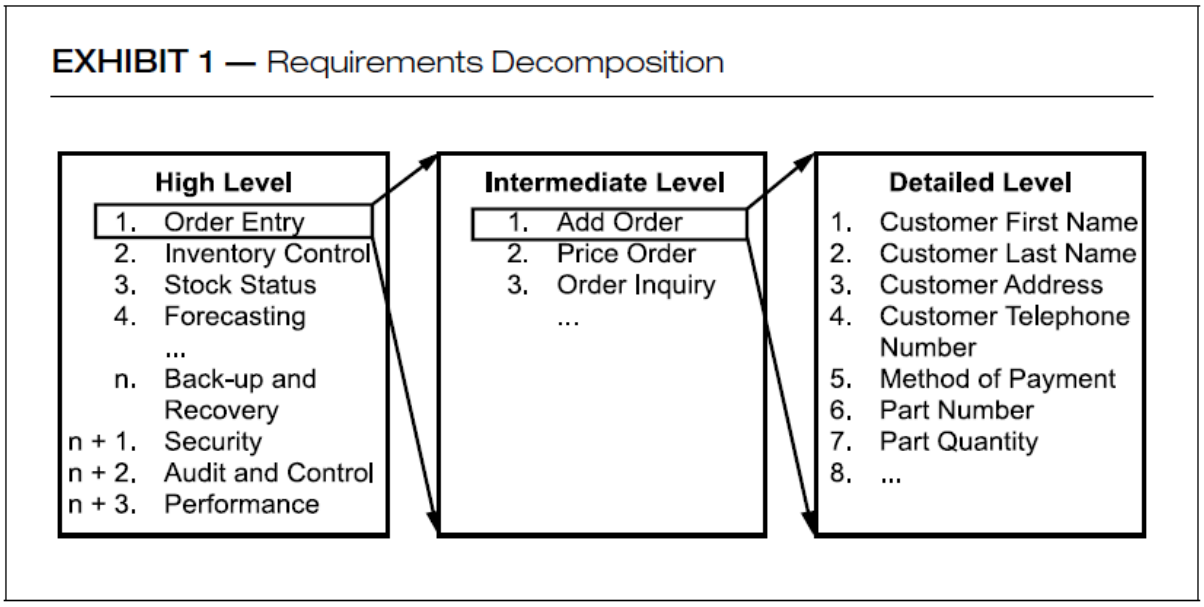
2.1.1 Decomposição de requisitos legais e regulatórios

A decomposição de qualquer requisito não é trivial (KOTONYA, Gerald; SOMMERVILLE, 1998). Diferentes técnicas, como definição de cenários ou divisão de uma história de usuário em várias, podem ser aplicadas, sendo cada uma mais vantajosa ou mais conveniente para um determinado contexto ou público. Além de experiência e maturidade da equipe envolvida, realizar as atividades relacionadas à decomposição de um requisito, normalmente, exige certo tempo, visto que, inicialmente, algo pode não ser bem especificado ou, até mesmo, não ter sido dito por alguém achar simples, "óbvio demais" para o contexto, ou estar, segundo Pohl (2010), no âmbito de percepção muito subjetiva. Acrescido a isto pode ser afirmado com base nos mesmos autores, dada subjetividade e do achar "simples" ou desnecessário, que utilizar a linguagem natural pode trazer certas dificuldades ao projeto desnecessárias, como ambiguidade, diferentes bases de conhecimento ou experiência, por exemplo.

Sendo requisitos, segundo Pohl (2010), em sua natureza: uma representação documentada de uma condição ou capacidade para um usuário resolver um problema ou alcançar um objetivo, ou deve ser alcançada, ou estar presente em um sistema, ou componente de sistema para satisfazer um contrato, norma especificação, ou outro documento formalmente importado. Como esperado, a decomposição de um requisito pode gerar novos requisitos, mas também atividades/tarefas. Esta ação (de decomposição) não é sempre feita de forma clara, o que pode dificultar ainda mais toda engenharia de requisitos.

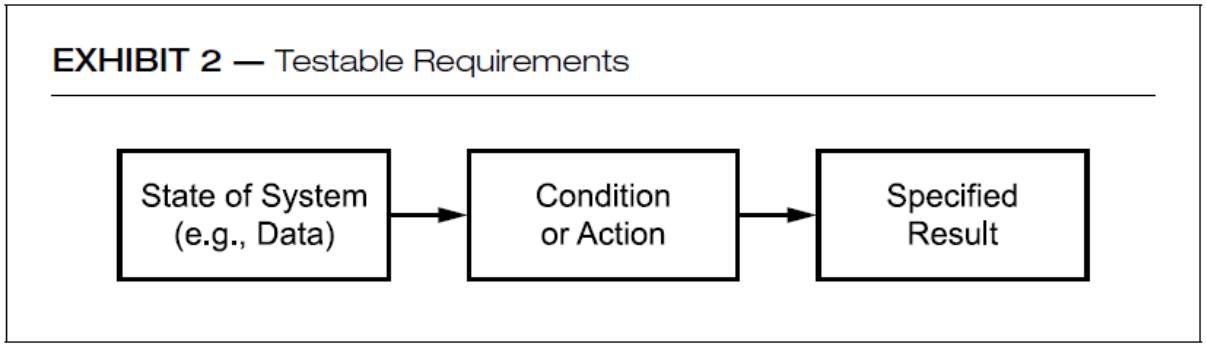
O requisito legal ou regulatório (não funcional) dada sua natureza, em sua maioria, acaba sendo expresso de forma muito abstrata, pouco quantitativa ou exequível. Sendo assim, enquanto o requisito legal ou regulatório (não funcional) não pode ser visto como testável, da forma proposta por Kotonya e Sommerville (1998) e por Wilson (2000), faz-se necessário decompô-lo. Dessa maneira, um requisito legal ou regulatório (não funcional) será decomposto quantas vezes forem necessárias ao ponto de serem possíveis encontrar as partes no sistema, que se deseja construir ou outrora construído, de forma rastreável e testá-las. Ainda, é importante que ora não funcional do tipo legal ou regulatório seja possível ser evidenciado por questões de conformidade legal e possíveis auditorias. A Figura 3 demonstra um exemplo de Wilson (2000) de decomposição ou refinamento ao ponto, que seja possível ser testada sua condição ou sua ação, como demonstrado na Figura 4 sobre o requisito testável.

Figura 3: Decomposição ou refinamento de requisito.



Fonte: (Wilson 2000).

Figura 4: Demonstração do processo de tornar-se um requisito testável.



Fonte: (Wilson 2000).

2.1.2 Priorização de requisitos legais ou regulatórios

A priorização de requisitos, como prática, auxilia a equipe de desenvolvimento a definir a ordem de implementação dos requisitos. Logicamente, isto somente deverá ocorrer após a solução de conflitos entre os requisitos, que porventura existam, e caso necessário com a medição de um jurista. De uma forma geral, os requisitos legais ou regulatórios, geralmente, têm sua prioridade maior do que os demais dada a sua criticidade e sanções definidas pelas

fontes legais ou regulatórias. Para Massey, Otto e Antón (2009), a priorização de requisitos legais ou regulatórios deve ser feita de forma distinta dos outros tipos de requisitos, visto que as técnicas convencionais não apoiariam, quando há diferentes tipos de requisitos ou artefatos. Ainda, esses autores defendem um processo em duas etapas: i) descobrir as implicações legais e ii) calcular uma pontuação de priorização. Para calcular essa pontuação existe uma fórmula que é um somatório que considera os requisitos não legais, os legais, que precisam de refinamento, os legais prontos para implementação, além de outros elementos como subseções mapeadas, subseções contidas, número de referências cruzadas e número de exceções.

Para equipes não habituadas a fazerem a priorização de requisitos, isto pode representar um custo a mais. A falta de conhecimento de técnicas ou de domínio pode penalizar os requisitos legais ou regulatórios e, consequentemente, o cliente em questão. Fatos corroborados no estudo realizado por Achimugu et al. (2014). Neste estudo, a atividade de priorização tem sido uma atividade bastante discutida no domínio da Engenharia de Requisitos, contudo sofre uma série de limitações, como falta de escalabilidade, métodos de lidar com atualizações de classificação durante os requisitos em evolução, coordenação entre as partes interessadas e questões de dependência entre os requisitos.

ICSSES COMMITTEE et al. (1998), desde 1998, tem como uma de suas recomendações a classificação por importância ou estabilidade dos requisitos, além de propor uma escala de aceitação (essencial, condicional e opcional).

2.1.3 Rastreabilidade e versionamento dos requisitos legais ou regulatórios

A rastreabilidade de requisitos tem por benefícios, segundo Pohl (2010):

i) a verificabilidade da implementação de um requisito no sistema;

ii) a identificação de propriedades desnecessárias do sistema;

iii) identificação dos requisitos desnecessários partindo do princípio da sua falta de ligação com qualquer outra fonte ou artefato do sistema;

iv) análise de impacto em possível mudanças nos sistemas;

v) reusabilidade de artefatos de requisitos em outros projetos;

vi) determinação de responsabilidade (*accountability*) retroativa de esforços de desenvolvimento de um requisito; e

vii) simplificação da manutenção por auxiliar a identificação dos componentes envolvidos na falha ou na alteração a ser feita.

Ramesh e Jarke (2001) indicaram que apenas informações classificadas relevantes devem ser registradas a partir das dimensões: que? quem? onde? como? por quê? quando? Enquanto Pohl (2010) ainda classificou os tipos de relacionamento, como:

i) rastreabilidade pré-especificação de requisitos - artefatos-fonte e requisito;

ii) rastreabilidade pós-especificação de requisitos - requisitos e artefatos advindos de atividades subsequentes de desenvolvimento; e

iii) rastreabilidade entre requisitos - mapeamento de dependência entre requisitos.

Para efeitos dos requisitos legais ou regulatórios é desejado que todos os artefatos dos sistemas sejam rastreáveis, entretanto o custo operacional e de manutenção pode ser alto, se isto não for feito desde o início do projeto com auxílio de um ferramental tecnológico. Para esses casos, sugere-se que pelo menos aquilo que estiver relacionado de alguma forma com os requisitos legais ou regulatórios esteja rastreável para maior garantia da conformidade legal e regulatória.

Podem ser utilizadas diferentes técnicas para representação do que foi exposto, como hyperlinks, matrizes, grafos de rastreabilidade. Contudo, o versionamento de um requisito é fundamental quando se trata de fontes legais ou regulatórias, que são tão instáveis. Cada fábrica de *software* terá a sua estratégia, o importante é que tenha uma eficiente e eficaz, pois a qualquer momento pode precisar. No Brasil, assim como em alguns lugares do mundo, algumas fontes legais ou regulatórias são publicadas e, às vésperas de entrar em vigor, são revogadas. Desta maneira, em não havendo o versionamento ficará muito mais difícil desfazer alterações feitas com controle de versionamento, de configurações e uma *baseline*. A existência de um comitê de gerenciamento e controle de mudanças de requisitos é algo fundamental, principalmente, para médio e grande sistemas.

2.2 Visualização da informação

Considerando a pesquisa realizada, julgou-se relevante destacar que a visualização da informação é um diferencial em qualquer fábrica de *software*, independente da metodologia de

desenvolvimento que se utilize, contudo mais ainda para aquelas que são ágeis, visto que as mudanças estão ocorrendo a todo momento, e decisões precisam ser tomadas a todo instante. Deve-se considerar que ainda há as infraestruturas de desenvolvimento e a operacional, que precisam de monitoramento constante. Assim, Spencer (2014) define a visualização da informação como algo que pode auxiliar a criação de um modelo mental de algo, e amplia/acelerando o desempenho cognitivo do ser humano.

Para Cooper Jr et al. (2009), as pesquisas feitas com aplicação da visualização da informação comparativamente a outro tipo de artefato descobriram que existiam lacunas e oportunidades na prática de engenharia de requisitos que, quando explorados, trazia bons resultados, e encurtava prazos de resposta quando as informações eram visuais. A teoria de Gestalt também pode explicar um pouco disso (PREECE, SHARP e ROGERS, 2015).

Sabendo que os seres humanos ainda possuem habilidade inexploradas e, até mesmo subutilizadas, como afirma Shneiderman (1996), sua taxonomia *Type by Task Taxonomy* (TTT) de visualização de informações, onde os itens têm atributos, realizar uma atividade de pesquisa selecionando todos os itens ou apenas alguns dados determinados parâmetros não teria uma carga cognitiva complexa. Desse modo, para esse autor, são tarefas básicas para um ser humano escanear, reconhecer e recuperar imagens rapidamente, bem como detectar mudanças no tamanho, cores, formas, movimentos ou texturas. Muito mais simples do que ler painéis imensos com informações escritas, mesmo que coloridas e brilhantes, mesmo quando essas informações são críticas às suas funções profissionais.

2.4 Direito Digital

O Marco Legal da Internet (BRASIL, 2014) trouxe como proposta o que viria a ser o Direito Digital, e tem suas particularidades, mas também que é composto por parte do Direito Civil, Direito Autoral, Direito Comercial, Direito Contratual, Direito Econômico, Direito Financeiro, Direito Tributário, Direito Penal, Direito Internacional, dentre outros. Segundo Peck (2013), “os elementos que estão a amparar o Direito Digital são os costumeiros são: a generalidade, a uniformidade, a continuidade, a durabilidade, e a notoriedade (ou publicidade)”. Entretanto o fator tempo é um dos seus principais diferenciais, visto que o tempo no meio digital é diferente do mundo físico, ora fugaz, ora perene, mas sempre diferente. Outras referências importantes são a informação como bem mais valioso, e a autorregulação, mesmo havendo leis e autoridades, há partes que não são regidas por essas. Para empresários, comerciantes, artistas

ou qualquer um que deseja comercializar algo pela internet há outra referência, segundo Negroponte (2002), a da riqueza inesgotável (infinitamente duplicado ou reproduzido), que se não bem administrado ou distribuído ao disponibilizar-se algo na internet, pode se perder o controle.

Ainda, podem ser destacadas para a sociedade moderna afetada pelas tecnologias da informação e da comunicação, e centro das cidades inteligentes, a "famosa" Sociedade 5.0 (TOKYO, 2020), como importantes práticas jurídicas, segundo Peck (2013), a analogia e a arbitragem. Bem como, segundo a mesma autora (PECK, 2013), a uniformidade, a continuidade, a notoriedade (divulgação das decisões arbitrais) e a prova (ou a inversão do ônus da prova) são exemplos de características necessárias para correta aplicação do Direito no âmbito digital. Isto deve se assemelhar para pessoas físicas, jurídicas e, agora, as ditas digitais, que são aquelas que de alguma forma só existem no meio digital, mas tem direitos e deveres como preconiza o novíssimo Direito Digital (PECK, 2013).

Segundo Peck (2013), outras preocupações do Direito Digital, tão exacerbada por conta do tempo e do espaço, são a vigência e a territorialidade, pois neste ramo do Direito estes dois conceitos ganham outra dimensão na atual sociedade tão convergente. Todas as mudanças culturais e comportamentais ditam o ritmo da evolução tecnológica, que não é o mesmo da legislativa, por isso a autorregulação acaba por atender melhor ao dinamismo, que as relações de Direito Digital exigem (PECK, 2013).

Acrescenta-se ainda que no ordenamento jurídico vigente, no Brasil, ninguém pode alegar desconhecimento da lei, Código Civil, Decreto-Lei 4657/42, Art. 3. Entretanto, considerando as leis, que regem o mundo digital, é obrigatório ao provedor do serviço, do comércio ou de qualquer ambiente virtual informar a seu público os procedimentos e regras às quais está submetido, e quais dados serão obtidos, armazenados, por quais prazos e o que será feito deles. Considerando isto, a árdua tarefa de conquistar ou manter a conformidade legal e regulatória encontra diferentes desafios além do campo legal.

2.5 Conformidade legal e regulatória

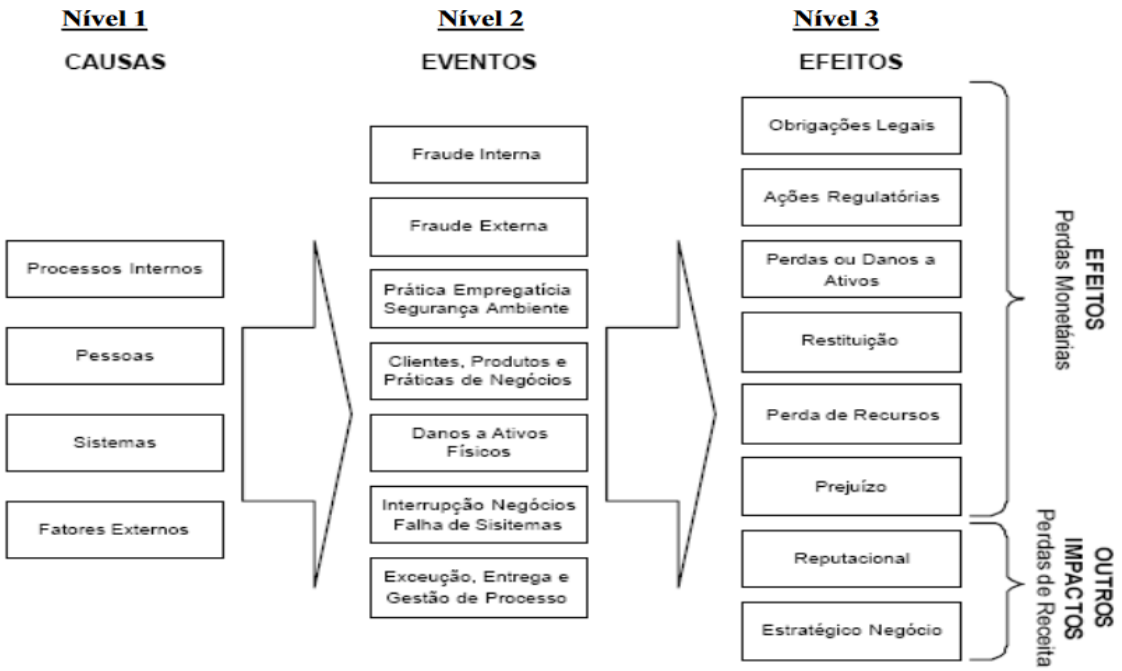
A conformidade legal e regulatória pode ser entendida, no contexto desta pesquisa, como a priorização das fontes legais e regulatórias às quais o sistema e a organização devem estar em consonância frente às outras necessidades. Outra definição é o alinhamento entre as necessidades externas (tais quais fontes legais e regulatórias, clientes, usuários, órgãos

fiscalizadores, fornecedores) e as necessidades internas (por exemplo, sistemas, inter sistemas, equipe).

A conformidade legal ou regulatória não é facultativa a quem deve ser consonante para com quem deve mantê-la (VARJU e CZINA, 2019). Entretanto, esta deve ser sempre contextualizada e dirimir qualquer conflito, que possa existir entre os interesses e os deveres a que tem por obrigação atender ao contexto, ao domínio, à nação, ao território ou inter território que for, por exemplo. Assim, a implementação da complexidade da conformidade legal e regulatória depende de vários fatores, bem como sua manutenção também (MAROSIN e GHANAVATI, 2015).

Desse modo, precisam ser observados à manutenção da conformidade legal e regulatória, dentro das necessidades internas, os planos, as políticas, os *softwares*, os *hardwares*, a infraestrutura, as equipes, a segurança, a comunicação, entre outros, sendo cada um com o menor grau de granularidade possível; bem como gerenciar a ética (inter) pessoal e nos negócios para Treviño et al. (TREVIÑO et al., 1999). As respostas a esses cuidados estão, normalmente, relacionadas ao melhoramento da eficácia social, organizacional, ética, legal, e eficiência na implementação e na validade dos requisitos legais ou regulatórios a partir de uma abordagem sócio-jurídica. A não conformidade traz diferentes riscos operacionais, segundo o Basiléia II (2019), que podem ir além das perdas monetárias e serem irreparáveis (Figura 2.5).

Figura 5: Estrutura de Risco Operacional segundo Basiléia II.



Fonte: Adaptado Guimarães (apud LIMA, 2007).

2.6 Políticas, planos e processos

Uma boa forma de iniciar a implementação da conformidade legal e regulatória de uma fábrica de *software* é começar pela estrutura e infraestrutura da instituição até chegar ao, modernamente, nomeado de "CTIC" - Centro de Tecnologias de Informação e de Comunicação. É preciso que haja políticas, planos e estatuto homologados e de amplo conhecimento.

Na sequência, logicamente, existem várias maneiras de fazer isso, podem ser feitas uma lista de projetos, lista de tarefas, pode ser usado o modelo PMBOK (PMI - PROJECT MANAGEMENT INSTITUTE, 2017) para um gerenciamento de projetos, pode ser usado o COBIT (IT GOVERNANCE INSTITUTE, 2012) para alinhar estes projetos ao negócio ou seguir o ITIL (KAISER, 2018) para planejar os serviços de TI. Tudo dependerá das políticas e dos planos estratégicos traçados pela instituição.

O que deve esperar, e deve ser iniciativa dos responsáveis pelas Tecnologias da informação e da comunicação (TIC) da instituição, principalmente, do que ocupa os cargos de CEO (*Chief Executive Officer*) e de CIO (*Chief Information Officer*) da instituição são os planejamentos de:

i) de contingência;

ii) de riscos;

iii) de continuidade de negócios ou plano de recuperação de desastres;

iv) de administração de crise (plano desenvolvido em conjunto, com definição de atividade, pessoas, dados lógicos e físicos);

v) de continuidade operacional (que inclui diretivas sobre o que fazer em cada operação em caso de incidente plano de recuperação - aplicação prática do plano de continuidade operacional); e

vi) de continuidade de negócio (que inclui plano de contingência, plano de administração de crises (PAC), plano de recuperação de desastres (PRD) e plano de continuidade operacional (PCO)).

Esses planejamentos são orientações básicas do Veras (2009) para continuidade de qualquer negócio considerando o data center componente central da infraestrutura de TI.

Outros planos de ação ou planejamentos, que podem incrementar e melhorar a colaboração, estruturação e continuidade das TIC na instituição, são listados a seguir:

i) governança de TIC;
ii) governança de pessoas;
iii) governança de aquisições;
iv) governança em saúde;
v) gestão de riscos e controle interno;
vi) governança de órgãos e entidades;
vii) governança de políticas públicas; e
viii) governança pública.

Quando se pensa em governança de negócios, automaticamente, deve-se pensar na estrutura de gerenciamento de riscos, e isso leva ao monitoramento e ao comprometimento. Monitorar e comprometer-se é conceber a estrutura para gerenciar riscos, implementar a gestão de riscos, monitorar e fazer a análise das questões críticas da estrutura, e estar comprometidos com a melhoria contínua da governança. O processo é cíclico: objetivo → atividades → resultados → *feedback* → reinicia-se o processo. Em tratando-se de processos é importante saber quem decide, quem tem a última palavra, além de sua razão de existência, e o que o processo é em sua essência. Já em se tratando de um procedimento seria necessário ter informações de como deve ser feito, para quem, quando e onde.

O Tribunal de Contas da União (TCU) considerando isso e diferentes fontes legais e regulatórias instituiu o que nomeou de iGovTI (Índice de Governança de Tecnologia da Informação), que vem a ser um índice que busca medir a situação de governança de tecnologia da informação (TI) de cada organização avaliada (NETO e DE CARVALHO, 2020). Esses índices estão divididos em três pilares: gestão de risco, gestão de continuidade e gestão de programas e projetos. A intenção é também a otimização pelas instituições da transformação digital; da retenção das pessoas na área de Tecnologia da Informação; da avaliação sistemática de tecnologia da informação; da visão estratégica de tecnologia da informação; do uso estratégico dos recursos; da atualização e aperfeiçoamento da Política de Governança de Tecnologia da Informação. Isto é um avanço público tanto quanto privado.

2.7 Cultura e profissionais generalistas *versus* especialistas

A cultura é algo inerente ao ser humano, é uma construção do inconsciente social, e oposto à natureza. Para Eagleton (2016), a cultura guarda em si uma transição histórica, entretanto se diferencia de civilização, e está intimamente ligada à relação da humanidade e aquilo que se chama de trabalho. Trazendo consigo um contraste entre evolução e revolução, que toda a humanidade experiencia em determinados momentos históricos ou não. Outras questões importantes a serem observadas e percebidas foram:

i) a cultura social (local/regional/nacional/internacional), que por si só a cultura já é um fenômeno social, e ao sobrecarregar o termo fica muito mais explícito que o conjunto de crenças, costumes, tradições são, não apenas de um estrato da sociedade, mas de grupo facilmente identificável em seus hábitos, podendo ser chamados de comunidades (analistas ou engenheiros de requisitos, desenvolvedores, testadores, analistas de redes, etc.);

ii) a cultura de desenvolvimento da fábrica de *software*, que a princípio não é intenção desta pesquisa modificá-la, onde com métodos, processos e práticas vão construído esta "herança", que faz parte da equipe, e é repassada a cada novo membro;

iii) a cultura legal é aquela que foi traduzida em leis, regimentos, regulamentos, normas, estatutos, e estão profundamente relacionados com as relações e a sua contemporaneidade; e

iv) cultura imaterial, que pode ser traduzida como algo que afeta o desenvolvimento, mas não pode impedir a manutenção da conformidade legal por mais que a cultura social ou cultura de desenvolvimento permitam ou, até mesmo, "tenha como prática contrária" a essa manutenção.

É preciso lidar com personas (dependendo da metodologia de desenvolvimento escolhida), pessoas físicas, pessoas jurídicas, pessoas digitais (PECK, 2013) e, ainda, para esta proposta é preciso ser discutida, uma incongruência muito comum quando são reunidas as partes interessadas. É inteligível e transparente as diferenças entre as palavras usuário, cliente, contratante, por exemplo, entretanto, quando começam os trabalhos a equipe de desenvolvedores quase encontra um caos hierárquico, o que causa perda de tempo, esforço desnecessário e desgastes emocionais e financeiros. Logo, definir rapidamente papéis e responsabilidades são atividades preponderantes para o sucesso do projeto e, se possível, que constem em contrato.

É importante, do mesmo modo, ter em mente que as formas, metodologias e técnicas de ensino e aprendizado de um adulto e suas motivações são diferentes (FREIRE, 1996; HENSCHKE, 2009; KNOWLES, 1978). Logo, artefatos, estratégias e tudo o que for fundamental a esse processo de melhor construção e adaptação deve ser lançado mão para melhor alcançar os resultados esperados. Sempre lembrando que durante todo o ciclo de desenvolvimento do sistema computacional serão vários os profissionais que apoiarão o desenvolvimento, a manutenção ou a evolução desse sistema.

Esses profissionais muitas das vezes não serão "especialistas" no assunto, no máximo, entendidos, experientes seja qual for a área pretendida no direito, no planejamento, na administração e, até mesmo, quando dentro da computação é bem possível encontrar um testador desenvolvendo ou vice-versa. Na computação, em algumas metodologias de desenvolvimento e manutenção de sistemas, como na maioria das metodologias ágeis, isso é até defendido! Por outro lado, sabe-se que um economista ou contador, por exemplo, não pode exercer os direitos legais de um advogado.

Neste ponto, o sistema tem que ser crível! Sua credibilidade, e não dos profissionais envolvidos, precisa ser um selo. As interações quanto mais aprimoradas melhor; usabilidade idem. Interfaces de última geração, com elementos, ergonomicamente, pensados para o público-alvo e menor esforço cognitivo perfeito. Entretanto, quem usa, atualmente, mesmo sem saber, carece que as informações, por mais básicas que sejam, encontram-se confiáveis, seguras e, se for caso, privadas. Para isso, contratante e fábrica de *software* são solidárias do início ao fim do ciclo de vida de um sistema (BRASIL, 2014).

2.8 Requisitos legais e regulatórios em metodologias ágeis

Assim como acontece com os profissionais envolvidos, para obtenção do "selo", para conformidade legal e regulatória não importa com qual metodologia e infraestrutura foram utilizadas, ou está sendo utilizado no ciclo de vida do sistema computacional. É fundamental que todos os elementos estejam em conformidade legal e regulatória e, eticamente, tudo tenha seguido um fluxo normal e esperado para isto. Desde que nada de ilegal tenha sido feito, o processo criativo é livre, e a inovação é bem-vinda.

Com o surgimento dos métodos ágeis nos anos 1990, houve uma mudança na visão sobre como desenvolver *softwares*, e essa mudança está associada também a cultura e a nova forma de pensar, segundo PRIKLADNICKI, WILLI e MILANI (2014). Para esses autores, o

enfoque estava nas pessoas, seus valores, princípios e práticas, e já não mais nos processos como nos métodos tradicionais. Entretanto, isso ao mesmo tempo não significa rejeitar processos, ferramentas, documentação abrangente, negociação de contratos ou planos preestabelecidos, a importância é que se transfigura. Desse modo, esses autores afirmaram que é uma "questão é como receber, avaliar e responder a elas (rápidas mudanças)." No contexto desta pesquisa, sem com isto perder a conformidade legal e regulatória.

O Manifesto Ágil (BECK, 2001), que define os 12 princípios, é o documento base para o início da adoção ou da transformação ágil de uma instituição. Esse documento foi mal interpretado ao longo de alguns anos por diferentes instituições, que entenderam não haver mais a necessidade de documentação, contratos, políticas ou planos. De forma natural e gradativamente, essas instituições passaram a ter problemas com a continuidade dos negócios, entregas e reuso, parcerias até culminar em problemas legais.

Nas pesquisas de campo realizadas, considerando as fábricas de *softwares* analisadas, as metodologias ágeis que se mostraram promissoras suas práticas e artefatos foram SCRUM, SCRUM adaptado e DevOps. Essas metodologias bem empregadas e seguidas, facilmente, podem produzir evidências e artefatos, que auxiliariam em um processo de auditoria para verificação da conformidade legal e regulatória, se bem orientado. Isso não significa dizer que outras metodologias, independentemente de serem ágeis, estão automaticamente excluídas, visto que esse processo não foi exaustivo ou extenso com esse propósito.

2.9 Trabalhos relacionados

Os trabalhos presentes nesta subseção influenciaram o olhar para as temáticas, que fundamentaram a pesquisa realizada. Como também, modificaram a perspectiva das exigências e da forma de trabalho com a intenção de haver conformidade legal e regulatória nos sistemas computacionais implementados, mantidos ou utilizados. Assim, inicialmente, a atuação junto a pesquisa de Santos (2017) permitiu um maior contato com o universo de conformidade legal e ambiente de transformação ágil e, a partir desde trabalho, se teve contato com o trabalho de Barboza (2015) que preocupado com a conformidade legal no planejamento de contratações de TI na Administração Pública Federal oferece uma abordagem para tratar com a Instrução Normativa 04/2014.

O trabalho de Albuquerque (2015) permitiu entender as relações sociais e legais a partir das pesquisas realizada para desenvolvimento do GenNormas. O GenNormas tornou mais

flexível o *framework* Nòmos, que foi criado para trabalhar com modelos i*, e aplicou no domínio de *e-commerce* em modelos de especificação de requisitos, como a Notação de Modelagem para Processos de Negócio (BPMN), em Diagrama de Caso de Uso e em Histórias de Usuário.

O Nòmos (INGOLFO et al., 2014; INGOLFO, SIENA e MYLOPOULOS, 2014) em sua terceira geração, possibilitou o deslumbramento de um modelo de metas para avaliar a conformidade com as leis aplicáveis a um determinado contexto, sendo que, nessa versão, incluem-se os conceitos de função e de requisito.

Para então, em um momento seguinte, visitar a pesquisa de Akhigbe (2016), que propôs em sua tese uma estrutura que os reguladores pudessem exibir o seu desempenho por meio de uma modelagem, assim como a avaliação fosse feita através de relatório de seus resultados. O *framework* criado (Regulator-Oriented Regulatory Intelligence Framework - RORIF) adotou uma abordagem de inteligência regulatória, que envolve o uso de dados, recursos de *Business Intelligence* (*BI*), e de algumas ferramentas analíticas existentes. Este trabalho mostrou uma diferente forma de tratar questões relacionadas a sistemas, à legislação e aos negócios.

2.10 Considerações

Esta fundamentação apresentou os principais termos, sem que com isto fosse buscado demonstrar todo o conhecimento construído ao longo dos anos de realização desta pesquisa com o objetivo de tornar o texto um pouco mais leve. Desse modo, tanto os temas quanto a linguagem utilizada foram mais branda o possível, visto a interdisciplinaridade transversal à pesquisa.

No próximo capítulo, encontra-se a revisão sistemática da literatura realizada considerando os anos 2014-2018.

3 Revisão Sistemática da Literatura

A manutenibilidade da conformidade legal e regulatória em sistemas computacionais da informação em ecossistemas ágeis pode ser mais complexa do que implementá-la. Principalmente, em ambiente cuja maturidade ainda é crescente, artefatos e ferramentas não estão calibrados para oferecerem aquilo que os interessados precisam para momentos de decisão, de manutenção ou de evolução do sistema. Desse modo, muitas pesquisas estão sendo feitas em diversas frentes para abranger da melhor forma possível esse universo tão vasto que é composto pelas fontes legais e regulatórias, os sistemas computacionais e seu apropriado ciclo de vida para conformidade legal e regulatória.

Esse capítulo explora a revisão sistemática da literatura baseada em Kitchenham e Charters (2007), Kitchenham et al. (2009), Dybå e Dingsøyr (2008) e Inayat et al. (2015). Esta revisão foi realizada buscando explorar o andamento das pesquisas, seus benefícios e desvantagens mencionados pelos autores dos trabalhos extraídos, na tarefa de execução das mesmas. A intenção foi também sumarizar as intenções desses autores, os domínios, as perguntas mais importantes, temáticas, onde foram aplicados essas pesquisas, e identificar como os requisitos legais ou regulatórios foram tratados pelos autores em suas pesquisas.

Embora a temática “conformidade legal e regulatória” não seja novidade em diferentes áreas do conhecimento (CARROLL, 1979), como também não é na Ciência da Computação, na Engenharia de Software, e mais especificamente na Engenharia de Requisitos pode se dizer que a maior preocupação aconteceu a partir dos anos 1990. Nesse período, começou a existir uma maior globalização, e os países tiveram que lidar com múltiplas legislações. Além disso, houve também embargos de grandes empresas com seus serviços baseados na internet por grandes nações, e lidar com a legislação local e a legislação internacional foram grandes desafios para essas empresas. Isso, de certa forma, impulsionou diversas discussões em diferentes campos, e um deles foi como instanciar sistemas de forma atender às leis locais, nacionais e internacionais; e mais ainda mantendo a conformidade legal e regulatória em todos os aspectos.

3.1 Conformidade legal e regulatória em ecossistemas ágeis de desenvolvimento de sistemas computacionais

A conformidade legal e regulatória em ecossistemas ágeis de desenvolvimento de sistemas computacionais não é facultativa. Isto é de difícil compreensão dos interessados no sistema, que esta conformidade não poderá ser negociada, e sempre será prioritária. É de suma importância, quando se verifica que sua definição é a estar em concordância com as fontes legais e regulatórias de um domínio, de um contexto. Seja no âmbito interno, externo, nacional ou internacional.

A maior dificuldade enfrentada, inicialmente, por profissionais da Computação é identificar o requisito legal ou regulatório em meio a tantos outros requisitos. Consequentemente, enquadrá-los com a evolução dos sistemas computacionais em seu domínio ou em seu contexto como adaptá-lo às novas fontes legais ou regulatórias, que passarão a reger o sistema. A mudança ou evolução nas fontes legais ou regulatórias pode gerar muitas dúvidas e conflitos legais, que geralmente, necessitam de um especialista, um jurista para saná-las de tão complexas, que se tornaram.

3.1.1 Trabalhos relacionados a revisão realizada

O trabalho de Mellado et al. (2010) está relacionado com esta pesquisa, quando ambos buscam realizar uma revisão sistemática para através desta e dentro dos processos de Engenharia de Requisitos, no caso de Mellado et al. (2010) especificamente os de segurança, encontrar outros trabalhos que relataram experiências no que difere o tratamento desse tipo de requisito; quais foram as técnicas, ferramentas e artefatos utilizados. Ressalta-se apenas que não houve a restrição em o ambiente ser puramente ágil para Mellado et al. (2010).

Em Inayat et al. (2015) a busca foi por mapear as evidências disponíveis sobre as práticas de engenharia de requisitos adotadas e os desafios enfrentados por equipes ágeis para entender como os problemas tradicionais de engenharia de requisitos são resolvidos usando engenharia ágil de requisitos. As descobertas foram interessantes, pois foram 17 práticas de Engenharia Ágil de Requisitos, cinco desafios rastreáveis à Engenharia de Requisitos Tradicional que foram superados por requisitos ágeis e oito desafios impostos pela prática da Engenharia Ágil de Requisitos. Os autores ainda sugerem como desafio o saber lidar com a Engenharia Ágil de Requisitos, os requisitos não funcionais e equipes auto-organizadas.

Para Schön, Thomaschewski e Escalona (2017) o aumento da complexidade dos sistemas, o desenvolvimento ágil, o envolvimento das partes interessadas durante a engenharia de requisitos têm sido essenciais para criar um ambiente colaborativo e com *feedbacks* constantes. A intenção foi contribuir para o desenvolvimento do corpo de conhecimento da instituição, avaliando o envolvimento do interessado e do usuário na Engenharia Ágil de Requisitos. Para isto, fornecem métodos, que tornam o desenvolvimento ágil de *software* mais centrado no humano, com as partes interessadas, as metodologias integradas, a compreensão, os artefatos e a documentação do sistema sendo compartilhados, e uma atenção especial aos requisitos não-funcionais. Isto faz com que essa pesquisa esteja associada a esta pesquisa pela sua intenção.

A pesquisa de Martins e Gorschek (2017) buscou em diferentes domínios, muitos deles considerados críticos para Engenharia de Software, quais abordagens estão disponíveis para captura, especificação e comunicação requisitos de segurança e para determinar os desafios restantes na Engenharia de Requisitos. Os autores citaram a grande distância entre a academia e a indústria. Ao final, os autores elaboram uma agenda de pesquisa com várias questões a serem respondidas por pesquisas futuras.

Por fim, quando se concentravam esforços para finalizar este estudo, foi publicado o mapeamento sistemático da literatura por Akhigbe, Amyot e Richards (2019). Este mapeamento é o que mais se aproxima da pesquisa que foi realizada, pois tem as mesmas preocupações com a conformidade legal e regulatória. A *string* de busca era formada da seguinte forma: ("*Legal Compliance*" *OR* "*Regulatory Compliance*") *AND* ("*Goal Model**"). Os resultados do mapeamento dos anos 2012 a 2016 enfatizam a necessidade de mais estudos fora da área da saúde, relacionados a contextos diferentes da privacidade, que visassem tarefas de promulgação de conformidade ou que levassem em consideração as preocupações dos reguladores.

Considerando o exposto, havia uma lacuna a ser preenchida com esta revisão considerando os requisitos legais ou regulatórios, as metodologias de desenvolvimento ágeis, seus artefatos, as técnicas e as ferramentas utilizadas.

3.2 Metodologia para realização da revisão sistemática

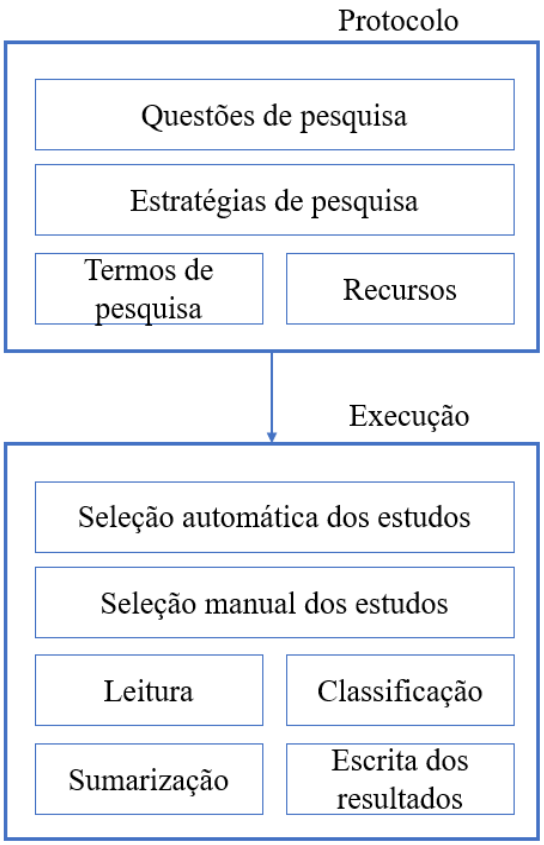
A metodologia utilizada baseou-se nas referências supracitadas e, ainda, complementarmente, em Wohlin (2014) para apoiar a técnica de "snowball sampling backward" para ampliar seu alcance. Tendo essas referências com anteparo, foi possível

identificar artigos relevantes para esta pesquisa por conta da exploração de seus achados, suas evidências, seus benefícios e suas desvantagens apontados pelos seus autores. Para melhor estruturar tanto a pesquisa a ser feita, como os achados e seus resultados foi delineado um protocolo que no relato da revisão de forma transparente, mas bem estruturada, para facilitar a leitura e a exibição dos resultados obtidos.

Para condução da revisão foi definido também como deveria ser o fluxo, assim se teria todos os passos a serem seguidos mapeados antes de iniciar a revisão. A Figura 6 ilustra os passos, que foram:

i) realização de buscas aleatórias a partir dos temas da pesquisa;
ii) análise dos resultados;
iii) definição do protocolo;
iv) busca e extração dos dados de estudos nas bases e indexadores escolhidos;
v) consolidação dos dados obtidos de estudos;
vi) remoção dos trabalhos repetidos;
vii) análise dos títulos e resumos;
viii) aplicação dos critérios de inclusão e de exclusão;
ix) leitura completa dos estudos selecionados;
x) aplicação dos critérios de qualidade;
xi) classificação dos estudos a serem utilizados;
xii) sumarização dos resultados; e
xiii) escrita dos resultados.

Figura 6: Demonstra o processo entre o protocolo implementado e sua execução.



Fonte: a autora.

Considerando todo o exposto, e a necessidade de garantir a conformidade legal e regulatória dos sistemas computacionais, as questões de pesquisa desta revisão preocupou-se com: os requisitos, os artefatos, as técnicas e as ferramentas. Assim, foram elaboradas três questões de pesquisa (QP) para nortear esta revisão:

QP1 - Como os requisitos legais são tratados (elicitados, documentados, verificados, validados, gerenciados - rastreados e mantidos) nos ecossistemas ágeis?

QP2 - Quais artefatos são utilizados para tratamento dos requisitos legais nos ecossistemas ágeis?

QP3 - Em que se diferem as técnicas, as ferramentas e os artefatos relacionados com os requisitos legais de outros tipos requisitos nos ecossistemas ágeis?

Para melhor simplificar as questões de pesquisa foi utilizado o método PICOC (KITCHENHAM e CHARTERS, 2007) - *population*, *intervention*, *control*, *outcome*, *context* - , visto que, inicialmente, elaboram-se os principais termos relacionados com o que se busca. Dessa forma, foi listado, primeiramente:

- População: leis, normas, regulamentos, padrões, políticas e requisitos legais ou regulatórios em sistemas computacionais.
- Intervenção: aplicação de método, metodologia, técnica, tecnologia, modelos, procedimentos, framework, guia, ferramenta, artefato, protótipo ou boa prática da Engenharia de Software ou da Engenharia de Requisitos.
- Controle: comparação aos ecossistemas tradicionais (ágeis versus tradicionais).
- Resultado: melhoramento das práticas da Engenharia de Requisitos relacionadas ao requisito legal ou regulatório; manutenção ou auditoria da conformidade legal ou regulatória nos sistemas computacionais.
- Contexto: requisitos legais ou regulatórios na Engenharia de Requisitos ou na Engenharia de Software para ecossistemas ágeis.

Como estratégia de busca foi adotado um processo dividido em três etapas:

i) extração automática a partir do uso de *string* de busca nas bases e indexadores de dados científicas selecionados;
ii) extração manual a partir dos eventos e periódicos definidos; e
iii) técnica de “snowball sampling backward” (WOHLIN, 2014).

As bases e indexador de busca adotados cumpriam os seguintes requisitos:

i) eram capazes de interpretar expressões lógicas e similares;
ii) permitiam busca pelo texto completo ou em campos específicos (título, resumo, palavras-chave);
iii) estavam disponíveis na instituição da pesquisadora;
iv) cobriam a área e as subáreas de pesquisa em interesse: Ciência da Computação, Engenharia de Software, Engenharia de Requisitos; e
v) não possuíam limites de palavras e combinações na *string* a ser utilizada, que afetassem a busca a ser feita.

Dessa maneira, foram selecionados: i) ACM Digital Library; ii) DBLP Computer Science Bibliography; e iii) Scopus.

Os termos, preliminarmente, definidos foram: requisito legal ou regulatório, conformidade legal ou regulatória, ágil, lei, Engenharia de Software, Engenharia de Requisitos. Na sequência, elaborou-se uma matriz de sinônimos (Tabela 1) e tabela PICOC (Tabela 2) para definição dos termos, que constaram na busca automatizada nos títulos, resumos e palavras-chave. Esta estratégia foi definida a partir das primeiras interações retornarem trabalhos não relevantes para o planejamento realizado.

Tabela 1: Matriz de sinônimos para termos para *string* de busca.

Requisito	**Conformidade**	**Legal**	**Ágil**
Requirement	Compliance	Legal	Agile
	Compliant	Law	Agility
		Legislative	Extreme Programming
		Legislation	XP
		Regulatory	Adaptive Software Development
		Regulation	ASD
		Mandatory	Crystal Blue
		Policy	Crystal Clear
		Standard	Crystal Methodologies
			Crystal Methodology
			Crystal Orange
			Crystal Red
			DSDM
			Dynamic System Development
			FDD
			Feature Driven Development
			Lean Software Development
			LD

			LSD
			TDD
			Test Driven Development
			Scrum

Tabela 2: Método PICOC (*population, intervention, control, outcome, context*).

Termo do PICOC	**Palavras-chave**
População (*Population*)	*requirement, compliance, compliant, law, legal, legislation, legislative, mandatory, policy, regulation, regulatory, standard*
Intervenção (*Intervention*)	*artifact, framework, good practice, guide, method, methodology, model, prototype, technique, technology, tool*
Controle (*Control*)	*traditional ecosystem*
Resultado (*Outcome*)	*artifact, framework, good practice, guide, method, methodology, model, prototype, technique, technology, tool, (legal compliance, compliant with law)*
Contexto (*Context*)	*agile ecosystem, Requirements Engineering, Software Engineering*

3.2.1 Documentação do processo de busca

i) Nome da base: ACM Digital Library

Endereço do site: http://dl.acm.org

String utilizada: acmdlTitle:(+(law legal legislation legislative mandatory policy regulation regulatory standard) +(compliance compliant requirement) +(agile agility scrum "extreme programming" xp "dynamic system development" dsdm "crystal methodology" "crystal methodologies" "crystal clear" "crystal orange" "crystal red" "crystal blue" "feature driven development" fdd "lean software development" "adaptive software development" "test driven development" tdd)) OR recordAbstract:(+(law legal legislation legislative mandatory policy regulation regulatory standard) +(compliance compliant requirement) +(agile agility scrum "extreme programming" xp "dynamic system development" dsdm "crystal methodology" "crystal methodologies" "crystal clear" "crystal orange" "crystal red" "crystal blue" "feature driven development" fdd "lean software development" "adaptive software development" "test driven development" tdd)) OR keywords.author.keyword:(+(law legal legislation legislative

mandatory policy regulation regulatory standard) +(compliance compliant requirement) +(agile agility scrum "extreme programming" xp "dynamic system development" dsdm "crystal methodology" "crystal methodologies" "crystal clear" "crystal orange" "crystal red" "crystal blue" "feature driven development" fdd "lean software development" "adaptive software development" "test driven development" tdd))
Configurações adicionais: nenhuma.
Resultado: 96 estudos.

ii) Nome da base: DBLP Computer Science Bibliography
Endereço do site: https://dblp.uni-trier.de/
String utilizada: "law | legal | legislation | legislative | mandatory | policy | regulation | regulatory | standard", "compliance | compliant | requirement", "agile | agility | scrum | extreme | xp | dsdm | fdd | tdd | crystal | lean | dynamic | adaptative | driven"
Configurações adicionais: nenhuma.
Resultado: 27 estudos.

iii) Nome do indexador: Scopus
Endereço do site: http://www.scopus.com
String utilizada: (TITLE-ABS-KEY ((law OR legal OR legislation OR legislative OR mandatory OR policy OR regulation OR regulatory OR standard) AND (compliance OR compliant OR requirement OR requirements) AND (agile OR agility OR scrum OR "extreme programming" OR xp OR "dynamic system development" OR dsdm OR "crystal methodologies" OR "crystal clear" OR "crystal orange" OR "crystal red" OR "crystal blue" OR "feature driven development" OR fdd OR "lean software development" OR "adaptive software development" OR "test driven development" OR tdd)))
Configurações adicionais: nenhuma.
Resultado: 1.176 estudos (659 estudos - filtro: Computer Science).

Nesta primeira etapa, um total de 782 estudos foram selecionados, a partir das bases e do indexador de busca elencados. Para segunda etapa, foram identificados eventos e periódicos especializados ou de interesse para busca manual, a lista que segue. Salienta-se, que após a realização da busca manual, foram identificados que os artigos de interesse já encontravam naqueles extraídos pela busca automática.

1. International Conference on Software Engineering (ICSE)
2. IEEE International Requirements Engineering Conference (RE)
3. International Workshop Series on Requirements Engineering and Law (RELAW)
4. Workshop em Engenharia de Requisitos (WER)
5. Brazilian Symposium on Software Engineering (SBES)
6. Requirements Engineering Journal (RE)
7. International Journal of Law and Information Technology (IJLIT)
8. European Journal of Law and Technology (EJLT)
9. Artificial Intelligence and Law (AILJ)

Para seleção dos estudos foram utilizados alguns critérios de inclusão e de exclusão que são listados a seguir:

1. Critérios de inclusão

a. Estudos cujos temas estão relacionados com requisitos legais ou regulatórios, conformidade legal ou regulatória, leis.

b. Estudos contextualizados aos ecossistemas ágeis.

c. Estudos que apresentem conceitos, teorias, *guidelines*, discussões, lições aprendidas e relatos de experiência sobre ecossistemas ágeis, fonte legal ou regulatória (leis, decretos, normas, regulamento, regimento) e conformidade ou requisito legal ou regulatório na grande área de Ciência da Computação ou nas áreas de Engenharia de Software ou Engenharia de Requisitos.

d. Estudos primários.

e. Estudos escritos na Língua Inglesa ou Língua Portuguesa.

f. Estudos publicados a partir do ano de 2014 até o ano de 2018 (os cinco últimos anos).

2. Critérios de exclusão

a. Capítulos de livro, chamada para congressos, palestras, relatórios dos workshops, livros, teses e dissertações.

b. Documentos incompletos, rascunhos, *slides* de apresentações.

c. Estudos que não puderem ser acessados completos a partir do portal de periódicos da CAPES.

d. Estudos que não tratem de ecossistemas ágeis, fonte legal ou regulatória (leis, decretos, normas, regulamento, regimento) e conformidade ou requisito legal ou regulatório na grande área de Ciência da Computação ou nas áreas de Engenharia de Software ou Engenharia de Requisitos.

e. Estudos que não forem primários.

f. Estudos escritos em outras línguas que não sejam a Inglesa ou a Portuguesa.

g. Estudos publicados antes do ano de 2014.

h. Estudos duplicados ou repetidos.

A extração dos dados foi realizada por etapas, sendo quatro ao todo. Na primeira, buscavam-se detalhes da publicação, como: autores, ano, título, fonte, resumo, palavras-chaves e objetivos; enquanto que na segunda etapa descrições do contexto, logo assuntos, tecnologias, indústria e características; para depois já, na terceira etapa, procurar pelos achados, ou melhor, resultados, comportamentos, ações, fenômeno, eventos e citações; desse modo, na última etapa, a quarta, examinavam-se campos específicos do formulário de extração de dados, como os termos do método PICOC (população, intervenção, controle, resultado, contexto).

Com os textos lidos e os dados extraídos foi possível fazer uma avaliação da qualidade dos estudos selecionados atribuindo-lhes valores, quando não especificado outro de maior relevância: não atende - 0 (zero); atende parcialmente - 0,5 (meio ponto); atende - 1 (um ponto). Adotaram-se apenas os critérios sugeridos por Dybå e Dingsøyr (2008), listados em seguida:

1. O estudo está baseado em pesquisas empíricas ou em relatos de experiência com base em relatórios ou na opinião de especialistas?

2. Existe uma definição clara dos objetivos da pesquisa?

3. Existe uma descrição adequada do contexto em que a pesquisa foi realizada?

4. O planejamento da pesquisa foi adequado para abordar os objetivos da pesquisa?

5. A estratégia de extração de dados foi adequada aos objetivos da pesquisa?

6. Havia um grupo de controle com o qual pudesse comparar tratamentos?

7. Os dados foram coletados de forma que abordasse as questões de pesquisa?

8. A análise dos dados foi suficientemente rigorosa?

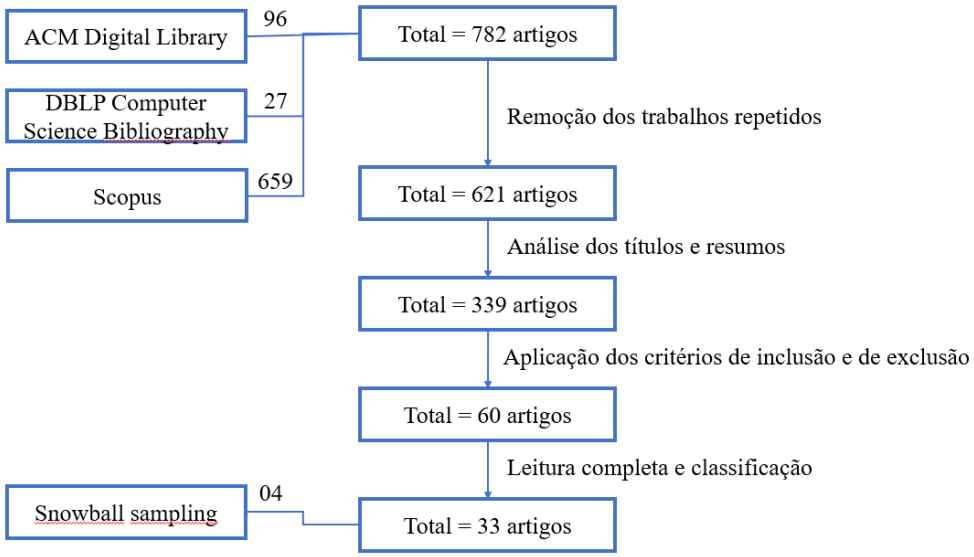
9. Será que a relação entre pesquisador e participantes foi considerada um grau adequado?

10. Existe uma indicação clara dos resultados?

11. É o estudo de valor para pesquisa ou prática?

A seguir, são demonstrados os resultados da revisão realizada seguindo todo processo descrito até então. Todavia, antes, será apresentada uma Figura 3.2 representando o processo de filtragem e número de artigos obtidos em cada uma das fases desta revisão.

Figura 7: Representa o processo de “filtragem”.



Fonte: a autora.

3.2.1 Resultados

Os artigos resultantes foram no total de 33 ao final do processo. A análise aqui apresentada foi descritiva com intenção de exibir os achados da pesquisa, que examinou os últimos cinco anos (2014-2018) à época de sua feitura. Na Tabela 3, constam títulos, autores e anos de publicação dos artigos selecionados. Podem ser observadas as parcerias e publicação de mesmos autores em anos diferentes, em algumas vezes com a mesma temática.

Tabela 3: Artigos selecionados na revisão sistemática da literatura.

ID	Título	Autor	Ano
01	The Odyssey: Modeling Privacy Threats in a Brave New World	Galvez R., Gurses S.	2018
02	Review of formal agile methods as cost-effective airworthiness certification processes	Blooshi M.A., Jafer S., Patel K.	2018

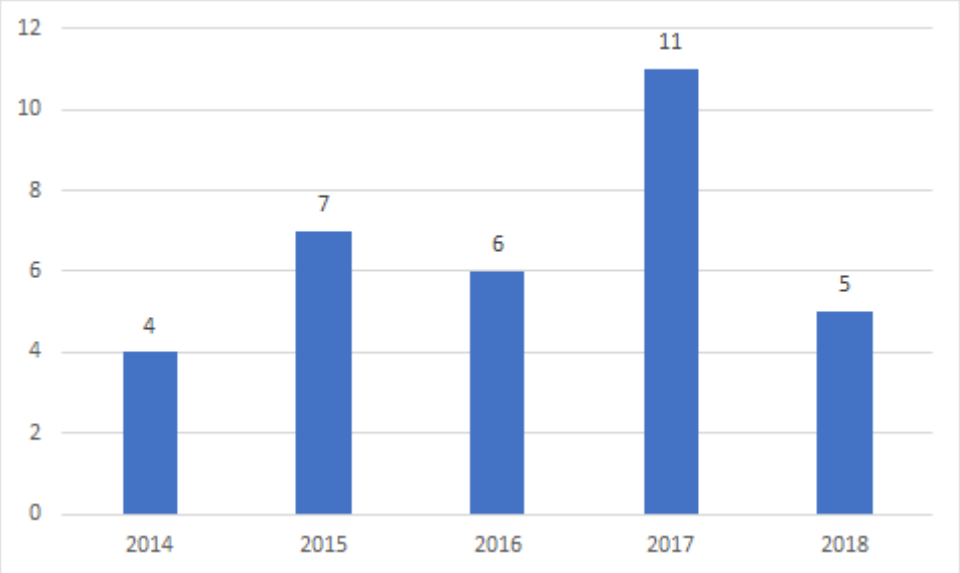
03	Regulated software meets DevOps	Laukkarinen T., Kuusinen K., Mikkonen T.	2018
04	Towards continuous security compliance in agile software development at scale	Moyon F., Beckers K., Klepper S., Lachberger P., Bruegge B.	2018
05	A hybrid assessment approach for medical device software development companies	Özcan-Top Ö., McCaffery F.	2018
06	An Architecture for Agile Systems Engineering of Secure Commercial Off-the-Shelf Mobile Communications	Gump J., Mazzuchi T., Sarkani S.	2017
07	Knowledge transfer for global roles in GSE	Gupta R.K., Anand T.	2017
08	Mobile medical app development with a focus on traceability	Trektere K., Regan G., Caffery F.M., Flood D., Lepmets M., Barry G.	2017
09	Security, compliance, and agile deployment of personal identifiable information solutions on a public cloud	Katsuno Y., Kundu A., Das K.K., Takahashi H., Schloss R., Dey P., Mohania M.	2017
10	DevOps in regulated software development: Case medical devices	Laukkarinen T., Kuusinen K., Mikkonen T.	2017
11	Towards a middleware and policy-based approach to compliance management for collaborative organizations interactions	González L., Ruggia R.	2017
12	Agile composition of compliant data analytics platforms	Le M., Jayaram K.R., Weinsberg Y., Dean D.J., Tao S.	2017
13	Meeting requirements imposed by secure software development standards and still remaining agile	Górski J., Łukasiewicz K.	2017
14	The Use of Analytic Hierarchy Process for Software Development Method Selection: A Perspective of e-Government in Indonesia	Helingo M., Purwandari B., Satria R., Solichah I.	2017
15	How Does Scrum Conform to the Regulatory Requirements Defined in MDevSPICE®?	Özden Özcan Top and Fergal McCaffery	2017
16	Analysis of DILRMP Project: Identifying the Applicability of Agile Project Management for Digital Transformation Projects in Government and Public Sector	Amrutaunshu Nerurkar and	2017

		Indrajit Das	
17	An agile development process for petrochemical safety conformant software	Myklebust T., Stalhane T., Lyngby N.	2016
18	Tailoring MDevSPICE® for mobile medical apps	Trektere K., McCaffery F., Lepmets M., Barry G.	2016
19	Experiences in the Development and Usage of a Privacy Requirements Framework	Oliver I.	2016
20	Business process elicitation from regulatory compliance documents: An E-government case study	Stratigaki C., Nikolaidou M., Loucopoulos P., Anagnostopoulos D.	2016
21	Quality assurance in scrum applied to safety critical software	Hanssen G.K., Haugset B., Stålhane T., Myklebust T., Kulbrandstad I.	2016
22	Big ideas paper - Policy-driven middleware for a legally-compliant Internet of Things	Jatinder Singh and Thomas F. J.-M. Pasquier and Jean Bacon and Julia E. Powles and Raluca Diaconu and David M. Eyers	2016
23	The role of CM in agile development of safety-critical software	Stålhane T., Myklebust T.	2015
24	A conceptual framework for enterprise agility	Nwokeji J.C., Clark T., Barn B., Kulkarni V.	2015
25	Assurance case integration with an agile development method	Doss O., Kelly T.	2015
26	Agile software development requires an agile approach for computer system validation of clinical trials software products	Kuchinke W., Krauth C., Karakoyun T.	2015
27	Securing scrum for VAHTI	Rindell K., Hyrynsalmi S., Leppänen V.	2015
28	Model-driven regulatory compliance - A case study of "Know Your Customer" regulations	Sagar Sunkle and Deepali Kholkar and Vinay Kulkarni	2015
29	Weekly Round Trips from Norms to Requirements and Tests:	Paolo Tonella and	2015

	An Industrial Experience Report	Roberto Tiella	
30	The application of an agile approach to it security risk management for SMES	Hutchinson D., Armitt C., Edwards-Lear D.	2014
31	From legislation towards the provision of services: An approach to agile implementation of legislation	Van Engers T., Nijssen S.	2014
32	Agile requirements engineering via paraconsistent reasoning	Ernst N.A., Borgida A., Jureta I.J., Mylopoulos J.	2014
33	SW process tailoring practice in medical device industry	Lian S.	2014

Na Figura 8, pode ser observada a distribuição dos estudos selecionados por ano. Uma questão que atraiu a atenção foi o ano de 2017 por possuir um número superior de artigos do que os outros anos. Neste mesmo ano, foi extinto o Workshop especializado em leis e computação (*Requirements Engineering and Law - RELAW*) dentro da maior conferência da área de Engenharia de Requisitos (*IEEE International Requirements Engineering Conference*).

Figura 8: Gráfico com a distribuição dos estudos selecionados por ano.

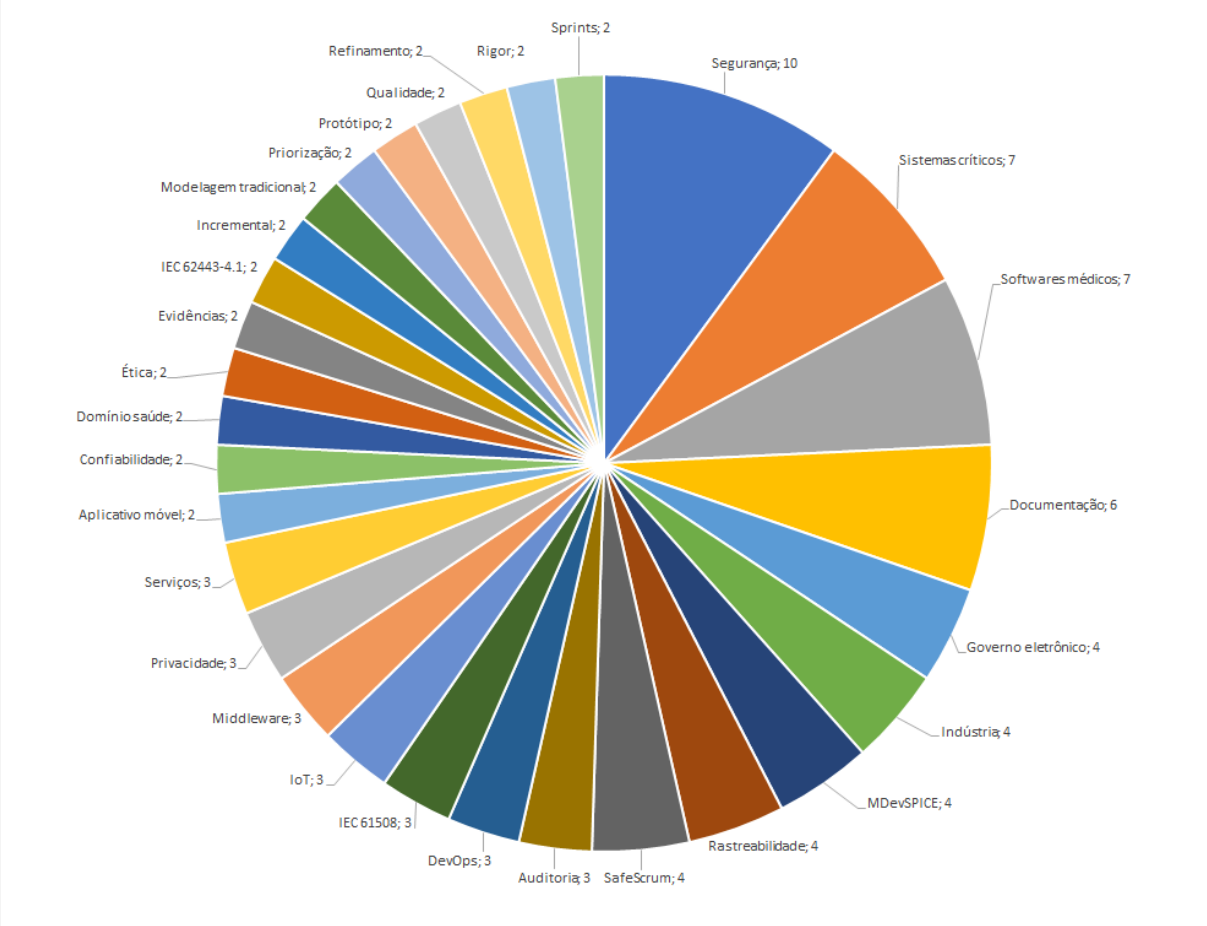


Fonte: a autora.

Nos estudos selecionados, além das palavras utilizadas para busca automatizada, foram encontradas as seguintes palavras com mais de uma ocorrência (Figura 9): segurança (10); sistemas críticos (7); softwares médicos (7); documentação (6); governo eletrônico (4);

indústria (4); MDevSPICE (4); rastreabilidade (4); SafeScrum (4); auditoria (3); DevOps (3); IEC 61508 (3); IoT (3); middleware (3); privacidade (3); serviços (3); aplicativo móvel (2); confiabilidade (2); domínio saúde (2); ética (2); evidências (2); IEC 62443-4.1 (2); incremental (2); modelagem tradicional (2); priorização (2); protótipo (2); qualidade (2); refinamento (2); rigor (2); sprints (2). Outras 112 palavras tiveram apenas uma ocorrência, portanto não são mencionadas.

Figura 9: Gráfico dos assuntos mais encontrados nos estudos selecionados.

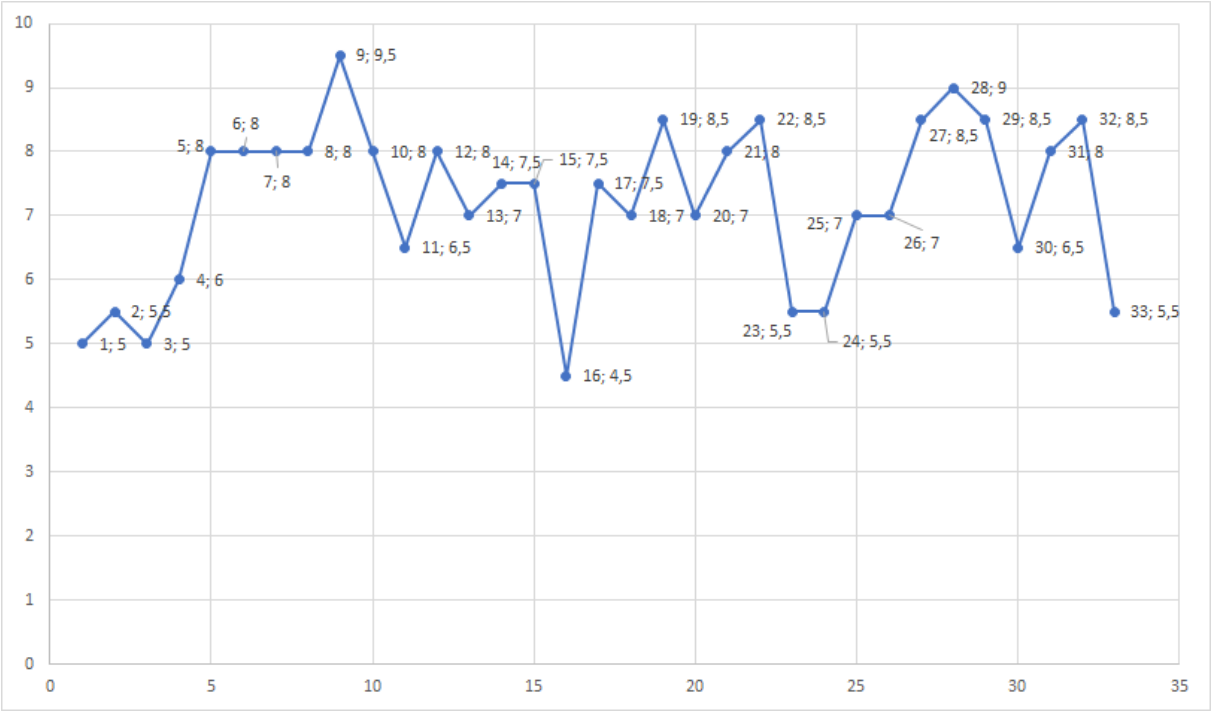


Fonte: a autora.

A Figura 10 exibe os valores atribuídos, quando considerados os critérios de qualidade citados no protocolo elaborado para esta revisão. Sendo o primeiro correspondente ao ID do artigo em questão, o caractere “;” foi utilizado como separador e, posteriormente, consta o somatório das notas recebidas nos critérios de qualidade, cujo valor máximo poderia ser 11 e o

mínimo zero. Não houve corte, visto que a intenção foi apenas identificar os trabalhos que mais poderiam contribuir com a pesquisa realizada.

Figura 10: Gráfico sobre a qualidade atribuída a cada estudo.



Fonte: a autora.

3.3 Resultados por questão de pesquisa

Dos 33 artigos, 19 responderam a três questões de pesquisa, 11 a duas questões, e o restante a apenas uma questão. Os trabalhos que responderam a primeira questão de pesquisa "**QP1 - Como os requisitos legais são tratados (elicitados, documentados, verificados, validados, gerenciados - rastreados e mantidos) nos ecossistemas ágeis?**", assim o fizeram das mais diferentes formas. Alguns utilizando, por exemplo: rastreamento de artefatos para haver provas de verificação de software (evidência de conformidade) ou do processo de desenvolvimento de software; construção do conhecimento para equipe e documentação mínima; arquivamento contínuo; uso de templates padrão; mapeamento de padrões de segurança; preocupando-se com códigos reutilizáveis e sustentáveis; menor tempo de lançamento (menor tempo entre as sprints); reutilização de utilização de soluções de conformidade; fazendo entregas contínuas; preocupação com a integração contínua; a solução

ser incremental; preocupações com a segurança e privacidade; preocupação com o emprego dos padrões IEC 61508, IEC 61511, IEC-62304, IEC-82304-1, IEC 60880; rigor onde for necessário, mas flexibilidade, eficiência, eficácia, confiabilidade, colaboração sempre; refinamento de técnicas, códigos e conhecimento; comunicação; consulta a um avaliador independente; qualidade de serviço; envolvimento das partes interessadas.

Com relação a segunda questão de pesquisa "**QP2 - Quais artefatos são utilizados para tratamento dos requisitos legais nos ecossistemas ágeis?**", os artefatos foram diversos. Alguns dos citados foram, por exemplo: integração contínua e práticas juntos aos interessados; notação BPMN; framework SAFe; framework MDevSPICE; linguagem KATA; tecnologias IoT; técnicas de prototipação; solução em nuvem da IBM SoftLayer; metodologias DevOps, SafeScrum, Scrum, Add-on; gerenciamento de configuração; uso de ontologia; planejamento detalhado; cooperação entre instituições; refinamento do processo; auditorias com maior frequência; metamodelos; middleware; sprints; spikes; backlog do produto; histórias de segurança; casos de abuso; soluções de governança, risco e conformidade (GRC); modelos de propósitos; técnica "conheça seu cliente"; gestão de negócios; casos de testes; atribuição de funções e de responsabilidades; foco nos recursos humanos; maiores esforços conjuntos da academia, negócios, governo; equipes de conhecimento multidisciplinar; uso de JIRA, GIT, Jenkins, Docker; emprego do CMMI; ISO/IEC 15504; matriz de mapa de partes interessadas.

Por fim, com relação a terceira questão de pesquisa "**QP3 - Em que se diferem as técnicas, as ferramentas e os artefatos relacionados com os requisitos legais de outros tipos requisitos nos ecossistemas ágeis?**", após a leitura de diversos artigos foi possível entender que está na essência da pergunta. Ao ler artigos das áreas de Direito, de Computação, que tinham como foco a conformidade legal e regulatória ou o requisito legal ou regulatório, o que transforma o foco do autor, do responsável, do profissional da Computação, do Direito. Até quando as ferramentas são as mesmas utilizadas pelas equipes, que não estão concentradas nesses objetivos, as estratégias, as preocupações alteram-se. Bem certo que há como motivação as sanções em decorrência do não cumprimento de fonte legal ou regulatória, todavia existe também a necessidade de corretude como vontade maior.

3.3.1 Sumarização dos estudos

Galvez e Gurses (2018) expõem a lacuna entre a modelagem em cascata e ágil para tratar problemas críticos, como a nova GDPR, e se propõe a criar modelos seguindo os princípios e serviços ágeis para enfrentar as ameaças inerentes à privacidade.

Blooshi, Jafer e Patel (2018) Fazem uma revisão sobre métodos ágeis aplicados a sistemas críticos, e o que deve ser priorizado nesses tipos de sistemas.

Os autores (LAUKKARINEN, KUUSINEN, MIKKONEN, 2018) disseram que o primeiro ponto a ser destacado era a intenção de aproximar DevOps, que prega a integração contínua, com a conformidade legal e regulatória. Para isso, foram melhoradas algumas práticas junto aos stakeholders.

Para Moyon et al. (2018) propuseram um método de arquivamento contínuo e desenvolvimento seguro para mapeamento de requisitos padrões de segurança dentro de processos ágeis de desenvolvimento. Para demonstrar o método utilizam BPMN e artefatos do *framework* SAFe, de acordo com a IEC 62443-4-1.

Özcan-Top e McCaffery (2018) fizeram uma apresentação de uma avaliação híbrida que combinou os métodos baseados em MDevSPICE® (método de avaliação de processos com etapas para priorização das necessidades de melhoria por meio do valor mapeamento de fluxo) e o uso da técnica KATA (permitindo a melhoria de processos). Essa abordagem integrou métodos ágeis no processo de desenvolvimento de software de dispositivos médicos, enquanto aderiu aos requisitos às normas regulamentares.

Os autores (GUMP, MAZZUCHI, SARKANI, 2017) apresentaram uma forma de desenvolvimento rápida baseada na tecnologia COTS para evolução dos sistemas e dos requisitos do governo federal para a Agência Nacional de Segurança dos Estados Unidos da América (NSA).

Gupta e Anand (2017) apresentaram as diferentes etapas percorridas por uma fábrica de software e sua evolução. Essa fábrica enfrentou diferentes desafios como: i) identificação de competências; ii) treinamento para o qual pode ser transmitido a outra pessoa que assumirá a função/função; iii) transferência de conhecimento de algumas funções identificadas para um grande sistema de software de missão crítica que precisava estar em conformidade com os requisitos regulatórios; iv) priorização com base na facilidade de transferência de conhecimento para diferentes áreas de trabalho. A fábrica está há 15 anos no mercado atendendo diferentes clientes e suas demandas, e acredita que sua experiência possa ser estendida a outras fábricas de software.

Trektere et al. (2017) apresentaram uma estrutura de desenvolvimento de aplicativo médico móvel, os principais critérios para tal estrutura e descreve como os resultados foram coletados através da realização de um dispositivo médico. Ainda, demonstra como o MDevSPICE (uma abordagem ágil de desenvolvimento de software) pode ser adaptada para oferecer suporte a aplicativos médicos móveis. Este artigo também afirma ter como um dos

principais critérios para aplicação médica móvel estrutura de desenvolvimento a rastreabilidade.

Os autores (Katsuno et al., 2017) propuseram uma abordagem para gerenciar a segurança e a privacidade de uma análise de educação-aprendizagem de solução em uma plataforma de nuvem pública, garantindo a conformidade com a Lei dos Direitos Educacionais e Privacidade da Família (FERPA). Também, é proposta uma nova abordagem de implantação ágil que é ao mesmo tempo rápida e automática. Um protótipo de uma solução de análise de aprendizagem foi implementado em uma nuvem pública SoftLayer, e o novo método de implantação foi avaliado em comparação com métodos.

Os autores (LAUKKARINEN, KUUSINEN, MIKKONEN, 2017) discutiram a adequação do DevOps para o desenvolvimento de software regulamentado para dispositivos médicos. Foram examinados dois padrões relacionados, IEC-62304 e IEC-82304-1, para obstáculos e benefícios do uso DevOps para desenvolvimento de softwares para dispositivos médicos. Estabelecer esses padrões para quais são os obstáculos para entrega contínua e integração, e que ferramentas de desenvolvimento podem ajudar a cumprir os requisitos de rastreabilidade e documentação destes padrões foram as conclusões desse trabalho.

González e Ruggia (2017), neste artigo, propuseram uma abordagem baseada em middleware e política para gerenciamento de conformidade para interações de organizações colaborativas. A abordagem compreende mecanismos de tempo de design (por exemplo, uma linguagem específica de domínio, uma linguagem de política) e mecanismos de tempo de execução (por exemplo, um ponto de aplicação de política, um serviço de obrigações) que estendem uma plataforma de integração baseada em middleware. A proposta visa promover a manutenção, flexibilidade, agilidade e reutilização das soluções de compliance nestes contextos, proporcionando os meios para especificar uniformemente os requisitos de compliance, bem como definir a forma como estes requisitos devem ser geridos numa plataforma de integração.

Le et al. (2017) apresentaram o projeto e a implementação de uma plataforma de middleware baseada em nuvem que dá suporte à composição e configuração sob demanda de mecanismos de segurança para facilitar a ativação da conformidade regulatória a partir das experiências e lições aprendidas com o uso da plataforma implementada para os sistemas analíticos seguros na IBM; e ainda destacam os benefícios da abordagem, discutindo o impacto no desempenho e as compensações de diferentes mecanismos de segurança com relação à conformidade regulatória.

Górski e Łukasiewicz (2017), no documento, apresentaram o método AgileSafe de seleção de práticas ágeis para projetos de desenvolvimento de *software*, que são restringidos por requisitos de garantia resultantes de padrões relacionados à proteção ou privacidade. Tais requisitos são representados por modelos de argumentação que explicam como as evidências coletadas durante a implementação de práticas ágeis irão apoiar a conformidade com os requisitos. A aplicação do método é demonstrada referindo-se a um estudo de caso de desenvolvimento de uma aplicação relacionada ao domínio médico que supostamente cumpre os requisitos impostos pela norma IEC 62443-4.1.

Helingo et al. (2017) disseram que ao fornecer serviços para o governo eletrônico para reduzir a burocracia e atingir prioridades nas políticas externas, em geral, requer um desenvolvimento de software com um procedimento padrão para atender à garantia de qualidade do software e de forma incremental. Porém, faltou investigação para esta seleção. Para resolver este problema, um estudo usando Analytic Hierarchy Process (AHP) foi conduzido. As variáveis de fator foram: pessoal, requisitos, aplicativos, organizações, negócios, operações e tecnologia. As alternativas de métodos de desenvolvimento de software são Waterfall, Incremental, Prototipagem, Extreme Programe, Scrum e Rational Unified Process. Os resultados mostram que a prototipagem é o desenvolvimento de software mais adequado método para Kemlu.

Özcan-Top e McCaffery (2017) afirmaram que, devido à alta regulamentação relacionada aos softwares para dispositivos médicos, são necessárias alta disciplina e que as evidências sejam fornecidas para fins de auditoria. Portanto, há uma transição para a agilidade no desenvolvimento de sistemas críticos de segurança, para construir sistemas de alta qualidade, encurtar o tempo de entrada no mercado, melhorar a satisfação de clientes e funcionários e garantir a segurança e confiabilidade. Assim, nesse artigo, foram investigados se os requisitos regulatórios definidos no MDevSPICE® foram atendidos adotando o método Scrum e quais processos e práticas adicionais devem ser realizados para garantir a segurança e conformidade regulatória no domínio da saúde.

Para os autores Nerurkar e Das (2017) a necessidade de um projeto ágil de gestão com uma análise detalhada de um dos grandes desafios que foi dimensionar projetos de governança eletrônica do modo de missão do governo da Índia, o Programa de Modernização de Registros Terrestres da Índia Digital (DILRMP).

Para os autores (MYKLEBUST, STALHANE, LYNGBY, 2016), os métodos ágeis estão ganhando popularidade crescente em áreas críticas de segurança, como a indústria petroquímica, visto que os métodos ágeis prometem custos reduzidos e menor tempo de

lançamento no mercado por meio do desenvolvimento incremental, menos produção de documentos desnecessários e código mais sustentável. Na indústria petroquímica, os fabricantes e os fornecedores de dispositivos devem usar o IEC 61508, enquanto os projetistas, os integradores e os usuários do sistema devem usar o IEC 61511. Assim, o desafio foi introduzir um desenvolvimento ágil sem comprometer a segurança, visto que este padrão impõe rigor e custos adicionais, mas a adaptação adequada de métodos ágeis pode adicionar flexibilidade e eficiência. A inspiração foram os trabalhos de IEC 61508 (Stålhane 2012) e IEC 60880 (Stålhane 2013), que resultaram em um método chamado SafeScrum. Os principais desafios são o IEC 61511 requisitos de gerenciamento de configuração, rastreabilidade, planejamento detalhado e documentação. Os autores buscam por outras empresas que desejem trabalhar cooperação para refinar o processo.

Trektere et al. (2016) utilizaram o framework MDevSPICE® conhecido por apoiar o desenvolvimento de aplicativos médicos introduzindo práticas ágeis na estrutura para desenvolver um aplicativo móvel. O foco estava em um aplicativo médico capaz de ter em seu cerne toda a documentação regulatória essencial para esse tipo de mercado na área da saúde.

O autor (OLIVER, 2016) defende que os requisitos de privacidade não foram corretamente desenvolvidos com a união dos domínios jurídico e da engenharia. Então, para resolver este problema, é proposto desenvolver estruturas ontológicas para auxiliar a comunicação entre esses domínios, e fornecer uma semântica comumente aceitável e uma estrutura pela qual os requisitos expressos em diferentes níveis de abstração possam ser vinculados e dar apoio ao refinamento. É sugerido, ainda que requisitos de privacidade e suas implementações potenciais podem ser explorados por meio do processo de desenvolvimento de software e idéias de suporte, como métodos ágeis e 'DevOps', em vez de ser um exercício 'add-on' - uma avaliação do impacto da privacidade.

Stratigaki et al. (2016) apresentaram um estudo de caso no governo eletrônico baseado na legislação grega, onde inúmeras fontes de requisitos de conformidade obrigam as organizações a avaliar seus processos de negócios, e garantir que cumpram as restrições estabelecidas. Para atender a esse esforço, as empresas devem focar em seus processos de negócios e agilidade, em conformidade, no contexto regulatório definido. O modelo proposto define as regras de conformidade descritas com base nos mesmos componentes principais dos processos de negócios (atividade, dados, função e evento) por meio de visualizações gráficas para permitir que os analistas de negócios extraiam modelos de processos de negócios das regras MTL (Metric Temporal Logic).

Os autores (Singh et al., 2016) defenderam que como as aplicações de IoT estão sujeitas à lei, devem haver mecanismos que permitam a aplicação da política específica, de forma que os sistemas se alinhem com as realidades jurídicas. A auditoria da aplicação da política deve auxiliar na distribuição de responsabilidades, demonstrar conformidade com a regulamentação e indicar se a política captura corretamente as responsabilidades legais. Como os sistemas e as obrigações evoluem dinamicamente, esse ciclo deve ser mantido continuamente. Isto se torna mais complexo em domínios federados, por isso uma sugestão de middleware desempenhando um papel fundamental no gerenciamento da IoT. Investigaram o uso de Information Flow Control (IFC) para gerenciar, e auditar fluxos de dados na computação em nuvem; um domínio onde a confiança pode ser bem fundamentada, os regulamentos são mais maduros e as responsabilidades associadas mais claras.

Stålhane e Myklebust (2015) utilizando gerenciamento de configuração e SafeScrum, para desenvolvimento ágil de software crítico para a segurança baseados nos os padrões IEC 61508 e EN 50128, disseram que foi possível realizar desenvolvimento ágil, desde que o foco estivesse no quê e não tanto foco em como.

Os autores (Nwokeji et al., 2015) propuseram um metamodelo onde as partes interessadas podem ser mais proativas e apoiar a tomada de decisões em relação ao gerenciamento de mudanças, como relação conformidade regulamentar e atualização, obsolescência de tecnologia no processo ágil de desenvolvimento.

Doss e Kelly (2015) utilizaram SafeScrum para o domínio automotivo, que é considerado um dos domínios dos sistemas críticos de segurança. Testaram os processos de engenharia de software em relação aos requisitos dos padrões de garantia de segurança de software, inclusive para a ISO 26262.

Os autores (KUCHINKE, KRAUTH, KARAKOYUN, 2015) selecionaram quatro grupos de desenvolvedores acadêmicos do projeto p-medicine da UE, que foram entrevistados para avaliar a prontidão de seus produtos desenvolvidos para serem usados em pesquisas clínicas em um ambiente regulamentado. As ferramentas de grupos dessa natureza devem passar por um processo denominado validação de sistema computacional (CSV) para cumprimento das Boas Práticas Clínicas (GCP), requisitos regulatórios e éticos. Uma análise dos resultados da pesquisa mostrou que existem lacunas consideráveis na manutenção de ferramentas, gestão da qualidade e documentação de conformidade. Como todos os grupos de desenvolvedores usavam métodos de desenvolvimento ágil, recomendações para garantia de qualidade ágil utilizável em grupos acadêmicos e um conceito de “conformidade por projeto”

foram desenvolvidos para aprimorar o gerenciamento de qualidade, preparar o desenvolvimento de ferramentas para validação de sistema de computador e uso em testes clínicos.

A coleção de padrões de segurança do governo finlandês, VAHTI, é um dos exemplos mais abrangentes desses padrões de níveis concretos e mensuráveis de segurança de software, e regulamentos internacionais, nacionais e de nível de indústria. Os autores (RINDELL, HYRYNSALMI, LEPPÄNEN, 2015) modificaram o método Scrum para apoiar o desenvolvimento utilizando VAHTI. Isso inclui modificações específicas de segurança, modificações aos sprints e inclusão de sprints e spikes de reforço especial para implementar os itens de segurança no backlog do produto. Os requisitos de segurança foram transformados em histórias de segurança, casos de abuso e outras tarefas relacionadas à segurança. A definição do feito em relação aos requisitos do VAHTI foi estabelecida e as etapas para alcançá-la foram descritas.

Os autores (SUNKLE, KHOLKAR, KULKARNI, 2015) destacaram o regime regulatório sem precedentes, que as empresas vêm enfrentando, e as soluções de governança, risco e conformidade (GRC) do setor são orientadas por documentos e por especialistas. Para melhor apoiar essas empresas, foi proposto otimizar a conformidade regulatória usando vários modelos de propósito de vários aspectos dos regulamentos, com o objetivo de alavancar tanto o rigor das técnicas formais quanto a perspectiva holística do GRC empresarial. Como resultados, são apresentados uma arquitetura orientada por modelo com base em um modelo conceitual de GRC integrado, que é capaz de enfrentar os principais desafios de conformidade regulatória; e uma técnica, usando as regulamentações, "Conheça seu Cliente", no contexto indiano, como estudo de caso, demonstraram a utilidade dessa arquitetura. Para os autores os resultados iniciais, com as regulamentações KYC foram promissores.

Tonella e Tiella (2015) descreveram a experiência de reengenharia dos softwares de um grande fornecedor de na Itália na área de gestão de negócios, com foco em normas e recursos humanos. Nesse processo, foi introduzido um novo processo de desenvolvimento ágil, visando diversos aspectos de um projeto de reengenharia em andamento. Focaram na derivação da implementação e dos casos de teste dos requisitos normativos, de modo a garantir o alinhamento entre os objetivos do teste e os comportamentos esperados do sistema expressos nos documentos de requisitos. Assim, o novo processo pode ser percebido como benéfico em vários aspectos, como a atribuição de funções e responsabilidades e a rastreabilidade das normas aos requisitos, código e testes.

Os autores (HUTCHINSON, ARMITT, EDWARDS-LEAR, 2014) descreveram a aplicação de uma abordagem ágil de gerenciamento de risco para realizar análises de risco

baseadas em ativos para atender aos requisitos de segurança da informação de PMEs (Pequenas e Médias Empresas). A instituição em estudo é um Centro de Assistência a Idosos (ACF) com responsabilidades legais e éticas. Para analisar e comunicar os riscos potenciais aos ativos de TI atuais e propor sugestões para mitigar e minimizar os fatores de risco, uma abordagem ágil de avaliação de risco de segurança de TI foi desenvolvida em um empreendimento de pesquisa colaborativa com ACF e seu Provedor de TI Externo (EIP).

Van Engers e Nijssen (2014) relataram a iniciativa de várias pessoas do governo holandês, academia e negócios, que se uniram com ideias concretas de cooperar estreitamente no desenvolvimento de uma implementação ágil da legislação, permitindo uma abordagem centrada no ser humano. O princípio utilizado foi: digital sempre que possível, pessoalmente quando necessário. As ênfases podem ser resumidas da seguinte forma: 1. Gestão do conhecimento pela equipe responsável pela política e implementação de serviços. 2.Separar a gestão de sistemas informáticos destinados a apoiar o tratamento de processos em larga escala, mas interligados. 3. Trabalhar o conhecimento multidisciplinar ao focar a política, a implementação de serviços e o fornecimento de informações na gestão do conhecimento e na preparação de especificações de TI. 4. Captura de especificações reutilizáveis e sustentáveis para processos de implementação de serviços e TI. 5. O desenvolvimento de métodos e padrões reconhecidos internacionalmente.

Ernst et al. (2014) lançaram um olhar sobre instituições inovadoras e sua necessidade de uma abordagem ágil em relação aos requisitos de produtos e serviços, para responder rapidamente e explorar as mudanças nas condições, principalmente, para acomodar os requisitos legais e não requisitos funcionais. Com isso utilizaram o framework RE-KOMBINE, que é baseado em uma linguagem proposicional para modelagem de requisitos chamada Techne, que toleram a presença de inconsistências. Fizeram um estudo de caso usando duas ferramentas de análise formal em modelos de proporção industrial, e a sua tolerância à informalidade foi útil durante a análise inicial de requisitos.

Lian (2014) compartilhou a experiência de adaptar o processo de modelo V para integrar as práticas AGILE, para atender aos requisitos regulamentares de desenvolvimento de software de dispositivo médico.

3.4 Discussão

A revisão permitiu alguns achados singulares, como: i) um trabalho que ao invés de utilizar histórias de usuário empregava histórias de segurança, e ao invés de casos de uso, casos de abuso, visto que seu domínio estava na área de segurança; ii) várias equipes fazendo uso da metodologia DevOps; iii) governo trabalhando em colaboração em si ou com seus cidadãos; iv) diferentes domínios que não os mais comuns como saúde, financeiro e governamental, e sim petroquímica, automobilística, cuidados para idosos, por exemplo; v) preocupação com privacidade e segurança; vi) maior atenção com rastreamento de artefatos e evidências legais ou regulatórias; vii) expressão da necessidade de documentação sem ser o código, mesmo que seja mínima.

As propostas de encaminhamentos para esta revisão são o compartilhamento com os pares e aplicação dos achados no andamento da pesquisa de doutoramento em andamento para aprofundamento e entendimento dos motivos/razão de ser. Haverá uma oportunidade imediata de confrontar os achados com os profissionais do mercado de Computação, e obter suas visões sobre seus ambientes frente aos relatos elaborados.

3.4.1 Ameaças à validade e limitações da revisão realizada

Embora tenha havido todo o cuidado, como toda pesquisa, há alguns limites que não puderam ser mitigados como a revisão ter sido feita por uma única pessoa. Também houve algumas ameaças à validade, que seguindo o que foi preconizado por Feldt e Magazinius (2010), podem ser descritas, como: i) validade de conclusão - por não se saber se o tratamento dado introduziu efeito estatisticamente significativo no resultado medido; ii) validade interna - por haver dúvidas se o tratamento causou o efeito no resultado ou outros fatores também assim o fizeram; iii) validade de construção - se tratamento corresponde à causa real ou efeito no que se estava interessado; iv) validade externa, transferibilidade - se a relação de causa e efeito mostrada seria válida em outras situações, os resultados podem ser generalizados ou aplicados em outros contextos.

3.5 Considerações

Esta revisão sistemática da literatura buscou por trabalhos no contexto na Engenharia de Requisitos e as metodologias ágeis (Engenharia Ágil de Requisitos) trata-se de requisitos legais ou regulatórios com a intenção da conformidade legal e regulatória dos sistemas computacionais. Após a formalização e execução de protocolo de pesquisa foram selecionados 33 artigos, sendo que 19 desses artigos responderam às três questões formuladas no protocolo da revisão. 11 artigos responderam apenas duas das três questões, e o restante apenas uma questão.

Os resultados encontrados mostram-se interessantes sob a ótica de haver diferentes esforços em diferentes domínios, todavia sempre prevalecem os relacionados os mais regulados, atualmente, que são os da saúde, financeiro e governamental, mesmo havendo fontes legais em todos os domínios.

No próximo capítulo, são apresentados os estudos exploratórios realizados para confrontar os resultados obtidos com essa revisão e os profissionais do mercado de trabalho.

4 Estudos Exploratórios

Os estudos exploratórios foram conduzidos com a intenção de estabelecer uma relação de prática ou não do mercado com os resultados obtidos a partir da revisão sistemática da literatura. Vislumbrou-se que correlacionando as práticas observadas com as práticas literárias poder-se-ia oferecer com maior propriedade uma solução, que, de fato, fosse incorporada pelas fábricas de *software* em seu cotidiano para otimizar o gerenciamento da conformidade legal e regulatória.

Desse modo, durante toda esta pesquisa, houve participações em trabalhos de outros pesquisadores, em alguns casos de forma integral e outros de forma pontual. Inicialmente, nos arranjos realizados, a intenção era apoiar algumas pesquisas, e em outras pesquisas o objetivo era trabalhar cooperativamente. Entretanto, aspectos relacionados puderam ser explorados nesses trabalhos, o que trouxe benefício para ambas as pesquisas, pois antes do uso dos artefatos programados para tal (ou de partes) foram definidos quais seriam utilizados em cada pesquisa. Assim, não haveria sobreposição de assuntos ou resultados. Esta tem se mostrado uma prática comum, quando se trabalha em laboratório, cujas pesquisas estão de algumas formas relacionadas, ou são reunidos pesquisadores com diferentes tipos de experiência.

Esta decisão apresentou-se muito rica, como processos em toda sua grandeza e relacionamentos na criação e na consolidação. Além disso, há também espaço mútuo para divulgação, colaboração, ensino-aprendizagem, dentre outros. Seguindo diferentes metodologias para cada parte do trabalho, mas tendo como um fio guia as obras de Flick (2008), Sampieri, Collado e Lucio (2014), Denzin e Lincoln (2017) e, Cassell, Cunliffe e Grandy (2017).

Em um momento solo, com o foco unicamente em conformidade legal e regulatória foram realizadas entrevistas. Também foram preparados questionários para distribuição em um momento oportuno após a situação de pandemia declarada pelas Nações Unidas, o que de fato não aconteceu. Nesta etapa, foi possível entender como responsáveis pelos órgãos de tecnologia da informação e da comunicação; de planejamento; de infraestrutura; de educação em ciência da computação, por exemplo, entendiam ou reconheciam fontes legais ou regulatórias, que deveriam ser a pedra angular de suas funções e atividades. Todos eram senhores de muita vivência e profissionais de renome. A experiência foi deverasmente aprazível.

.

Tabela 4: Sumarização dos projetos feitos em colaboração

Estudo	Metodologia	Interesse	Materiais utilizados	Participantes	Condução	Impressões	Conclusões
Projeto 1	Estudo de caso	Conhecer um caso concreto de uma fábrica de *software*	Gravador de áudio, papel e canetas	Dois analistas de requisitos	Entrevistas e material para arqueologia	Dificuldades de diferentes naturezas	Técnicas, artefatos e ferramentas ultrapassados; inexistência de cuidados para com a conformidade legal ou regulatória
Projeto 2	Pesquisa-ação	Oportunidade de apoiar a transformação ágil e a iniciativa dos primeiros passos relacionados aos requisitos legais ou regulatórios	Apresentações, gravadores de áudio e de vídeo, formulários, papel e canetas	Três analistas e um gerente de equipe	Observações, discussões e encaminhamentos	Necessidade de apresentar todas as rotinas e obter uma resposta sobre a corretude ou não dessas	(Alguns exemplos) necessidade de atualização profissional e replicação; melhoramento da comunicação; uso de repositórios para FLR, versionamento de documentação; realização de tratamento para transformação de todos os requisitos em testáveis
Projeto 3	Realização de entrevistas e aplicação de questionários	Conhecer os tratamentos para conformidade legal e regulatória em diferentes contextos de aplicação (de petrolífero a educação) e as necessidades	Apresentações, gravadores de áudios, formulários, papel, canetas	Nove gerentes de equipe e seis desenvolvedores	Entrevistas e questionários	Grande preocupação com o sigilo e a privacidade das informações; pouca ou nenhuma forma de visualização da informação, que necessitavam; falta de conhecimento relacionados à conformidade legal e regulatória	Necessidade de definição de visualizações da informação importantes para as atividades e papéis desempenhados; conhecimento e tratamento para a conformidade legal e regulatória

		de visualização da informação					
Projeto 4	Etnografia organizacional	Conhecer o público-alvo e suas dificuldades; entender as dinâmicas das equipes, e conhecer os diferentes desafios enfrentados com relação à conformidade legal e regulatória	Roteiros, gravador de áudio, termos, papel e canetas	Um gestor de órgão de tecnologia da informação e da comunicação, um diretor de sistema, dois gerentes de equipe e oito analistas de requisitos	Entrevistas com data e horários marcados	Problemas com acesso à informação, diferentes desafios e oportunidades; pouco ou nenhum conhecimento relacionado à conformidade legal e regulatória; ambiente de pouca colaboração e escassez de padronização	Técnicas, artefatos e ferramentas desatualizados ou insuficientes; pouco ou nenhum conhecimento relacionado à conformidade legal e regulatória
Projeto 5	Aplicação de questionário	Entender as dinâmicas em empresas incubadas, e conhecer os diferentes desafios enfrentados com relação à conformidade legal e regulatória	Formulário Web	31 representantes dessas empresas incubadas, mas apenas dois desses representantes conheciam a temática conformidade legal e regulatória	Preenchimento do formulário	Estratégias diferentes para lidar com a conformidade legal e regulatória	Pouco ou nenhum conhecimento relacionado à conformidade legal e regulatória

4.1 Caracterização dos projetos em colaboração

Como havia diversidade nos objetivos das pesquisas, os projetos em colaboração também seguiram a mesma linha. Por questões de privacidade e segurança, nomes e outras informações foram omitidas para garantir aos participantes e aos colaboradores suas identidades e participações o sigilo necessário. Os participantes foram distintos para cada um dos projetos e, consequentemente, houve uma variedade das instituições, onde esses participantes atuavam no mercado. As instituições eram de médio a grande porte, considerando a classificação dada pelo IBGE (2020). Os estudos foram sumarizados na Tabela 4, e descritos na sequência.

O primeiro projeto em colaboração (i) era composto por uma fábrica de *software* e um órgão de controle e fiscalização público. Nessa colaboração, ficou bem nítido que, na fábrica de *software*, embora houvesse recursos humanos e financeiros à época, as metodologias utilizadas não estavam bem impregnadas na equipe, bem implantada e os artefatos não estavam bem definidos ou atualizados. As equipes (uma de cada analista de requisitos) não conversavam, ou trocavam experiências. As equipes desconheciam quase que por completo o que seria um requisito legal ou regulatório. As equipes, normalmente, recebiam como requisito de usuário quase todo e qualquer requisito. Assim como, assuntos relacionados com rastreabilidade ou monitoramento. No órgão de controle e fiscalização público, este setor na hierarquia não tinha uma importância, no momento, talvez adequada, logo a prioridade não era o desenvolvimento de sistema, e sim a rede e sua manutenção. Por outro lado, os profissionais, que lá estavam, tinham mais conhecimento sobre requisitos legais ou regulatórios, e conformidade legal.

No segundo projeto em colaboração (ii), o público era formado por estudantes de Engenharia de Requisitos. Como profissionais em formação o conteúdo da disciplina de Engenharia de Requisitos foi-lhes apresentado no decorrer do curso de forma teoria e prática, até em formato de desafios de engenharia de requisitos, modelagem, documentação e desenvolvimento de um produto. Foi uma experiência interessante, pois foi possível percorrer todo o caminho juntos. Para as aulas práticas, foram sorteados tipos incomuns de organizações, incluídos diferentes desafios (dentre esses requisitos legais ou regulatórios, conformidade legal, rastreabilidade, testes). A responsável por esta pesquisa e outra pesquisadora atuaram como clientes e orientadoras da disciplina. Também, foi realizado um experimento de cunho de modelagem social com esses mesmos estudantes e, surpreendentemente, houve a preocupação com a identificação e manutenção da conformidade legal e regulatória. Todos os estudantes

apresentaram ao término da disciplina todas as fases dos seus projetos e a conclusão, que inclusive dois desses projetos foram implementados por organizações reais.

Enquanto no terceiro projeto em colaboração (iii), o objetivo inicial era um trabalho apenas com gerente de projeto e suas necessidades de visualização da informação para tomada de decisão. Com a evolução da pesquisa foi percebido que os desenvolvedores também tinham necessidades importantes a serem atendidas, e alguns também atuavam como gerente de projeto ou papéis equivalentes frente aos clientes, logo possui necessidades informacionais visuais equivalentes. Os 15 participantes foram convidados a atuarem ativamente. Eram de diferentes organizações públicas e privadas, enfrentando as mais diferentes situações, e utilizando, para isso cada um uma metodologia própria ou uma já consolidada no mercado de desenvolvimento de sistemas computacionais. Apenas dois gerentes e um desenvolvedor tinham conhecimento relacionado à conformidade legal e regulatória e aos requisitos legais ou regulatórios. Havia, por parte de alguns participantes, um receio acima do comum, um medo com o vazamento ou publicidade de algumas informações, que pudesse identificá-los ou suas organizações. Com esta preocupação alguns dados foram até suprimidos para maior segurança ainda desses participantes, e submetidos a suas aprovações. Cabe ainda ressaltar que os segmentos de mercado também eram bem diversificados: de petrolífera a educação, passando por controle e fiscalização do trânsito a alimentação.

No quarto projeto em colaboração (iv), em uma fábrica de *software* de alto desempenho e grande porte, segundo IBGE (2020), é responsável por um total de sete sistemas, que servem a própria comunidade e mais de 50 outras instituições pelo Brasil. Dessa fábrica foram escolhidos dois de seus maiores sistemas, e com isso seus oito analistas de requisitos envolvidos para esse estudo em questão. Particularmente, esta fábrica de *software* recebeu interações em três momentos diferentes, e temporariamente, distantes por cerca de um ano entre cada interação. Na primeira, havia um cenário de construção de que seria importante, e a opção por construir políticas e planos visando a conformidade legal e regulatória, bem como todo o ferramental a ser utilizado. Na segunda interação, muitos artefatos desatualizados ou em desuso, poucos profissionais da área de requisitos - e trabalhando distantes das equipes de desenvolvimento ou de produção, profissionais buscando alternativas para melhorar metodologias e artefatos de trabalhos. Na terceira interação, o ambiente estava mais propício a novas ideias, algumas já inclusive haviam sido sugeridas na interação anterior, o que possibilitou um estudo mais aprofundado dos problemas de possíveis encaminhamentos.

Assim, a opção foi utilizar uma etnografia organizacional, tendo como referências os estudos de Ybema et al. (2009) e Angrosino (2007). Foram feitas observações in loco, coletas

de materiais e entrevistas com *Chief Executive Officer* (CEO), *Chief Technical Officer* (CTO), *Chief Product Officer* (CPO) e, ainda, com os Subdiretores dos dois maiores sistemas e os respectivos analistas de requisitos desses sistemas. Havia, como já dito, mais de 50 clientes distribuídos pelo país desses dois maiores sistemas dessa fábrica de *software*. Existe uma rede de colaboração entre alguns parceiros-clientes dessa fábrica tanto para produção de artefatos documentais como de código de produção/operacional, que se revertem para todo o grupo que assim desejar. Outra cultura bem disseminada na equipe era que os analistas de requisitos eram analistas de negócio, além disso, ocorria a possibilidade de remoção para outros cargos desde que preenchidos os pré-requisitos.

Evidencia-se que os termos, ou até mesmo os conceitos, requisito legal ou regulatório, conformidade legal ou regulatória, evidência legal ou regulatória, auditoria legal ou regulatória eram desconhecidos pelos participantes até o momento do estudo. Isso foi uma surpresa ruim, pois os sistemas em questão estavam impregnados de requisitos legais ou regulatórios. Para os participantes, todavia, a maioria, os via apenas como requisitos do usuário. Outra questão a ser observada, era a dependência dos desenvolvedores e testadores para com os analistas de requisitos para atividades serem realizadas. Mais uma questão que impactava na cadeia produtiva, e poderia ser dramática se apenas algo saísse fora do esperado. Entende-se que foi possível de diferentes formas contribuir com a fábrica de *software* na teoria, na prática e na construção de conceitos ao final do projeto no entender de todos os participantes.

Para o quinto projeto em colaboração (v) com também uma instituição incubadoras de empresas, e foram observadas algumas organizações, que se encontravam em fase de experimentação e inovação empreendedora de negócios para desenvolvimento da economia e de pessoas. Nesse projeto, foi realizada uma seleção/captação de empresas, que estavam pré-incubadas ou incubadas. A partir disso, foi realizado um convite para participação do preenchimento de um questionário. Nesse questionário, as perguntas relacionadas aos requisitos legais ou regulatórios somente eram disponibilizadas quando os participantes respondiam que esse tipo de requisitos em seus sistemas. Havia uma breve explicação do que seria esse tipo de requisito, para aqueles que não estavam familiarizados com o termo. Na sequência, havia nove perguntas sobre a temática.

Inicialmente, foram contatadas 34 organizações, 31 organizações responderam ao questionário, mas apenas duas disseram que tinham em seus sistemas requisitos legais ou regulatórios. Foi interessante observar que cada uma tinha estratégias diferentes para lidar com esses requisitos e sua fonte legal ou regulatória; utilizavam alguma técnica para rastreamento dos requisitos; e em ambos os casos possuíam apoio técnico especializado do corpo técnico da

organização para dirimir dúvidas, conflitos, por exemplo. Fato raro, na maioria das organizações. Quando há algum apoio, é externo ou contratado, assumido, geralmente, somente caráter consultivo.

Houve outras participações importantes para formação, mas em temáticas não relacionadas com esta tese, que não serão relatadas neste texto. A seguir, a narrativa do projeto sobre conformidade legal e regulatória.

4.2 Projeto com foco em conformidade legal e regulatória

As experiências passadas foram importantes para entender como as organizações e pessoas fundamentais para essas organizações compreendiam e tratavam as questões legais e regulatórias dentro e fora dos relacionamentos com clientes, outras organizações, órgãos reguladores, dentre outros. Por outro lado, foi interessante a prática de oferecer a um grupo de estudantes o que há de mais recente em termos de requisitos legais e regulatórios com vistas à conformidade legal e regulatória. Esta vivência trouxe visões de como abordar estas temáticas da melhor forma possível com profissionais do mercado atarefado em muitos afazeres e sem condições em paralelizar com mais uma plausível técnica, metodologia, *framework*, por exemplo. A equipe precisaria entender a necessidade e investir na proposta.

Para iniciar esta nova fase, munida das informações já obtidas nos projetos em colaboração, o primeiro passo foi realizar um estudo de caso e uma pesquisa-ação com uma equipe reduzida, para testar uma primeira abordagem e os conceitos construídos. Desse modo, levando em consideração os artefatos e ferramental já utilizados pela equipe, propôs-se algumas modificações, como, por exemplo: o uso de um sistema para gerenciamento de projetos, com vistas a gerenciar os artefatos; o emprego de controle de versionamento da documentação; a adoção de padrões para artefatos produzidos.

No momento seguinte, precisava-se expandir a visibilidade e entender as necessidades do público-alvo da pesquisa. Assim, entrevistaram-se os participantes que tiveram como perfis os de direção, de gestão, de planejamento, de engenheiros/analistas de requisitos ou auditores, sendo que o foco final do seu trabalho precisava ser o de planejar, manter ou auditar a conformidade legal e regulatória dos sistemas computacionais, dos quais fossem responsáveis naquele momento de sua participação. Para isto, foram entrevistados um auditor, quatro desenvolvedores, dez analistas de requisitos, cinco gestores (*Chief Product Officer* - CPO), dois

diretores (sendo um *Chief Technical Officer* - CTO, e um *Chief Information Officer* - CIO), e até mesmo dois diretores executivos (*Chief Executive Officer* - CEO).

4.2.1 Estudo de caso e pesquisa-ação

Seguindo as metodologias de Yin (2017) e RUNESON et al. (2012) buscou-se realizar um estudo de caso exploratório parte com a participação de outras duas pesquisadoras, além de dois analistas de requisitos de uma fábrica de *software*, que se encontravam em um momento de oportunidade de crescimento na profissão a partir dos resultados dos estudos, que estavam empreendendo. Desse modo, as pesquisadoras foram convidadas a contribuir de forma *ad hoc*.

Nos primeiros encontros, foram solicitados todos os materiais e acesso para visualização das propostas a serem implementadas pelos analistas. Ambos estavam bastante empolgados com as possibilidades de promover mudanças e, com isso, melhorias, pois sabiam que seus artefatos e ferramentas já estavam ultrapassados. Isto pode ser observado na entrevista realizada e nas primeiras observações de campo realizadas. Foram coletados alguns exemplos de artefatos para estudos e proposta de melhorias.

Com o material coletado, análise da entrevista, foi observado que para esses profissionais havia grande dificuldade de diferenciar requisitos do usuário, do negócio, e legais e regulatórios, por conta da forma como era obtida a informação. Os requisitos, em sua maioria, eram tratados como de usuários. Não se sabia a fonte, na maioria das vezes. Nos encontros seguintes, com análise das evidências, novas entrevistas e observações de campo, algumas triangulações puderam ser feitas, o que culminou em algumas propostas para os analistas de requisitos.

Em uma fase posterior, após planejamento, foi implementada a fase de pesquisa-ação (WHITEHEAD e MCNIFF, 2000; MCNIFF e WHITEHEAD, 2006). A intenção foi, além de apoiar a iniciativa de ambos, também transformar um problema operacional em solução institucional. Para exemplificar orientações encaminhadas:

i) atualização profissional e replicação aos outros profissionais de forma colaborativa e periódica;

ii) definição de alguns canais de comunicação formais;

iii) uso de repositório para documentação, fontes legais e regulatórias, além dos códigos-fonte e testes;

iv) versionamento de documentação;

v) versionamento dos requisitos;

vi) tratamento para transformação dos requisitos não funcionais em testáveis;

vii) melhor refinamento das histórias dos usuários;

viii) rastreamento dos artefatos via ferramental já disponível, bastando ajustar as configurações;

ix) inclusão de uma seção para requisitos legais e regulatórios (instituição totalmente fundamentada em fontes legais e regulatórias);

x) definição dos meios de priorização dos requisitos para as sprints;

xi) melhor dimensionamento das *sprints*; e

xii) visualização das informações dos projetos das equipes.

4.2.2 Entrevistas

A escolha foi aproveitar todas as oportunidades oferecidas pelos respondentes dentro de sua exígua agenda, além de oportunidades dentro do projeto de outros pesquisadores do grupo de pesquisa do Laboratório de Especificação e Testes de Software (LETS). Havia roteiros com perguntas abertas e perguntas fechadas, roteiros apenas delineadores da entrevista (Apêndice A). Nestes roteiros, eram abordados assuntos mais diversos como rotinas, estratégias, preocupações, principais órgãos fiscalizadores, dificuldades, projetos futuros, auditorias internas e externas. Outra questão importante a ser destacada foi que alguns respondentes tiveram suas entrevistas interrompidas muitas vezes ou remarcadas, até feitas em diferentes momentos, pois a opção também foi observar a sua rotina de trabalho.

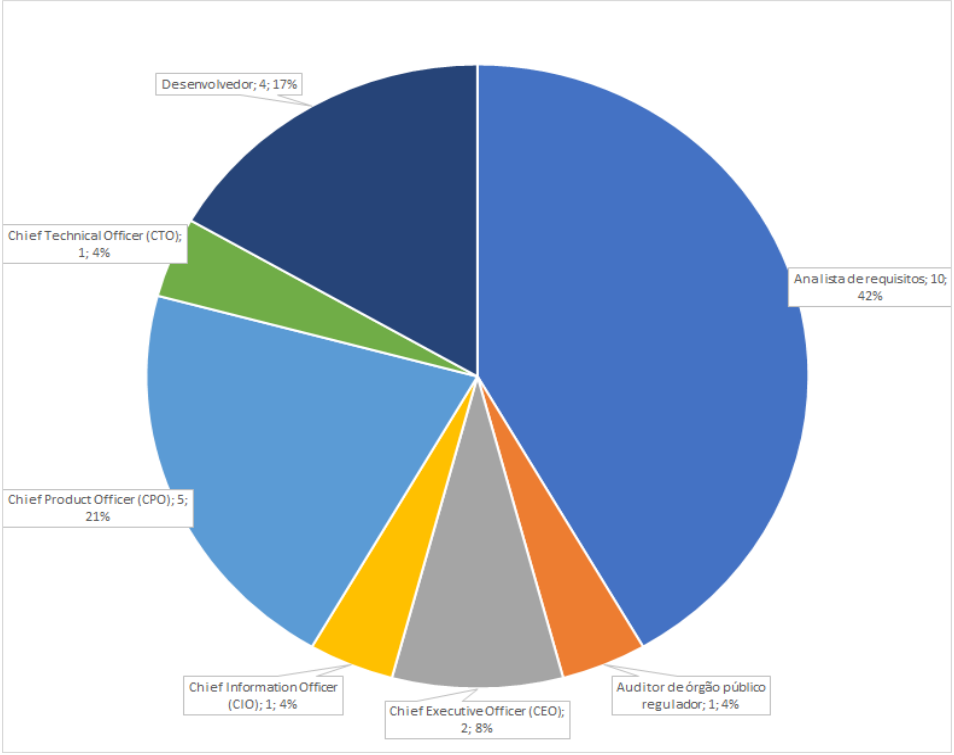
Ao seu modo, todas as entrevistas seguiram um roteiro de perguntas abertas, para que fosse aproveitado todo e qualquer espaço de interação ou atravessamento durante a entrevista. Acredita-se que o meio não foi perturbado, e sim enriquecido com tais decisões. A todos os respondentes foram explicadas e esclarecidas a pesquisa, que estava sendo realizada, e solicitadas tanto a assinatura do termo de “Termo de Consentimento Livre e Esclarecido - TCLE” (Apêndice A.2) e a autorização nos “Termo de Cessão de Direitos para Uso de Imagem e Voz” (Apêndice A.3) a gravação em áudio, que foram realizadas durante cada interação.

4.2.2.1 Caracterização dos participantes

Foram feitos vários convites, entretanto por diferentes motivos participaram desta fase da pesquisa exploratória 24 pessoas, sendo: um auditor, quatro desenvolvedores, dez analistas de requisitos, cinco gestores (*Chief Product Officer* - CPO), dois diretores (sendo um *Chief*

Technical Officer - CTO, e um *Chief Information Officer* - CIO), e até mesmo dois diretores executivos (*Chief Executive Officer* - CEO). O fato de os perfis serem variados ampliou o horizonte com relação às necessidades e desafios enfrentados pelos profissionais da Computação, quando se trata de manter a conformidade legal e regulatória de um sistema computacional em todo seu ciclo de vida. A Figura 11 apresenta o perfil dos participantes das entrevistas, sendo que primeiro é informado o nome do perfil, depois a quantidade de participantes e, por último, a sua porcentagem com relação ao todo.

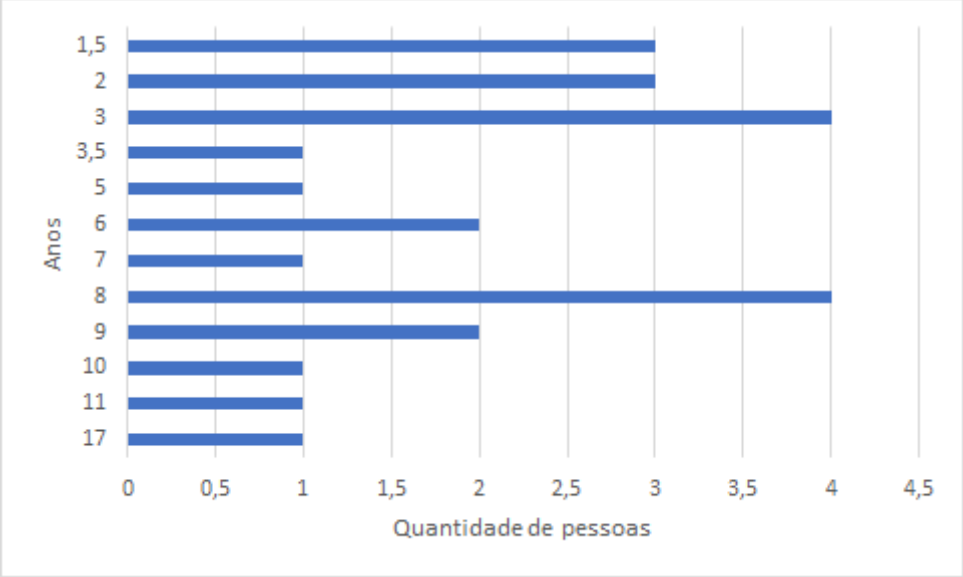
Figura 11: Gráfico do perfil dos participantes das entrevistas.



Fonte: a autora.

Todos os participantes mostraram-se interessados na temática da pesquisa, embora alguns a desconhecessem. A faixa etária variou de 24 a 49 anos, e a experiência de um ano e seis meses a 17 anos de profissão na Computação (Figura 12). Várias dessas pessoas já tiveram outras experiências na Computação, além da função/cargo que ocupam agora, o que pode ter enriquecido sua visão e competências. Todavia, senão corridos, podem perpetrar maus hábitos. Algumas dessas pessoas trabalhavam juntas, mas outras trabalhavam em instituições e Estados diferentes.

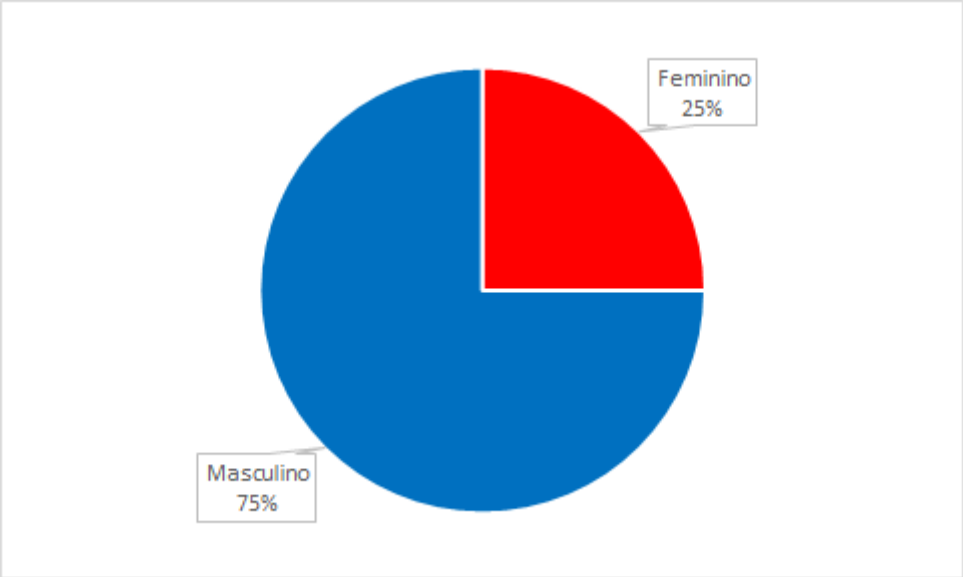
Figura 12: Gráfico apresentando o tempo de experiência no cargo dos respondentes.



Fonte: a autora.

Nesse pequeno universo, apenas seis pessoas são do sexo feminino, enquanto outras 18 são do sexo masculino (Figura 13). A Tabela 5 demonstra o que foi escrito.

Figura 13: Gráfico da distribuição dos respondentes por sexo.



Fonte: a autora.

Tabela 5: Caracterização dos participantes das entrevistas.

Cargo	**Tempo de experiência**	**Idade**	**Sexo**
Auditor de órgão público regulador	08 anos	40	M
Analista de requisitos	08 anos	36	M
Analista de requisitos	08 anos	38	M
Analista de requisitos	01 ano e 06 meses	24	F
Analista de requisitos	08 anos	36	M
Analista de requisitos	09 anos	41	M
Analista de requisitos	01 ano e 06 meses	27	M
Analista de requisitos	03 anos	33	M
Analista de requisitos	10 anos	37	M
Analista de requisitos	09 anos	36	F
Analista de requisitos	01 ano e 06 meses	28	M
Chief Product Officer (CPO)	17 anos	49	M
Chief Product Officer (CPO)	07 anos	37	M
Chief Product Officer (CPO)	06 anos	45	M
Chief Product Officer (CPO)	11 anos	36	F
Chief Product Officer (CPO)	02 anos	40	M
Chief Technical Officer (CTO)	02 anos	36	F
Chief Information Officer (CIO)	03 anos	46	M
Chief Executive Officer (CEO)	06 anos	48	F
Chief Executive Officer (CEO)	02 anos	43	M
Desenvolvedor	05 anos	25	M
Desenvolvedor	03 anos e 06 meses	29	F

Desenvolvedor	03 anos	28	M
Desenvolvedor	03 anos	28	M

4.2.2.2 Caracterização dos artefatos utilizados

Os convidados à participação receberam um *e-mail* com um convite, onde havia uma breve explicação do que consistia a pesquisa, e solicitando, caso concordassem em participar, escolhessem um local, um dia e um horário mais convenientes para si ou escolhessem dentre algumas opções oferecidas, na mensagem enviada. Foi preparado um *kit* para cada entrevista contendo: um roteiro específico para cada entrevistado, um gravador, uma apresentação da pesquisa impressa, um guia de termos, quatro vias do Termo de Consentimento Livre e Esclarecido (TCLE), quatro vias do Termo de Cessão e Uso de Imagem, Áudio e Vídeo (TCUIAV), folhas avulsas, canetas, lapiseiras e borracha. Os artefatos utilizados encontram-se representados no Apêndice A.

Para as entrevistas, foram feitos os cumprimentos iniciais, uma apresentação, e uma explicação mais detalhada dos objetivos da pesquisa. Na sequência, foram explicados o Termo de Consentimento Livre e Esclarecido e Termo de Cessão e Uso de Imagem, Áudio e Vídeo, e solicitado seus preenchimentos e assinaturas. Outro passo, foi o pedido de permissão de gravação do áudio da entrevista. Com o consentimento verbalizado, ligou-se o gravador, e foi repetida a pergunta, para que ficasse gravado o consentimento também. Assim, iniciou-se todas as entrevistas.

Havia sempre um roteiro previamente planejado para facilitar o encaminhamento, todavia a intenção era sempre que o entrevistado falasse naturalmente sobre sua rotina, dificuldades, procedimentos, decisões, desafios enfrentados no cotidiano, como os superou, dentre outros assuntos. Observou-se que as temáticas conformidade, legalidade, auditoria, fiscalização como outras de mesma categoria não surgiam naturalmente na conversa. Precisaram sempre ser introduzidas por perguntas, o que fez o roteiro ser muito útil por estar contextualizado a cada cargo ocupado por aquele que iria ser entrevistado.

4.2.3 Caracterização dos desafios e oportunidades

Os participantes de mais alto nível na cadeia como, por exemplo, os *CEO* e *CIO* conheciam as suas obrigações e responsabilidades por se interessarem pela temática, pela força

da lei, pela experiência própria ou alheia de ter sofrido alguma sanção ou ter sido oferecido um prazo para o ajuste, terem feito alguma atualização institucional. Entretanto, essas mesmas pessoas relataram a dificuldade de conscientização da comunidade onde estavam inseridas, seja por falta de recursos financeiros, humanos e, até mesmo, por desinteresse das pessoas. Foi relatado que a comunidade não conhecia os serviços dos órgãos como um todo, apenas uma pequena parte, que se restringia o acesso à internet, sistemas corporativos e *e-mails*.

O investimento na área sempre dependia de quem assumisse a cadeira principal, e visse a área como um custo ou um investimento. Nos últimos anos, têm sido anos bons, pois as subáreas estavam mais integradas para esses entrevistados, e com as políticas e planos estabelecidos, as metas foram alcançadas em quase sua totalidade. Entretanto, ainda não havia conformidade legal e regulatória. Uma queixa geral foi o volume de leis e de alterações ocorridas em curtos períodos temporais.

Foi dito que o serviço público tem perdido muitos profissionais para o mercado privado, por conta de diferentes atrativos como melhores salários, flexibilidade de horário e de local de trabalho, mudança de país, dentre outros benefícios. Enquanto, quem trabalhava no mercado privado, reclamava do ritmo frenético dos acontecimentos e das exigências impostas, mas não tinha do que reclamar com relação ao financeiro e ao ambiente de trabalho. Nesta situação, havia alguns desenvolvedores e gestores. Estes poucos sabiam de fontes legais ou regulatórias; conheciam um pouco de conformidade legal e regulatória por conta de algum sistema crítico, que tinha exigido.

Os participantes com cargo de gestão estavam encontrando dificuldades, mas estavam vendo como oportunidades, a busca, por exemplo, de: ferramentas de gestão e gerenciamento; treinamentos para suas equipes (no estilo um faz a capacitação em algo e replica para os outros); participação em eventos da área; criação de comitês nas instituições para retirar de dentro dos órgãos de Computação a decisão maior (o objetivo é ter uma cadeira); padronizações; versionamentos; algumas iniciativas para melhorar a visão da comunidade e captar ajuda com a promoção de eventos do tipo *Hackathons*, *Hackday* para buscar soluções, pessoas interessadas.

Quando o assunto foi conformidade legal e regulatória, fontes legais ou regulatórias e requisitos legais ou regulatórios, os gestores disseram que cumpriam as solicitações, mas não conseguiam rastrear as mudanças totalmente. O ferramental disponível não ajudava. Dois deles estavam implantando novo ferramental, inclusive com visualizações da informação para facilitar este processo, mas ainda não podiam responder por isto. As evidências legais que

tinham eram sempre o código e o encaminhamento da solicitação da alteração feita pelo órgão de origem.

Para os analistas de requisitos, exceto um, e para os desenvolvedores, os requisitos legais ou regulatórios eram desconhecidos. Esse tipo de requisito era, normalmente, tratado como requisito de usuário, visto que vinha por solicitação de um usuário ou um órgão específico. Até a documentação, a sinalização ou sua priorização no desenvolvimento no sistema era feita como um simples requisito de usuário. Para esse analista de requisito, que tinha maiores informações, na apuração dos motivos, soubesse que já havia algum tempo de experiência (nove anos) e sua formação foi específica para área de Engenharia de Requisitos, fato não comum para os outros analistas.

Com relação ao auditor de órgão público regulador, este explicou que atuava a partir de denúncias ou a partir de relatórios de inteligência, e que era impressionante o despreparo dos órgãos, que são fiscalizados por sua instituição. Quando há inconformidade, a instituição precisava fazer um plano de ação explicando como resolveria o problema encontrado dentro do prazo estipulado. Assim, haveria nova fiscalização ou verificação, e se for constatado o mesmo problema, seria aplicado uma sanção. As equipes eram sempre multidisciplinares, mesmo quando o problema era de inconformidade na área de tecnologia da informação e da comunicação. Ao final, percebeu-se que não existe nenhuma abordagem usada para tratar os requisitos legais e regulatórios e nenhuma forma de acompanhar a conformidade.

4.3 Discussões e considerações

Foi muito comum encontrar quem não soubesse nada sobre conformidade, fonte ou requisitos legais ou regulatórios. Havia aqueles que se arriscavam a dizer que era algo ligado às leis, sem muita certeza. Quem mais conhecia estava em posições executivas, e não operacionais. Isto pode ser um problema a longo prazo, pois os que precisam lidar, tratar e gerenciar os requisitos e as fontes legais ou regulatórios estavam agindo em total imperícia, e podendo estar provocando sem saber a inconformidade legal e regulatória nos sistemas, em que eram responsáveis.

Logicamente, não é apenas o tipo de requisito que muda, e sim a forma de ver, tratar, gerenciá-lo, visto que, normalmente, o tempo é curto e os recursos humanos e financeiros mais

escassos ainda. Este tipo de requisito precisa de um tratamento especial desde o início, pois o tratamento a posteriori é cada vez mais custoso. Evidências de sua implementação precisam existir, qualquer alteração que envolva algum requisito deste tipo precisa ser bem estudada, e passar pelo comitê de controle e de mudanças. Assim, novos testes devem ser feitos para verificação de não ter havido a inconformidade legal e regulatória tão indesejada.

Sabe-se que existem problemas muitos mais antigos na Engenharia de Requisitos e na Engenharia de Software, por outro lado este é um problema tão antigo quanto, todavia ainda desconhecido por muitos desavisados profissionais de longa data da Computação. Logo, em posse dos resultados obtidos com a revisão sistemática da literatura (Capítulo 3) e com estes resultados das pesquisas exploratórias realizadas pretende-se promover uma solução que ajude a mitigar as dificuldades encontradas nestes estudos apresentados.

No próximo Capítulo, é apresentada a solução construída a partir da revisão sistemática da literatura e das investigações realizadas junto ao mercado, que poderá se beneficiado dos resultados obtidos.

5 Framework

A necessidade de construção ou evolução de um sistema computacional pode ter diferentes motivações. Seja qual for essa motivação, delimitar as fronteiras de um sistema, de seu domínio e de seu contexto são fundamentais sempre. Isto dá-se tanto no âmbito da Engenharia de Requisitos, mas também é preciso assim fazê-lo no que tange aos aspectos legais desse sistema computacional. Conhecer o domínio e o contexto do sistema pode ser um exercício de antecipação e imaginação.

Assim, é necessário associar a experiência, a criatividade, o envolvimento, o emprego de, talvez, diferentes técnicas para melhor entendimento da necessidade, do desejo, das possibilidades e das limitações de um sistema computacional. Isso está resumido, mas nessa fase o importante é a definição dos limites. Ao serem estabelecidos esses limites, onde haverá partes interessadas, sistemas em operação, processos (de negócio, técnicos, pessoas e papéis, estruturas organizacionais e componentes da infraestrutura de TI), eventos, interfaces, segundo Pohl (2010).

Uma solução possível faz parte desta pesquisa, mas não extingue o problema. Dessa forma, como preconizado por Leshem e Trafford (2007), uma resposta básica é apresentada em forma de *framework* conceitual para a conformidade legal e regulatória (*regulatory and legal compliance*) dos sistemas computacionais em todo seu ciclo de vida - desenvolvimento, manutenção ou evolução. Isto posto, deverá acontecer, independentemente, da metodologia de desenvolvimento, mesmo o *framework* tendo sido instanciado em metodologias ágeis, inicialmente. A intenção é facilitar toda existência do ciclo de vida do sistema computacional e das possíveis auditorias de tecnologia da informação, as que venham tal sistema ser submetido, visto que o mesmo deve prover informações para tal.

5.1 Solução Proposta

Considerando o estado da arte e a indústria na Engenharia de Software e na Engenharia de Requisitos, foi criado por esta pesquisa um *framework*, que preenchesse uma lacuna entre artefatos, processos e modelos já existentes à conformidade legal e regulatória dos sistemas computacionais. Independentemente da metodologia de desenvolvimento escolhida, o *framework* poderá ser utilizado dada a sua flexibilidade de adequação ao processo de

desenvolvimento em si. Assim sendo, o processo não será representado, e sim os elementos essenciais para o adequado funcionamento do *framework*.

É de entendimento da pesquisadora que os processos de Engenharia de Requisitos devem ser promovidos com pequenas alterações, como a construção e manutenção de um modelo de rastreabilidade de artefatos e outro para requisitos, que apresente um destaque maior para os relacionamentos com os requisitos legais ou regulatórios; em existindo um documento de descrição de caso de uso, haja uma seção de "Requisitos Legais ou Regulatórios", sejam incluídos identificadores de origem e do requisito em si, por exemplo. Declaração em contrato de definições de termos, de papéis e de responsabilidades, as formas de comunicação, dentre outros itens tão valorosos, deve ser feita para o processo de desenvolvimento de *software* ser mais eficaz e eficiente. Vislumbra-se que balizando as relações de forma mais concreta e contratual, a gestão dessas relações torna-se mais fácil, todavia os mecanismos para definição dessa gestão não devem esquecer os dispositivos que as fontes legais e regulatórias determinam.

Em se tratando do uso de metodologias ágeis, há algumas preocupações, mas de forma alguma impedimentos. A primeira preocupação tange a atividade de Elicitação (RIFAUT, 2011), seja qual for a forma escolhida para tal propósito, a orientação é seguir sempre o modelo de rastreamento de artefatos e de requisitos instituído, explorar e refinar os requisitos legais ou regulatórios ao ponto de esses serem testáveis, como demonstrado, no Capítulo 2, Figura 2.2. Assim, a atividade de Documentação será provavelmente mais simples, entretanto exigirá cuidados como a criação e a manutenção de endereçamento entre esses artefatos e requisitos. Dessa forma, o objetivo é que haja sempre a identificação rápida, precisa e relevante dos impactos das modificações porventura a serem feitas nas outras atividades como Validação e Negociação, e Gerenciamento. Essas quatro atividades centrais são postas por Pohl (POHL, 2010). Anteriormente, Kotonya e Sommerville (1998) dividiram as atividades em Elicitação, Análise e Negociação, Documentação e Validação, o que não interfere na governança essencial dessas atividades utilizando o *Framework* proposto.

Ainda, sobre as metodologias ágeis, o processo de engenharia de requisitos também pode ser adaptativo, iterativo e incremental como proposto por Leffingwell (LEFFINGWELL, 2011). Neste ponto, a orientação, além das orientações anteriores, é utilizar o máximo possível de visualizações das informações (algumas ferramentas podem ajudar nisso), seguindo o que preconiza Schneiderman - "Overview first, zoom and filter, then details-on-demand" (SHNEIDERMAN, 1996). Sempre que viável sugere-se explorar/desenvolver o requisito legal ou regulatório refinando, suficientemente, para ser este ser desenvolvido em uma única *sprint*

- “foco no trabalho individual, tempo para criar um protótipo e um prazo impreterível” - definição dos autores do termo (KNAPP, ZERATSKY e KOWITZ, 2016).

5.2 A transformação de uma fonte legal ou regulatória em requisito legal ou regulatório

O exemplo do uso das histórias de usuário (*user stories*) é interessante, pois permite o refinamento, além do rastreamento. Desse modo, identifica-se a história do usuário, verifica-se as leis associadas, cria-se um requisito legal ou regulatório, e o refina até o ponto deste ser testável e implementável. Quando necessário, divide-se o requisito em diferentes requisitos ou até atividades, nunca esquecendo de antes priorizá-lo. Dessa forma, para uma história de usuário (Tabela 6), onde o usuário diz que deseja fazer um acesso no sistema de forma segura, podem-se haver os seguintes desdobramentos:

Tabela 6: Exemplo de história de usuário com requisito legal.

ID: HU00078
“Não quero que meus dados de compras sejam disponibilizados a terceiros.”
[Observações]

Fonte: a autora.

Chegou o momento de reunir todas as informações relevantes, o que significa neste momento, objetivos e infraestrutura do sistema computacional, regulamentos da instituição, interessados no sistema e toda e qualquer fonte legal ou regulatória, que verse sobre o domínio e contexto do requisito em questão devem ser reunidos. Neste exemplo, pensando que a instituição é de capital nacional fechado, e obrigatoriamente deve atender as ISO/IEC 18044:2004 (gestão de incidentes de segurança da informação), 27001:2013 (procedimentos e recomendações sobre Sistemas de Gestão de Segurança da Informação), 27002:2015 (Código de Práticas para Gestão da Segurança da Informação); ISO/DIS 31000:2017 (Gestão de Risco); ABNT ISO/IEC 15999:2008 (Gestão de Continuidade de Negócios), 20000:2011 (Gerenciamento de Serviços a legislação), legislação pátria, como a Constituição Federal de 1988, os Códigos Civil e Penal, e demais leis, atualmente, em vigor. Como o comércio e o

comércio eletrônico podem ser entendidos como algo muito antigo, espera-se também sua autorregulação. Desse modo, instituições, que tenham sistemas computacionais, precisam oferecer políticas de privacidade e de segurança, além de um termo de serviços.

Pela história de usuário está sendo solicitado algo que, a princípio, pode até infringir a lei se os dados forem de obrigação do provedor do serviço armazenar. Entretanto, estas questões podem ser tratadas e esclarecidas na política de privacidade e de segurança, e no termo de serviços e, para caso o usuário não concorde com as políticas ou os termos, o serviço não poderá ser prestado. A lei tem sempre maior precedência a qualquer requisito de usuário uma vez que a lei não é facultativa!

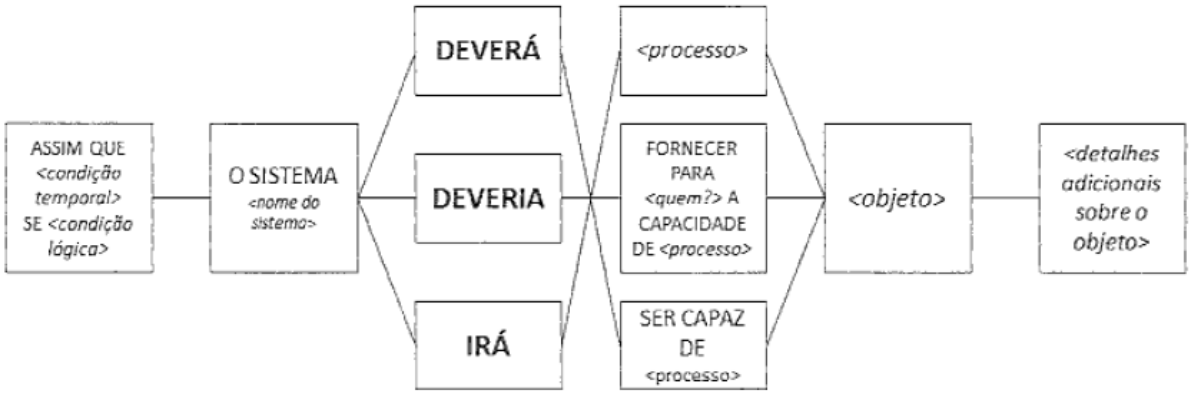
No contexto da história do usuário, há as palavras: dados, compra, disponibilizados, terceiros. A primeira fonte legal ou regulatória a ser consultada é a Constituição Federal, depois o Código Civil. Contudo, sem mencionar fontes específicas de cada Estado ou município, quando se trata da relação consumidor e provedor de serviços ou comércio (eletrônico ou convencional), atualmente, um conjunto interessante de fontes a serem observados que são Código de Defesa do Consumidor, Lei do e-Commerce, Marco Civil da Internet, Lei Geral de Proteção de Dados Pessoais - LGPD. Há várias situações já tratadas neste conjunto de fontes legais. Observe que os passos a seguir podem auxiliar na construção dos requisitos:

1. Verifique a viabilidade da história do usuário;
2. Identifique as palavras-chave;
3. Esteja ciente do domínio/contexto do sistema computacional;
4. Lembre-se que todo serviço ou produto traz consigo uma política de privacidade e de segurança, além de termos de serviços previamente construídos pela instituição;
5. Busque por fontes legais ou regulatórias de forma hierárquica legal e regulatória. A Constituição, o Código Civil e o Código Penal são a base das fontes legais ou regulatórias de qualquer relação no Brasil;
6. Identifique o artigo, inciso ou parágrafo específico, que trata o caso detalhadamente;
7. Defina ou formalize o requisito propriamente dito;
8. Refine o requisito o quanto for necessário até que o mesmo seja testável.

Existe também um *template* (Figura 14), que pode ajudar para criação de requisitos completos, com especificações de condições lógicas e temporais de Pohl (2010), que pode ser

utilizado com exemplo, onde o analista/engenheiro de requisitos faz as adaptações necessárias à situação enfrentada (KIYAVITSKAYA, KRAUSOVÁ e ZANNONE, 2008).

Figura 14: O *template* de requisitos completos, com especificações de condições temporais e lógicas.



Fonte: Pohl (2010).

O Apêndice B apresenta um *template* dos atributos, que um requisito legal ou regulatório pode possuir de forma a atender as demandas por refinamento, ser testável e rastreável. Além disso, foi incluído no Apêndice C exemplos da transformação de uma história de usuário em requisito legal ou regulatório e o refinamento (ou a derivação) de requisito legal ou regulatório.

Ressalta-se que, nos exemplos postos no Apêndice C, mesmo o usuário solicitando algo, que foi retratado pela história de usuário, isto era contraditório à lei, logo não pode ser atendido. Não importa, a lei sempre prevalece, e tem maior prioridade. Esta história de usuário gerou, a título de exemplo, três requisitos legais ou regulatórios. Os requisitos têm seus identificadores e suas origens bem definidas em seus cabeçalhos.

5.3 Componentes do *Framework*

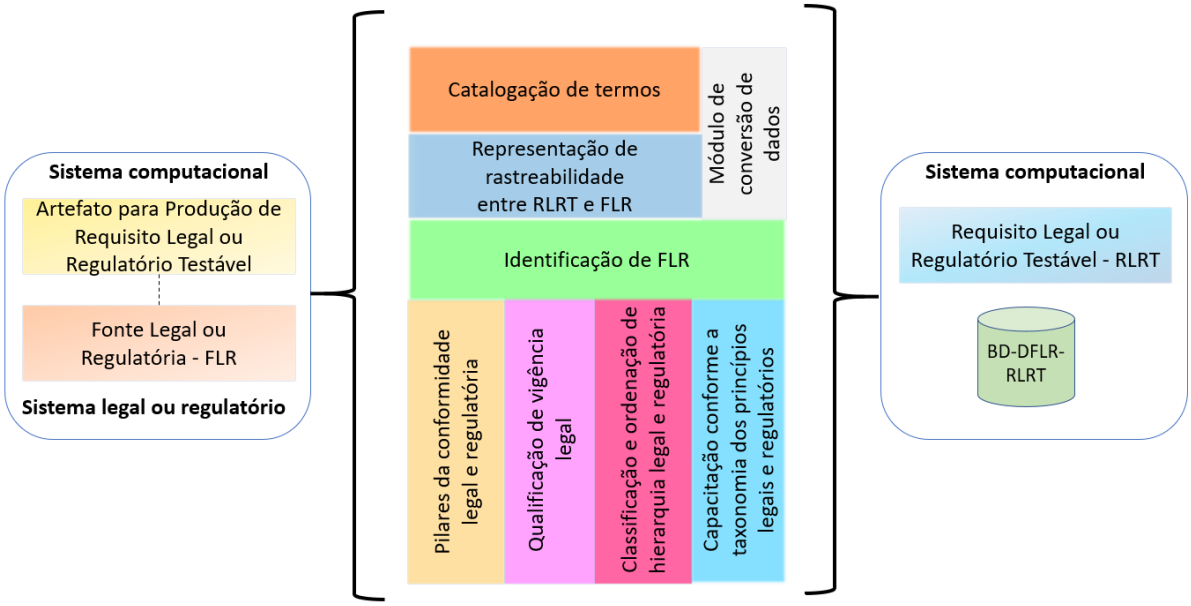
O *Framework* é composto por diferentes elementos, cuja intenção foi tratar uma problemática apresentada no decorrer desta pesquisa. Esses elementos não são opcionais para o correto funcionamento do *framework*, mas existe certa flexibilidade na forma de sua implementação considerando que o crescimento é progressivo e proporcional aos projetos de sistemas computacionais abarcados pelas organizações. As entradas são os requisitos legais ou

regulatórios (vinda do sistema computacional) e as fontes legais ou regulatórias (sistema legal ou regulatório, que o sistema computacional está inserido). Há um repositório não representado, que apoia versionamento, divisões, diferentes sistemas, se assim for conveniente.

Nesta versão, que teve sua atualização mais recente após avaliação junto ao público-alvo, são oito elementos que compõem o *Framework*, como podem ser vistos na Figura 15. Esses elementos podem ser observados sob três perspectivas: **conceitual, interativa e computacional**. Dessa forma, seriam considerados conceituais os elementos (i) Pilares da Conformidade Legal e Regulatória; (ii) Qualificação de Vigência Legal; (iii) Capacitação conforme a Taxonomia dos Princípios Legais e Regulatórios; (iv) Classificação e Ordenação de hierarquia legal e regulatória. Os elementos interativos seriam (v) Identificação de Fontes Legais ou Regulatórias (FLR); vi) Representação de Rastreabilidade entre Requisitos Legais ou Regulatórios Testáveis (RLRT) e Fontes Legais ou Regulatórias (FLR); e vii) Catalogação de Termos. Enquanto o elemento (viii) Módulo de Conversão de Dados seria elemento computacional

Este *Framework*, que tem como objetivo gerenciar a conformidade legal e regulatória, foi construído para funcionar independentemente do tipo de sistema computacional e, também, apoiar mais de um sistema, bem como suas características permitem o reuso e customização de seus componentes. Nas próximas seções cada elemento do *Framework* será apresentado separadamente.

Figura 15: Visão Geral do *Framework*.



Fonte: a autora.

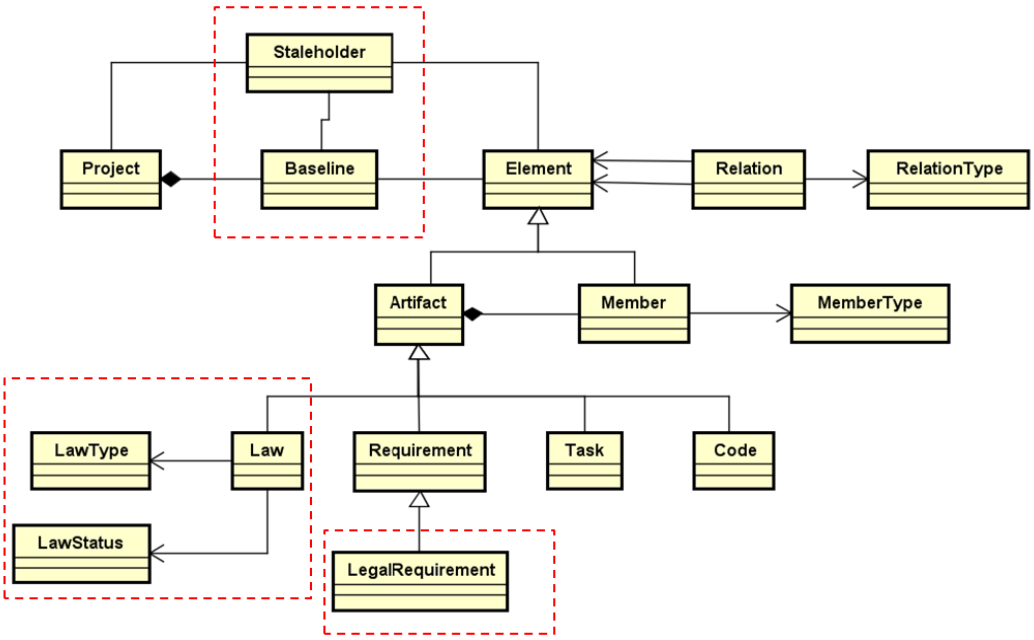
5.3.1 Pilares da conformidade legal e regulatória

Entende-se que fundamentando a conformidade legal e regulatória em alguns pilares esta obrigação torna-se menos complexa, e mais prática. Esses pilares evidenciam a necessidade da instituição preparar-se para estar em conformidade legal e regulatória, antes mesmo que venha a estar à frente de projetos de sistemas computacionais. Dessa forma, podem ser destacados como pilares estruturantes para melhor apoiar o *Framework* os descritos a seguir:

I. Documentação, planos, políticas publicizados – sugere-se que a construção desses documentos aconteça de forma colaborativa ou cooperativa, pois é senso comum que o engajamento dos envolvidos passe a ser maior. Por outro lado, a divulgação, o treinamento, e o que for necessário para entendimento de todos dos documentos, planos e políticas estabelecidos devem ser feitos;
II. Comunicação – deve dar-se de diferentes formas e formatos - o objetivo alcançar e atender às necessidades de todos os interessados (*stakeholders*) do sistema computacional em si;
III. Governança – é preciso haver regras bem estabelecidas e tidas como obrigação pelas partes envolvidas (VARJU e CZINA, 2019), e que podem estabelecer forma de priorização e atualização das fontes legais ou regulatórias, assim como dos artefatos gerados;
IV. Evidências legais – há a necessidade de toda e qualquer informação classificada estrategicamente, mesmo que sejam provas não eletrônicas devem fazer parte do rol do ciclo de vida do sistema computacional em questão;
V. Uso de ferramentas tecnológicas em todos os níveis de operação, quando possível – para obter, analisar, preservar, apresentar as informações, por exemplo. Isto pode criar facilidades no manuseio das informações;
VI. Monitoração dos artefatos, senão de todos, mas dos definidos estrategicamente como os mais importantes pela instituição – isto pode indicar alterações na estrutura e nos artefatos fundamentais para manutenção da conformidade legal e regulatória;
VII. Rastreamento dos artefatos – isto permitirá identificar os relacionamentos entre os artefatos, que estão se relacionando. Quando necessário, dentre outros benefícios, auxilia a verificar o impacto de possíveis mudanças; o reuso de

artefatos em outros projetos; facilita a identificação de responsabilidades; simplifica a manutenção do sistema computacional (POHL, 2010). Para fins de modelo rastreabilidade, a Figura 16 ilustra o modelo, que foi utilizado e implementado em 2017 (SANTOS, MIRANDA e LUCENA, 2017).

Figura 16: Modelo de rastreabilidade para requisitos legais.



Fonte: SANTOS, MIRANDA e LUCENA, 2017.

VIII. Priorização de requisitos – não é uma tarefa simples. Em se tratando de requisitos legais ou regulatórios, esta atividade torna-se um pouco mais complexa, visto que, normalmente, este tipo de requisito tem maior precedência do que os outros por conta do seu custo de não implementação, seu risco, sua importância. Entretanto, outros critérios – como, por exemplo, data que a fonte entrará em vigor, penalidades, custos de implementação – podem ser considerados, sem esquecer que os requisitos legais ou regulatórios são mandatórios.

IX. Visualização da informação – a equipe ganha agilidade, quando a informação é gráfica ao invés de textual. No entanto, cada membro/papel desempenhado por uma pessoa da equipe precisará de visualizações específicas. É recomendado um

estudo para melhor adequação, como seleção, ocultação ou combinação de elementos a serem exibidos (SPENCER, 2014).

X. Controle de configuração e de mudanças – deve ser feito por um comitê, e não por uma única pessoa. Este comitê necessita ser formado, anteriormente, com a intenção de promover o gerenciamento de configuração e mudanças de requisitos. Os pedidos precisam ser justificados e embasados, com análise de impacto e prioridade, pois podem ser estruturantes e alterarem drasticamente a arquitetura e a conformidade legal e regulatória do sistema computacional.

XI. Preservação dos artefatos, da arquitetura, das estruturas e de suas cópias – em um mundo aparentemente com recursos infinitos, há que se pensar, todavia que a finitude é dada pelo seu custo financeiro, tempo ou espaço; pelo menos um desse será seu abalizador. O objetivo é a recuperação do sistema computacional em caso de falhas severas ou não, mas também preservação histórica;

XII. Curadoria em diferentes níveis – deve ser empregada, por exemplo: a) documentação, planos, políticas; b) evidências legais; c) artefatos, arquitetura e estruturas. A intenção de uso, reuso, transformação, preservação, armazenamento, dentre outras atividades do ciclo de curadoria.

5.3.2 Qualificação de Vigência Legal

O elemento **Qualificação da Vigência Legal** trata dos diferentes *status* que uma fonte legal ou regulatória pode possuir. Isto é relevante, para que determinado *status* possa se determinar ou planejar ações perante a vigência de uma fonte legal ou regulatória. Assim, um requisito pode ter sua prioridade alterada ou, ainda, entrar para lista dos requisitos que precisarão ser mudados ou removidos pelo Comitê de Configuração e Mudanças por conta de seu novo *status*. Recentemente, por exemplo, a Lei de LGPD mudou de nome, de número, e por diversas vezes mudou de vigência, o que deixou a sociedade e o mundo dos negócios um tanto quanto despreparados para mudanças, que há muito já estavam previstas.

Sugere-se que a documentação da **Qualificação da Vigência Legal** seja feita utilizando os atributos id e tipo, onde id é identificador, e tipo comportará os *status* descritos no diagrama de transição de estados da vigência da fonte legal ou regulatória (Figura 17), conforme (SILEX, 2013), são definidos como:

i) publicada - veiculação dos atos normativos em periódico oficial;

ii) prorrogada (prorrogação de vigência) - evento pelo qual a fonte legal ou regulatória, ou dispositivo tem o seu período de vigência ampliado (que pode ser por tempo determinado ou indeterminado);

iii) em vacância - período entre a publicação e a entrada em vigor da fonte legal ou regulatória;

iv) revogada - evento pelo qual se retira expressamente a vigência de fonte legal ou regulatória no todo ou de dispositivo de fonte legal ou regulatória;

v) alterada - texto de norma jurídica que estabelece disposições gerais ou especiais a diploma legal;

vi) convertida - aprovação de medida provisória e sua transformação em fonte legal ou regulatória;

vii) rejeitada - ato pelo qual o Poder Legislativo, por meio de um decreto legislativo, rejeita o texto de uma fonte legal ou regulatória;

viii) declarada insubsistente - evento que retira do mundo jurídico atos com defeito de validade (atos inválidos), produzindo efeitos retroativos à data em que o ato foi emitido (efeitos *ex tunc*). Excepcionalmente, no âmbito das normas infralegais, o termo anulação pode ser utilizado na acepção de revogação;

ix) suprimida - o termo "suprimida" foi utilizado em normas promulgadas na primeira metade do século XX com o sentido de "revogação". Supressão de dispositivo - caso em que o dispositivo acrescido pela medida provisória perde a sua vigência por conta da rejeição ou decurso de prazo da medida provisória ou ainda por ausência de sua previsão pela lei de conversão;

x) prejudicada - situação que encerra a vigência da medida provisória por edição de fonte legal ou regulatória que trata sobre a mesma matéria comunicada ao Poder Executivo pelo Poder Legislativo;

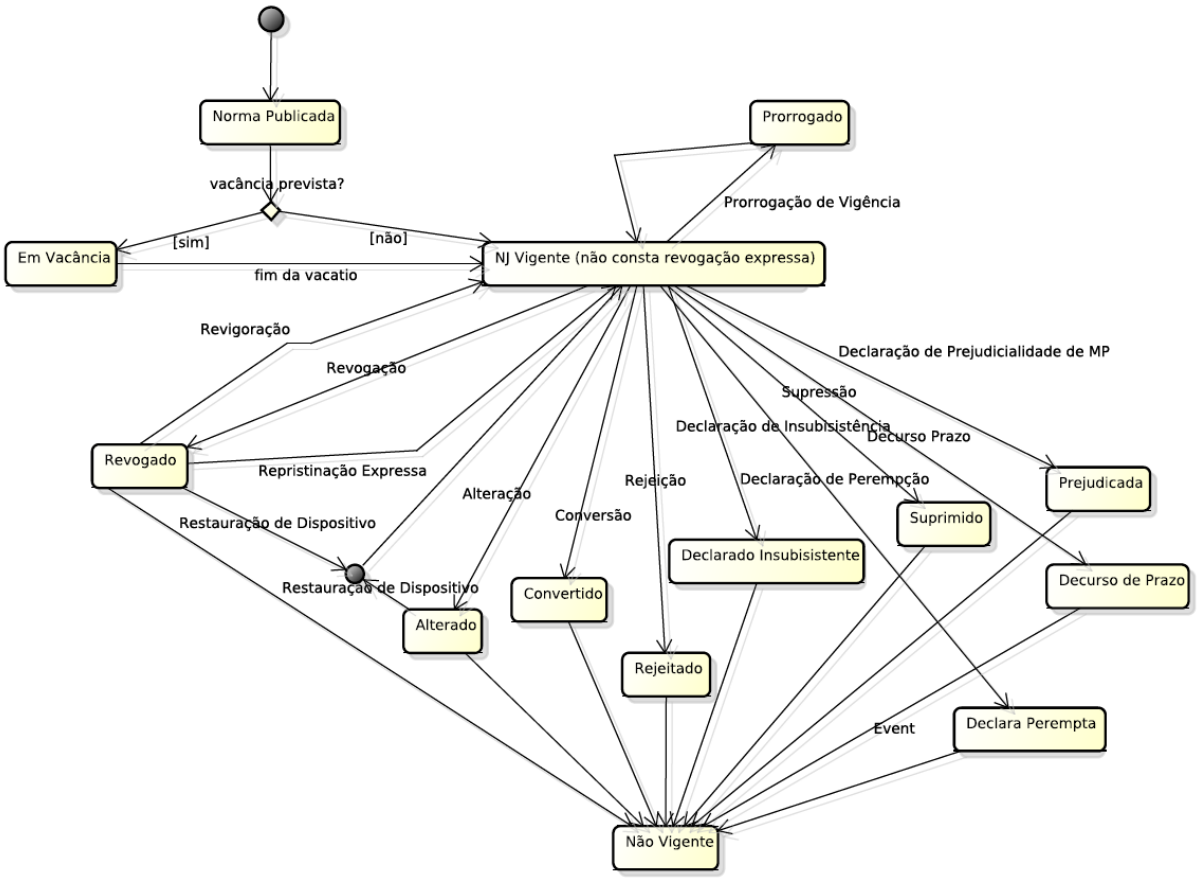
xi) decurso de prazo - evento que encerra um prazo expressamente estabelecido;

xii) declarada perempta - ato pelo qual se declara a perempção de concessão ou permissão;

xiii) vigente - é a existência da norma no ordenamento jurídico por um ou mais períodos temporais. Uma fonte legal ou regulatória vige até que outra a revogue ou até que expire o prazo nela previsto. Situa-se a vigência como marco intermédio entre a existência, que se formaliza pela promulgação, e a eficácia, que decorre da observância social da norma.

xiv) não vigente - é a não vigência. vide: vigente.

Figura 17: Diagrama de transição de estados da vigência da norma.



Fonte: SILEX, 2013.

5.3.3 Classificação e ordenação de hierarquia legal e regulatória

No elemento **Classificação e Ordenação de Hierarquia Legal e Regulatória** está configurado precedência normal verticalizada decorrente do princípio da unidade do ordenamento e da supremacia da Constituição (LENZA, 2017). Não se pode esquecer que há microssistemas dentro do próprio Direito, e uma dicotomia entre o público e privado. Outra questão importante a ser destacada quando se fala dos poderes municipais, estaduais e federal não existe uma clara relação ao Direito, pois a precedência pode ser por localidade, o mais perto primeiro. Ainda, há situações que devem considerar a existência de sistemas bipartites ou tripartites, onde há presença de espaços intergovernamentais para decisões e atuações.

Assim, pode-se rechaçar a ideia kelseniana que "o Direito seja um mero regulador da força, que seria seu conteúdo, admitindo-a como um meio", segundo Bobbio e de Cicco (1999). Esses autores destacam que as normas jurídicas não devem ser vistas de forma isolada, mas em

um conjunto ou complexo de normas, que constituem o ordenamento jurídico. Logo, para esses mesmos autores, o ordenamento jurídico permite se ter como produto uma organização complexa e dinâmica, a partir da qual uma determinada norma se torna eficaz considerando a natureza e a entidade das sanções, além das pessoas que devam exercê-las durante a sua execução. A dinamicidade pode ser percebida no fato das normas serem originadas umas das outras através de contínuas delegações de poder.

Sugere-se, então, que a documentação do elemento **Classificação e Ordenação de Hierarquia Legal e Regulatória** seja feita utilizando os atributos id e tipo, que deve seguir a hierarquia legal e regulatória a ser seguida encontra-se logo após, que foi definida depois de alguns estudos em livros como Barroso (2017), Lenza (2017) e Peck (2013). Sendo que as fontes são expostas em ordem crescente, logo pode ser entendida como de maior abrangência a Constituição Federal e as emendas constitucionais promulgadas.

1. Constituição Federal e emendas constitucionais promulgadas
2. Tratados internacionais e direitos humanos
3. Leis complementares
4. Leis ordinárias
5. Leis delegadas
6. Medidas provisórias
7. Decretos legislativos e resoluções
8. Decretos autônomos
9. Legislação estadual
10. Atos normativos secundários
11. Leis anteriores à Constituição em vigor
12. Leis que tenham sido revogadas
13. Leis municipais em face da Constituição Federal
14. Propostas de emenda constitucional ou projetos de lei
15. Súmulas
16. Normas técnicas
17. Contratos

5.3.4 Capacitação conforme a Taxonomia dos Princípios Legais e Regulatórios

No Brasil, a formalização para proteção dos dados dos usuários, das instituições no meio computacional pode-se dizer que aconteceu com o Marco Civil da Internet (BRASIL, 2014) e, posteriormente, com a Lei de Proteção Geral de Dados Pessoais de 2019 (BRASIL, 2019). Entretanto, a Constituição, o Direito Civil e o Direito Penal já equiparavam os delitos, os crimes cibernéticos aos comuns em seus julgamentos, e ampliando as sanções dadas as proporções que tomavam alguns desses. No exterior, leis específicas datavam de muito antes das nacionais. Para Tamò-Larrieux, Tamò-Larrieux e Seyfried (2018) entenderam que havia a necessidade uma taxonomia que contivesse os princípios legais. Sendo que estes princípios seriam relativos: à legalidade do processamento de dados; ao design de processamento de dados; aos direitos dos indivíduos; e à conformidade e aplicação. Considerando isto os autores traçam diferentes parâmetros, para que os sistemas computacionais, por exemplo, consigam atingir o seu propósito.

Assim, para cumprir com os princípios relativos à legalidade do processamento de dados são necessários: legalidade, justiça e transparência; consentimento informado e outros meios para processamento legal de dados; limitação de propósito. Para os princípios relativos ao design de processamento de dados de sistemas são precisos: minimização de dados e proporcionalidade, uso, divulgação e limitação de armazenamento; segurança de dados; anonimato e pseudoanonimato; qualidade e precisão de dados. Enquanto para os princípios relativos aos direitos dos indivíduos são fundamentais: princípio de participação; Direitos de Informação e Acesso; direitos de reação, apagamento e objeção. E por último, mas não menos importante, os princípios relativos à conformidade e aplicação são necessários: avaliações de responsabilidade, responsabilidade e risco; entidades de supervisão governamental e de definição de padrões; previsão de sanções e compensação.

Considerando o exposto, os atributos definidos para o elemento **Capacitação conforme a Taxonomia dos Princípios Legais e Regulatórios** foram: id, fonte legal ou regulatória, consentimento do usuário, limitação de propósito, anonimato ou pseudoanonimato, data de armazenamento, data do último acesso, tempo limite de uso, tempo limite de armazenamento, entidade de supervisão governamental. Estes atributos foram escolhidos por materializar a taxonomia e dar maior autonomia, transparência e controle aos usuários dos seus dados, que estão sendo utilizados pelo sistema computacional. Desta forma, o sistema computacional também deverá ser preparado para isto.

Assim, o id é um atributo de identificação única; fonte legal ou regulatória será onde é informado do dispositivo legal, que permitiu o acesso aos dados. Consentimento do usuário é um atributo de resposta afirmativa ou negativa indicando o seu consentimento - é importante destacar que, em alguns casos, o usuário não oferecendo seu consentimento, o serviço ou o produto não poderá ser ofertado. Desde apresentação das políticas e dos termos ao usuário tem que ficar claro qual é propósito do serviço ou produto, dessa maneira o usuário poderá informar neste atributo, a limitação de propósito, se ficou clara ou não a proposta de serviço ou de consumo de um produto. Em algumas situações, é permitido ao usuário de um serviço, para o público externo, anonimato ou um "pseudoanonimato"; isto configurando-se como fato deve ser solicitado ao usuário um pseudônimo ou simplesmente que deixe a informação "vazia".

A nova Lei de Proteção Geral de Dados Pessoais de 2019 (BRASIL, 2019) estabelece prazos para o armazenamento de dados de acordo com o tipo de dado, logo é necessário saber quando foi obtido o dado, qual é o tipo para definir tempo limite de armazenamento. Já o tempo limite de uso é algo negociável e definido nas políticas e termos, desde que não contrarie a lei. Data do último acesso armazenará a última vez que o usuário teve acesso aos seus dados por acesso direto ou por solicitação. Para facilitar o encaminhamento, auditorias e fiscalizações futuras, o atributo entidade de supervisão governamental armazena o órgão, a agência interessada nas informações facilitando também a manutenção da conformidade legal e regulatória junto a essa entidade.

5.3.5 Identificação de Fontes Legais ou Regulatórias (FLR)

O elemento **Identificação de Fonte Legal ou Regulatória (FLR)** é o responsável pela comunicação com tudo aquilo que estiver externo ao *framework*, servindo de interface com o sistema computacional. Neste elemento, também há conexões com todos os outros elementos do *framework.*

Este elemento pode ser considerado um elemento central. Isto salienta a importância de se ter em sua documentação alguns atributos bem destacados com sua origem, projeto que de início a sua existência no *framework*; sua fonte legal ou regulatória para os casos, onde haja alguma dúvida ou seja necessário verificar a dependência, por exemplo. Outro atributo seria a descrição para permitir em poucas palavras uma explicação do identificador; sua vigência estaria documentada em atributo de mesmo nome e auxiliaria aos profissionais de Computação ou interessados de forma geral a verificar se há algo a ser feito com relação ao identificador em si; autoria seria para informar o responsável pelo cadastramento e data da autoria, a data deste

cadastramento em si; o atributo observação, na maioria dos casos, pode ser utilizado como para colocar explicações ou alguma necessidade de intervenção ou o motivo da necessidade da fonte. Sendo assim, são atributos a serem documentados deste componente: id, origem, fonte legal ou regulatória, descrição, vigência, autoria, data da autoria, observação.

5.3.6 Representação de Rastreabilidade entre Requisitos Legais ou Regulatórios Testáveis (RLRT) e Fontes Legais ou Regulatórias (FLR)

O elemento **Representação de Rastreabilidade entre Requisitos Legais ou Regulatórios Testáveis (RLRT) e Fontes Legais ou Regulatórias (FLR)** é parte do modelo de rastreabilidade implementada que permite a união entre a fonte e o requisito testável. Então, a partir deste elemento poder-se-á construir toda a história legal e regulatória do sistema computacional, bem como de seu versionamento e de sua conformidade.

Para isto os atributos a serem utilizados na documentação são: id, idFLR, idRLRT, domínio-contexto, versão, autoria, data da autoria. O id é um atributo de identificação único, idFLR e idRLRT viriam da identificação da fonte legal ou regulatória e identificação do requisito legal ou regulatório testável, respectivamente; ao passo que domínio-contexto deve ser atribuído de acordo com projeto ao qual faz parte. O atributo versão permitirá o versionamento, algo tão importante nos projetos computacionais, se utilizado corretamente. Ao passo que os atributos autoria e data de autoria devem ser empregados para rastreamento do responsável pela criação/modificação dos atributos.

5.3.7 Catalogação de termos

O elemento **Catalogação de Termos** tem como razão de sua existência a unificação do entendimento e de esclarecimento dos termos jurídico, legais, regulatórios ou de qualquer termo encontrado no âmbito das normas, que tenha gerado dúvida ou precisou de algum esclarecimento. Assim, seus usuários cadastram o termo, sua descrição, e um exemplo de aplicação ou uma explicação no contexto de uso. Isto permite que os usuários do *framework* aos poucos criem o seu próprio glossário.

A documentação do elemento **Catalogação de Termos** recomenda-se ser feita utilizando os seguintes atributos: id, termo, descrição, exemplo de aplicação ou explicação no contexto de uso. Assim, o id servirá como identificador do termo cadastrado; o termo então conterá o termo propriamente dito, enquanto em descrição terá uma breve descrição do termo,

seguindo de exemplo de aplicação ou uma explicação no contexto de uso armazenado em um atributo de mesmo nome.

5.3.8 Módulo de conversão de dados

O **Módulo de Exportação de Dados** permite que o usuário do *framework* escolha quais os tipos de dados que quer exportar e o formato (XML ou JSON), e assim o faça para carregar em outra ferramenta, compartilhar bases entre equipes ou instituições, ou, simplesmente, para ter uma cópia de segurança dos dados armazenados no repositório. Os formatos escolhidos foram os comumente utilizados pelas ferramentas disponíveis no mercado para diferentes fins. Isto pode auxiliar os profissionais de Computação a utilizarem os dados gerados no *Framework* para outros fins que não os previstos por esta pesquisa.

5.3.9 Repositório do *Framework*

O **repositório do *Framework*** poderá ser alimentado diretamente pelos outros componentes, quando necessário, todavia é flexível à alimentação, classificação, manipulação do usuário do *Framework* por meio de outras ferramentas, logicamente o histórico desta manipulação é armazenado. A intenção é oferecer mais opções de informações diretas, maior reuso e flexibilização de seu conteúdo no atual e em novos projetos.

Sugere-se que a documentação do **repositório do *Framework*** seja feita utilizando os atributos, como: id, tipo/denominação de FLR, descrição, status, vigência, domínio (*tags*), contexto (*tags*), classificação (*tags*), projetos (*tags*), destaques, relacionamentos (como outras FLR), esfera de aplicação (federal, estadual, municipal, área do conhecimento etc.), regulamentações, responsáveis, origem.

No contexto do repositório, foram sugeridas *tags* como informações para atributos indicados, por entender que são significativas, facilitam o trabalho para quem as preenchem, e quem está trabalhando junto no contexto em si; além disso há um modelo de termo, onde essas *tags* podem ser preenchidas e descritas para “os que virão”. Dessa forma, não são criados nenhum outro problema quando os passos são seguidos corretamente.

No contexto do repositório do *framework,* o atributo id é uma identificação única, enquanto tipo/denominação de FLR está hierarquia que a fonte legal ou regulatória ocupa. O atributo descrição possibilita uma breve definição do que trata a fonte legal ou regulatória; para no atributo status indicar seu ou não por algum projeto no momento da consulta. O atributo vigência está estritamente ligado ao modelo de vigência utilizado pelo *framework*, assim só

sendo permitido como informação àquelas que constam no modelo. Nos atributos domínio, contexto, classificação, projetos, os profissionais de Computação poderão utilizar as *tags* mais convenientes e significativas para equipe para explicar o domínio, contexto, classificação e projeto em questão considerando sempre lembrando "daqueles que virão", seu reuso, futuras manutenções ou evoluções do sistema computacional, então fazendo uso consciente o modelo de termos para melhor definir as *tags* utilizadas pelas equipes em seus projetos.

Uma fonte legal ou regulatória pode ter alguns destaques por conta disso existe um atributo nomeado de destaques para contemplar os armazenamentos dessas informações que são bastantes úteis no cotidiano, bem os seus relacionamentos (como outras FLR) podem e devem ser guardados para futuras consultas. A esfera de aplicação (federal, estadual, municipal, área do conhecimento etc.) é relevante para identificação de domínio/contexto, de outras FLR importantes, bem como de entidades regulatórias ou fiscalizatórias. Algumas fontes legais ou regulatórias não bastam por si, precisam de regulamentações para entrarem em vigor, por exemplo; e para armazenar as suas regulamentações existe o atributo regulamentações. Para os atributos responsáveis espera-se a indicação das pessoas que trabalharam na formalização da fonte legal ou regulatória como parte do projeto; e o atributo origem deverá ser armazenado a identificação do projeto iniciou a fonte no repositório.

5.4 Fluxos de atividades

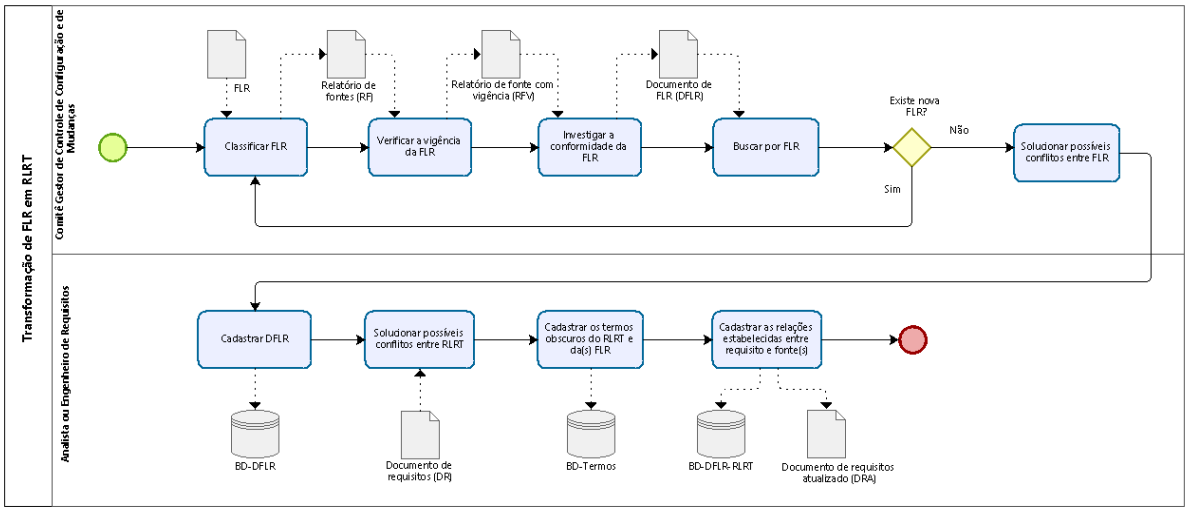
Para facilitar o entendimento do uso deste *Framework* pelas equipes, na avaliação que seria realizada em seguida, foi necessária a construção de fluxos de atividades (Diagrama 5.1 e Diagrama 5.2), como sugestões de uso. A incorporação do *Framework* às atividades cotidianas de uma equipe responsável por sistemas computacionais, no que tange aos requisitos legais e regulatórios, pode exigir certo esforço, se a equipe anteriormente não observava essa obrigatoriedade. Esse esforço ou custo operacional foi uma grande questão levantada pelos respondentes da avaliação realizada. Todavia, àqueles que isto era uma situação a ser mensurada, ao final da avaliação, concluíram que era compensatória a relação de sua utilização para a conformidade legal e regulatória e os custos oriundos.

A apresentação realizada antes das entrevistas possuía uma versão simplificada dos Diagramas 5.1 e 5.2 para melhor leitura pelos respondentes. Além disso, a intenção era permitir, em uma visão elementar, mas não ideal, que profissionais pudessem vislumbrar as atividades a partir de um único papel, o deles próprio. Posto que, nos estudos exploratórios realizados

(Capítulo 4), a maioria dos profissionais não dispunham de nenhum apoio jurídico. Desse modo, foi explicado também que o *Framework* previa um uso adaptável e escalável, de forma a promover a sustentabilidade a partir do reuso e da flexível incorporação aos ambientes já estabelecidos, quando os mesmos permitiam isto. Entretanto exigia algum esforço inicial para sistematização, implantação e sensibilização dos interessados com relação aos pilares desse *Framework*.

A Figura 18 contém o diagrama, que representa uma sugestão para a transformação de fonte(s) legal(is) ou regulatória(s) - FLR - em requisito(s) legal(is) ou regulatório(s) testável(is) - RLRT. O fluxo de atividades relacionadas gera diferentes documentos e relatórios como artefatos, que podem ter sua criação automatizada, quando utilizadas ferramentas computacionais e estratégias de rastreabilidade. Esse fluxo é apenas um exemplo da aplicação do Framework. Muitas outras ações poderiam ser diagramadas, como por exemplo a verificação de fontes já cadastradas e atualização dessas; ou a substituição de antigas fontes e atualização dos requisitos.

Figura 18: Diagrama da transformação de fonte(s) legal(is) ou regulatória(s) - FLR - em requisito(s) legal(is) ou regulatório(s) testável(is) - RLRT.

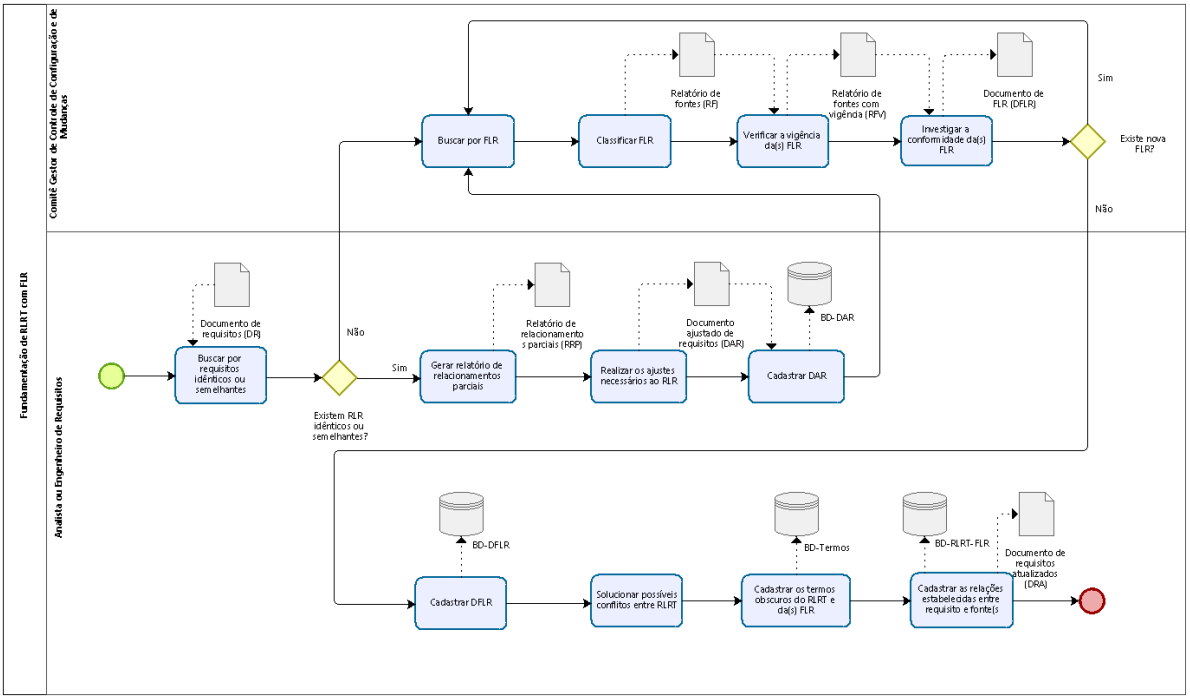


Fonte: a autora.

A Figura 19 contém o diagrama, que trata de uma sugestão para atividades relacionadas a fundamentação de requisito(s) legal(is) ou regulatório(s) testável(is) - RLRT - a partir de fonte(s) legal(is) ou regulatória(s) - FLR. Neste caso, a opção foi entender que o *Framework* já estaria sendo utilizado pela equipe há algum tempo, para que houvesse a necessidade de

buscar/verificar a presença de requisitos já presentes no repositório dos projetos dos sistemas computacionais. Assim, existiria a obrigação de buscar, possivelmente, informações para reuso dessas. Como no exemplo anterior, diferentes documentos e artefatos são gerados. A automatização dessa geração dependerá do ferramental utilizado pela equipe em si.

Figura 19: Diagrama sobre fundamentação de requisito(s) legal(is) ou regulatório(s) testável(is) - RLRT - a partir de fonte(s) legal(is) ou regulatória(s) - FLR.



Fonte: a autora.

Durante a apresentação, houve quem já tentasse visualizar, dentro de seu fluxo de atividades, as melhores estratégias de utilização. Dessa maneira, surgiram sugestões com relação: à participação do comitê gestor; à validação pelo *product owner*; à mediação de conflitos entre requisitos e entre fontes legais ou regulatórias; a criação de guias/manuais para explicação dos elementos do *Framework*; ao oferecimento de banco de fontes legais ou regulatórias; à pluralidade do uso; à uniformização dos processos; à governança como combustível; à segregação de papéis; à redefinição da documentação mínima; à cobertura legal e regulatória a ser levantada; à priorização com relação ao *backlog*; e ao reuso para redução de pontos de manutenção.

5.5 Auditoria de tecnologias da informação e da comunicação

Um dos focos desta pesquisa foi a possível auditoria de tecnologias da informação e da comunicação, e para isto foi preciso ter como propósito em cada fase de um artefato, que possa ser utilizado como evidência legal da ação/evento para indexação do relacionamento e rastreamento e verificação da conformidade legal e sua integridade. Dada a natureza volátil de alguns desses artefatos é importante aguardar seu histórico (data de criação, datas de modificação, responsáveis por esses fatos, motivação, por exemplo). Fato que traz certa dificuldade em ambiente que envolve desenvolvimento ágil (OCHODEK e KOPCZYŃSKA, 2018).

Pelo plano nacional, é mandatória haver uma equipe interna e uma equipe externa de auditores regularmente exercendo esse papel com fins de manutenibilidade da conformidade legal e regulatória independente da natureza do sistema computacional. Entretanto, isto é muito comum ser verificado em fábricas de software para área financeira ou médica, cuja legislação e as penalidades são mais explícitas e rígidas (AKHIGBE, AMYOT e RICHARDS, 2019).

A auditoria interna deve acontecer de forma proativa, programada e quando algum incidente ocorre. Sendo que cada uma cumpre um papel importante junto à instituição e às partes interessadas. Normalmente, deve existir na instituição um plano de investigação (*planning memo*), que oferece as diretrizes a serem seguidas em caso de necessidade. Esse documento deve ser "vivo", constantemente revisto e atualizado, quando devido.

Em caso de incidente, auditoria mais grave e não programada, a equipe interna, investigador indicado ou auditores terceirizados devem atentar-se para diferentes fatores como profissionalismo, discrição, respeito, integridade, isenção, competência técnica, imparcialidade, por exemplo. Durante todo processo é importante a guarda ou custódia de documentos, mas também estreita comunicação com a área jurídica da instituição. Ao final, o relatório precisa ser feito através de relatório não necessariamente ao denunciante, contudo sempre ao Comitê de Ética.

Outra questão a ser discutida é a visão ampla da lei, da auditoria e da Ciência da Computação sobre a definição de sistema de computação: software + hardware + infraestrutura + telecomunicações + pessoas. Primeiro ponto destacado por esta definição é que um sistema "não é só um software", algo que por natureza é abstrato e intangível (SOMMERVILLE, 2015), além de retomar a questão da necessidade da preparação das pessoas e, por último, incluir a infraestrutura (hardware, softwares básicos, telecomunicações, segurança, dentre outros). Dessa

forma, a integração entre todos os gestores para decisões e planejamentos passaram a ser ainda mais importante do que no passado, onde havia clara separação entre “hardware” e “software”. A partir dessa integração pode-se buscar, planejar, obter e manter a conformidade legal e regulatória.

5.6 Discussões e considerações

Considerando o que foi exposto, o *framework* visa atender aos profissionais de Computação, sem com isso impedir uma ampla visão de todos os interessados no sistema computacional como um todo. Os componentes escolhidos foram aqueles que após uma fase de prototipação mostraram-se mais eficientes e eficazes no processo de apoio ao profissional, sem exigir mais um trabalho hercúleo. A intenção sempre foi uso e reuso, transformação e evolução, e mitigação de retrabalho.

Nesta fase, de prototipação do *Framework*, foram utilizados materiais básicos para uma prototipação, como: *post-its*, canetas e folhas de tamanho A4 coloridas. O sistema computacional com seus artefatos, arquitetura, infraestrutura, diferentes modelos de rastreabilidade, papéis e responsabilidades, partes interessadas, domínio e contexto, além de alguns processos de desenvolvimento também foram representados de um lado.

Por outro lado, a solução foi se apresentando aos poucos. Até que em uma interação já estava-se formalizando um *framework*, que inicialmente tinha outros componentes. Com o refinamento, ficaram os elementos apresentados, que foram revistos e refinados. Entende-se que esses são os elementos mínimos para implementação do *framework* na perspectiva da implementação e manutenção da conformidade legal e regulatória.

Antes, porém, foi construindo-se quais deveriam ser os pilares para a conformidade legal e regulatória; sem antes esquecer que a dificuldade de se definir ou refinar um requisito, seja de qual tipo for. Então, julgou-se necessário ter uma seção para tratar a transformação de requisito, que é uma tarefa mais relevante para Engenharia de Requisitos e de Software. Finalizando com uma seção sobre o processo de auditoria das tecnologias da informação e da comunicação, que se desdobra na conformidade legal e regulatória do sistema computacional.

É importante salientar que a intenção não foi extinguir ou menosprezar a participação de juristas nas equipes, mas sim também apoiá-los, quando presentes, ou sustentar/instrumentar, minimamente, equipes que, porventura, não os possuam com esteio. É reconhecida a hostilidade das fontes legais ou regulatórias para os profissionais da Computação, em sua maioria. Sem

mencionar as dificuldades presentes em tratar os conflitos dos requisitos convencionais, o que se dirá daqueles que são legais ou regulatórios. Para estes casos, recomenda-se a busca pelo apoio de juristas institucionais ou contratados de forma *ad hoc*.

A versão atual já considera as melhorias sugeridas pelos respondentes do processo de avaliação. Como melhorias, foram sugeridas: a utilização dos princípios de Gestalt para produção de visualizações apropriadas; destacar melhor a rastreabilidade e o versionamento existentes entre os artefatos gerados, e da importância da catalogação de termos para os atuais e os futuros membros das equipes; melhorar a explicação da taxonomia; falar sobre a possibilidade de interoperação entre instituições a partir do Módulo de Conversão de Dados; e alterar a ordem dos quatro elementos conceituais do *Framework* para melhor entendimento destes.

Este capítulo tratou do *Framework* e seus elementos. Apresentando os elementos de fundamentação, explicação e justificativa para haver um *framework* como resultado desta pesquisa. No próximo capítulo, é apresentada a avaliação deste *Framework* junto a representantes do público-alvo.

6 Avaliação do *Framework*

O objetivo deste Capítulo foi apresentar a avaliação realizada para o Framework apresentado no Capítulo 5 e, dessa maneira, identificar possíveis problemas na sua construção, bem como sua utilidade junto a representantes do público-alvo. Para esta avaliação, foi planejado **um estudo de caso exploratório** (YIN, 2018) utilizando **dois instrumentos**: **um questionário positivista** e **uma entrevista semiestruturada** construtivista, como preconizado por Silverman (2014) e Uribe (2007). Com esses instrumentos, buscaram-se obter informações também sobre o participante e sua experiência com as temáticas: fontes legais e regulatórias, requisitos legais e regulatórios, conformidade legal e regulatória, rastreabilidade, visualização da informação, reuso e sustentabilidade no ambiente de concepção, de manutenção e de evolução de sistemas computacionais.

A construção dos instrumentos considerou que o *Framework* proposto possuía elementos conceituais incomuns à maioria dos participantes. Sendo assim, o formulário construído para o questionário trazia algumas explicações ou exemplos para auxiliar a resposta. Assim como, antes da entrevista foi realizada uma breve apresentação com os termos e os conceitos básicos, estrutura do *Framework*, propostas de fluxos de atividades e exemplos de uso. Tudo isto, com a intenção de familiarizar ou alinhar conceitos e conteúdo para estabelecer o melhor aproveitamento do espaço-tempo dos participantes e dos resultados obtidos.

Essa avaliação foi feita considerando a metodologia qualitativa, uma pesquisa de levantamento, visto que seria a primeira aplicação do *Framework* a um grupo de pessoas fora do contexto, onde este foi concebido (academia). Além disso, havia a necessidade de obtenção de informações complexas e detalhadas dos participantes, tendo como intenção uma visão exploratória e sem uma preocupação fundamentada na coleta de dados estruturada ou numérica.

Nas seções seguintes, são apresentados o planejamento e desenho da avaliação; análise dos resultados de cada instrumento; discussão dos resultados obtidos; e considerações acerca da avaliação realizada.

6.1 Planejamento e desenho da avaliação

Nesta seção, são apresentados: a metodologia empregada, o planejamento para abordagem dos participantes, perfil dos participantes em um estudo de caso exploratório, os instrumentos e ferramentas utilizados.

Esta avaliação utilizou instrumentos estruturados e semiestruturados com a finalidade de obter as impressões dos participantes e a serventia do *Framework* no âmbito das organizações, das fábricas de *software* e no processo de auditoria da conformidade legal e regulatória. Para coletar dados demográficos e experiência dos participantes foi utilizado um questionário (usando um formulário Web). Enquanto para a apresentação dos termos, dos conceitos, do *Framework*, propriamente dito, fluxos de atividades e exemplos relacionados com a manutenção e a evolução da conformidade legal e regulatória, foram apresentados na forma de seminário.

6.1.1 Metodologia do estudo

Para atingir o propósito dessa avaliação, foram definidos o problema, as questões de pesquisa (QP), os objetivos (geral e específicos), tipos de instrumentos a serem utilizados e público-alvo.

Assim, o **problema examinado** foi o de verificar a utilidade do *Framework* para conformidade legal e regulatória junto ao público-alvo no ciclo de vida dos sistemas computacionais. Além disso, descobrir os desafios não vencidos pelo *Framework* com o objetivo de mitigá-los. Ao mesmo tempo que as **questões de pesquisa** foram definidas da seguinte forma:

- **QP1:** O *Framework* auxilia na identificação das fontes legais ou regulatórias e dos requisitos legais ou regulatórios de um sistema computacional?
- **QP2:** O *Framework* promove a sustentabilidade dos sistemas computacionais a partir do reuso das fontes legais ou regulatórias e dos requisitos legais ou regulatórios?
- **QP3:** Os elementos do *Framework* melhoraram seu planejamento e ações do dia a dia?
- **QP4:** Os elementos do *Framework* são suficientes para atender a demanda atual de artefatos para planejamento, gerenciamento e manutenção da conformidade legal e regulatória?
- **QP5:** A inserção do *Framework* na rotina da equipe traz quais benefícios ou malefícios?

O **objetivo geral** desta avaliação foi confirmar a utilidade do *framework* proposto para gerenciamento da conformidade legal e regulatória dos sistemas computacionais. Para isto, foram traçados os seguintes objetivos específicos:

- **Objetivo específico 1**: Levantar informações a partir das entrevistas se o *Framework* facilita a identificação da hierarquia das fontes legais ou regulatórias a serem atendidas;
- **Objetivo específico 2:** Identificar se o elemento de Qualificação de Vigência Legal ajuda a planejar melhor as *sprints* de um projeto de um sistema computacional;
- **Objetivo específico 3**: Verificar se o elemento Catalogação de Termos auxilia a equipe a entender termos utilizados nos documentos aplicados no ciclo de vida de um sistema computacional;
- **Objetivo específico 4**: Averiguar se a criação de rastreabilidade proposta entre todos os artefatos relacionados com os requisitos legais ou regulatórios e as fontes legais ou regulatórias pode ser útil de que forma no cotidiano;
- **Objetivo específico 5**: Questionar se o elemento Módulo de Conversão de Dados é útil no dia a dia do profissional;
- **Objetivo específico 6**: Identificar se a taxonomia utilizada como base foi capaz de resolver questões de privacidade e segurança;
- **Objetivo específico 7**: Verificar se o reuso e a sustentabilidade são práticas na instituição, e qual o ganho que se pode ter com essas práticas oferecidas pelo *Framework*;
- **Objetivo específico 8**: Levantar quais foram os benefícios e malefícios inseridos com uso do *Framework*.

6.1.2 Planejamento das entrevistas e do questionário

A construção dos instrumentos de pesquisa foi feita em etapas. Na primeira etapa, foi feito um documento indicando o desenho metodológico a ser seguido e os roteiros para o questionário, a entrevista e um guia com a definição da sequência do conjunto de passos a serem percorridos pela entrevistadora. Na sequência, foram construídos os termos: Termo de Consentimento Livre e Esclarecido (TCLE) e Termo de Cessão e Uso de Imagem, Áudio e Vídeo (TCUIAV). Para então, serem feitas as definições da lista de convidados e dos modelos de mensagens eletrônicas (e-mails) para cada uma das diferentes situações. Todos estes itens constam listados e representados no Apêndice D.

As situações previstas foram: convite à participação da avaliação; reiteração do convite à participação da avaliação; encaminhamento do pedido de preenchimento de formulário do questionário; reiteração para o pedido de preenchimento do formulário do questionário;

informação da sala remoto para entrevista, reiteração para participação da entrevista após falta; agradecimento.

Ainda foram elaboradas quatro planilhas eletrônicas para disponibilização dos dias/horários disponíveis, para controle dos agendamentos realizados, para mapeamento e anonimização dos participantes e para armazenamento das respostas dos usuários. Também foi gerado um modelo para criação e documentação de requisitos.

Assim, as ferramentas utilizadas para apoio foram, basicamente, correio eletrônico institucional e a suíte Google. Logo, foram enviadas mensagens eletrônicas a partir do correio eletrônico institucional. Com Google Sheets foram criadas e disponibilizadas algumas planilhas; já com Google Forms foi produzido e disponibilizado o questionário; enquanto Google Slides foi utilizado para criação e apresentação de *slides* sobre *Framework* proposto. Por fim, Google Meet foi empregado para realização e gravação das entrevistas, e Google Docs para transcrição das entrevistas.

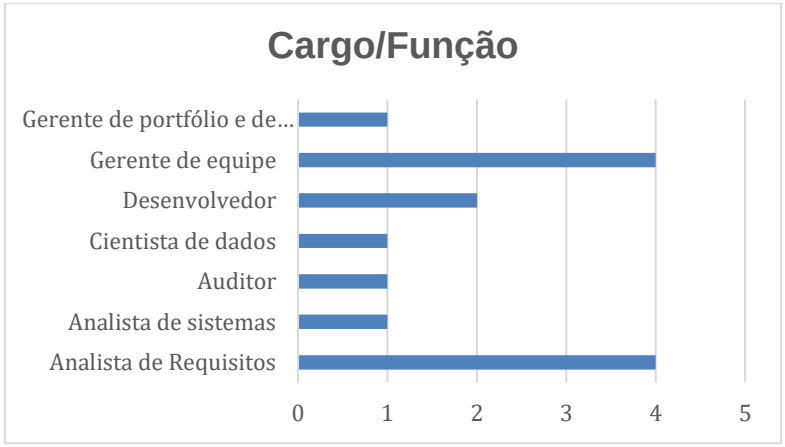
Antes da aplicação do questionário e da realização da entrevista com os participantes, para fins de ajustes e testes dos instrumentos e das ferramentas, foi efetuado um teste piloto com um participante, que tinha as mesmas características do público-alvo almejado.

6.1.2.1 Participantes/Respondentes

Foi definido que o perfil do público-alvo seria similar aos potenciais usuários do *Framework* proposto. Dessa forma, foram convidadas 26 pessoas com perfis entre auditores, gestores, líderes de equipe, analistas/engenheiros de requisitos e desenvolvedores (Figura 20). Apenas 14 pessoas aceitaram participar, enquanto as outras negaram a participação por diferentes razões, como: falta de tempo; contrato de confidencialidade assinado na organização em que trabalhava; não ter mais o perfil esperado.

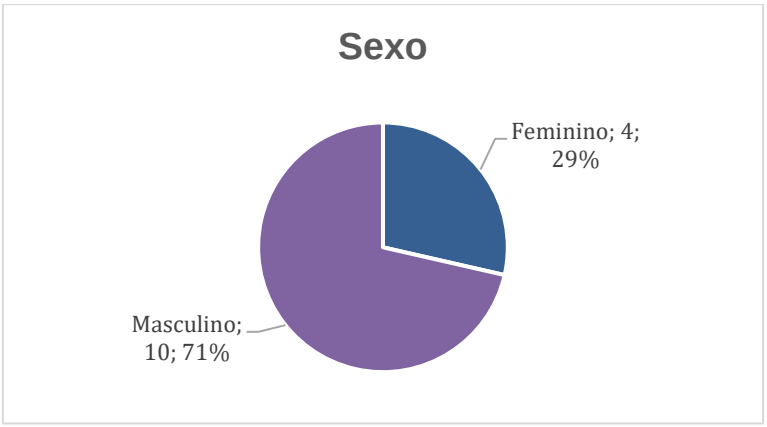
Das pessoas que aceitaram participar, as idades estavam entre 26 e 42 anos, sendo quatro do sexo feminino e dez do sexo masculino (Figura 21). Quando foram perguntadas sobre a formação acadêmica mais elevada, que possuía: uma pessoa respondeu ter o Ensino Superior Incompleto, cinco responderam ter o Ensino Superior Completo, três Pós-Graduação *Lato Sensu* na área de Ciência da Computação, e cinco Pós-Graduação *Stricto Sensu* (Mestrado) na área de Ciência da Computação (Figura 22).

Figura 20: Gráfico dos Cargos/Funções dos respondentes da pesquisa.



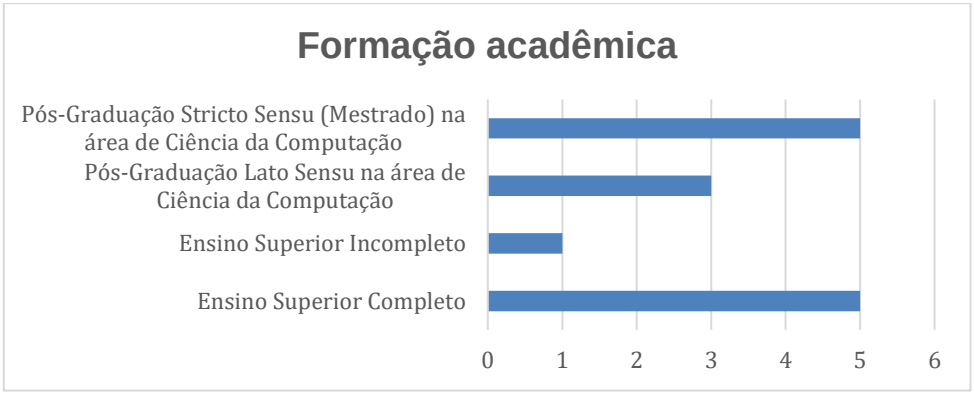
Fonte: a autora.

Figura 21: Gráfico da distribuição dos respondentes por sexo.



Fonte: a autora.

Figura 22: Gráfico da formação acadêmica dos respondentes.



Fonte: a autora.

Os perfis profissionais dividiram-se em quatro gerentes de equipe, quatro analistas de requisitos, dois desenvolvedores, um auditor, um analista de sistema, um gerente de portfólio e de produtos e uma cientista de dados. O tempo de atuação exercido nos cargos/funções variou da seguinte forma: sete pessoas tinham entre um e três anos, quatro entre quatro e seis anos, e três com mais de dez anos atuando nos cargos/funções. Todas essas informações foram sumarizadas na Tabela 6.1, todavia precisa ser esclarecido que a identificação dos participantes/respondentes foi atribuída de forma aleatória para fins de manutenção do anonimato e da privacidade.

Tabela 6.1 - Perfis dos participantes/respondentes

Idade	**Sexo**	**Formação acadêmica**	**Cargo/Função**	**Tempo de atuação na área**
42	Masculino	Pós-Graduação Stricto Sensu (Mestrado) na área de Ciência da Computação	Auditor	Entre um e três anos
36	Feminino	Ensino Superior Completo	Analista de Requisitos	Mais de dez anos
26	Feminino	Ensino Superior Completo	Analista de Requisitos	Entre um e três anos
30	Feminino	Pós-Graduação Stricto Sensu (Mestrado) na área de Ciência da Computação	Cientista de dados	Entre um e três anos
28	Masculino	Pós-Graduação Stricto Sensu (Mestrado) na área de Ciência da Computação	Analista de sistemas	Entre quatro e seis anos
37	Masculino	Ensino Superior Completo	Desenvolvedor	Mais de dez anos
31	Masculino	Ensino Superior Incompleto	Desenvolvedor	Mais de dez anos
39	Feminino	Pós-Graduação Lato Sensu na área de Ciência da Computação	Gerente de equipe	Entre um e três anos
30	Masculino	Ensino Superior Completo	Analista de Requisitos	Entre quatro e seis anos
36	Masculino	Pós-Graduação Lato Sensu na área de Ciência da	Analista de Requisitos	Entre quatro e seis anos

		Computação		
38	Masculino	Pós-Graduação Stricto Sensu (Mestrado) na área de Ciência da Computação	Gerente de portfólio e de produtos	Entre um e três anos
41	Masculino	Pós-Graduação Lato Sensu na área de Ciência da Computação	Gerente de equipe	Entre um e três anos
30	Masculino	Pós-Graduação Stricto Sensu (Mestrado) na área de Ciência da Computação	Gerente de equipe	Entre quatro e seis anos
34	Masculino	Ensino Superior Completo	Gerente de equipe	Entre um e três anos

6.1.2.2 Questionário

O levantamento de dados utilizando este instrumento (questionário) foi definido como condição prévia para participação nas etapas seguintes aos participantes, o que pode caracterizar o estudo como transversal - pelos dados serem recolhidos em espaço de tempo pré-definido (VIEIRA, 2009). A intenção foi a obtenção de informações demográficas e sobre a experiência laboral dos respondentes. Foram elaboradas questões padronizadas. Sendo essas ora abertas ora fechadas. Não foi estipulado tempo de resposta para cada pergunta, entretanto, na maioria dos casos, a resposta era obrigatória.

A abordagem escolhida para esse instrumento foi positivista, buscando conhecimentos de seis tipos diferentes de conhecimento com relação aos respondentes: fatos, crenças, padrões de ação, comportamento presente ou passado, e razões conscientes (SELLTIZ et al., 1964 apud SILVERMAN, 2014). Houve o cuidado de incluir algumas explicações de termos ou conceitos, e manter a mesma sequência da realização das perguntas para garantir a paridade das condições de estímulo e, por conseguinte, da medição.

Assim, os respondentes receberam um endereço na Internet (link) para um formulário previamente preparado com questões acerca de sua idade, sexo, formação acadêmica, cargo/função ocupada profissionalmente. Além disso, foram feitas perguntas a respeito das temáticas: i) sustentabilidade e reuso; rastreabilidade; ii) visualização da informação; iii)

ferramentas computacionais utilizadas no cotidiano para rastreamento, visualização da informação, atualização e refinamento dos dados; iv) requisitos legais ou regulatórios; v) instrumentos e evidências de conformidade legal e regulatória; e vi) auditoria nos sistemas computacionais.

6.1.2.3 Entrevista

Como preparação para a etapa das entrevistas remotas, os respondentes assistiram uma apresentação síncrona sobre conceitos e termos utilizados na pesquisa, bem como uma explicação sobre cada elemento do *Framework* e dois exemplos de sua aplicação no ambiente de uma fábrica de software. Como foi sugerido que interrompessem caso sentissem necessidade, todos os respondentes durante a apresentação fizeram perguntas sobre o conteúdo, e alguns citaram sua experiência para ilustrar o que estavam perguntando ou para confirmar o acontecimento de determinada situação no seu dia a dia. A intenção desta apresentação foi fazer com que todos os respondentes pudessem alcançar o mesmo nível de conhecimento sobre o tema "*Framework* para conformidade legal e regulatória" e o seu uso para apoiar a construção e o gerenciamento da conformidade legal e regulatória dos sistemas computacionais.

A abordagem adotada para construção das perguntas abertas foi positivo-construtivista, pois ainda havia a necessidade de obter dos respondentes informações sobre: fatos, crenças, padrões de ação, comportamento presente ou passado, e razões conscientes (SELLTIZ et al., 1964 apud SILVERMAN, 2014). Além disso, existia um espaço para, a partir da resposta, construir mutuamente novas perguntas de forma ativa, e um protocolo a ser seguido para essas interações.

Considerando isto, a maior parte das perguntas permitiam uma resposta imediata, entretanto as mesmas foram complementadas com interrogações dos tipos: Como? Por quê? O objetivo foi levar o respondente a refletir sobre sua resposta, as temáticas envolvidas, e a concepção e o emprego do *Framework* em questão. Desse modo, o respondente precisava relacionar sua opinião com sua experiência pessoal e laboral e a possível utilização do *Framework* no seu cotidiano. Portanto, foi preciso também adotar a escuta ativa (NOAKS e WINCUP, 2004).

Assim, Denzin e Lincoln (2011) afirmaram que fidedignidade, credibilidade, transferibilidade e confirmabilidade caracterizam uso de entrevistas em estudo de caso interpretativo, onde há necessidade de obter-se validade interna e externa. Assim, foi possível dividir com o respondente a reflexão, a responsabilidade e a ética da investigação feita sobre

fatos, crenças, padrões de ação, comportamento presente ou passado, e razões conscientes. Isto foi corroborado também com a confirmação de alguns participantes na identificação de problemas ou erros cometidos pela falta de conhecimento de atividades necessárias para promover a conformidade legal e regulatória, como afirmado por esses respondentes em seus depoimentos.

6.2 Análise das respostas ao questionário e as entrevistas

A Análise das respostas ao questionário foi fundamentada na Análise do Discurso (FOUCAULT, 2013). Isto porque o objetivo foi estabelecer relações entre a história e prática concreta, poder e saber, visto que essas relações estavam presentes na fala dos respondentes, e que se implicam mutuamente. O discurso em si está para além dos símbolos linguísticos, tem uma realidade construída através da história, da cultura, das relações em que se estiveram/estão imersos.

Assim, partiu-se do mais concreto para o mais abstrato, a partir de uma reflexão sobre um novo conhecimento adquirido durante o processo de interação com os respondentes e instrumentos (questionário, entrevista) utilizados para tal fim. Salientando que durante esta análise, o conhecimento adquirido transitou por diferentes níveis da instância do percurso narrativo, como (FIORIN, 2001):

i) o narrativo - conhecimento adquirido e transformação de um estado inicial a um estado final, que compreende quatro fases, que podem não se completadas: manipulação, competência, performance e sanção;

ii) o discursivo - as formas abstratas do nível narrativo foram revestidas pela concretude dos fatos, produzindo “as variações (sociais, religiosas, econômicas, por exemplo) de conteúdos narrativos invariáveis (tempo, espaço, personagens, circunstâncias)”; e

iii) da manifestação - plano de expressão (verbal e gestual) e plano de conteúdo (imanência - existência da causa na própria causa), articulação dos elementos que compõem o discurso.

Foram empregadas mais de 260 horas na transcrição e nas análises de todo o material obtido para triangulação das fontes de dados comparados e verificados entre si, com as respostas dos questionários e intervenções durante a apresentação e as perguntas. Sendo necessária a

verificação do contexto e do perfil traçado previamente com o discurso construído e proferido na ocasião, e ciente do rito imposto ao momento de fala e de silêncio. Para Foucault (1971), é a vontade da verdade, que fundamenta, reforça e aprofunda o discurso.

6.2.1 Resultados da análise das respostas ao questionário

O objetivo inicial foi que os respondentes fossem submetidos às questões antes da entrevista propriamente dita, para que fosse permitido o conhecimento do seu perfil. Dessa forma, dúvidas relacionadas às perguntas do questionário e da entrevista poderiam ser esclarecidas durante a entrevista mediante um acolhimento e uma contextualização na fala da entrevistadora.

Os respondentes foram identificados pela letra "R" seguidos dois dígitos sequenciais, para que fosse garantido e mantido o anonimato de acordo com que foi preconizado no TCLE e aceito pelos mesmos. Então, R01 até R14 foram os respondentes, tendo sido descartadas as respostas do respondente piloto e de dois respondentes, um que não aceitou o TCLE e outro que respondeu por duas vezes o questionário.

A primeira pergunta, depois das perguntas relacionadas aos dados demográficos, indagava sobre as principais **atribuições** dos respondentes. Com isto, foi possível observar que todos os respondentes acumulavam diferentes funções, e de certa forma estavam sobrecarregados. O que amplia a discussão de o uso Framework por profissionais de Computação como apoio às atividades e funções já acumuladas, bem como o papel desse profissional, que, normalmente, não recebe auxílio ou é obrigado a exercer atribuições de forma não qualificada para tanto. Para melhor clareza, seguem alguns exemplos:

- R03 - "Levantamento de requisitos, usando técnicas como entrevistas, questionários, prototipação. Criação de diagramas, fluxos, análise de negócio, especificações, atividades de aceitação de requisitos, treinamento com o usuário, atuação em projetos ágeis." (sic)
- R09 - "Elaboração de documentação técnica de especificações de requisitos, atendimento negocial às Instituições Parceiras (Clientes), treinamentos e apresentações dos sistemas, priorização de demandas, atuação como *Product Owner* nas *sprints* do time de desenvolvimento, entre outras." (sic)

- R12 - “Avaliação de equipe, acompanhamento de sustentação e evolução de produtos, melhorias de processos, implantação de metodologias, acompanhamento de indicadores, métricas.” (sic)
- R13 - “Assegurar que o projeto seja desenvolvido e concluído dentro do escopo, prazo e custos previstos; auxiliar o BPO em manter o backlog do produto atualizado; auxiliar na definição de prioridades para releases do produto; avaliar o impacto do produto perante os usuários; organização dos times ágeis, fomento sua auto-organização e trabalho multidisciplinar; identificar necessidade de capacitação para o time, comunicação entre área de negócio, patrocinador e time de desenvolvimento; desenvolver estratégias para manter o time focado, motivado e produtivo no desenvolvimento dos incrementos do produto, reunião com stakeholders, participar em reuniões de planejamento e revisão de sprints, entre outros.” (sic)
- R14 - “Gerenciar equipe de desenvolvimento, lidar com analistas de negócio.” (sic)

Quando perguntados sobre as suas **principais dificuldades e desafios** no desempenho das suas atribuições no cotidiano, as respostas assumiram a manifestação da exaustão e da intenção de melhor promover suas atividades cotidianas por parte de alguns respondentes:

- R02 - “A necessidade de urgência das demandas que causa pouco tempo para análise.” (sic)
- R03 - “A junção de muitas atividades.” (sic)
- R05 - “Falta de tempo para manter a documentação atualizada.” (sic)
- R08 - “São inúmeras, gerenciar uma equipe a distância tem sido o maior desafio. Manter a produtividade e também motivar.” (sic)
- R09 - “Mudanças constantes na legislação que funciona como base para o desenvolvimento do sistema. Durante sprints de evolução, o time de desenvolvimento é altamente dependente do analista, diminuindo consideravelmente a produtividade quando ele não está presente por algum motivo (férias, treinamentos, outras atribuições, etc). Dificuldade em gerir as atividades em momentos de alta demanda.” (sic)
- R12 - “Por ainda não achar ter conhecimento necessário para implantação de melhoria nos processos e liderança de pessoas apesar gostar e estudar sobre a área.” (sic)
- R13 - “Eliminar ruídos de comunicação, manter os times de *back-end, front-end*, UX e infraestrutura alinhados, pouca disponibilidade da área de negócio para envolvido com

o time de desenvolvimento durante a sprint, elevado grau de incerteza na elicitação de alguns requisitos, equipe reduzida e deadlines desafiadores."

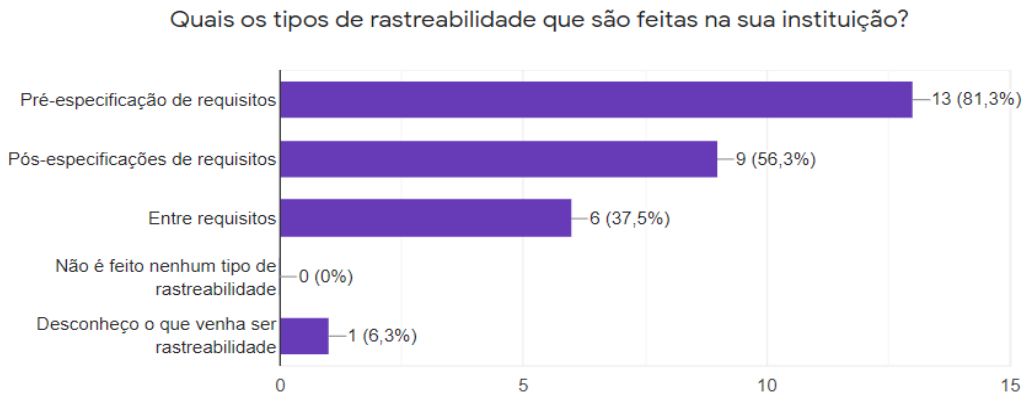
- R14 - "Tempo." (sic)

Para a pergunta sobre **o reuso e a sustentabilidade** serem práticas na instituição dos respondentes, 11 responderam que havia esta preocupação. Sendo que dois respondentes expuseram que esta era uma preocupação recente. Por outro lado, um respondente afirmou que não existia essa preocupação, e dois que não entendiam os conceitos e os preceitos relacionados com reuso e sustentabilidade em projetos de sistemas computacionais.

- R02 - "Não sei definir se sim ou não pois não tenho clareza desses conceitos." (sic)
- R08 - "Não entendi muito bem a pergunta, posso responder melhor na entrevista." (sic)

Os tipos de rastreabilidade feitas na sua instituição foram interrogados, na pergunta seguinte. Sabendo que este conceito poderia não ser familiar aos respondentes, embora pudesse ser uma prática da organização, foi incluída uma explicação a respeito da temática. Ademais, nesta pergunta de múltiplas escolhas eram oferecidas as opções: pré-especificação de requisitos; pós-especificações de requisitos; entre requisitos; não é feito nenhum tipo de rastreabilidade; desconheço o que venha ser rastreabilidade. Considerando as opções oferecidas, 13 responderam que era feita "pré-especificação de requisitos", nove responderam fazer a "pós-especificações de requisitos", seis respondentes selecionaram a opção "entre requisitos", e ninguém respondeu "não é feito nenhum tipo de rastreabilidade". A opção "desconheço o que venha ser rastreabilidade" foi escolhida por um respondente, e este identificou-se como analista de requisitos. Esse panorama é ilustrado na Figura 23.

Figura 23: Gráfico com os tipos de rastreabilidade realizadas.



Fonte: a autora

A presença dos **tipos de visualização** da informação em diferentes contextos e níveis praticados na sua instituição foi investigado junto aos respondentes para entender suas práticas e necessidades informacionais cotidianas. Dessa maneira, foram observadas três respondentes que não entenderam o conceito de visualização da informação ou não possuíam em suas instituições meios visuais considerando a pergunta feita. Por outro lado, havia outros 11 respondentes com diferentes formas de visualização da informação, como nos exemplos a seguir. Outra informação importante nesse relato foi encontrar que muitos dos respondentes possuíam materiais textuais pelos quais eram utilizados para tomada de decisão.

- R01 - “Infográficos dispostos no site da instituição; Portal da transparência; Decisões do [redacted]; Resoluções; Portarias; Relatórios de auditoria; Gráficos, listas e tabelas nos relatórios informativos produzidos pelo setor; pequenos dashboards para visualização dos dados.”. O nome da instituição foi suprimido por questões de anonimato.
- R04 - “Para meus projetos pessoas, desde visualizações de dados com simples gráficos, como gráficos de barra e linha, até gráficos que dão uma visão mais estatística, como *boxplots*.” (sic)
- R07 - “Ferramentas como JIRA/Confluence e Office365 onde são registradas as atas, as especificações e mudanças de requisitos e rastreabilidade de *issues*.” (sic)
- R08 - “Trabalho os gráficos para acompanhamento das equipes extraídos do sistema de gerenciamento.” (sic)
- R09 - “Especificação de Casos de Uso. Cenários de Testes BDD. Descrição da demanda em tarefas.” (sic)
- R13 - “A visualização das informações ocorre em nível estratégico, negocial e operacional! Sendo produzidos artefatos para visualização agregado ou analítica do dado, conforme o seu contexto (Donos de Produto, Stakeholders, Patrocinadores, Usuários...).”(sic)

Sobre **o uso de ferramentas para gerenciamento de requisitos**, quatro respondentes afirmaram não possuir nenhuma ferramenta para este fim, e os outros dez respondentes afirmaram que usavam uma ou mais ferramentas. Para esses dez respondentes, foi questionado se a(s) ferramenta(s) ofereciam recursos como rastreamento, visualização da informação, atualização dos dados, assim como seu refinamento, por exemplo. Para quatro respondentes apenas uma parte dessas funcionalidades são usadas, enquanto para um respondente a

ferramenta utilizada não oferecia nenhuma das funcionalidades exemplificadas. Para cinco respondentes, a(s) ferramenta(s) disponha(m) das funcionalidades citadas, dentre outras:

- R01 - “Apenas visualização da informação e atualização dos dados.” (sic)
- R06 - “A ferramenta (IBM/Rational ALM) oferece rastreamento entre requisitos, entre requisito e código, visualização do conteúdo, dinâmica de revisões e histórico de alterações.” (sic)
- R11 - “Apenas visualização e controle de versão.” (sic)
- R13 - “sim, mas não são especializadas para gestão de requisitos! Costumamos utilizar o Azure Boards (Visão negocial), The Manager (Ferramenta própria) e o GitLAB (Visão simplificada para desenvolvedores)” (sic)

Quanto à **presença de requisitos legais ou regulatórios** nos sistemas computacionais, que estavam sob a gestão dos respondentes, um respondeu que não havia e 13 responderam que sim. A estes 13 respondentes, foi pedido que comentassem um pouco sobre esses requisitos legais ou regulatórios que estivessem presentes nos sistemas computacionais com que os respondentes trabalhavam. Um dos respondentes (R06) aproveitou bem o espaço oferecido para registrar sua percepção dos requisitos legais ou regulatórios e as práticas ágeis. Isto foi ilustrado nos exemplos a seguir.

- R01 - “Requisitos legais ou regulatórios estão sempre presentes nos pequenos sistemas e relatórios que desenvolvemos. Principalmente porque o produto de nossas atividades tem forte relação com a privacidade, segurança e qualidade das informações que tratamos. Essa preocupação foi intensificada recentemente com a entrada em vigor da Lei Nº 13.709, DE 14 de Agosto de 2018 (lei geral de proteção aos dados pessoais - LGPD).” (sic)
- R02 - “Geralmente são resoluções da própria [redacted], lei do estágio, etc.”. O nome da instituição foi suprimido.
- R05 - “Os requisitos legais ou regulatórios presentes nos sistemas são inerentes tanto ao regimento interno da instituição quanto nas leis de diversos órgãos municipais e estaduais. Algumas vezes, esse requisito fica explícito na aplicação para entendimento do usuário ou, até mesmo, o link para o documento oficial no qual o mesmo está inserido (a descrição da lei).” (sic)

- R06 - “"Dos sistemas que trabalhei, aquele que possuía maior presença e influência de requisitos legais foi o Autorizador de Notas Fiscais Eletrônicas (NF-e) da [redacted]. Um autorizador de NF-e implementa um manual de regras tributárias - emitido por um conselho técnico vinculado ao Ministério da Fazenda. Para mim, o principal desafio em trabalhar com requisitos legais é a forma como o requisito interage com o método de trabalho da equipe. Há pelo menos 20 anos, as equipes são incentivadas a trabalhar com técnicas ágeis, se aproximar do cliente dos produtos, a fim de - em parceria - refinar e aprimorar os requisitos de cada solução. Na minha experiência ao lidar com requisitos legais - a margem que a equipe de desenvolvimento tinha para criar e propor soluções - é muito pequena ou inexistente. Eu penso que em sistemas fortemente influenciados por normas legais seja comum que o debate sobre os requisitos tenha acontecido muito antes de seu conteúdo chegar pra equipe de desenvolvimento. Quando recebíamos as mudanças numa regra (ou novas regras), a portaria/lei/norma já havia sido assinada e/ou publicada. Nesse tipo de ambiente, o ágil pode continuar sendo utilizado, mas não existe espaço pra que a equipe possa de fato construir uma solução de forma dialética com o dono do produto.” O nome da instituição foi suprimido.
- R07 - “Na atual são todos baseados em leis do [redacted].
  Já no [redacted], existe uma gama de fatores que regulamentam o sistema, desde a cobrança de multas e juros que são diferentes de acordo com artigos e normas próprias.” Os nomes das instituições foram suprimidos.
- R09 - “O sistema automatiza processos da administração pública, logo, é gerido pelas leis que definem como esses processos precisam acontecer. Além disso, também está sujeito a normativas gerais para desenvolvimento de sistemas, como Lei Geral de Proteção de Dados, Lei de Transparência, exigências de acessibilidade, entre outras.” (sic)

Considerando os sistemas de informação sob gestão dos respondentes, foram perguntados quais eram **os instrumentos e as evidências de conformidade legal e regulatória**. Foi verificado que os respondentes não possuíam instrumentos ou estratégias para evidenciar a conformidade legal e regulatória, que não fossem os documentos textuais ou as homologações feitas. Dessa forma, pode ser entendido que os diferentes artefatos produzidos após a fase de elicitação e, por conseguinte, os sistemas computacionais oriundos dessas especificações ficavam fragilizados à ruptura da conformidade legal e regulatória a qualquer momento. Exemplos foram listados a seguir:

- R01 - “Sempre que necessário, incluímos referências à legislação em nossos relatórios. No caso da LGPD, uma evidência clara de cumprimento da conformidade legal também pode ser notada com a ocultação de informações sensíveis nos relatórios e sistemas que produzimos (mascaramento dos dados).” (sic)
- R06 - “No caso da NF-e, a norma é editada por um comitê técnico vinculado ao [redacted] no formato de um manual. O manual é divulgado publicamente no portal nacional da nota fiscal eletrônica.” O nome da instituição foi suprimido.
- R08 - “As resoluções.” (sic)
- R09 - “A especificação de casos de uso informa os requisitos legais utilizados como base na construção da funcionalidade (apenas quando ela foi criada para atender um requisito legal específico).”
- R13 - “Não há um instrumento formal, neste caso são estabelecidos critérios de aceitação nas histórias de usuário para atender os requisitos de conformidade legal ou regulatória, quando aplicáveis!” (sic)
- R14 - “homologação com o cliente” (sic)

Para a pergunta sobre **ter sofrido ou participado de alguma auditoria** no âmbito dos sistemas computacionais em que trabalhava ou trabalhou, dois respondentes sofreram e outros dois participaram de auditorias. No entanto, os dez respondentes restantes não sofreram ou participaram de auditorias. A seguir, o relato dos respondentes que sofreram ou participaram de auditorias.

- R06 - “Apenas auditorias internas. No caso da [redacted], entre 2014 e 2017 tínhamos um setor interno responsável por monitorar a qualidade do processo de desenvolvimento. Essa auditoria avaliava as evidências produzidas pelos projetos (principalmente requisitos e testes) e os indicadores de produtividade (prazo e custo dos projetos). Os gerentes de projetos eram obrigados a submeter seus projetos à auditoria e as não-conformidades apontadas podiam gerar ações corretivas (com impactos diversos).” O nome da instituição foi suprimido.
- R08 - “Não diretamente. Recebemos pedidos de relatório para justificar retornos às auditorias realizadas nos setores da [redacted].” O nome da instituição foi suprimido.

- R09 - “Por se tratar de um sistema que controla o patrimônio de instituições públicas federais (dentre outras coisas), já sofremos auditorias de órgãos controladores ([redacted], [redacted]) para avaliar como esse controle é realizado, quais informações são armazenadas e consultadas e se o sistema está seguindo o exigido por esses órgãos. A auditoria foi mais focada na instituição que utiliza o sistema do que no sistema em si.” Os nomes das instituições foram suprimidos.
- R13 - “Nunca sofri auditoria in loco, mas já participei de vários ciclos de autodiagnóstico sobre governança de TI do [redacted] e o [redacted] ([redacted]).” Os nomes das instituições e os índices foram suprimidos.

6.2.2 Resultados da análise das respostas à entrevista

A apresentação feita para entrevista foi de suma importância para os respondentes, visto que todos procuraram contextualizar em suas instituições os termos, os conceitos e os exemplos relacionados com as fontes, os requisitos legais ou regulatórios, a conformidade legal e regulatória. Aproveitando o espaço para sanar dúvidas de situações reais vivenciadas em seus cotidianos. Além disso, houve respondentes identificando problemas em suas metodologias, seus processos e sistemas computacionais produzidos durante essa etapa da avaliação do *Framework.*

Foi interessante observar que intervenções feitas acerca das temáticas desta pesquisa, em uma fábrica de *software*, vêm produzindo resultados relevantes com relação à conformidade legal e regulatória. É fato que, os avanços ao longo dos últimos quatro anos, poderiam ser maiores, todavia, considerando que não havia nenhuma preocupação, é um ganho diferenciar, promover um tratamento especial, e rastrear os requisitos legais ou regulatórios.

As identificações dos respondentes continuaram sendo feitas pela letra “R” e um número sequencial para fins de manutenção da privacidade e anonimato.

O elemento “**Classificação e Ordenação de Hierarquia Legal**” do *Framework* teve sua funcionalidade questionada aos respondentes sobre a facilidade na identificação da hierarquia das fontes legais ou regulatórias a serem atendidas. Para todos os respondentes a resposta foi afirmativa, sendo que para alguns respondentes tornava o encaminhamento mais intuitivo, ajudava também na solução de conflitos e nas buscas por outras fontes legais ou regulatórias. Por outro lado, um respondente deixou claro, que na sua visão, o usuário precisaria de alguma expertise na área de Direito. Alguns exemplos das falas dos respondentes:

- R01 - “Sim, é importante para tirar o conflito.” (sic)
- R04 - “Ele facilita sim… Você tem essa informação claramente no *Framework*.” (sic)
- R05 - “Sim, facilita… no caso, ele me ajuda entender quais leis estão relacionadas a certo requisito e usar essas leis para armazenar requisitos semelhantes ao que eu estou elicitando… mapear as leis que estão relacionadas a um requisito e, porventura, a futuros requisitos.” (sic)
- R06 - “Eu entendo que a abordagem que você utilizou é intuitiva. Ele ajuda sim, mas ela exige uma certa familiaridade do usuário com o tema (e o tema é o Direito). A hierarquia legal não é a geográfica… existem temas de atuação concorrentes… se isto tudo não estiver entendido você pode dar um sistema perfeito que o usuário vai usar errado… é do Direito… sua solução exige um certo nível de entendimento do Direito, mas eu reafirmo que os níveis hierárquicos que você colocou, eu achei isso adequado… deu vontade de ver o sistema… o caminho que você está seguindo é excelente.” (sic)
- R07 - “Sim, por isso que eu comentei que no [redacted], nós usávamos dentro do código e não resolvia, e aqui onde estou trabalhando agora está tudo no Confluence (JIRA)… não é fácil achar, mas tem as modificações, quem alterou, porquê alterou… facilita muito…” O nome da instituição foi suprimido.

O melhoramento do planejamento das *sprints* de um projeto de um sistema computacional a partir do elemento “**Qualificação de Vigência Legal**” do *Framework* foi indagado aos respondentes. A resposta foi que haveria melhoria até para priorização. Um respondente ponderou que, para sprints mais curtas, como era o caso em que atualmente trabalhava, apenas parcialmente para situações próximas. Assim, seguem das respostas:

- R01 - “Com certeza, eu ia fazer esse comentário durante a apresentação. Você pode priorizar de outra forma.” (sic)
- R03 - “Sim, e muito… principalmente quando temos que justificar o porquê determinadas demandas passaram na frente.” (sic)
- R04 - “Sim, com certeza… é importante para priorização e até colocar em produção, então você tendo isso ajuda sem dúvidas.” (sic)
- R05 - “Acho que não, pois o planejamento é feito das sprints mais recentes… é muito difícil ter uma lei que vai alterar sprint, mas pode acontecer… havendo ajuda sim… havendo uma data que uma lei seja extinta sim… se for algo próximo, sim... senão não tem como saber de algo que vai alterar e se vai ajudar… parcialmente sim.” (sic)

- R06 - “Sim… certamente… a vigência é importante para decidir não só a data da implementação, mas também de implantação… ele serve para planejar o ciclo de implementação de desenvolvimento quanto também o ciclo de implantação das versões…” (sic)
- R07 - “Sim, mas eu fico com um questionamento… e quando são vigências temporárias? Como eu veria isso? Eu queria saber como seria o match…” (sic)
- R13 - “Não se cairia, no velho viés do que é mais fácil de se implementar.” (sic)
- R14 - “Facilitaria a priorização com relação ao backlog.” (sic)

O elemento “**Catalogação de Termos**” apresentado para os respondentes teve sua funcionalidade questionada quanto ao seu auxílio no entendimento dos termos utilizados nos documentos do ciclo de vida de um sistema computacional. Os respondentes foram unânimes em afirmar positivamente o auxílio, como pode ser observado nas respostas a seguir:

- R01 - “Acho que sim, pois inclui informações jurídicas e da área. Até agiliza depois o próprio desenvolvimento. Quanto mais a turma que está implementando ali entender os termos jurídicos, coisas que são externas à equipe mais se organizando.” (sic)
- R03 - “Muito! Um ponto que sofremos muito é entender os termos jurídicos… para um novato que acaba de chegar na empresa… é uma forma de reduzir a curva de aprendizado em processo Scrum… isso é muito importante.” (sic)
- R04 - “Sim, porque imagino que pessoas mais antigas na equipe já irão saber, mas as pessoas não são eternas… chega gente nova… precisa até mesmo para manter a consistência… o conhecimento compartilhado entre todo mundo da equipe… até para treinamento de novas pessoas na equipe.” (sic)
- R06 - “Sim… perfeito… talvez não seja tão essencial… eu entendo que seu *Framework* tem uma essência que não esse elemento… esse módulo é muito útil… a essência do seu *Framework* são esses pilares, o monitoramento das fontes… aí é a espinha dorsal…, mas é importante também.” (sic)
- R07 - “Era o que eu mais iria usar! Eu cheguei a consultar a advogados de fora do [redacted]… eu não vou negar: quando passei a duvidar dos advogados, eu passei a ter um caderninho com os termos anotados, e utilizar a partir disso… assim como toda a equipe…, mas eu fiz do meu lado, pois os outros não estavam preocupados…” O nome da instituição foi suprimido.
- R08 - “A exemplificação ajuda muito no entendimento.” (sic)

- R09 - “A catalogação é fundamental." (sic)
- R10 - “A catalogação, o registro da forma como é feito me surpreendeu.” (sic)
- R14 - “A catalogação de termos facilita até o repasse de atividades e tarefas.” (sic)

A criação de **rastreabilidade** entre todos os artefatos relacionados com os requisitos legais ou regulatórios e as fontes legais ou regulatórias é feita no elemento “**Representação de rastreabilidade entre RLRT e FLR**”. Para alguns respondentes isto ajudaria, por exemplo, na manutenção, na tomada de decisão, nos possíveis impactos de uma alteração. Para outros, o custo e a complexidade são fatores críticos para sua realização, e o que talvez não compense o esforço. Fatos não corroborados por especialistas da área (GOTEL et al., 2012; ESPINOZA e GARBAJOSA, 2011; LUCIA e QUSEF, 2010; ALVES e ALVES, 2009). A exemplificação com as falas dos respondentes pode ilustrar essas observações:

- R01 - “Rastreabilidade ajuda quando você vai manter… você está diminuindo o seu trabalho futuro, mas no primeiro momento é só trabalho, depois quando se fazer alteração… acompanhar a evolução do sistema, do requisito é muito útil… quando se precisa saber o porquê um campo foi criado… uma lei estipulou que havia necessidade… e na manutenção, mas no desenvolvimento é só trabalho.” (sic)
- R02 - “A rastreabilidade é muito difícil de ser feita. É a maior dificuldade que tenho até hoje. O *Framework* fazendo isto por mim seria muito importante para saber onde encontrar o que se procura…” (sic)
- R04 - “Na tomada de decisão… na auditoria para verificar a conformidade." (sic)
- R05 - “Auxilia a conhecer possíveis impactos nos requisitos… como nas alterações das leis, eu tenho como saber quais os requisitos podem ser impactados por elas. Da mesma forma que se estiver modificando um requisito, eu vou poder verificar com essa lei… então vale tanto para ida quanto para volta… se mudar uma lei quanto requisitos serão impactados, e se eu alterar um requisito quantas leis eu posso contradizer… então terei que ter mais cuidado.” (sic)
- R06 - “Sim, sim... perfeito… eu entendo que nos dois exemplos que você mostrou no final eu produzo um quadro e, sobretudo no segundo, eu tenho um histórico da fonte à esquerda e à direita o detalhe daquela fonte que tem a ver com o meu tema… esse quadro que você produz, ele é o principal produto do seu trabalho… todo esse trabalho do *Framework*, ele está muito em função desse quadro… eu acredito com você que um dia vamos ver esse sistema completo, e aí vai ficar mais fácil entender os múltiplos valores

que ele tem… esse quadro sobretudo muito importante. A vigência e a rastreabilidade são, que se o tempo lhe obrigar, o núcleo, a essência são esses elementos, então os módulos de termos e exportação podem ser deixados, pois eles são a espinha. A espinha, a essência do desenho, e que faz ele importante são os pilares, a atenção com a vigência, os elementos que fazem a rastreabilidade…" (sic)

- R07 - "Pode ficar complexo… a lei pode cair… e tenho que lembrar de ajustar… pode facilitar até certo ponto e a partir de um determinado tempo complicar pensando nas metodologias ágeis… eu não vejo como a "bala de prata" ... pode acontecer de depois de muitas interações, a documentação ficar extensa… como já aconteceu eu li o início de uma documentação, e pulei para o final… quando eu percebi, eu tinha cometido um erro, porque não li a documentação inteira…" (sic)
- R08 - "Criar a rastreabilidade no *Framework* não parece ser tão simples… é muito demorada…" (sic)
- R09 - "Fiquei muito interessado no rastreamento das leis dadas às mudanças… a rastreabilidade seria o principal ganho…" (sic)
- R11 - "Minha preocupação é com o custo… Quanto tempo levaria a mais…" (sic)

A **sustentabilidade** dos sistemas computacionais, a partir do **reuso** das fontes legais ou regulatórias e dos requisitos legais e regulatórios, possibilitada pelo elemento "**Representação de rastreabilidade entre RLRT e FLR**" foi apontada como uma vantagem a mais do *Framework*. Quando questionada a forma que isto poderia auxiliar no cotidiano dos respondentes, foi possível perceber que cada um buscou uma perspectiva diferente para responder esta questão, como exemplificado a seguir:

- R07 - "Volta ao mesmo ponto que eu já falei: eu teria todos os pontos rastreados e auxiliaria uma auditoria…" (sic)
- R08 - "Reuso e versionamento são vantagens… sem retrabalho…" (sic)
- R10 - "Já houve situação que com o reaproveitamento pude criar uma nova ferramenta…" (sic)
- R12 - "É um ganho. Só em não ter que escrever o requisito em vários lugares…" (sic)
- R13 - "Torna o projeto escalável e sustentável…" (sic)
- R14 - "Auxilia reduzindo os pontos de manutenção…" (sic)

Aos respondentes foi perguntado se e como os elementos do *Framework* poderiam **melhorar o planejamento e as ações** no dia a dia deles. Foram levantadas diferentes possibilidades, como demonstrado nos relatos a seguir:

- R01 - “Evitar perda na organização… só não ajuda na velocidade…, mas sem o *Framework* teria que se fazer também, então com o *Framework* ajuda… se você tem que fazer é melhor com um conjunto de passos… ajuda na segurança… fica muito alinhadinho… é clássico mais seguro, mais lento.” (sic)
- R02 - “Gostei do que vi… Achei totalmente aplicável…” (sic)
- R03 - “Sim… Dá um norte… Ajuda muito a aprender sobre um sistema…”
- R04 - “Vão melhorar no sentido da auditoria… vão auxiliar na tomada de decisões, uma vez que eu tenho tudo aquilo... fontes alinhadas, requisitos… tudo ajustado em um único *template*, eu posso olhar… bater o olho, e tomar decisões… no planejamento, com relação a data mesmo… com relação à vigência com certeza saber minhas prioridades, o que colocar em produção e quando colocar em produção, dessa forma…”
- R05 - “O mais importante para mim foi relacionar os requisitos e as FLR… então você buscando os requisitos testável você está buscando se aproximar da funcionalidade… então você aproxima a lei da parte funcional… outra parte importantíssima foi o catálogo de termos, pois às vezes a equipe de TI é jovem… para um profissional jovem é difícil ler uma lei, uma norma… mesmo ela associada ao que está sendo feito… outro ponto é a vigência… o que pode ser feito para considerar uma lei ou não… e auditar uma norma… aproveitar um momento que você está elicitando um requisito e vai colocando os documentos da hierarquia legal e colocando na base legal da empresa, da instituição…” (sic)
- R06 - “Potencialmente está se criando uma técnica para esse trabalho que já se faz, mas se pessoas dentro de uma mesma autarquia fazem de forma diferente… instituições de mesmo nível fazem cada um ao seu modo… existe um potencial do Framework criar uma forma…” (sic)
- R07 - “Principalmente, com relação ao porquê eu fiz aquela alteração… eu teria a rastreabilidade… não em todos os pontos, mas principalmente naqueles relacionados com a lei…” (sic)
- R10 - “Entender a demanda…” (sic)
- R13 - “Possibilita entender o negócio na prática e tomar decisões…” (sic)

A utilidade do elemento "**Módulo de Conversão de Dados**" no cotidiano foi interrogada aos respondentes, para que fosse possível explorar o potencial desse elemento. Houve diferentes visões da importância e das possibilidades oferecidas, como podem contempladas, imediatamente:

- R01 - "Para desfrutar do potencial deste módulo, deveria haver uma padronização dos dados... ele minimizaria o trabalho de busca, mas tem que haver uma padronização…" (sic)
- R04 - "Com certeza… se eu tenho uma ferramenta que faça backup, e possa importar para outra ferramenta, algum outro sistema que esteja ativo na minha equipe, sem dúvida, espalhar as informações que eu utilizo… se eu quiser utilizar em outro projeto." (sic)
- R05 - "Uma forma de serviço de concentrar as normas associadas de diferentes órgãos, e facilitar o reuso…" (sic)
- R06 - "A sua solução é mais robusta com esse módulo, mas se o tempo lhe obrigar, abra mão desse módulo. Ele não é a essência da sua solução…" (sic)
- R07 - "Não vejo, pois eu trabalho com sistemas totalmente diferentes!" (sic)
- R10 - "Compartilhar as soluções com colegas…" (sic)
- R13 - "Criação de repositórios, comunidades de fontes (legais e regulatórias) comuns…" (sic)

As questões relacionadas à **privacidade** e à **segurança** foram também encaminhadas no elemento "**Capacitação conforme a Taxonomia dos Princípios Legais e Regulatórios**". Quando indagado se esse elemento seria capaz de auxiliar nestas questões, alguns respondentes tiveram dúvidas com relação ao termo "taxonomia". Doravante a explicação do termo, do elemento e do seu papel, ainda assim, houve respondente inseguro em sua resposta. Enquanto outros foram até enfáticos ao responder que sim, ou que atrapalharia o processo, mesmo sendo benéfico sua função. Isto pode ser visto nos exemplos listados:

- R01 - "Com certeza… dá mais segurança… a parte que eu mais vi é que evita que seja usada uma lei que não é lei…" (sic)
- R04 - "De fato vai ajudar na privacidade… vai me ajudar levar essa questão, mas se o sistema vai atender ou não, eu não tenho essa garantia…" (sic)

- R05 - “Passa a ser necessário a partir do ponto que você precisa ter sistemas de acordo com as leis… Vai mitigar a lidar com isso…” (sic)
- R06 - “Se eu tiver uma solução que permita a fazer a rastreabilidade das fontes e não atender essa taxonomia dos princípios legais e regulatórios, eu nada tenho… Sim, ele é tão essencial… ele faz parte do núcleo duro dessa solução…” (sic)
- R07 - “De privacidade sim, mas de segurança eu fico em dúvida… estando na Internet, tudo fica público… a LGPD está tentando esconder, mas quebrando o código você tem o acesso…” (sic)
- R09 - “A LGPD é a preocupação do momento… burocratiza o processo…” (sic)
- R10 - “Eu precisaria de uma capacitação para melhor entender e aplicar…” (sic)
- R12 - “A taxonomia me surpreendeu… Acho que sim… dá mais segurança…” (sic)

Foi inquirido aos respondentes se os elementos do *Framework* apresentado seriam suficientes para atender a demanda atual de artefatos para **planejamento, gerenciamento e manutenção da conformidade legal e regulatória**. As respostas foram ricas do ponto de vista que foram feitas até sugestões de melhorias, antes mesmo que fosse perguntado por essas. Os exemplos podem demonstrar isto:

- R01 - “Tá massa… é bem completinho… parece uma coisa que basta… apenas com a experiência para saber…” (sic)
- R03 - “Gostei do *Framework*… Tem coisas que eu nem havia pensado!” (sic)
- R04 - “Eu senti falta da verificação dos conflitos entre requisitos e entre leis…” (sic)
- R05 - “Não necessita de novos elementos…, mas em uma situação onde você vai mapear uma FLR você sabe quais os requisitos estão associados… assim como quando você vai alterar um requisito… você precisa saber quais leis você vai infringir… então eu acho que precisa de um passo para remapear se houve alterações nas FLR…” (sic)
- R06 - “As características, que eu me lembro como essenciais de um requisito legal, aparecem no seu desenho… são atendidos pelo *Framework*… sua solução é muito abrangente… os requisitos legais são visíveis e bem representados no *Framework* que você está me apresentando.” (sic)
- R07 - “Aparentemente, sim, mas eu não tenho certeza… numa experiência eu implementei o MVP antes de verificar as leis relacionadas e, ao final, eu não tinha atendido oito leis… isso inviabilizou a continuidade do projeto, porque eu perdi para a

concorrência… talvez tenha que ter algo que obrigue antes de começar a implementação, a pesquisa de leis e regulamentos…" (sic)

- R08 - "Fiquei impressionada com a completude do trabalho… não acrescentaria mais nada…" (sic)
- R09 - "A longo prazo têm que valer a pena…" (sic)
- R10 - "Melhoraria a documentação de uma forma geral… o estudo do Direito é disperso… Eu gostaria ter uma consulta, uma busca automatizada como recurso…" (sic)
- R11 - "Poderia haver uma apresentação para as equipes sob minha gestão?" (sic)
- R12 - "Eu gostaria que houvesse uma apresentação para [redacted]…" (sic) O nome da instituição foi suprimido.

Com uma possível inserção do *Framework* na rotina das equipes, foram questionados quais **benefícios ou malefícios** poderiam ser presumíveis. Com relação aos benefícios, a rastreabilidade e a conformidade com as leis e a regulação foram as mais indicadas. A preocupação com o tempo e o custo a mais foram os mais citados, como malefícios no ciclo de desenvolvimento, manutenção e evolução de um sistema computacional. Seguem alguns exemplos de falas dos respondentes:

- R01 - "Malefício é a velocidade do desenvolvimento. Você vai perder tempo, mas os benefícios seriam melhor entendimento do que se está desenvolvendo, pois você vai olhar para empresa, para o domínio, para a legislação, para a sociedade… você consegue levar para outros sistemas e para outras empresas… você consegue ter uma visão geral, mais ampla dos limites, barreiras… você desenvolve com mais segurança e dizer que você segue as leis… evita perda financeira, de reputação, multa ou processos por perda de dados, vazamento… você ganha esse tempo depois… e tem a questão dos dados sensíveis…" (sic)
- R02 - "O transtorno passa, e o benefício fica…" (sic)
- R04 - "Como benefícios: a facilidade do rastreio, a facilidade da verificação da conformidade legal… isto vai facilitar bastante… e malefício, eu diria… eu acho que talvez esse passo a mais de criar a documentação, mas existem certos malefícios que é melhor você ter, porque você está guardando informação, que vai lhe ajudar no futuro… é melhor do que não ter… é uma coisa que vai acontecer a equipe vai precisar ter, então a manutenção disso talvez gere algum custo, mas é um custo que se não tivesse, numa questão de auditoria, o custo poderia ser muito maior… não sei como agilizar o cadastro

dessa informações… talvez a manutenção seja mais fácil… mas é custo que no futuro será benéfico…" (sic)

- R05 - "Benefícios, como eu disse algumas duas ou três perguntas atrás, são: mapear as leis, mapear quais leis podem ser contraditas com um requisito… esse é um ponto mais importante que vai ajudar a mitigar os erros da análise de requisitos. Quanto aos malefícios, é mais com relação ao tempo que vai ser necessário para atender isso… uma dificuldade é, numa equipe Scrum, vai ser o P.O. que vai alimentar essas bases… um apoio seria o cliente se envolver… talvez um passo de validação… talvez seria um atributo de validação… envolvimento do cliente…" (sic)
- R06 - "É complementarmente aproveitável nas instâncias em que produz os requisitos e trata dos requisitos… é uma ferramenta adequadíssima nestas instâncias… os lugares onde o tempo já escasso talvez isso traga um problema… fora essa ressalva só vejo benefícios." (sic)
- R07 - "Iria trazer benefícios, mas muitas brigas como malefícios, pois a equipe no [redacted] não é muito maleável, então adoção por completo seria difícil, e começariam a atrasar as entregas…" O nome da instituição foi suprimido.
- R11 - "Minha preocupação é com o custo, a especialização dos analistas e o tempo que se levaria a mais…" (sic)

Foi perguntado **se algo havia decepcionado** aos respondentes, estes foram unânimes em responder que não, todavia houve ressalvas em suas colocações. As ressalvas foram as seguintes:

- R01 - "Nada… senti falta de código, implementação, mas entendo que é uma pesquisa extensa…" (sic)
- R04 - "Não… não teve nenhum momento que eu pensei isso não tenha nada a ver, talvez alguém da área de Direito pudesse agregar, mas na minha visão da área de TI não tive nenhuma decepção… está muito claro e muito útil naquilo que ele faz e naquilo que ele ajuda…" (sic)
- R05 - "Nada… mas vejo a necessidade da parte jurídica… seria importante ajudar a interpretar, a consolidar o entendimento das normas… seria crucial…" (sic)
- R06 - "Eu esperava um *framework,* e você tem muito mais do que um *framework*… Quando eu entendi que você tinha muito mais que *framework,* aí dá vontade de ver muito mais… eu queria ver o modelo de dados, telas… não é isso… você tem muito

mais, mas foca na sua essência e, talvez naquela periferia que é bem-vinda… então assim, a expectativa pessoal foi… eu fiz um exercício pessoal de resgatar a memória… o diálogo foi excelente…" (sic)

- R07 - "Não… como eu vim aberto para ouvir para saber se adotaria ou não…" (sic)
- R09 - "Não, mas encontrar as leis seria muito difícil para mim…" (sic)

Com relação a **algo ter surpreendido**, os respondentes destacaram possíveis benefícios e a possibilidade de já pôr em prática alguns dos encaminhamentos dados durante a apresentação. Existiu também quem elogiou a forma como foram engendrados os elementos para composição do *Framework*. A seguir, alguns exemplos de respostas:

- R01 - "Descobrir o quanto é importante, e que o *Framework* ataca isso… Algo como você não está sozinho… tenho que desenvolver um sistema em conformidade com a lei, e tendo o *Framework* você nem precisa aprender tudo é só seguir esse conjunto de passos… você vai ficar tranquilo…" (sic)
- R02 - "Abriu a minha mente…" (sic)
- R03 - "Tenho interesse em utilizar…" (sic)
- R04 - "Sim… pela simplicidade… pude entender perfeitamente como ele funciona." (sic)
- R05 - "A completude… mapear FLR, mapear os requisitos… tanto na ida como na volta… quais os requisitos serão impactados numa mudança da FLR. Quanto na vigência de FLR, se um requisito vai ser impactado…" (sic)
- R06 - "O conteúdo que você tem é muito mais do que um *framework*… este assunto é interdisciplinar, ninguém isoladamente é capaz de fazer, de produzir esse conteúdo que você tem aí… tanto que esse conteúdo não existe… tanto o cara de TI não consegue fazer sozinho… o cara do Direito também não… o auditor também não… imagino que esteja sendo muito doloroso fazê-lo por causa disso, mas alguém iria fazer… tem um conteúdo muito denso e promissor… você tem um conteúdo grande, complexo, muito abrangente…" (sic)
- R07 - "O módulo da rastreabilidade… é módulo aonde você vai "linkar" e prever as relações com diferentes leis e até as leis internacionais…" (sic)
- R10 - "A uniformização de processos…" (sic)
- R12 - "Já foi aplicar alguns conceitos nas minhas práticas…" (sic)

Agora, com relação ao momento que houve **maior dificuldade em entender o *Framework***, e a que poderia ser atribuída esta dificuldade, a maioria dos respondentes relatou a dificuldade com os termos utilizados. Dúvidas que foram esclarecidas, pontualmente, quando perguntado explicitamente, ou, como alguns disseram ao longo da apresentação e da exemplificação da aplicação do *Framework* em casos hipotéticos. Alguns relatos são explicitados a seguir:

- R01 - "Na parte da hierarquia… as relações… um ponto que um verbo pode alterar o que tem que ser feito… lei é fogo… entender a lei, que parte é um requisito… Ah! Taxonomia… esse termo não é comum para mim, mas quando você explicou eu entendi…" (sic)
- R02 - "A taxonomia foi difícil de entender… Acho que foi por conta da nomenclatura…" (sic)
- R03 - "Inicialmente, com os termos utilizados… depois fui entendendo melhor…" (sic)
- R04 - "Os quatro elementos de baixo por eu não ser da área de Direito, mas com a sua explicação eu pude entender." (sic)
- R05 - "A falta de conhecimento prévio do que seria alguns termos, mas com a explicação eu entendi…" (sic)
- R06 - "Quando você falou no e-mail que trataria de um *framework*, eu esperava um simples *framework*." (sic)
- R07 - "O segundo exemplo foi mais complicado… provavelmente, por eu não conhecer o Marco, apesar de ser da área… tinha muitas entradas, e eu não consegui relacionar com outras experiências, assim como aconteceu com o primeiro exemplo…" (sic)
- R08 - "Os exemplos clarificaram as explicações…" (sic)
- R10 - "Os termos mais teóricos foram difíceis, no início… mas com os exemplos, eu entendi…" (sic)
- R12 - "Os termos, inicialmente, me dificultaram o entendimento, mas com a explicação foi tudo resolvido…" (sic)
- R13 - "Os subprocessos para classificação… Talvez minha falta de experiência…" (sic)

Quando questionados sobre sugestões para o **melhoramento do *Framework***, os respondentes citaram: a inclusão de diagramas e a utilização de princípios de Gestalt para visualização (R04); a criação de um guia para explicar os elementos do *Framework*, profissionais com certa experiência em interpretar leis e conhecer as formas da lei, e a

catalogação dos termos ser concomitante (R05); aplicar o *Framework* em outras instâncias, como especialistas e equipes de preparação do requisito, os diferentes níveis de usuários, e a necessidade do usuário possuir certa experimentação na área jurídica (R06), sugestão similar à de R05; uniformização dos elementos (R10); apresentação do Framework para sua equipe de trabalho (R11, R12); incluir o tratamento dos requisitos legais ou regulatórios apenas após a obtenção do MVP - *Minimum Viable Product* (R13). Isso contraria a experiência de R07, que foi tratar as questões legais após a apresentação de um projeto a partir do MVP. Esse foi perdido pela falta de observância das questões legais e regulatórias, como explicitado em seu relato.

6.4 Limitações e ameaças à validade

O fato de o *Framework* ser conceitual impediu a aplicação deste em ambientes conhecidos como fábrica de software. Por esse motivo, foram escolhidos instrumentos, questionário e entrevista, como forma de realizar uma pesquisa qualitativa, e obter as primeiras impressões do público-alvo deste *Framework*. Entretanto, isto exigiu dos respondentes certo grau de abstração e contextualização do seu uso em suas instituições no desempenho de suas atividades cotidianas.

Alguns termos utilizados nesta pesquisa também eram novos para esses respondentes, como fontes legais ou regulatórias, rastreabilidade, visualização da informação, hierarquia legal e regulatória, vigência legal. Posto isto, em alguns casos, além da apresentação realizada a todos os respondentes, foi necessário definir os termos e exemplificar com o contexto de uso para os respondentes.

Foram considerados os autores Travassos, Gurov e Amaral (2002), Wainer (2007) e Wieringa (2014) para identificar, mitigar as ameaças à validade da avaliação realizada, todavia algumas ameaças ainda poderiam influenciar nos resultados obtidos. Assim, com relação à validade interna, o desenho dos instrumentos e a experiência de alguns participantes pode ter influenciado com relação à testagem, visto que os instrumentos, de certa forma, poderiam beneficiar os respondentes mais experientes nas temáticas relacionadas à pesquisa. Em contrapartida, a maturação e a expectativa desses mesmos respondentes mais experientes puderam ter se sentido desmotivados durante a utilização dos instrumentos.

Com relação à validade externa, mesmo havendo a preocupação de selecionar participantes do público-alvo desejado, houve a necessidade de descartar duas participações

pelo fato de estarem mais exercendo cargos/funções não compatíveis ao perfil definido. Igualmente, ainda há ameaça relacionada ao tempo.

6.5 Discussão e considerações

O *Framework* mostrou-se bem estável na versão apresentada aos respondentes, visto que, na opinião desses respondentes: i) o *Framework* auxilia na identificação das fontes legais ou regulatórias e dos requisitos legais ou regulatórios de um sistema computacional; ii) promove a sustentabilidade dos sistemas computacionais a partir do reuso das fontes legais ou regulatórias e dos requisitos legais ou regulatórios; iii) que os elementos do *Framework* podem melhorar o planejamento e ações do dia a dia; e iv) esses elementos são suficientes para atender a demanda atual de artefatos para planejamento, gerenciamento e manutenção da conformidade legal e regulatória.

Com relação a quais benefícios ou malefícios a inserção do *Framework* na rotina da equipe pode trazer, foram citados como benefícios: melhor entendimento do produto/serviço; facilidade do rastreio de todo o sistema; facilidade da verificação da conformidade; auditorias facilitadas e maiores chances de sucesso; mapeamento facilitado das fontes legais e regulatórias e dos requisitos legais e regulatórios; mitigação dos erros de análise dos requisitos; reuso e sustentabilidade em todo ambiente de desenvolvimento e manutenção - redução do retrabalho; catalogação de todos os termos e apropriação desses pelas equipes; facilidade de repasse para membros de outras equipes ou treinamento de novos membros; clareza, padronização, rastreabilidade e versionamento de todos os artefatos; documentação de todas as decisões das equipes e de todas as imposições legais e regulatórias; uniformização dos processos; integração dos requisitos como alma do negócio; solução adaptável e escalável; evolução como propósito; visualização contextualizada (para quem e quando); tratamento de dispositivos (legais e regulatórios) efetivos e temporários; interoperação de dados e de ambientes; e flexibilidade de implantação e uso do *Framework.*

Já com relação aos malefícios, a questão do tempo gasto na documentação foi quase unânime, sendo que para alguns respondentes isto seria compensado no futuro quando houvesse a necessidade de treinamento de novos membros da equipe; atualização de requisitos ou fontes legais ou regulatórias durante o ciclo de vida do sistema; compartilhamento de bases entre organizações; em processos de auditoria, por exemplo. Outros malefícios citados foram

velocidade de desenvolvimento prejudicado; esforço para manutenção das informações; custo de produção e de tempo aumentados; dificuldade de levantamento de todas as fontes legais e regulatórias de forma mais automatizada; e maior especialização do analista.

Com relação aos objetivos específicos foi possível apurar que, considerando as respostas dos participantes: i) o *Framework* facilita a identificação da hierarquia das fontes legais ou regulatórias a serem atendidas; ii) o modelo de vigência ajuda a planejar melhor as sprints de um projeto de um sistema computacional; iii) o modelo de termos auxilia a equipe a entender termos utilizados nos documentos aplicados no ciclo de vida de um sistema computacional; iv) a criação de rastreabilidade proposta entre todos os artefatos relacionados com os requisitos legais ou regulatórios e as fontes legais ou regulatórias pode ser útil de diferentes formas, como na atualização e manutenção dos artefatos, na tomada de decisões pela equipe, na verificação da conformidade legal e regulatória; v) o modelo de exportação de dados será útil no seu dia a dia, principalmente, no que se refere a interoperabilidade de dados e ambientes, e manutenção das informações contidas no *Framework*; vi) a taxonomia utilizada como base ajuda a orientar questões de privacidade e segurança, mas não as resolver; vii) o reuso e a sustentabilidade não eram práticas das instituições da maioria dos respondentes, entretanto todos viam como ganho essas práticas oferecidas pelo *Framework*, como agilidade e padronização no desenvolvimento, menor esforço para manutenção por exemplo; viii) houve diferentes benefícios e malefícios citados pelos respondentes com a inserção *Framework* em suas equipes de trabalho.

Ressalta-se que alguns respondentes ficaram interessados no resultado desta pesquisa, e pediram para serem comunicados dos resultados. Outros respondentes mostraram-se propensos a utilizarem em suas instituições a solução implementada a partir do *Framework* proposto e apresentado na fase das entrevistas. Foi destacado ainda o carácter informacional e instrutivo que a apresentação e o *Framework* tiveram para esses profissionais.

A avaliação feita com alguns representantes do público-alvo permitiu maior entendimento do uso e da aplicação em ambiente do tipo fábrica de *software*, e de melhorias que podem ser aplicadas ao *Framework* proposto por esta pesquisa. Algumas dessas melhorias foram incorporadas na versão final do *Framework* (apresentada no Capítulo anterior), outras como estavam relacionadas às metodologias utilizadas nas organizações ficaram como sugestões aos participantes e aos possíveis usuários da solução.

No próximo capítulo, são tecidas as considerações finais desta pesquisa.

7 Considerações Finais

Contemplando a problemática exposta no Capítulo 1, que está relacionada ao tratamento dos requisitos legais ou regulatórios de forma a manter a conformidade legal e regulatória, bem como auxiliar o processo de auditoria e agências reguladoras ou fiscalizadoras, entende-se que o *Framework* criado e seus artefatos podem ser uma solução viável. Suprimindo ou minimizando os esforços dos interessados no processo de desenvolvimento e no ciclo de vida de um sistema computacional em toda sua complexidade de implementação, manutenção e evolução. Lembrando que, atualmente, as fábricas de *software* não possuem o interesse exclusivo de comercializar somente o produto e, sim, a solução, que inclui os serviços, a evolução relacionada aos sistemas computacionais oferecidos.

Para melhor entender o universo, foi fundamentada (Capítulo 2 - Fundamentação Teórica) a pesquisa nos termos, que seriam basilares para tal propósito. Enquanto, no Capítulo 3 - Revisão Bibliográfica da Literatura, buscou-se o estado da arte considerando o foco do momento que era requisito, conformidade legal e regulatória em ambiente ou utilizando metodologias ágeis, que até então poderia modificar o contorno da pesquisa em andamento. Com as análises feitas, persistia a dúvida se faria alguma diferença para o *Framework* a ser criado naquele momento estar instanciado em um nicho de tipos de metodologias tradicionais ou ágeis.

Com esta dúvida, partiu-se para a realização de estudos exploratórios de diferentes abordagens (Capítulo 4 - Estudos Exploratórios) e, logo nas primeiras interações ao tratar com fábricas de *software* em processo de adoção ou transformação ágil, foi possível perceber que o *Framework* poderia ser algo a parte desde que algumas premissas/orientações fossem seguidas, como efetivos pilares para construção de sistemas computacionais em conformidade legal e regulatória.

Assim, o *Framework* (Capítulo 5 - *Framework*) pode ver o sistema computacional, seu processo de desenvolvimento, artefatos, arquitetura e infraestrutura como algo independente. Os seus elos seriam formados apenas por alguns identificadores entre os requisitos legais ou regulatórios, e algumas informações que podem auxiliar o processo de manutenção da busca por novas fontes do domínio ou contexto que o sistema esteja inserido.

Para verificar que os elementos deste *Framework* poderiam corresponder às necessidades informacionais e à conformidade legal e regulatória, foram realizadas avaliações junto a representantes do público-alvo (Capítulo 6 - Avaliação do *Framework*). Os instrumentos utilizados foram um questionário, uma apresentação e entrevistas com as pessoas, em um total

de 14, que se disponibilizaram a participar deste processo. Foi interessante desenvolver e observar que a narrativa construída pode também ampliar conhecimentos e alertar para os problemas da inconformidade legal e regulatória nos ambientes aos quais os respondentes estavam imersos. Além disso, claro, obter impressões e saber quais seriam as adequações fundamentais na visão dos respondentes para real implantação dos elementos do *Framework* proposto, foi de suma relevância, para que fossem realizados os ajustes necessários.

7.1 Contribuições a serem destacadas

A principal contribuição desta pesquisa foi um *framework* flexível às metodologias utilizadas pelas fábricas de *software*, que pode possibilitar a promoção e a manutenção da conformidade legal e regulatória. Este propósito está fundamentado a partir da proposta do uso de determinados artefatos, das técnicas de rastreabilidade e visualização da informação, de identificação de fontes legais e regulatórias para engenharia e documentação de requisitos legais ou regulatórias, e de possibilitar a existência de evidências legais e regulatória nos sistemas computacionais.

Assim, podem ser citadas algumas contribuições produzidas por esta pesquisa:

i) levantamento do estado da arte e da indústria na engenharia de requisitos legais ou regulatórios;

ii) identificação dos principais desafios relacionados à conformidade legal e regulatória dos sistemas relatadas na literatura;

iii) considerando a literatura, identificação das principais estratégias utilizadas pela comunidade no tratamento das temáticas abordadas (fontes e requisitos legais ou regulatórios, artefatos, metodologias ágeis de desenvolvimento, conformidade legal e regulatória);

iv) definição de estratégias para transformação de fontes legais ou regulatórias em requisitos legais ou relatórios e, estes por sua vez, em requisitos testáveis;

v) identificação e promoção das evidências legais e regulatórias a serem produzidas em cada etapa do processo de desenvolvimento, manutenção ou evolução dos sistemas computacionais;

vi) resultados de entrevistas realizadas com os interessados em diferentes situações e etapas do processo de desenvolvimento, manutenção e evolução de sistemas computacionais e, também algumas destas como colaboração em outras pesquisas;

vii) resultados de etnografia organizacional realizada em parceria com outros pesquisadores;

viii) definição de *framework* para promoção e manutenção da conformidade legal e regulatória;

ix) avaliação com representantes do público-alvo do *framework* para validação e verificação da proposta e evolução dos elementos, que compõem este *framework*.

Além disso, foram investigadas as estratégias adotadas pelos analistas/engenheiros de requisitos em equipes agilistas, e a forma de realizar a rastreabilidade dos requisitos legais ou regulatórios pelas equipes agilistas. Dessa forma, puderam também ser apresentados os artefatos utilizados para documentação e gerenciamento dos requisitos legais ou regulatórios, e especificar formas alternativas que melhorem a recuperação dos artefatos relacionados com os requisitos legais ou regulatórios. Alternativas foram oferecidas para evidenciar a conformidade legal e regulatória dos sistemas computacionais e, além disso, facilidades na manutenção e evolução desses sistemas sem que isto seja traduzida em inconformidade legal ou regulatória.

Todavia, não seria possível se não houvesse sido feita a Revisão Sistemática da Literatura (Capítulo 3), que trouxe um resumo do esforço da comunidade acadêmica e industrial para alavancar ou melhorar o tratamento das fontes legais ou regulatórias, e a energia gasta por toda a sociedade para manter seus sistemas computacionais em conformidade com tudo e, agora, mais do que nunca com essas fontes legais ou regulatórias de forma legítima e condizente com a Sociedade 5.0, que se deseja ser.

7.2 Publicações decorrentes do processo de doutoramento

Ao longo desse período de doutoramento, foi possível realizar diferentes colaborações, que resultaram em trabalhos de pesquisa e, consequentemente, seus resultados foram publicados em diferentes veículos de divulgação científica. Inclusive o artigo intitulado de "Aplicação da Etnografia no Contexto de Fábrica de *Software* na Perspectiva da Engenharia de Requisitos" recebeu o prêmio de *best paper* da conferência. A seguir são listados os mais recentes resultados:

- Artigos completos publicados em periódicos:

SOUZA, L. T. M.; MIRANDA, E.; LUCENA, M.; GOMES, A. Desafios e Práticas da Engenharia de Requisitos no Contexto de Fábrica de Software com foco na Documentação e Gestão do Conhecimento. Cadernos do IME-Série Informática, v. 42, p. 98, 2019. https://doi.org/10.12957/cadinf.2019.47530, v. 42, p. 98, 2019.

PENHA, F.; MIRANDA, E.; LUCENA, M.; LUCENA, L.; ALENCAR, F.; SÁ FILHO, C. Actor's social complexity: a proposal for managing the iStar model. JOURNAL OF SOFTWARE ENGINEERING RESEARCH AND DEVELOPMENT, v. 6, p. 1-11, 2018.

- Trabalhos completos publicados em anais de congressos:

SOUZA, L.; MIRANDA, E.; LUCENA, M; A. GOMES. Aplicação da Etnografia no Contexto de Fábrica de Software na Perspectiva da Engenharia de Requisitos. In: Workshop de Engenharia de Requisitos, 2019, Recife. WER 2019, 2019. v. 1. p. 1-10. (Prêmio de best paper da conferência).

EPIFÂNIO, J. C.; MIRANDA, E.; TRINDADE, G.; LUCENA, M.; SILVA, L. A Qualitative Study of Teaching Requirements Engineering in Universities. In: The XXXIII Brazilian Symposium, 2019, Salvador. Proceedings of the XXXIII Brazilian Symposium on Software Engineering - SBES 2019, 2019. p. 161-165.

SANTOS, I.; MIRANDA, E.; LUCENA, M. Rastreamento e Gerenciamento de Requisitos em Busca da Conformidade Legal. In: XX Ibero-American Conference on Software Engineering, 2017, Buenos Aires. XX Ibero-American Conference on Software Engineering, 2017. v. 1. p. 15-29.

- Trabalhos completos em fase de submissão:

MIRANDA, E; TRINDADE, G.; LUCENA, M. An Analysis of Traceability in Agile Environments from the Visualization of Information in the Software Factory: the Experience of Managers and Developers. IEEE Access, 2021.

SOUZA, L. T. M.; MIRANDA, E.; LUCENA, M.; GOMES, A. Fundamentals for Documenting Software Requirements Based on Informational Needs. IEEE Access, 2021.

7.3 Trabalhos futuros

Como trabalhos futuros a essa tese, vislumbram-se:

- A realização de uma nova avaliação do *Framework* por especialistas em Direito para identificar possíveis contribuições nos trabalhos desses profissionais;
- A aplicação do *Framework* em fábricas de *software*, que utilizem diferentes metodologias de desenvolvimento, para avaliar a robustez frente a diferentes desafios enfrentados por profissionais da área de computação;
- A atualização e a extensão da revisão sistemática da literatura realizada com a intenção de ampliá-la e promover uma visão mais atual do estado da arte;
- A diagramação de novos fluxos de atividades do uso do *Framework* em situações experienciadas por profissionais de diferentes níveis de atuação;
- A criação de um curso para ministrar o conteúdo relacionado à conformidade legal e regulatória em sistemas computacionais no intuito de formar profissionais com expertises fundamentais ao processo de implementação, manutenção e evolução dessa conformidade;
- A implementação computacional do *Framework* em si, para que os profissionais encontrem em um único instrumento todos os elementos, que precisam para o processo de implementação, manutenção e evolução dessa conformidade;
- A concepção e instanciação de repositórios públicos básicos para fontes legais ou regulatórias para determinados domínios de sistemas computacionais.

7.4 Conclusões finais

Os temas relacionados a essa tese ofereceram desafios relacionados ao fato de serem inter e multidisciplinares, além de pouco explorados nas perspectivas acadêmicas e da indústria.

Isto foi perplexo sob o ponto de vista da importância inerente, todavia negligenciada por boa parte daqueles que, de alguma forma, estão por circunstância interessados no ciclo de vida de sistemas computacionais. Sabe-se ainda que há muito o que se fazer, quando consideradas as bases legais e regulatórias do país, e a infraestrutura necessária para incorporar a cultura da obrigatoriedade da conformidade legal e regulatória nas instituições e sistemas computacionais.

A finalização e avaliação do *Framework* criado mostrou a factibilidade de oferecer à comunidade uma alternativa viável aos seus anseios demonstrados nos estudos exploratórios. Observa-se que, principalmente, analistas/engenheiros de requisitos, gerentes de projetos eram um público desamparado por um ferramental ou diretrizes que lhes apoiassem em suas rotinas para implementação, manutenção e evolução da conformidade legal e regulatória. Muitos ainda são surpreendidos em auditorias ou fiscalizações, quando julgam que seus sistemas estão em total conformidade com a lei. A utilização do *Framework* criado e avaliado poderá auxiliar a esses profissionais em todo o ciclo de vida dos sistemas computacionais.

É preciso lançar luz ao caminho a ser trilhado por interessados nos sistemas computacionais e sua real conformidade legal e regulatória. Para isso, além de oferecer um *Framework*, foram criados ou sistematizados conceitos, estruturas e conhecimentos que estão para além da Computação. Todavia, continua sendo imprescindível o interesse e a dedicação dos profissionais e dos interessados nas temáticas sobre as quais versam esta pesquisa. Principalmente, considerando a inter e a multidisciplinaridade inerentes a todo o processo em si, bem como a volatilidade dos insumos utilizados.

Referências

ACHIMUGU, P.; SELAMAT, A.; IBRAHIM, R.; MAHRIN, M. N. R. A systematic literature review of software requirements prioritization research. Information and software technology, v. 56, n. 6, p. 568-585, 2014.

AKHIGBE, O. Towards a Regulator-Oriented Regulatory Intelligence Framework. In: 2016 IEEE 24th International Requirements Engineering Conference (RE). IEEE, 2016. p. 415-420.

AKHIGBE, O.; AMYOT, D.; RICHARDS, G. A systematic literature mapping of goal and non-goal modelling methods for legal and regulatory compliance. Requirements Engineering, v. 24, n. 4, p. 459-481, 2019.

ALBUQUERQUE, H. O. GenNormas: um processo genérico para a conformidade legal na engenharia de requisitos. 2014. Dissertação de Mestrado. Programa de Pós-graduação em Informática. Universidade Federal da Paraíba.

ALVES, S. R.; ALVES, A. L. Engenharia de Requisitos em Metodologias Ágeis. 2009.

ANAND, T.; GUPTA, R. K. Knowledge transfer for global roles in GSE. In: Proceedings of the 12th International Conference on Global Software Engineering. 2017. p. 81-85.

ANGROSINO, M. Doing Ethnographic and Observational Research. Sage, 2007.

BARBOZA, L. S. Uma abordagem para garantia da conformidade legal no planejamento de contratações de TI na Administração Pública Federal. 2015. Dissertação de Mestrado. Programa de Pós-graduação em Informática Aplicada. Universidade Federal Rural de Pernambuco.

BARROSO, L. R. Curso de direito constitucional contemporâneo. Saraiva Educação SA, 2017.

_____. O controle de constitucionalidade no direito brasileiro. Saraiva Educação SA, 2017.

BASILÉIA II (Basel II): International Convergence of Capital Measurement and Capital Standards: A Revised Framework.2005. Disponível em: <http://www.bis.org>. Acesso em: 03 mar. 2019.

BAUMAN, Z. Globalization: The human consequences. Columbia University Press, 1998.

_____. Liquid modernity. John Wiley & Sons, 2013.

BECK, Kent et al. The agile manifesto. 2001.

BECK, U. What is globalization? John Wiley & Sons, 2018.

BETTIOL, M. Knowledge Management and Industry 4.0: New Paradigms for Value Creation. 2020.

BHATIA, J.; BREAUX, T. D. Towards an information type lexicon for privacy policies. In: 2015 IEEE eighth international workshop on requirements engineering and law (RELAW). IEEE, 2015. p. 19-24.

BLOOSHI, M. Al; JAFER, S.; PATEL, K. Review of Formal Agile Methods as Cost-Effective Airworthiness Certification Processes. Journal of Aerospace Information Systems, v. 15, n. 8, p. 471-484, 2018.

BOBBIO, N.; DE CICCO, C. Teoria do Ordenamento Jurídico. UnB, 1999.

BRASIL. Constituição Federal de 1988. Brasília - DF: [s.n.], 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 14/10/2019.

_____. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm Acesso em: 14/10/2019.

_____. Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, ano 151, n. 77, p. 1, 24 abr. 2014.

CARROLL, A. B. A three-dimensional conceptual model of corporate performance. Academy of management review, v. 4, n. 4, p. 497-505, 1979.

CASSELL, C.; CUNLIFFE, A. L.; GRANDY, G. (Ed.). The SAGE handbook of qualitative business and management research methods. Sage, 2017.

COHEN-KOPLIN, K. Processo e Constituição: apresentação da dicotomia e de sua superação. In: Anais do VI Colóquio De Pesquisa. Porto Alegre: UNIRITTER, 2010.

CONSELHO NACIONAL DE ARQUIVOS (BRASIL). CÂMARA TÉCNICA DE DOCUMENTOS ELECTRÓNICOS. e-ARQ Brasil: modelo de requisitos para sistemas informatizados de gestão arquivística de documentos. Arquivo Nacional, 2011.

COOPER JR, J. R.; LEE, S. W.; GANDHI, R. A.; GOTEL, O. Requirements engineering visualization: a survey on the state-of-the-art. In: 2009 Fourth International Workshop on Requirements Engineering Visualization. IEEE, 2009. p. 46-55.

CORDIS. Community Research and Development Information Service (CORDIS) - EUR-Lex - acesso ao direito da União Europeia. Disponível em: <https://eur-lex.europa.eu/>. Acesso em: 21/03/2018.

CRESWELL, J. W.; CRESWELL, J. D. Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications, 2017.

DE OLIVEIRA, C. A. A. O processo civil na perspectiva dos direitos fundamentais. Cadernos do Programa de Pós-Graduação em Direito–PPGDir./UFRGS, v. 2, n. 4, 2004.

DENZIN, N. K.; LINCOLN, Y. S. Qualitative Research Planning: Theories and Approaches. 2006.

_____. The Sage handbook of qualitative research. 2017.

DIKERT, K.; PAASIVAARA, M.; LASSENIUS, C. Challenges and success factors for large-scale agile transformations: A systematic literature review. Journal of Systems and Software, v. 119, p. 87-108, 2016.

DOSS, O.; KELLY, T. Assurance case integration with an agile development method. In: Agile Processes in Software Engineering and Extreme Programming: 16th International Conference, XP 2015, Helsinki, Finland, May 25-29, 2015, Proceedings. Springer, 2015. p. 347.

DYBÅ, T.; DINGSØYR, T. Empirical studies of agile software development: A systematic review. Information and software technology, v. 50, n. 9-10, p. 833-859, 2008.

EAGLETON, T. Culture. Yale University Press, 2016.

ERNST, N. A., BORGIDA, A., JURETA, I. J., MYLOPOULOS, J. Agile requirements engineering via paraconsistent reasoning. Information Systems, v. 43, p. 100-116, 2014.

ESPINOZA, A.; GARBAJOSA, J. A Study to Support Agile Methods more Effectively through Traceability. Innovations in Systems and Software Engineering, Springer, v. 7, n. 1, p. 5369, 2011.

FAO. FAOLEX Database - Food and Agriculture Organization of the United Nations. Disponível em: <http://www.fao.org/>. Acesso em: 29/08/2020.

FELDT, R.; MAGAZINIUS, A. Validity threats in empirical software engineering research-an initial survey. In: Seke. 2010. p. 374-379.

FIORIN, J. L. Elementos de análise do discurso. Contexto, 2001.

FLICK, U. Managing quality in qualitative research. Sage, 2008.

FOUCAULT, Michel. Archaeology of knowledge. routledge, 2013.

_____. Orders of discourse. Social science information, v. 10, n. 2, p. 7-30, 1971.

FREIRE, P. Pedagogia da autonomia: saberes necessários à prática educativa. 17ª ed. São Paulo: Paz e Terra, 1996.

GALVEZ, R.; GURSES, S. The odyssey: Modeling privacy threats in a brave new world. In: 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE, 2018. p. 87-94.

GARG, R.; NAUDTS, B.; VERBRUGGE, S.; STILLER, B. Modeling legal and regulative requirements for ranking alternatives of cloud-based services. In: 2015 IEEE Eighth International Workshop on Requirements Engineering and Law (RELAW). IEEE, 2015. p. 25-32.

GONÇALVES, C. R. Direito Civil Brasileiro 3-Contratos e Atos Unilaterais. Saraiva Educação SA, 2017.

GONZÁLEZ, L.; RUGGIA, R. Towards a Middleware and Policy-based Approach to Compliance Management for Collaborative Organizations Interactions. In: ICSOFT. 2017. p. 414-420.

GORDON, D. G.; BREAUX, T. D. Comparing requirements from multiple jurisdictions. In: 2011 Fourth International Workshop on Requirements Engineering and Law. IEEE, 2011. p. 43-49.

GÓRSKI, J.; ŁUKASIEWICZ, K. Meeting requirements imposed by secure software development standards and still remaining agile. In: International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security. Springer, Cham, 2017. p. 3-15.

GOTEL, O.; CLELAND-HUANG, J.; ZISMAN, A.; HAYES, J. H.; DEKHTYAR, A.; MÄDER, P.; EGYED, A.; GRÜNBACHER, P.; ANTONIOL, G.; e MALETIC, J. Glossary of Traceability Terms (v1. 0). Software and Systems Traceability, Springer, p. 413, 2012.

GUMP, J.; MAZZUCHI, T.; SARKANI, S. An Architecture for Agile Systems Engineering of Secure Commercial Off-the-Shelf Mobile Communications. Systems Engineering, v. 20, n. 1, p. 71-91, 2017.

HANSSEN, G. K., HAUGSET, B., STÅLHANE, T., MYKLEBUST, T., KULBRANDSTAD, I. Quality assurance in scrum applied to safety critical software. In: International Conference on Agile Software Development. Springer, Cham, 2016. p. 92-103.

HELINGO, M., PURWANDARI, B., SATRIA, R., SOLICHAH, I. The use of Analytic Hierarchy Process for software development method selection: A perspective of e-Government in Indonesia. Procedia Computer Science, v. 124, p. 405-414, 2017.

HENSCHKE, J. A. A Productive Decade of Andragogy's History and Philosophy 2000-2009. In Assessing and Evaluating Adult Learning in Career and Technical Education. Wang, V. [Ed]. Zhejiang University Press, Hangzhou, China, 2009.

HUTCHINSON, D.; ARMITT, C.; EDWARDS-LEAR, D. The application of an agile approach to it security risk management for SMES. 2014.

IBGE. Demografia das Empresas e Estatísticas de Empreendedorismo 2018. Estudos e pesquisas. Informação econômica. ISBN 978-65-87201-26-9. Rio de Janeiro: IBGE, 2020.

ICSSES COMMITTEE et al. I. Electronics Engineers, and I.-SS Board, IEEE recommended practice for software requirements specifications: approved 25 June 1998, vol. 830. 1998.

INAYAT, I.; SALIM, S. S.; MARCZAK, S.; DANEVA, M.; e SHAMSHIRBAND, S. A systematic literature review on agile requirements engineering practices and challenges. Computers in human behavior, v. 51, p. 915-929, 2015.

INGOLFO, S., JURETA, I., SIENA, A., PERINI, A., E SUSI, A. Nomos 3: Legal compliance of roles and requirements. In: International Conference on Conceptual Modeling. Springer, Cham, 2014. p. 275-288.

INGOLFO, S.; SIENA, A.; MYLOPOULOS, J. Goals and Compliance in Nomos 3. In: iStar. 2014.

IT GOVERNANCE INSTITUTE. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. ISACA. 2012.

JALES, L. Neoprocessualismo: reflexos neoconstitucionais. João Pessoa: Ideia, 2012.

JOWETT, B. et al. (Ed.). The republic of Plato. London; New York: Macmillan, 1888.

KAISER, A. K. ITIL and DevOps: An Analysis. In: Reinventing ITIL® in the Age of DevOps. Apress, Berkeley, CA, 2018. p. 63-75.

KASAULI, R.; KNAUSS, E.; HORKOFF, J.; LIEBEL, G.; e DE OLIVEIRA NETO, F. G. Requirements engineering challenges and practices in large-scale agile system development. Journal of Systems and Software, v. 172, p. 110851, 2021.

KATSUNO, Y.; KUNDU, A.; DAS, K. K.; TAKAHASHI, H.; SCHLOSS, R.; DEY, P.; MOHANIA, M. Security, compliance, and agile deployment of personal identifiable information solutions on a public cloud. In: 2016 IEEE 9th International Conference on Cloud Computing (CLOUD). IEEE, 2016. p. 359-366.

KITCHENHAM, B., BRERETON, O. P., BUDGEN, D., TURNER, M., BAILEY, J., LINKMAN, S. Systematic literature reviews in software engineering – a systematic literature review. Information and software technology, v. 51, n. 1, p. 7-15, 2009.

KITCHENHAM, B.; CHARTERS, S. Guidelines for performing systematic literature reviews in software engineering. 2007.

KIYAVITSKAYA, N.; KRAUSOVÁ, A.; ZANNONE, N. Why eliciting and managing legal requirements is hard. In: 2008 Requirements Engineering and Law. IEEE, 2008. p. 26-30.

KNAPP, J.; ZERATSKY, J.; KOWITZ, B. Sprint: How to solve big problems and test new ideas in just five days. Simon and Schuster, 2016.

KNOWLES, M. S. Andragogy: Adult Learning Theory in Perspective. Community College Review, 5(3), 9–20. 1978. doi:10.1177/009155217800500302.

KOTONYA, G; SOMMERVILLE, Ia. Requirements engineering: processes and techniques. John Wiley & Sons, Inc., 1998.

KUCHINKE, W.; KRAUTH, C.; KARAKOYUN, T. Agile software development requires an agile approach for computer system validation of clinical trials software products. In: eChallenges e-2014 Conference Proceedings. IEEE, 2014. p. 1-8.

LAUKKARINEN, T.; KUUSINEN, K.; MIKKONEN, T. DevOps in regulated software development: case medical devices. In: 2017 IEEE/ACM 39th International Conference on Software Engineering: New Ideas and Emerging Technologies Results Track (ICSE-NIER). IEEE, 2017. p. 15-18.

_____. Regulated software meets DevOps. Information and Software Technology, v. 97, p. 176-178, 2018.

LE, M., JAYARAM, K. R., WEINSBERG, Y., DEAN, D. J., TAO, S. Agile Composition of Compliant Data Analytics Platforms. In: 2017 IEEE International Conference on Cloud Engineering (IC2E). IEEE, 2017. p. 51-58.

LEFFINGWELL, D. Agile software requirements: lean requirements practices for teams, programs, and the enterprise. Addison-Wesley Professional, 2011.

LENZA, P. Direito constitucional esquematizado®. Saraiva Educação SA, 2017.

LESHEM, S.; TRAFFORD, V. Overlooking the Conceptual Framework. Innovations in education and Teaching International, v. 44, n. 1, p. 93-105, 2007.

LexML. Projeto LexML - Modelo de Requisitos para Sistemas Informatizados de Gestão da Informação Jurídica - SILEX. Disponível em: <http://silex.lexml.gov.br/>. Acessado em: 21/03/2018.

LIAN, S. SW process tailoring practice in medical device industry. In: Proceedings of the 2014 International Conference on Software and System Process. 2014. p. 193-194.

LIMA, L. F. Estudo sobre a Gestão Qualitativa do Risco Operacional como Prática de governança corporativa em Instituições Financeiras no Brasil. 2007, 168 p. Dissertação

(Mestrado em Ciências Contábeis e Financeiras). Pontifícia Universidade Católica de São Paulo, São Paulo, 2007.

LUCIA, A. D.; QUSEF, A. Requirements Engineering in Agile Software Development. Journal of Emerging Technologies in Web Intelligence, Academy Publisher, PO Box 40 Oulu 90571 Finland, v. 2, n. 3, p. 212-220, 2010.

MAROSIN, D.; GHANAVATI, S. Measuring and managing the design restriction of enterprise architecture (EA) principles on EA models. In: 2015 IEEE Eighth International Workshop on Requirements Engineering and Law (RELAW). IEEE, 2015. p. 37-46.

MARTINS, L. E. G.; GORSCHEK, T. Requirements engineering for safety-critical systems: overview and challenges. IEEE Software, v. 34, n. 4, p. 49-57, 2017.

MARX, G. T. Of methods and manners for aspiring sociologists: 37 moral imperatives. Am Soc 28, 102–125 (1997). https://doi.org/10.1007/s12108-997-1029-9.

MASSEY, A. K.; OTTO, P. N.; ANTÓN, A. I. Prioritizing legal requirements. In: 2009 Second International Workshop on Requirements Engineering and Law. IEEE, 2009. p. 27-32.

MCNIFF, J.; WHITEHEAD, J. Action research in organisations. Psychology Press, 2000.

MELLADO, D.; BLANCO, C.; SÁNCHEZ, L. E.; FERNÁNDEZ-MEDINA, E. A systematic review of security requirements engineering. Computer Standards & Interfaces, v. 32, n. 4, p. 153-165, 2010.

MILANI, F. Digital Business Analysis. Springer, 2019.

MOYON, F., BECKERS, K., KLEPPER, S., LACHBERGER, P., BRUEGGE, B. Towards continuous security compliance in agile software development at scale. In: 2018 IEEE/ACM 4th International Workshop on Rapid Continuous Software Engineering (RCoSE). IEEE, 2018. p. 31-34.

MYKLEBUST, T.; STÅLHANE, T.; LYNGBY, N. An agile development process for petrochemical safety conformant software. In: 2016 Annual Reliability and Maintainability Symposium (RAMS). IEEE, 2016. p. 1-6.

NERURKAR, A.; DAS, I. Analysis of DILRMP Project: Identifying the Applicability of Agile Project Management for Digital Transformation Projects in Government and Public Sector. In: Proceedings of the Special Collection on eGovernment Innovations in India. 2017. p. 34-38.

SOUZA NETO, J.; DE CARVALHO, L. E. M. A Avaliação da Governança de TI da administração pública sob a ótica dos princípios da governança corporativa. Revista do Serviço Público, v. 71, p. 345-374, 2020.

NOAKS, L.; WINCUP, E. Introducing Qualitative Methods series: Criminological Research: Understanding Qualitative Methods. 2004.

NWOKEJI, J. C.; CLARK, T.; BARN, B.; KULKARNI, V. A conceptual framework for enterprise agility. In: Proceedings of the 30th Annual ACM Symposium on Applied Computing. 2015. p. 1242-1244.

OCHODEK, M.; KOPCZYŃSKA, S. Perceived importance of agile requirements engineering practices – a survey. Journal of Systems and Software, v. 143, p. 29-43, 2018.

OLIVER, I. Experiences in the development and usage of a privacy requirements framework. In: 2016 IEEE 24th International Requirements Engineering Conference (RE). IEEE, 2016. p. 293-302.

ÖZCAN-TOP, Ö.; MCCAFFERY, F. A hybrid assessment approach for medical device software development companies. Journal of Software: Evolution and Process, v. 30, n. 7, p. e1929, 2018.

_____. How Does Scrum Conform to the Regulatory Requirements Defined in MDevSPICE®? In: International Conference on Software Process Improvement and Capability Determination. Springer, Cham, 2017. p. 257-268.

PASQUALINO, Roberto. Thinking in Systems: The Long-Term Impacts of Short-Term Business growth. In: Corporate Sustainability in Practice. Springer, Cham. p. 41-61. 2021.

PECK, P. Direito Digital. rev., atual. e ampl., de acordo com as Leis n. 12.735 e 12.737, de 2012. São Paulo: Saraiva, 2013.

PINHEIRO, P. P. Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018-LGPD. Saraiva Educação SA, 2020.

PMI - PROJECT MANAGEMENT INSTITUTE. Guia PMBOK®: Um Guia para o Conjunto de Conhecimentos em Gerenciamento de Projetos. Sexta edição, Pennsylvania: PMI, 2017.

POHL, K. Requirements Engineering: fundamentals, principles, and techniques. Springer Publishing Company, Incorporated, 2010.

PREECE, J.; SHARP, H.; ROGERS, Y. Interaction design: beyond human-computer interaction. John Wiley & Sons, 2015.

PRIKLADNICKI, R.; WILLI, R.; MILANI, F. Métodos ágeis para desenvolvimento de software. Bookman Editora, 2014.

RAMESH, B.; CAO, L.; BASKERVILLE, R. Agile requirements engineering practices and challenges: an empirical study. Information Systems Journal, v. 20, n. 5, p. 449-480, 2010.

RAMESH, B.; JARKE, M. Toward reference models for requirements traceability. IEEE transactions on software engineering, v. 27, n. 1, p. 58-93, 2001.

REALE, M. Lições preliminares de direito. 27ª Edição. 11ª Tiragem. Saraiva Educação SA. 2012.

RIFAUT, A. Compliance management with measurement frameworks. In: 2011 Fourth International Workshop on Requirements Engineering and Law. IEEE, 2011. p. 15-24.

RINDELL, K.; HYRYNSALMI, S.; LEPPÄNEN, V. Securing Scrum for VAHTI. In: SPLST. 2015. p. 236-250.

RUNESON, P.; HOST, M.; RAINER, A.; REGNELL, B. Case study research in software engineering: Guidelines and examples. John Wiley & Sons, 2012.

SABHARWAL, A. Digital curation in the digital humanities: Preserving and promoting archival and special collections. Chandos Publishing, 2015.

SAMPIERI, R. H.; COLLADO, C. F.; LUCIO, M. P. B. Metodología de la investigación. 6ª ed. México: Mcgraw-Hill, 2014.

SANTOS, I. C. C. Gestão de requisitos legais com foco na conformidade dos sistemas com a legislação vigente. 2017. Dissertação de Mestrado. Brasil.

SANTOS, I.; MIRANDA, E.; LUCENA, M. Rastreamento e Gerenciamento de Requisitos em Busca da Conformidade Legal. In: CIbSE. 2017. p. 319-332.

SCHÖN, E. M.; THOMASCHEWSKI, J.; ESCALONA, M. J. Agile Requirements Engineering: A systematic literature review. Computer Standards & Interfaces, v. 49, p. 79-91, 2017.

SELLTIZ, C.; JAHODA, M.; DEUTSCH, M.; COOK, S. W. Research Methods in Social Relations, New York: Holt, Reinhart and Winston. Inc., l964.

SHNEIDERMAN, B. The eyes have it: A task by data type taxonomy for information visualizations. In: Proceedings 1996 IEEE symposium on visual languages. IEEE, 1996. p. 336-343.

SIENA, A.; MYLOPOULOS, J.; PERINI, A., SUSI, A. From laws to requirements. In: 2008 Requirements Engineering and Law. IEEE, 2008. p. 6-10.

SILEX, G. de T. Modelo de requisitos para sistemas informatizados de gestão da informação jurídica. 2013.

SILVERMAN, D. Interpreting qualitative data. 2014.

SINGH, J., PASQUIER, T., BACON, J., POWLES, J., DIACONU, R., EYERS, D. Big ideas paper: Policy-driven middleware for a legally-compliant Internet of Things. In: Proceedings of the 17th International Middleware Conference. 2016. p. 1-15.

SOMMERVILLE, I. Software Engineering. 10th. In: Book Software Engineering. 10th, Series Software Engineering. Addison-Wesley, 2016.

SOUZA, J. G. S., FERREIRA, N. D. M., KUSSAMA, L. Y., DE OLIVEIRA, R. M. N., & ARIMA, C. H. Gestão de riscos de segurança da informação e governança de TI no setor público. 2017.

SOUZA, L. T. M. Documentação de requisitos e compartilhamento do conhecimento: uma proposta a partir de um estudo etnográfico. 2019. Dissertação de Mestrado. Brasil.

SPENCER, R. Information Visualization: An Introduction. 3rd Ed. Springer. 2014.

STÅLHANE, T.; MYKLEBUST, T. The role of CM in Agile development of safety-critical software. In: International Conference on Computer Safety, Reliability, and Security. Springer, Cham, 2014. p. 386-396.

STRATIGAKI, C., NIKOLAIDOU, M., LOUCOPOULOS, P., ANAGNOSTOPOULOS, D. Business process elicitation from regulatory compliance documents: an E-Government case study. In: 2016 IEEE 18th conference on business informatics (CBI). IEEE, 2016. p. 8-13.

SUNKLE, S.; KHOLKAR, D.; KULKARNI, V. Model-driven regulatory compliance: A case study of “Know Your Customer” regulations. In: 2015 ACM/IEEE 18th International Conference on Model Driven Engineering Languages and Systems (MODELS). IEEE, 2015. p. 436-445.

TAMÒ-LARRIEUX, A.; TAMÒ-LARRIEUX; SEYFRIED. Designing for privacy and its legal framework. Cham: Springer, 2018.

TOKYO, The. Society 5.0 A People-centric Super-smart Society: A People-centric Super-smart Society. 2020. https://doi.org/10.1007/978-981-15-2989-4.

TONELLA, P.; TIELLA, R. Weekly round trips from norms to requirements and tests: an industrial experience report. In: 2015 IEEE/ACM 2nd International Workshop on Requirements Engineering and Testing. IEEE, 2015. p. 20-26.

TRAVASSOS, G. H.; GUROV, D.; AMARAL, E. A. G. G. Introdução à Engenharia de Software Experimental. 2002.

TREKTERE, K., MCCAFFERY, F., LEPMETS, M., BARRY, G. Tailoring MDevSPICE® for mobile medical apps. In: 2016 IEEE/ACM International Conference on Software and System Processes (ICSSP). IEEE, 2016. p. 106-110.

TREKTERE, K., REGAN, G., CAFFERY, F. M., FLOOD, D., LEPMETS, M., BARRY, G. Mobile medical app development with a focus on traceability. Journal of Software: Evolution and Process, v. 29, n. 11, p. e1861, 2017.

TREVIÑO, L. K., WEAVER, G. R., GIBSON, D. G., TOFFLER, B. L. Managing ethics and legal compliance: What works and what hurts. California management review, v. 41, n. 2, p. 131-151, 1999.

TRINDADE, G. O. Visualização da rastreabilidade em projetos ágeis através de dados contidos em ferramentas de apoio à gerência de projetos. 2018. Dissertação de Mestrado. Brasil.

URIBE, F. G. O. La entrevista de investigación en las ciencias sociales. Limusa, 2007.

VALLON, R., ESTACIO, B. J. S., PRIKLADNICKI, R., GRECHENIG, T. Systematic literature review on agile practices in global software development. Information and Software Technology, v. 96, p. 161-180, 2018.

VAN ENGERS, T.; NIJSSEN, S. From legislation towards the provision of services. In: International Conference on Electronic Government and the Information Systems Perspective. Springer, Cham, 2014. p. 163-172.

VARJU, M.; CZINA, V. Between Compliance and Particularism. In: Between Compliance and Particularism. Springer, Cham, 2019. p. 1-20.

VERAS, M. Datacenter: componente central da infraestrutura de TI. Rio de Janeiro: Brasport, 2009.

VIEIRA, S. Como elaborar questionários. In: Como elaborar questionários. 2009. p. 159.

WAINER, J. et al. Métodos de pesquisa quantitativa e qualitativa para a Ciência da Computação. Atualização em Informática, v. 1, p. 221-262, 2007.

WEISS, Robert S. Learning from strangers: The art and method of qualitative interview studies. Simon and Schuster, 1995.

WHITEHEAD, J.; MCNIFF, J. Action research: Living theory. Sage, 2006.

WIERINGA, R. J. Design science methodology for information systems and software engineering. Springer, 2014.

WILSON, P. B. Sizing software with testable requirements. Systems Development Management, 2000.

WOHLIN, C. Guidelines for snowballing in systematic literature studies and a replication in software engineering. In: Proceedings of the 18th international conference on evaluation and assessment in software engineering. 2014. p. 1-10.

YBEMA, S.; YANOW, D.; WELS, H.; KAMSTEEG, F. H. (Eds.). Organizational ethnography: Studying the complexity of everyday life. Sage, 2009.

YIN, R. K. Case study research and applications: Design and methods. Sage publications, 2017.

Apêndices

- Apêndice A – Instrumentos de apoio aos estudos exploratórios
- Apêndice B – *Template* para criação de documentação de um requisito
- Apêndice C – Exemplos de história de usuário com requisito legal ou regulatório e sua relação com a legislação aplicável
- Apêndice D – Instrumentos de apoio à avaliação do *Framework* proposto

Apêndice A - Instrumentos de Apoio aos Estudos Exploratórios

Apêndice A.1 – Formulário de categorização do(a) candidato(a)

Nome completo: _____

Idade: _____ anos Sexo: _____ Estado civil: _____ Nº de filhos: _____

E-mail: _____

Formação acadêmica:

( ) Ensino médio técnico ( ) Universitária ( ) Pós-graduação *lato sensu* ( ) Pós-graduação *stricto sensu*

Nome do curso: _____

Experiência profissional:

Tempo de experiência em ambientes de desenvolvimento de software: **_____ ano(s) e _____ mês(es).**

Como você classificaria sua experiência em desenvolvimento de software?
( ) Baixa ( ) Média ( ) Alta

Você tem desenvolvido *software* como membro de equipe? **( ) Sim ( ) Não**
Se sim, qual é o número de membros desta equipe (incluindo você)? **_____ membros.**

Dentre os papéis encontrados no processo de desenvolvimento de software, marque as opções que você desempenha ou se identifica?

( ) Gerente de projeto ( ) Analista/Engenheiro de Requisitos ( ) Arquiteto de Software
( ) Desenvolvedor de Software ( ) Consultor interno ( ) Consultor externo
( ) Outro: _____.

Dentre as disciplinas trabalhadas no processo de desenvolvimento de *software*, marque as com que você mais se identifica?

( ) Gerenc. de Projeto ( ) Eng. de Requisitos ( ) Arq. de Software ( ) Implementação

Para modelar um problema/solução, quais destas linguagens de modelagem/notação você já utilizou?

( ) BPMN ( ) Framework iStar ( ) UML ( ) SoaML ( ) Outra: _____.

Caso você tenha marcado uma das opções acima, como você classifica o seu conhecimento dos modelos propostos pelo Framework?

( ) Básico ( ) Intermediário ( ) Avançado ( ) Especialista

Você aceitaria participar de uma pequena entrevista em um dia/horário que lhe fosse mais conveniente?
( ) Não ( ) Sim

Apêndice A.2 – Termo de Consentimento Livre e Esclarecido (TCLE)

Eu, _____,
de nacionalidade _____, tendo nascido em: _____/_____/_____,
estado civil _____, profissão _____,
domiciliado(a) à _____
_____
_____
,inscrito(a) no Cadastro de Pessoas Físicas sob o nº _____, inscrito(a) no Registro Geral sob o nº _____, emitido por _____, em: _____/_____/_____, estou sendo convidado(a) a participar de um estudo relacionado como o projeto de pesquisa nomeado "Documentação e Rastreabilidade de Artefatos para Evolução Sustentável de Sistemas Computacionais", cujo o objetivo é oferecer subsídios adequados à documentação e à rastreabilidade dos artefatos do ciclo de vida de sistemas para equipes na indústria de desenvolvimento de sistemas. Sendo que, nesta fase do projeto, o foco estará na conformidade legal desses sistemas.

A minha participação no referido estudo será no sentido de auxiliar a investigação sobre as dificuldades e as estratégias utilizadas na documentação e na rastreabilidade de artefatos para evolução sustentável de sistemas computacionais a partir de uma abordagem etnográfica e observação participante.

Fui alertado(a) de que, da pesquisa a se realizar, posso esperar alguns benefícios, tais como: aprendizagem da abordagem e dos artefatos de desenvolvimento de *software*. Recebi, por outro lado, os esclarecimentos necessários sobre os possíveis desconfortos e riscos decorrentes do estudo, levando-se em conta que é uma pesquisa, e os resultados positivos ou negativos somente serão obtidos após a sua realização. Poderei sentir cansaço ou fadiga pelo número de horas dispensadas na realização do estudo. Estou ciente de que minha privacidade será respeitada, ou seja, meu nome ou qualquer outro dado ou elemento que possa, de qualquer forma, identificar-me, será mantido em sigilo. Além disso, saliento que tenho conhecimento de que a documentação produzida será mantida por até dois anos para fins legais. Também fui informado(a) de que posso me recusar a participar do estudo, ou retirar meu consentimento até a finalização da execução das atividades do experimento, sem precisar justificar, e de, por desejar sair da pesquisa, não sofrerei qualquer prejuízo à assistência que venho recebendo.

É assegurada a assistência durante toda pesquisa, bem como o livre acesso a todas as informações e os esclarecimentos adicionais sobre o estudo e suas consequências, enfim, tudo o que eu queira saber antes, durante e depois da minha participação. Enfim, tendo sido orientado(a) quanto ao teor de todo o aqui mencionado e compreendido a natureza e o objetivo do já referido estudo, manifesto meu livre consentimento em participar, estando totalmente ciente de que não há nenhum valor econômico, a receber ou a pagar, por minha participação.

A saber, as pesquisadoras envolvidas com o referido estudo são:

Profa. Márcia Jacyntha Nunes Rodrigues Lucena (coordenadora) - *e-mail*: marcia@dimap.ufrn.br.

Erica Esteves Cunha de Miranda - *e-mail*: erica@ppgsc.ufrn.br.

Por esta ser a expressão da minha vontade, assino o presente termo em duas vias de igual teor.

_____, _____/_____/_____. _____

Assinatura do(a) participante

E-mail do(a) participante: _____

Telefone(s) do(a) participante: _____

Apêndice A.3 – Termo de Cessão e Uso de Imagem, Áudio e Vídeo (TCUIAV)

Eu, _____,
inscrito(a) no Cadastro de Pessoas Físicas sob o nº _____, neste ato denominado participante, outorgo o seguinte termo de cessão e uso.

O(A) participante autoriza de livre e espontânea vontade a captação, fixação, utilização e divulgação da sua imagem e voz para serem inseridos e utilizado no Brasil e no exterior, através de todos e quaisquer meios de comunicação ao público, tais como, mas não se limitando, artigos científicos, internet e materiais promocionais relacionados com do estudo denominado "Documentação e Rastreabilidade de Artefatos para Evolução Sustentável de Sistemas Computacionais", cujo o objetivo é oferecer subsídios adequados à documentação e à rastreabilidade dos artefatos do ciclo de vida de sistemas para equipes na indústria de desenvolvimento de sistemas computacionais. Sendo que, nesta fase do projeto, o foco estará na conformidade legal desses sistemas". Ainda, afirmo que estou ciente de não haver para tanto qualquer tipo de remuneração.

A saber, as pesquisadoras envolvidas com o referido estudo são:
Profa. Márcia Jacyntha Nunes Rodrigues Lucena (coordenadora) - *e-mail*: marcia@dimap.ufrn.br.
Erica Esteves Cunha de Miranda - *e-mail*: erica@ppgsc.ufrn.br.

Por esta ser a expressão da minha vontade, declaro que autorizo como descrito acima sem que nada haja a ser reclamado a título de direitos conexos à minha imagem, voz ou a qualquer outro, e assino o presente termo em duas vias de igual teor.

_____, _____/_____/_____. _____

Assinatura do(a) participante

Apêndice A.4 – Mapeamento dos dados dos participantes e identificações utilizadas no estudo

Esse mapeamento visa permitir maior privacidade nos documentos produzidos por avaliadores e participantes

ID	Nome completo do(a) participante	ID Texto	ID Artigo	ID Artigo
001				
002				
003				
004				
005				
006				
007				
008				
009				
010				
011				
012				
013				
014				
015				
016				
017				
018				
019				
020				
021				
022				
023				
024				
025				

Apêndice A.5 – Roteiro para entrevista com Presidente do Comitê de Priorização, *Chief Executive Officer* (*CEO*) ou *Chief Product Officer* (*CPO*)

ID: _____.

Primárias

1. Os membros da sua equipe sabem da existência da hierarquia das "fontes legais ou regulatórias"? (Constituição Federal, Emendas, Tratados Internacionais, Leis Complementares, Leis específicas ou especiais, Leis ordinárias, Medidas Provisória, Leis delegadas, Decretos Legislativos, Resoluções, Decretos, Portarias, Contratos, Normas, Regimentos, Regulamentos, por exemplo).
2. Como sua nova posição na instituição pode ajudar a manutenção e evolução da conformidade legal e regulatória dos sistemas computacionais?
3. Qual é sua opinião sobre a base de "textos legais" no sistema? Como esta base é utilizada pelo senhor e sua equipe? O que pode ser melhorado?
4. Em que contribuiria para sua equipe, a existência de repositório único, classificado e alimentado com todos as "fontes legais ou regulatórias" (de diferentes de tipos e níveis) relacionados com os projetos dos sistemas computacionais utilizados pela instituição e de acordo com os interesses dos interessados (*stakeholders*)?
5. Como o senhor entende por evidência legal, quando nos referimos a implementação de requisitos legais em sistemas computacionais? O senhor possuiria evidências, e está seguro de que a instituição cumpre com toda a legislação e regulamentos obrigatórios, possuindo políticas, planos e práticas claramente definidos, implementados, divulgados e auditáveis?
6. Com relação aos requisitos legais e normativos de segurança e privacidade da informação (uma tendência do momento, e direito de pessoas jurídicas e físicas), o senhor possui evidências, e está seguro de que a instituição os atende? Em que nível da segurança da informação relacionada aos ativos da informação a diretoria e a instituição atendem as expectativas e percepções dos *stakeholders* (interessados), e àquelas estabelecidas em "textos legais"?
7. Quais são as métricas mais utilizadas (ou na sua opinião, apropriadas, caso não existam métricas definidas) para avaliar a qualidade dos produtos e serviços oferecidos pela instituição à diretoria apresentam a qualidade necessária, na sua opinião? E quanto a instituição?
8. Respeitando a gestão (planejamento, aquisição, estruturação, custódia, distribuição, atualização, preservação, por exemplo) das informações institucionais, como isto é feito com as informações do Repositório Institucional (RI) da instituição? Estas ações estão fundamentadas e geridas com base em quais "textos legais"?
9. Qual é o nível de apoio, atribuição de importância e compreensão do primeiro escalão da instituição, quanto aos riscos inerentes à TIC e seus impactos para o negócio da instituição? (secretários, superintendentes, diretores, presidência e conselhos)
10. Como é feito o alinhamento da conformidade dos processos do negócio com a conformidade legal e regulatória dos sistemas computacionais e serviços de TIC institucionais?

Secundárias

11. Há uma política geral associada a auditoria externa de TIC? Qual? E quanto a existência de uma política geral associada a auditoria interna de TIC? Qual? Quem seriam esses auditores? Eles possuem treinamento e certificações adequadas às atividades relacionadas a uma auditoria interna de TIC?
12. Quais são as estratégias adotadas para identificar uma "fonte legal ou regulatória" relacionado a um novo requisito? Quais artefatos são utilizados para alertar a presença de novas "fontes legais ou regulatórias", que podem gerar novos ou revogar requisitos legais em sistemas computacionais junto a instituição?

13. Como é o processo para definir o que exatamente tem que ser feito dado uma “fonte legal ou regulatória”? Existe um processo ou fluxo pré-definido? Quem apoia a diretoria no entendimento da “fonte legal ou regulatória”?
14. Como são decididos os conflitos entre diferentes “textos legais”? Ou os requisitos já implementados no sistema computacional em produção? E quando o conflito está nos requisitos legais em si? Quem é o responsável por arbitrar?
15. Há alguma diferença no tratamento do requisito legal?
16. Quais são as principais dificuldades em trabalhar com os requisitos legais? Seria:
    a. Identificar as "fontes legais ou regulatórias";
    b. Escolher quais as "fontes legais ou regulatórias" são aplicáveis ao domínio ou ao contexto do sistema computacional;
    c. Extrair os direitos e as obrigações relevantes desses “textos legais”;
    d. Conciliar as "fontes legais ou regulatórias" aplicáveis e as tecnologias disponíveis; ou
    e. Tratar a dinamicidade das "fontes legais ou regulatórias" para manter a conformidade legal e regulatória dos sistemas computacionais.
17. O senhor já teve problemas internos/externos ou processos administrativos relacionados com requisitos legais não atendidos ou atendidos de forma incorreta? Se sim, conte-me como foi a experiência.
18. Padrões, aspectos legais, métodos e melhores práticas são incorporados nos processos administrativos? Existem documentos destas incorporações, e estes disponibilizados aos interessados? Estes processos são verificados e atualizados com que frequência?

Encerramento

1. Comentar alguma questão que ficou em aberta, ou aproveitar algum gancho.
2. Agradecimento.

Apêndice A.6 – Roteiro para entrevista por *e-mail* para *Chief Executive Officer* (*CEO*) ou *Chief Product Officer* (*CPO*)

ID: _____.

Formação acadêmica

1. Qual é a sua formação acadêmica?
2. Quais são seus cursos complementares?
3. O senhor teria alguma certificação para desempenhar suas atividades? Foi exigido pela instituição?

Experiências profissionais

1. Há quanto tempo o senhor trabalha profissionalmente na área de Planejamento e Administração?
2. Quanto a sua experiência profissional, há quanto tempo o senhor ocupa seu cargo atual?
3. Qual é a função que o senhor ocupa no momento? Quais são as atividades que o senhor desempenha?
4. Explique um pouco sobre sua função e suas atividades na instituição.
5. Quais foram suas outras experiências profissionais?
6. O senhor já participou da criação de planos, avaliações e autoavaliações na instituição?
7. Quais estratégias o senhor utiliza para se atualizar? Quais são as oferecidas pela instituição?

Trabalho na CTI

1. Como aconteceu o convite de trabalhar junto à CTI?
2. Quais foram os seus papéis, funções, ações e atividades assumidos? Foram definidos processos, procedimentos e fluxos? Estes foram documentados? Conte-me como foi sua experiência no trabalho junto à CTI.
3. Como são as suas interações junto ao Comitê de Priorização? Quais foram os documentos produzidos, e a partir de qual referencial teórico ou prático? Estes foram feitos de forma colaborativa ou cooperativa? Estão disponíveis para a comunidade?

Ser *Chief Executive Officer* (CEO) ou *Chief Product Officer* (CPO)

1. Dentro da sua gestão e considerando sua experiência, qual é a importância da diretoria para instituição?
2. Quais são os perfis e os cargos presentes na diretoria? e o número de pessoas em cada um desses?
3. Quais são suas novas atribuições como diretor de Planejamento? Quais destas atingem direta ou indiretamente a CTI?
4. Qual é ou foi a sua maior dificuldade ao assumir a diretoria?
5. O senhor pretende modificar o organograma da diretoria? Como será esse organograma depois inclusive com as últimas alterações nos recursos humanos?
6. Como o senhor gerencia, e controla todas as atividades da diretoria? Quais são as estratégias utilizadas? Quais são as ferramentas utilizadas? Quais são as estratégias utilizadas para relacionar (rastrear) todas as informações das equipes e da diretoria?
7. O senhor participa de quais grupos de auditoria, controle, gestão ou gerenciamento estratégicos, de tomada de decisão ou consultivos, como por exemplo comitês/comissões/grupos de trabalho? Saberia informar por quais motivos foi escolhido?

8. Como o senhor pensa em garantir a articulação entre os órgãos da instituição? Quais são as suas estratégias e seus planos para esta gestão?
9. O senhor poderia enviar/compartilhar documentos, decisões, fluxos, "fontes legais e regulatórias" ou qualquer outro material, mesmo que sejam tarjadas as informações sigilosas e confidenciais, relacionados com a implementação, a manutenção e a evolução da conformidade legal ou regulatória dos sistemas computacionais, da gestão e da governança da informação da instituição?

Sua equipe e interseções

1. Quais são os papéis e as responsabilidades necessários hoje para operacionalizar e gerir a instituição prioritariamente ou além dos já existentes?
2. Como é solicitado um novo membro? Como é justificada a solicitação?
3. Como são distribuídos os membros pelas equipes?
4. Como são divididas essas pessoas dentre as equipes existentes?
5. Existe alguma interseção clara entre as equipes? Inclusive considerando atividades, necessidades, prioridades e cronogramas?
6. Como é feita a integração entre estas equipes?
7. Quais foram/são as iniciativas para melhorar esta integração?
8. Quais são os indicadores de produtividade, qualidade e competências utilizados?
9. Como são promovidas e retribuídas aquisição de maior produtividade, qualidade e competências nos recursos humanos da diretoria? E como são penalizados nos casos contrários?
10. O senhor acredita que é conhecida a hierarquia de comando e as responsabilidades de cada cargo/função dentro da diretoria? Como são decididos os conflitos? Quem é o árbitro final?
11. Para o senhor seria relevante ter a sistematização dos desdobramentos relacionados à perda de um membro da equipe? (Lembrando que a perda de um membro na equipe pode levar a perda de conhecimento) É importante ter essa informação? Por quê?

Conformidade legal e regulatória

1. É conhecida a hierarquia das fontes legais e regulatórias (Constituição Federal, Emendas, Tratados Internacionais, lei complementar, lei específica ou especial, lei ordinária, medida provisória, lei delegada, decreto legislativo, resolução, decreto, portaria, contratos, normas, regimentos, regulamentos, por exemplo) pelos membros da sua equipe?
2. Antes do levantamento do contexto, como as operações da instituição, elicitação dos requisitos, por exemplo, em algum momento, são buscadas fontes legais ou regulatórias relacionadas? Em quais momentos são buscados esses textos legais? São buscados sistemas semelhantes dentre os "concorrentes" antes de demandar algo a CTI?
3. Como é o processo para definir o que exatamente tem que ser feito dado uma "fonte legal ou regulatória"? Existe um fluxo pré-definido?
4. Como são decididos os conflitos entre diferentes "fontes legais e regulatórias"? ou os requisitos já implementados no sistema em produção? e quando o conflito está nos requisitos legais em si?
5. Quando há conflito entre diferentes "fontes legais e regulatórias", quem é o responsável por arbitrar?
6. Quem apoia a diretoria nisso no entendimento da "fonte legal ou regulatória"? Há especialistas na área de Direito, que apoiam o entendimento e a definição do que deve ser realmente feito dado o domínio dos sistemas computacionais utilizados pela diretoria? Quem seria esta pessoa:

um especialista em Direito, uma consultoria contratada, alguém que seja parte da sua equipe, ou alguém da equipe de desenvolvimento (CTI)? Se sim, como eles atuam?

7. Como é tratada a transição dos estados da vigência da lei dentro da diretoria? (norma publicada, vacância, vigente, prorrogada, revogada, alterada, convertida, rejeitada, por exemplo)
8. Como são identificados nas "fontes legais e regulatórias", o que se referem a direitos, obrigações, promulgação, publicação e vigência/revogação? Como são tratados?
9. Considerando a preocupação nacional e internacional com o direito de privacidade e segurança, o que tem sido feito neste sentido pela diretoria?
10. Em que nível a segurança da informação relacionada aos ativos de informação a diretoria de planejamento e a CTI atendem as expectativas e percepções dos stakeholders (interessados)?
11. As políticas, planos e diretrizes são disponibilizadas a todos os interessados?
12. A manutenção da conformidade legal está em maior ou menor grau de importância, quando solicitada uma alteração nos sistemas computacionais por algum membro da sua equipe?
13. Como é feito o alinhamento da conformidade dos processos de negócio com a conformidade legal e regulatória dos sistemas computacionais e serviços de TIC institucionais?
14. Quais seriam os possíveis órgãos fiscalizadores ou instituições reguladoras interessadas na verificação da conformidade legal e regulatória dos sistemas computacionais utilizados pela diretoria?
15. Em algum momento houve alguma auditoria interna/externa relacionada à conformidade legal e regulatória dos sistemas computacionais (*softwares*, documentação, infraestrutura, processos, por exemplo)? Como foi a experiência?
16. Os auditores, ou área responsável por tratar do tema, possuem autonomia para a atuação? Em que momento ou fase de um projeto ocorreram essas auditorias?

Requisitos legais

1. Quais são as estratégias adotadas para identificar as leis, as normas ou toda e qualquer fonte legal ou regulatória relacionado a um novo requisito? Quais artefatos são utilizados para alertar a presença de requisitos legais, quando são necessárias manutenções ou evoluções dos sistemas computacionais junto a CTI?
2. Como são feitas as extrações das informações legais da fonte legal ou regulatória? Onde são armazenadas/refinadas/especificadas antes de serem implementadas? (por exemplo, na especificação, na tarefa no sistema de gerenciamento de projeto)
3. Há alguma diferença de tratamento do requisito legal ou regulatório?
4. Quais são as principais dificuldades em trabalhar com os requisitos legais: **i)** identificar as "fontes legais ou regulatórias"; **ii)** escolher quais as "fontes legais e regulatórias" são aplicáveis ao domínio; **iii)** extrair os direitos e as obrigações relevantes dessas "fontes legais e regulatórias"; **iv)** conciliar as "fontes legais ou regulatórias" aplicáveis e as tecnologias disponíveis; ou **v)** tratar a dinamicidade das "fontes legais e regulatórias"?
5. O senhor já teve problemas internos/externos ou processos administrativos relacionados com requisitos legais não atendidos ou atendidos de forma incorreta?
6. Que tipo de problemas, comumente, são encontrados na engenharia de requisitos legais feita pela CTI? Saberia dizer a origem destes problemas? (imperfeição, imprecisão, dinâmica, ambiguidade dos requisitos ou das "fontes legais ou regulatórias").
7. Como o senhor entende por evidência legal, quando nos referimos a implementação de requisitos legais?
8. Como são negadas ou priorizadas as demandas relacionadas às TIC? Os critérios estão documentados, e são revistos com que frequência?

Apêndice A.7 – Roteiro para entrevista com *Chief Executive Officer* (*CEO*)

ID: _____.

Ser *Chief Executive Officer*

1. Qual foi a sua maior dificuldade?
2. Qual era o organograma antes da sua chegada? Como está esse organograma depois inclusive com as últimas demissões, realocações, rescisões de contratos?
3. Como a sra. gerencia e controla todas as atividades do CTI? Quais são as estratégias utilizadas? Quais são as ferramentas utilizadas? Quais são as estratégias utilizadas para relacionar (rastrear) todas as informações das equipes e do CTI?
4. É conhecida a hierarquia de comando e as responsabilidades de cada cargo? Como são decididos os conflitos? Quem é o árbitro final?
5. A sra. participa de quais grupos de auditoria, controle, gestão ou gerenciamento estratégicos, de tomada de decisão ou consultivos, como por exemplo comitês/comissões/grupos de trabalho? A sra. poderia enviar/compartilhar documentos, decisões, fluxos, "textos legais" ou qualquer outro material, mesmo que sejam tarjadas as informações sigilosas e confidenciais?

Sua equipe

1. Qual é o número de membros em cada equipe?
2. Quais são as equipes existentes?
3. Quantos são servidores ativos?7
4. Quantos são contratados?
5. Quantos são estagiários?
6. Como é solicitado um novo membro? Como é justificada a solicitação?
7. Como são distribuídos os membros pelas equipes?
8. Como é o processo de contratação via fundação?
9. Como é ter que administrar esses diferentes relacionamentos dentre os recursos humanos?
10. Como são divididas essas pessoas dentre as equipes existentes?
11. Existe alguma interseção clara entre as equipes de sistemas e infraestrutura? Inclusive considerando atividades, necessidades, prioridades e cronogramas?
12. Como é feita a integração entre estas equipes?
13. Quais foram/são as iniciativas para melhorar esta integração?
14. Em um outro momento, a sra. informou-nos que diferentes ações estavam em andamento para valorização dos recursos humanos. Como estão estas ações, investimentos e participação para valorização das pessoas, desenvolvimento ou aprimoramento de suas habilidades?
15. Quais são os indicadores de produtividade, qualidade e competências utilizados?
16. Como são promovidas e retribuídas aquisição de maior produtividade, qualidade e competências nos recursos humanos da instituição? E como são penalizados nos casos contrários?
17. Para a sra. seria relevante ter a sistematização dos desdobramentos relacionados à perda de um membro da equipe? (Lembrando que a perda de um membro na equipe pode levar a perda de conhecimento) É importante ter essa informação? Por quê?

Expansão da instituição (pessoal, infraestrutura e sistemas)

1. Como aconteceu a expansão da instituição considerando os sistemas e a infraestrutura? Vocês foram consultados? Houve planejamento?

2. Como isso vem afetando os serviços, a infraestrutura e os sistemas dentro instituição?
3. Quantos são os sistemas, módulos, centros, aplicativos, ativos, por exemplo, de responsabilidade da instituição? Como é feito este controle?
4. Como são as tomadas de decisão para alteração de tecnologia, evolução ou descontinuidade de módulos ou serviços?
5. Como são feitas as comunicações de mudanças tanto para equipe, como para a comunidade interna e externa? Qual é a hierarquia desta comunicação de mudanças?

Políticas, normas, planos e procedimentos

1. Existe um modelo institucional para governança e gestão de TI da instituição?
2. Como foi a participação da instituição na criação do PDTI?
3. Existem planos ou políticas definidas para organização e recuperação da informação? Como são feitos? Como são atualizados?
4. Como são auditados os atendimentos às normas e aos padrões dentro da instituição? Existem pessoas nas equipes certificadas?
5. Como são auditados os atendimentos às "fontes legais ou regulatórias" dentro da instituição?
6. Quem é responsável pelas auditorias internas e externas?

Parque tecnológico

1. Qual é o impacto da implantação do Parque Tecnológico para a instituição?
2. Quais são as ações e as responsabilidades da instituição com relação ao Parque Tecnológico?
3. Já existiam planos ou contratos com as cooperações técnicas relacionadas aos sistemas, à infraestrutura, à criação do parque tecnológico, à expansão dos data centers, à replicação do *datacenter*?

Requisitos legais

1. A sra. acredita que sua equipe entende que requisitos legais se diferenciam de quaisquer outros requisitos? (direito, obrigações, promulgação, publicação e vigência/revogação) E suas implicações?
2. Quais são as principais dificuldades em trabalhar com os requisitos legais: identificar as "fontes legais ou regulatórias", escolher quais as "fontes legais ou regulatórias" são aplicáveis ao domínio, extração dos direitos e obrigações relevantes desses “textos legais”, conciliação das "fontes legais ou regulatórias" aplicáveis e as tecnologias disponíveis, ou dinamicidade das "fontes legais ou regulatórias"?
3. Os artefatos da Engenharia de Requisitos são utilizados para alertar a presença de requisitos legais pensando em futuras manutenções ou evoluções?
4. Houve alguma mudança significativa/drástica com a alteração das ferramentas e processos por conta de “textos legais” internos ou externos? Como foi recebida e atendida essa demanda?
5. Entre os diferentes níveis hierárquicos da instituição, órgãos de fomento, de agências de regulação/fiscalização/avaliação, e instituições parceiras como chegam as novas “regras”, as demandas, as cobranças e, depois, é feita a prestação de conta?
6. A sra. já teve problemas internos/externos ou processos administrativos relacionados com requisitos legais não atendidos ou atendidos de forma incorreta?

Conformidade legal

1. Como vocês sabem que há uma nova “fonte legal ou regulatória” a ser atendida?
2. É conhecida a hierarquia das fontes legais ou regulatórias (Constituição Federal, Emendas, Tratados Internacionais, lei complementar, lei específica ou especial, lei ordinária, medida

provisória, lei delegada, decreto legislativo, resolução, decreto, portaria, contratos, normas, regimentos, regulamentos, por exemplo) pelos membros da equipe?

3. Qual é o processo para definir o que exatamente tem que ser feito dado uma "fonte legal ou regulatória"? Existe um fluxo pré-definido?
4. Como são decididos os conflitos entre diferentes "textos legais"? Ou requisitos já implementados no sistema?
5. Quando há conflito entre diferentes "textos legais" quem é o responsável por arbitrar?
6. A fonte legal ou regulatória é reconhecidamente imperfeita, imprecisa, dinâmica, ambígua. Quem apoia vocês nisso? Há especialistas na área de Direito que apoiam o entendimento e a definição do que deve ser realmente implementado? Como é a relação com os procuradores?
7. Quais são os canais disponíveis para comunicação de inconformidade legal? Algum deste mecanismo já foi usado?
8. Hoje, é possível garantir ou evidenciar a conformidade legal nos sistemas, na infraestrutura de TI, nos processos, nos contratos ou qualquer outro artefato que seja de responsabilidade da instituição? Como?
9. Quais são as evidências legais possíveis de serem apresentadas ou produzidas em um determinado tempo estipulado para demonstrar a conformidade?
10. Vocês adotam algum modelo de análise da conformidade legal ou um modelo de atividades da conformidade legal para verificar a conformidade legal, quando é feita uma manutenção ou evolução dos serviços (sistemas, infra, armazenamento, preservação, recuperação de informações, por exemplo) de TI?
11. Como é feito o alinhamento da conformidade dos processos de negócio com a conformidade legal dos sistemas computacionais e serviços de TI institucionais?
12. Em algum momento houve alguma auditoria interna/externa relacionada à conformidade legal dos sistemas computacionais (*softwares*, documentação, infraestrutura, processos, por exemplo)? Como foi a experiência?
13. Como foram decididos quais seriam as categorias e os dados disponibilizados no portal dos dados abertos? Qual é a equipe responsável pela criação e manutenção do portal?
14. Como foi feita a disponibilização do portal dos dados abertos? Com que frequência são atualizados os conjuntos de dados?
15. Como e com que frequência são auditados os dados disponibilizados neste portal?
16. Considerando a preocupação nacional e internacional com o direito de privacidade e segurança, o que tem sido feito neste sentido pela instituição?
17. Na última conversa, a sra. comentou sobre problemas com direito de propriedade dos sistemas. Como está sendo tratado isso? Existe alguma comissão ou orientação por parte dos procuradores ou especialistas em direito da instituição?
18. Como estão sendo feitos os processos atuais para atender o direito de propriedade dos sistemas, processos, métodos, por exemplo, produzidos na instituição?
19. Há profissionais que auxiliem a compreensão ou a definição de fontes legais ou regulatórias aplicadas ao domínio dos sistemas a serem desenvolvidos/mantidos? Quem seria esta pessoa, uma especialista em Direito, uma consultoria contratada, alguém que seja parte da equipe de desenvolvimento ou alguém dentre os stakeholders na sua instituição/equipe? Se sim, como eles atuam?
20. Antes do levantamento do contexto, com as operações das instituições, elicitação dos requisitos, por exemplo, em algum momento são buscadas as fontes legais ou regulatórias relacionadas? Em quais momentos são buscadas?
21. Como a sra. entende evidência legal, quando nos referimos a implementação de requisitos legais ou regulatórios?

22. Quais são as evidências legais planejadas para uma futura auditoria do sistema desenvolvido?
23. quais seriam os possíveis órgãos fiscalizadores ou instituições reguladoras interessadas na verificação da conformidade legal e regulatória do sistema desenvolvido/utilizado?
24. A manutenção da conformidade legal e regulatória está em maior ou menor grau de importância, quando solicitada uma alteração no sistema?
25. Como é documentada e verificada a conformidade legal e regulatória do sistema?
26. Há alguma sistemática definida para essa documentação ou verificação? Se sim, há alguma periodicidade pré-definida?
27. São realizadas auditorias internas e externas como prática de uma política?
28. As auditorias são feitas por profissionais internos e por profissionais independentes?
29. As auditorias são aplicadas em quais fases do ciclo de desenvolvimento?
30. Na nossa última conversa, a sra. comentou sobre os problemas com o direito de propriedade dos sistemas. Como está sendo tratado isso? Existe alguma comissão ou orientação por parte dos procuradores ou especialista em Direito da instituição?
31. Como estão sendo feitos os processos atuais para atender o direito de propriedade dos sistemas, processos, métodos, por exemplo, produzidos pela instituição atualmente?
32. Há comitês? Se sim, qual tem sido o papel dos comitês?

Finalização

1. A sra. teria alguma sugestão que melhoraria sua gestão, considerando os aspectos legais envolvidos? (comportamento mais proativo, repositório oficial das "fontes legais ou regulatórias" classificado, com mecanismos de busca novos processos ou fluxos de trabalho, especialistas no domínio, melhor rastreabilidade da informação, outros tipos de visualização)
2. A sra. teria alguma observação adicional?
3. A sra. teria alguma sugestão a mais?
   Quanto à comissão externa, seria possível o repasse dos documentos da comissão de priorização e definição do conteúdo das *sprints*?

Apêndice A.8 – Roteiro para entrevista com *Chief Executive Officer* (*CEO*) sobre o Tribunal de Contas da União

ID: _____.

Com relação ao sistema de governança corporativa:

1. A organização define e comunica formalmente papéis e responsabilidades para a governança corporativa?
2. A organização dispõe de um comitê de direção estratégica formalmente instituído, que auxilia nas decisões relativas às diretrizes, estratégias, políticas e no acompanhamento da gestão institucional?
3. A organização realiza avaliações sobre a definição e compreensão dos papéis e responsabilidades organizacionais?
4. A organização dispõe de um código de ética formalmente instituído, bem como divulga e monitora o seu cumprimento?
5. A organização dispõe de uma política corporativa de gestão de riscos formalmente instituída como norma de cumprimento obrigatório?
6. A organização dispõe de uma política corporativa de gestão de continuidade do negócio formalmente instituída como norma de cumprimento obrigatório?

Com relação ao sistema de governança de TI:

1. A organização define e comunica formalmente papéis e responsabilidades mais relevantes para a governança e a gestão de TI?
2. A organização dispõe de um comitê de TI formalmente instituído, composto por representantes de áreas relevantes da organização?
3. O comitê de TI realiza as atividades previstas em seu ato constitutivo?
4. A organização prioriza as ações de TI com apoio do comitê de TI (ou colegiado equivalente), que atua como instância consultiva da alta administração?

Com relação à entrega de resultado da TI:

1. A organização define formalmente diretrizes para o planejamento de TI?
2. A organização define formalmente diretrizes para gestão do portfólio de projetos e serviços de TI, inclusive para definição de critérios de priorização e de alocação orçamentária?
3. A organização define formalmente diretrizes para contratação de bens e serviços de TI?
4. A organização define formalmente diretrizes para avaliação do desempenho dos serviços de TI?

Com relação aos riscos de TI:

1. A organização define formalmente as diretrizes para gestão dos riscos de TI aos quais o negócio está exposto?
2. A organização define e comunica formalmente papéis e responsabilidades pela gestão de riscos de TI?
3. A organização define formalmente os níveis de risco de TI aceitáveis na consecução de seus objetivos (apetite a risco)?
4. A organização toma decisões estratégicas considerando os níveis de risco de TI definidos?

Com relação ao pessoal de TI:

1. A organização define formalmente diretrizes para garantir o desenvolvimento de competências e a retenção de gestores de TI?
2. A organização define formalmente diretrizes para garantir o desenvolvimento de competências e a retenção de pessoal técnico de TI?
3. A organização define formalmente diretrizes para avaliação e incentivo ao desempenho de gestores de TI?
4. A organização define formalmente diretrizes para avaliação e incentivo ao desempenho de pessoal técnico de TI?
5. A organização define formalmente diretrizes para escolha dos líderes da área de TI, ocupantes dos cargos de chefia e de assessoramento?

Com relação ao monitoramento da governança e da gestão de TI:

1. A organização define formalmente diretrizes para avaliação da governança e da gestão de TI?
2. A organização realiza avaliação periódica de governança e de gestão de TI?
3. A organização realiza avaliação periódica de sistemas de informação?
4. A organização realiza avaliação periódica de segurança da informação?
5. A organização realiza avaliação periódica de contratos de TI?

Com relação à auditoria interna:

1. A auditoria interna possui pessoal capacitado para avaliar a governança e a gestão de TI (quantitativo capacitado para essa avaliação: 2)?
2. A auditoria interna monitora as ações de governança e de gestão de TI?
3. A organização aprova, de forma periódica, plano de auditoria que inclua avaliação da governança e da gestão de TI?
4. A auditoria interna avalia a gestão de riscos de TI?
5. A auditoria interna avalia os riscos considerados críticos para o negócio e a eficácia dos respectivos controles?

Com relação ao planejamento estratégico institucional:

1. A organização executa periodicamente processo de planejamento estratégico institucional?
2. O processo de planejamento estratégico institucional prevê a participação das áreas mais relevantes da organização?
3. O processo de planejamento estratégico institucional prevê a participação da área de TI?
4. A organização possui plano estratégico institucional vigente, formalmente instituído pelo seu dirigente máximo?
5. O plano estratégico institucional vigente contém metas associadas aos indicadores de resultado? Quais seriam eles?
6. O plano estratégico institucional vigente está publicado na internet para acesso livre?

Com relação ao planejamento de tecnologia da informação:

1. A organização executa periodicamente processo de planejamento de TI?
2. O processo de planejamento de TI prevê a participação das áreas mais relevantes da organização?
3. O processo de planejamento de TI prevê a participação do comitê de TI?
4. O processo de planejamento de TI está formalmente instituído como norma de cumprimento obrigatório?
5. A organização possui plano de TI vigente, formalmente instituído pelo seu dirigente máximo?

6. O plano de TI vigente contempla objetivos, indicadores e metas para a TI, com os objetivos explicitamente alinhados aos objetivos de negócio constantes do plano estratégico institucional?
7. O plano de TI vigente contém alocação de recursos (orçamentários, humanos e materiais) e estratégia de execução indireta (terceirização)?
8. A execução do plano de TI vigente é acompanhada periodicamente quanto ao alcance das metas estabelecidas, para correção de desvios?
9. O plano de TI vigente vincula as ações (atividades e projetos) a indicadores e metas de negócio?
10. O plano de TI vigente fundamenta a proposta orçamentária de TI?

Com relação à informatização dos processos organizacionais:

1. A organização identifica e mapeia os principais processos de negócio?
2. Os principais processos de negócio da organização são suportados por sistemas informatizados?
3. Há catálogo publicado com informações atualizadas de cada um dos sistemas informatizados?
4. A organização designa formalmente responsáveis da área de negócio para a gestão dos respectivos sistemas informatizados?

Com relação à transparência das informações relacionadas à gestão e ao uso de TI:

1. Os planos de TI vigentes são divulgados na internet, sendo facilmente acessados?
2. As informações sobre o alcance dos objetivos de TI planejados são divulgadas na internet, sendo facilmente acessadas?
3. As informações sobre o acompanhamento das ações e dos projetos de TI são divulgadas na internet, sendo facilmente acessadas?
4. Os editais, seus respectivos anexos e os resultados das licitações de TI (inteiro teor) são divulgados na internet, sendo facilmente acessados?
5. Os estudos técnicos preliminares (inteiro teor) são divulgados na internet, juntamente com os editais de licitação de TI, sendo facilmente acessados?
6. Os contratos de TI e os respectivos aditivos (inteiro teor) são divulgados na internet, sendo facilmente acessados?
7. A execução orçamentária de TI, ao longo do exercício, é divulgada na internet, sendo facilmente acessada?
8. As informações sobre gestão e uso de TI divulgadas pela organização atendem aos princípios dos “Dados Abertos Governamentais” (http://dados.gov.br/dados-abertos)?

Com relação ao acesso a informações e a sua divulgação:

1. A organização cataloga as informações de interesse coletivo ou geral por ela produzidas ou custodiadas?
2. A organização publica conjuntos de dados aderentes aos princípios de dados abertos?

Com relação ao desenvolvimento de competências de TI:

1. A organização define as competências necessárias para o pessoal de TI executar suas atividades?
2. A organização define critérios para avaliação e atendimento dos pedidos de capacitação?
3. A organização elabora, periodicamente, plano de capacitação para suprir as necessidades de desenvolvimento de competências de TI?
4. A organização acompanha a execução do plano de capacitação, com identificação e correção de desvios?
5. A organização avalia a execução do plano de capacitação, verificando se os objetivos e resultados esperados foram alcançados?
6. O plano de capacitação inclui o desenvolvimento de competências em gestão de TI?

7. O plano de capacitação inclui o desenvolvimento de competências em contratação de bens e serviços de TI e na gestão dos contratos decorrentes?
8. As informações sobre gestão e uso de TI divulgadas pela organização atendem aos princípios dos "Dados Abertos Governamentais" (http://dados.gov.br/dados-abertos)?

Com relação ao desempenho do pessoal de TI:

1. A organização estabelece metas de desempenho para o pessoal de TI?
2. A organização avalia periodicamente o desempenho do pessoal de TI?
3. A organização estabelece benefícios, financeiros ou não, em função do desempenho alcançado pelo pessoal de TI?

Com relação à força de trabalho de TI:

1. Quantitativo aprovado como força de trabalho em TI:
2. Quantitativo necessário (ideal) como força de trabalho em TI:
3. Quantitativo total da força de trabalho existente (real) em TI:
4. Quantitativo de servidores/empregados públicos efetivos da carreira de TI da própria instituição:
5. Quantitativo de servidores/empregados públicos efetivos de outras carreiras (não TI) da própria instituição:
6. Quantitativo de servidores/empregados públicos cedidos de outras instituições públicas:
7. Quantitativo de servidores/empregados públicos não efetivos em cargos de livre nomeação:
8. Quantitativo de estagiários lotados na área de TI:
9. Quantitativo de terceirizados de TI que trabalham regularmente no ambiente da instituição (contratos de serviços continuados com cessão de mão de obra)?
10. Quantitativo de terceirizados de TI que trabalham no ambiente da instituição para execução de projetos de tempo determinado?
11. Quantitativo de servidores/empregados públicos do quadro de TI que NÃO atuam na área de TI da instituição:
12. Quantitativo de servidores/empregados públicos do quadro de TI que NÃO atuam na instituição:
13. Quais?
14. O quantitativo considerado ideal (item b) foi estimado com base em estudo técnico de avaliação quantitativa e qualitativa do quadro de pessoal da área de TI?

Com relação aos processos de gerenciamento de serviços de TI:

1. A organização executa processo de gerenciamento do catálogo de serviços?
2. O processo de gerenciamento do catálogo de serviços está formalmente instituído como norma de cumprimento obrigatório?
3. A organização executa processo de gerenciamento da continuidade dos serviços de TI?
4. O processo de gerenciamento de continuidade dos serviços de TI está formalmente instituído como norma de cumprimento obrigatório?
5. A organização executa processo de gerenciamento de mudanças?
6. O processo de gerenciamento de mudanças está formalmente instituído como norma de cumprimento obrigatório?
7. A organização executa processo de gerenciamento de configuração e ativos?
8. O processo de gerenciamento de configuração e ativos está formalmente instituído como norma de cumprimento obrigatório?
9. A organização executa processo de gerenciamento de liberação e implantação?
10. O processo de gerenciamento de liberação e implantação está formalmente instituído como norma de cumprimento obrigatório?

11. A organização executa processo de gerenciamento de incidentes?
12. O processo de gerenciamento de incidentes está formalmente instituído como norma de cumprimento obrigatório?
13. A organização executa processo de gerenciamento de problemas?
14. O processo de gerenciamento de problemas está formalmente instituído como norma de cumprimento obrigatório?
15. Com relação ao gerenciamento de nível de serviço de TI:
16. A organização mantém um catálogo publicado e atualizado dos serviços de TI oferecidos às áreas clientes, incluindo os níveis de serviço definidos?
17. Os níveis de serviço são formalmente definidos entre a área de TI e as áreas clientes (Acordo de Nível de Serviço - ANS)?
18. Os ANS incluem, como indicador de nível de serviço, o grau de satisfação dos usuários, apurado mediante a avaliação dos serviços de TI pelas áreas clientes?
19. A área de TI monitora o alcance dos níveis de serviço definidos?
20. A área de TI implementa ações corretivas em caso de não alcance dos níveis de serviço definidos?
21. A área de TI comunica periodicamente o resultado desse monitoramento às áreas clientes?

Com relação à gestão de riscos de TI:

1. A organização identifica os riscos de TI dos processos críticos de negócio?
2. A organização avalia os riscos de TI dos processos críticos de negócio?
3. A organização trata os riscos de TI dos processos críticos de negócio com base em um plano de tratamento de risco?
4. A organização executa um processo de gestão de riscos de TI?
5. O processo de gestão de riscos de TI está formalmente instituído como norma de cumprimento obrigatório?

Com relação à gestão corporativa da segurança da informação:

- <u>Políticas e Responsabilidades</u>

1. A organização dispõe de uma política de segurança da informação formalmente instituída como norma de cumprimento obrigatório?
2. A organização dispõe de comitê de segurança da informação formalmente instituído, responsável por formular e conduzir diretrizes para a segurança da informação corporativa, composto por representantes de áreas relevantes da organização?
3. A organização possui um gestor de segurança da informação formalmente designado, responsável pelas ações corporativas de segurança da informação?
4. A organização dispõe de política de controle de acesso à informação e aos recursos e serviços de TI formalmente instituída, como norma de cumprimento obrigatório?
5. A organização dispõe de política de cópias de segurança (backup) formalmente instituída como norma de cumprimento obrigatório?

<u>- Controles e Atividades</u>

1. A organização executa processo de gestão de ativos, assegurando a definição de responsabilidades e a manutenção de inventário dos ativos?
2. O processo de gestão de ativos está formalmente instituído como norma de cumprimento obrigatório?
3. A organização executa processo para classificação e tratamento de informações?

4. O processo para classificação e tratamento de informações está formalmente instituído como norma de cumprimento obrigatório?
5. A organização implementa controles para garantir a proteção adequada ao grau de confidencialidade de cada classe de informação?
6. A organização executa processo de gestão de riscos de segurança da informação?
7. O processo de gestão de riscos de segurança da informação está formalmente instituído como norma de cumprimento obrigatório?
8. A organização executa processo de gestão de vulnerabilidades técnicas de TI, com objetivo de reduzir o risco de exploração de vulnerabilidades conhecidas?
9. O processo de gestão de vulnerabilidades técnicas de TI está formalmente instituído como norma de cumprimento obrigatório?
10. A organização executa processo de monitoramento do uso dos recursos de TI, com objetivo de detectar atividades não autorizadas?
11. O processo de monitoramento do uso dos recursos de TI está formalmente instituído como norma de cumprimento obrigatório?
12. A organização executa processo de gestão de incidentes de segurança da informação?
13. O processo de gestão de incidentes de segurança da informação está formalmente instituído como norma de cumprimento obrigatório?
14. A organização possui equipe de tratamento e resposta a incidentes de segurança em redes computacionais, formalmente instituída?
15. A organização realiza, de forma periódica, ações de conscientização, educação e treinamento em segurança da informação para seus colaboradores?
16. A organização utiliza sistema criptográfico, aderente ao processo de certificação digital da ICP-Brasil, para garantir a autenticidade (autoria e integridade) das informações?

Com relação ao processo de *software*:

1. A organização executa um processo de software, com o objetivo de assegurar que o *software* a ser desenvolvido, direta ou indiretamente, atenda às suas necessidades?
2. O processo de *software* é acompanhado por meio de mensurações, com indicadores quantitativos e metas de processo a cumprir?
3. O processo de *software* é periodicamente revisado e melhorado com base nas mensurações obtidas?
4. A organização possui pessoal próprio capacitado para gerir a execução do processo de *software*?
5. O processo de *software* está formalmente instituído como norma de cumprimento obrigatório?

Com relação ao gerenciamento de projetos de TI:

1. A organização possui portfólio de projetos de TI?
2. A organização executa processo de gerenciamento de projetos de TI?
3. O processo de gerenciamento de projetos de TI é acompanhado por meio de mensurações, com indicadores quantitativos e metas de processo a cumprir?
4. O processo de gerenciamento de projetos de TI é periodicamente revisado e melhorado com base nas mensurações obtidas?
5. O processo de gerenciamento de projetos de TI está formalmente instituído como norma de cumprimento obrigatório?
6. A organização possui um escritório de projetos, ao menos para projetos de TI?

Com relação às contratações de serviços de TI:

1. A organização realiza estudos técnicos preliminares para avaliar a viabilidade da contratação?

2. A organização explicita, nos autos, as necessidades de negócio que se pretende atender com a contratação?
3. A organização explicita, nos autos, os indicadores dos benefícios de negócio que serão alcançados?
4. A organização explicita, nos autos, o alinhamento entre a contratação e os planos estratégico institucional e de TI vigentes?
5. A organização realiza análise dos riscos que possam comprometer o sucesso do processo de contratação e dos resultados que atendam as necessidades de negócio?
6. A organização adota métricas objetivas para mensuração de resultados do contrato?
7. A organização realiza os pagamentos dos contratos em função da mensuração objetiva dos resultados entregues e aceitos?
8. A organização realiza a análise dos benefícios reais já obtidos, utilizando-a como critério para prorrogar o contrato?
9. A organização diferencia e define formalmente os papéis de gestor e fiscal do contrato?

Com relação ao processo de planejamento das contratações de TI:

1. A organização possui procedimentos internos que auxiliam na padronização das atividades de planejamento das contratações de TI?
2. A organização executa processo de planejamento das contratações de TI?
3. O processo de planejamento das contratações de TI é acompanhado por meio de mensurações, com indicadores quantitativos e metas de processo a cumprir?
4. O processo de planejamento das contratações de TI é periodicamente revisado e melhorado com base nas mensurações obtidas?
5. O processo de planejamento das contratações está formalmente instituído como norma de cumprimento obrigatório?

Com relação ao processo de gestão dos contratos de TI:

1. A organização possui procedimentos internos que auxiliam na padronização das atividades de gestão de contratos de TI?
2. A organização executa processo de gestão de contratos de TI?
3. O processo de gestão de contratos de TI é acompanhado por meio de mensurações, com indicadores quantitativos e metas de processo a cumprir?
4. O processo de gestão de contratos de TI é periodicamente revisado e melhorado com base nas mensurações obtidas?
5. O processo de gestão de contratos de TI está formalmente instituído como norma de cumprimento obrigatório?

Com relação às contratações de TI (bens ou serviços) realizadas em sua gestão, informe:

1. Contratações realizadas:
2. Contratações que adotaram o sistema de registro de preço (RP), em que a própria organização foi gerenciadora da ata, com participação de outras instituições no planejamento (RP conjunto):
3. Contratações que adotaram o sistema de registro de preço, em que a própria organização foi gerenciadora da ata, sem participação de outras instituições no planejamento (RP solitário):
4. Contratações que adotaram o sistema de registro de preço, em que a organização foi órgão participante:
5. Contratações por adesão tardia a ata de registro de preço (“carona”), em que a organização não foi órgão participante:
6. Contratações por dispensa de licitação por contrato emergencial:

7. Contratações por dispensa de licitação para contratar órgão/entidade da Administração Pública (Lei 8.666/1993, art. 24, VIII ou XVI ou XXIII):
8. Contratações por inexigibilidade de licitação:

*Resultados esperados para 2019

Com relação aos objetivos de TI planejados pela organização, informe as metas mais relevantes para cumprimento em 2019 (até cinco):

Nome do Objetivo	Indicador	Meta 2019	Percentual de cumprimento da meta

Com relação aos projetos de TI:

Projetos encerrados em 2018				
Nome do projeto de TI	**Breve descrição**	**Custo estimado (R$ mil)**	**Percentual de execução física**	**Percentual de atraso**

Projetos de 2019 em andamento				
Nome do projeto de TI	**Breve descrição**	**Custo estimado (R$ mil)**	**Percentual de execução física**	**Percentual de atraso**

Com relação aos principais serviços de TI que sustentam as atividades da organização, informe:

Nome do serviço de TI	Principal indicador de nível de serviço	Meta 2018	Percentual de cumprimento da meta

Com relação ao rol de serviços públicos disponíveis (a exemplo daqueles constantes da Carta de Serviços ao Cidadão):

1. A organização presta serviços públicos diretamente ao cidadão?
2. A organização presta serviços públicos diretamente à instituição privada?
3. Quantidade de serviços públicos disponíveis (total, contando serviços presenciais ou prestados sob a forma eletrônica):
4. Quantidade de serviços públicos passíveis de serem prestados sob a forma eletrônica (integral ou parcialmente):
5. Quantidade de serviços públicos prestados integralmente sob a forma eletrônica, não exigindo o comparecimento do usuário (não se considera serviço, por si só, o agendamento de serviços presenciais):
6. Quantidade de serviços públicos prestados parcialmente sob a forma eletrônica, em que é exigido o comparecimento do usuário em alguma etapa do serviço (não se considera serviço, por si só, o agendamento de serviços presenciais):

Razões para que os serviços passíveis de prestação sob a forma eletrônica não sejam assim prestados:

1. Restrições legais?
2. Necessidade de autenticação do usuário?
3. Falta de recursos financeiros?
4. Falta de recursos humanos?
5. Falta de conhecimentos e habilidades técnicas?
6. Falta de infraestrutura?
7. Falta de agilidade da organização?
8. Falta de priorização de projetos?
9. Preocupações com segurança?
10. Perfil dos usuários impossibilita/dificulta a prestação eletrônica do serviço?
11. Necessidade de integração com órgãos ou entidades públicas federais?

12. Necessidade de integração com órgãos ou entidades públicas estaduais, distritais ou municipais?
13. Outras. Qual(is)?

Com relação aos serviços públicos prestados sob a forma eletrônica disponíveis:

1. Os serviços são acessíveis via internet:
2. Os serviços acessíveis via internet implementam as recomendações do Modelo de Acessibilidade de Governo Eletrônico (eMAG), previstas no Programa de Governo Eletrônico Brasileiro?
3. Os serviços oferecidos por meio eletrônico adotam os Padrões de Interoperabilidade de Governo Eletrônico (ePING), previstos no Programa de Governo Eletrônico Brasileiro?
4. Os serviços acessíveis via internet observam as recomendações dos Padrões *Web* em Governo Eletrônico (ePWG), previstas no Programa de Governo Eletrônico Brasileiro?
5. A instituição elabora, divulga e atualiza a sua Carta de Serviços ao Cidadão, conforme estabelecido no art. 11 do Decreto 6.932/2009, ou documento similar no caso de instituição que não pertença ao Poder Executivo Federal?
6. Os serviços públicos prestados sob a forma eletrônica são avaliados pelo usuário por meio de pesquisas periódicas de satisfação?
7. Os resultados das avaliações dos serviços públicos prestados sob a forma eletrônica são divulgados aos usuários?
8. A organização possui perfil oficial em rede social com a finalidade de descobrir e atender às necessidades do usuário?
9. Há metas definidas para a ampliação da oferta de serviços públicos prestados sob a forma eletrônica?
10. Os serviços públicos prestados sob a forma eletrônica estão disponíveis/cadastrados no portal servicos.gov.br?
11. Nos serviços prestados integralmente por meio eletrônico, há alternativas para provê-los aos usuários com limitação de uso, como por exemplo, prestação do serviço por algum posto de atendimento?
12. Nos serviços prestados integralmente por meio eletrônico, o usuário consegue finalizar o serviço sem a necessidade de acessar ou utilizar-se de outros meios, a exemplo de realização de cadastros, consultas ou emissão de certidões em outros sítios eletrônicos?
13. Novos serviços são concebidos para serem prestados prioritariamente sob a forma eletrônica?

Apêndice A.9 – Roteiro para entrevista por e-mail para *Chief Executive Officer* (*CEO*)

Ser *Chief Executive Officer* (CEO)

1. O que é ser *Chief Executive Officer* no CTI?
2. Como foi o seu convite para assumir como *Chief Executive Officer*?
3. Qual era a sua principal missão ao assumir a CTI?
4. Qual foi o cenário encontrado com relação às equipes, aos ambientes, à infraestrutura, às pró-reitorias, à reitoria, ao atendimento ao usuário, à contração de serviços e pessoas, aos materiais de consumo e permanentes, dentre outros?
5. Como foi a recepção por parte da equipe?
6. Qual foi a sua maior dificuldade?
7. Qual era o organograma antes da sua chegada? Como está esse organograma depois inclusive com as últimas demissões, realocações, rescisões de contratos?
8. Como a sra. gerencia e controla todas as atividades do CTI? Quais são as estratégias utilizadas? Quais são as ferramentas utilizadas? Quais são as estratégias utilizadas para relacionar (rastrear) todas as informações das equipes e do CTI?
9. É conhecida a hierarquia de comando e as responsabilidades de cada cargo? Como são decididos os conflitos? Quem é o árbitro final?
10. A sra. participa de quais grupos de auditoria, controle, gestão ou gerenciamento estratégicos, de tomada de decisão ou consultivos, como por exemplo comitês/comissões/grupos de trabalho? A sra. poderia enviar/compartilhar documentos, decisões, fluxos, "textos legais" ou qualquer outro material, mesmo que sejam tarjadas as informações sigilosas e confidenciais?

Sua equipe

1. Qual é o número de membros em cada equipe?
2. Quais são as equipes existentes?
3. Quantos são servidores ativos?7
4. Quantos são contratados?
5. Quantos são estagiários?
6. Como é solicitado um novo membro? Como é justificada a solicitação?
7. Como são distribuídos os membros pelas equipes?
8. Como é o processo de contratação via fundação?
9. Como é ter que administrar esses diferentes relacionamentos dentre os recursos humanos?
10. Como são divididas essas pessoas dentre as equipes existentes?
11. Existe alguma interseção clara entre as equipes de sistemas e infraestrutura? Inclusive considerando atividades, necessidades, prioridades e cronogramas?
12. Como é feita a integração entre estas equipes?
13. Quais foram/são as iniciativas para melhorar esta integração?
14. Em um outro momento, a sra. informou-nos que diferentes ações estavam em andamento para valorização dos recursos humanos. Como estão estas ações, investimentos e participação para valorização das pessoas, desenvolvimento ou aprimoramento de suas habilidades?
15. Quais são os indicadores de produtividade, qualidade e competências utilizados?
16. Como são promovidas e retribuídas aquisição de maior produtividade, qualidade e competências nos recursos humanos da CTI? E como são penalizados nos casos contrários? Para a sra. seria relevante ter a sistematização dos desdobramentos relacionados à perda de um membro da equipe? (Lembrando que a perda de um membro na equipe pode levar a perda de conhecimento) É importante ter essa informação? Por quê?

Apêndice A.10 – Roteiro para entrevista com auditor de controle externo

ID: _____.

Formação acadêmica

1. Qual é a sua formação acadêmica?
2. Quais são seus cursos complementares?
3. Você tem alguma certificação para desempenhar suas atividades? Foi exigido pela instituição?

Experiências profissionais

1. Há quanto tempo você trabalha profissionalmente na área de TI?
2. Quanto a sua experiência profissional, há quanto tempo você ocupa seu cargo atual?
3. Qual é a função que você ocupa no momento? Quais atividades você desempenha?
4. Explique um pouco sobre sua função e suas atividades.
5. Qual foi sua maior dificuldade?
6. Quais foram suas outras experiências profissionais?
7. Quais estratégias você utiliza para se atualizar? Quais são as oferecidas pela sua própria instituição?

Metodologias ágeis

1. Qual é sua experiência com metodologias ágeis de desenvolvimento?
2. Você poderia me citar quais metodologias ágeis de desenvolvimento já teve experiência?
3. Quais são os artefatos auditados pelo seu órgão, principalmente? Por quê?
4. Quais artefatos você gostaria que fossem "obrigatórios" a todos sistemas computacionais em seu ciclo de desenvolvimento, manutenção ou evolução?
5. Quais são as metodologias e artefatos mais encontrados no desempenho de suas atividades?
6. Nos artefatos produzidos como resultado de suas atividades, são sugeridos artefatos, métodos, metodologias ou qualquer outra coisa, que possam alterar a forma de trabalho da instituição auditada?
7. O foco dos artefatos produzidos por sua equipe é mais informativo da situação encontrada, indicativos de problemas e adequações/sanções a serem aplicados, ou educativos?

Gestão e gerenciamento de TI

1. Dentro da sua gestão e considerando sua experiência, qual é a importância do seu órgão para sua instituição?
2. Quais são os perfis e os cargos presentes no seu órgão?
3. Atualmente, quais são as principais áreas de atuação do seu órgão: governança, programas e políticas, segurança, sistemas, dados, compartilhamento de conhecimento, infraestrutura, contratações de TI?
4. Como são estabelecidas as parcerias com instituições, como Ministério Público, TCU, JUCERN, Receita Federal, Detran, Governo do Estado e outras, que disponibilizam bancos de dados, para que possa se fazer cruzamentos de informações, construindo-se a partir de uma matriz de riscos?
5. Quais são os artefatos produzidos pelo seu órgão?
6. É possível saber quem são as pessoas envolvidas na produção desses artefatos (até mesmo com o legal)? É importante ter essa informação? Por quê? Como você gerencia isto?
7. Como essas pessoas são envolvidas? Saber isso é importante pra você? Por quê?

8. Se houver alguma mudança, seria importante para você conhecê-la? Como isso seria feito?
9. Para você seria relevante ter a sistematização dos desdobramentos relacionados à perda de um membro da equipe? (Lembrando que a perda de um membro na equipe pode levar a perda de conhecimento) É importante ter essa informação? Por quê?
10. Você saberia dizer como são verificadas a conformidade legal e regulatória dos sistemas internos? e dos sistemas externos?

Gestão da informação

1. Como são elaborados planos, políticas, regulamentos, normativas e planejamento estratégico do órgão?
2. Existem repositórios para as leis estaduais e as leis municipais? Como é feito o gerenciamento destas leis?
3. Como é feita a divulgação das novas leis ou status das leis antigas?
4. Com a integração das bases, quais são as ações, as atividades realizadas com estas informações? Qual instituição/órgão foi responsável pela integração? Onde está esta base integrada?
5. Quando você está orientando, supervisionando, coordenando ou fiscalizando, quais são as suas preocupações? Por quê?
6. Você é responsável pela realização de diligências e complemento da instrução dos processos administrativos, que lhe sejam encaminhados para análise? Como isto é feito?
7. Você é responsável por emitir pareceres e manifestações a respeito de uma questão jurídica suscitada?
8. Como é sua abordagem, quando necessário realizar o controle externo ou interno?
9. Técnicas, ferramentas e artefatos utilizados nas suas atividades?
10. Quais são os sistemas de gestão da informação utilizados pela sua instituição? Como estão sendo planejados e utilizados esses e novos sistemas de gestão da informação? Quem é o público-alvo dessa gestão da informação?
11. Qual é o órgão responsável por atender a LAI?
12. Como são promovidos os acessos à informação ao público (transparência)?
13. Como são medidas qualidade e satisfação dos usuários com relação aos sistemas computacionais e serviços oferecidos pelo seu órgão?

Rastreabilidade e visualização (recuperação da informação)

1. Como são auditados os sistemas computacionais por sua equipe em suas atividades? Existem processos, procedimentos, fluxos? Quais ferramentas são utilizadas?
2. É importante para você saber a origem do requisito legal do artefato auditado? Como deveria estar documentado para ser auditado?
3. Você faz uso de alguma estratégia ou ferramenta de visualização dos relacionamentos entre os artefatos dos sistemas auditados? Qual o papel e em quais momentos são/foram importantes na auditoria essas estratégias ou visualizações? Alguma experiência para relatar? Caso contrário, ter uma visualização dos relacionamentos entre os artefatos seria útil no seu dia a dia? Por quê?
4. A visualização poderia ser relevante para lhe ajudar a identificar problemas, requisitos legais não implementados e, assim, a inconformidade do sistema? Por quê? Se sim, quais tipos de visualização seriam mais adequadas nas classes indicadas por você?
5. Você gostaria de ter algum tipo de visualização sobre alguns dados que não tem hoje, e não foi perguntado sobre?

Conformidade legal e regulatória (e requisitos legais)

1. Para você, o que seria requisito legal?

2. Como são priorizados os requisitos legais dentro de sua instituição?
3. Como são arbitrados os possíveis conflitos?
4. Para você, o que seria conformidade legal e regulatória?
5. É conhecida a hierarquia das fontes legais ou regulatórias (Constituição Federal, Emendas, Tratados Internacionais, lei complementar, lei específica ou especial, lei ordinária, medida provisória, lei delegada, decreto legislativo, resolução, decreto, portaria, contratos, normas, regimentos, regulamentos, por exemplo) pelos membros da sua equipe?
6. Como são relatados os problemas encontrados nas auditorias? Quais são os critérios para o estabelecimento de prazos para adequação e sanções para os problemas encontrados?
7. De que forma acontece a iniciativa de realizar uma auditoria externa ou interna por sua equipe?
8. A instituição auditada tem algum representante, que acompanha todo o processo de auditoria realizado por sua equipe? Por quê? Como esse acompanhamento é feito?
9. Antes do levantamento do contexto, como as operações da instituição, público-alvo, por exemplo, em algum momento, são buscadas fontes legais ou regulatórias relacionados ao que será auditado? Em quais momentos são buscados esses textos legais para embasar a auditoria em andamento ou futuras? Quais são suas fontes utilizadas?
10. Qual é o processo ou procedimento para definir o que exatamente tem que ser feito dada uma "fonte legal ou regulatória", que devem estar implementados nos sistemas computacionais auditados? Existe um fluxo pré-definido?
11. Como são verificadas as implementações destes textos legais?
12. Você teria algum checklist para realizar essas auditorias?
13. Quem apoia vocês nisso e no entendimento da "fonte legal ou regulatória", sendo sua equipe da área de TI? Há especialistas na área de Direito, que apoiam o entendimento e a definição do que deve ser realmente auditado no que foi implementado?
14. Quais seriam os possíveis órgãos fiscalizadores ou instituições reguladoras interessadas na verificação da conformidade legal dos sistemas por sua instituição?
15. Quais seriam os possíveis órgãos fiscalizadores ou instituições reguladoras interessadas na verificação da conformidade legal dos sistemas da sua instituição?
16. Em algum momento houve alguma auditoria interna/externa relacionada à conformidade legal dos sistemas computacionais (softwares, documentação, infraestrutura, processos, por exemplo) da sua instituição? Como foi a experiência?
17. Estas auditorias são aplicadas em quais fases do ciclo de desenvolvimento, manutenção ou evolução dos sistemas computacionais?

Índices, parâmetros e aprimoramentos para auditoria de sistemas computacionais

1. Quais são os índices de procedimentos padronizados e informatizados para auditoria de sistemas computacionais?
2. Quais são os indicadores utilizados pela sua instituição nas áreas de gestão e governança de TI?
3. Como estão sendo aprimorados o apoio ao controle da adequação à legislação?
4. Como estão sendo aprimorados e padronizados os processos de trabalho e instrumentos de controle?
5. Quais são ações efetivas em andamento para o uso da tecnologia da informação por sua instituição?
6. Quais são os indicadores de produtividade, qualidade e competências utilizados por sua instituição? E por você?
7. Como são promovidas e retribuídas aquisição de maior produtividade, qualidade e competências nos recursos humanos da instituição? E como são penalizados nos casos contrários?

8. Você sabe como são/serão medidos os índices estabelecidos no Portfólio de Indicadores da sua instituição, como: 1. Índice de cadastramento de jurisdicionado no portal do gestor; 2. Índice de atraso de prestação de contas; 3. Índice de seletividade em ações de controle; 4. Índice de fiscalizações concomitantes; **5. Índice de satisfação dos servidores com as soluções de TI**; **6. Índice de utilização das soluções de TI; 7. Índice de implantação do processo eletrônico na sua instituição**; 8. Índice de ações realizadas de fortalecimento do controle social; 9. Índice de demandas sociais apresentadas a sua instituição, por meio da Ouvidoria; 10. Índice de servidores que cumpriram a meta mínima de horas/ano de capacitação; 11. Índice de nível de satisfação com o dirigente; 12. Índice de relação custo-benefício da sua instituição?

Finalização

1. Você teria alguma sugestão que melhoraria sua gestão, considerando os aspectos legais envolvidos, mas que ainda não conseguiu implementar? (Por exemplo, comportamento mais proativo, repositório oficial das "fontes legais ou regulatórias" classificado, com mecanismos de busca de novos processos ou fluxos de trabalho, especialistas no domínio, melhor rastreabilidade da informação, outros tipos de visualização)
2. Você teria alguma observação adicional?
3. Você teria alguma sugestão a mais com relação a este estudo?
4. Você participa de quais grupos de auditoria, controle, gestão ou gerenciamento estratégicos, de tomada de decisão ou consultivos, como comitês/comissões/grupos de trabalho?
5. Você poderia enviar/compartilhar documentos, decisões, fluxos, “textos legais” ou qualquer outro material, mesmo que sejam tarjadas as informações sigilosas e confidenciais?
6. Você aceitaria receber algumas questões por e-mail? ( ) sim ( ) não

Apêndice A.11 – Roteiro para entrevista sobre as NBR ISO/IEC 38500, 31000 e 27005

Adaptado de Souza et al., 2017.

ID: _____.

Gestão de Risco de Segurança da Informação (GRSI)

1. Os indivíduos e grupos da organização compreendem suas responsabilidades e atuam respeitando a demanda de TI?
2. A estratégia de negócio considera as capacidades atuais e futuras de TI?
3. As aquisições de TI possuem razões válidas embasadas em análises transparentes, contínuas e apropriadas?
4. A TI se adequa e apoia a organização fornecendo serviços baseados em níveis e com qualidade?
5. A TI cumpre com toda a legislação e regulamentos obrigatórios, possuindo políticas e práticas claramente definidas, implementadas e fiscalizadas?
6. As políticas, práticas e decisões de TI demonstram respeito pelo comportamento humano, incluindo as necessidades atuais e futuras das pessoas?

Governança de TI (GTI)

1. Qual o nível de apoio e compreensão dos diretores quanto aos riscos inerentes à TI e seus impactos para o negócio?
2. Os controles implementados pelos gerentes de TI atendem aos requisitos do negócio?
3. A organização atende aos requisitos legais e normativos de segurança da informação?
4. Em que nível a segurança da informação relacionada aos ativos de informação atende às expectativas e percepções dos stakeholders?
5. Qual é o valor estratégico do processo que trata as informações do negócio?
6. Qual é a criticidade dos ativos de informação envolvidos com as informações do negócio?
7. Qual é a importância, do ponto de vista do negócio, da disponibilidade, confidencialidade e integridade das informações?
8. Qual é a importância, do ponto de vista operacional, da disponibilidade, confidencialidade e integridade das informações?
9. Com que frequência ocorrem perdas da disponibilidade, confidencialidade e integridade de informações?
10. Qual é o nível de importância das operações comprometidas com a TI?
11. Qual é o nível do impacto para o negócio da perda de informação causada por um incidente de segurança da informação?
12. Qual é o impacto da interrupção do negócio causado por um incidente de segurança da informação?
13. Qual o nível do impacto causado por um incidente de segurança da informação para a reputação da organização?
14. Qual é o impacto o não atendimento de requisitos legais e normativos de segurança da informação trariam para o negócio?
15. Há um comitê de governança, riscos e conformidade na instituição?
16. Há um comitê de controle de mudanças (CCM)? Como são feitas solicitações de melhorias, defeitos, mudanças de requisitos, inclusão de novos recursos ou novas demandas e evolução dos sistemas?

17. Como são negadas ou priorizadas as demandas de TI? Os critérios estão documentados, e são revistos com que frequência?
18. É mantido o histórico dessas solicitações de melhorias, defeitos, mudanças de requisitos, inclusão de novos recursos ou novas demandas, evolução dos sistemas?
19. Há uma política geral associada a auditoria interna? Qual? Quem seriam esses auditores?
20. Políticas e diretrizes são disponibilizadas a todos os interessados?
21. Padrões, aspectos legais, métodos e melhores práticas são disponibilizados para consultá-los? São atualizados com que frequência?
22. Quais são os papéis e responsabilidades necessários hoje para operacionalizar e gerir a instituição?

Apêndice A.12 – Roteiro para entrevista com *Chief Information Officer* (CIO)

ID: _____.

Políticas, normas, planos e procedimentos

1. Existe um modelo institucional para governança e gestão de TI da instituição?
2. Existem planos ou políticas definidas para desenvolvimento, manutenção e evolução dos sistemas? Como são feitos? Como são atualizados?
3. Existem planos ou políticas definidas para organização e recuperação da informação? Como são feitos? Como são atualizados?
4. Como são recebidas ou promovidas as inovações?
5. Como são auditados os atendimentos às normas e aos padrões dentro da CTI? Existem pessoas nas equipes certificadas? Como foi escolhido o perfil, e qual é a periodicidade desta verificação?

Conformidade legal e regulatória

1. É conhecida a hierarquia das fontes legais ou regulatórias (Constituição Federal, Emendas, Tratados Internacionais, lei complementar, lei específica ou especial, lei ordinária, medida provisória, lei delegada, decreto legislativo, resolução, decreto, portaria, contratos, normas, regimentos, regulamentos, por exemplo) pelos membros da equipe?
2. Antes do levantamento do contexto, como as operações da instituição, elicitação dos requisitos, por exemplo, em algum momento, são buscadas fontes legais ou regulatórias relacionadas? Em quais momentos são buscados esses textos legais? São buscados sistemas semelhantes dentre os "concorrentes"?
3. Qual é o processo para definir o que exatamente tem que ser feito dado uma "fonte legal ou regulatória"? Existe um fluxo pré-definido?
4. Como são decididos os conflitos entre diferentes "fontes legais ou regulatórias"? Ou os requisitos já implementados no sistema? E quando o conflito está nos requisitos legais em si?
5. Quando há conflito entre diferentes "fontes legais ou regulatórias" quem é o responsável por arbitrar?
6. Quem apoia vocês nisso no entendimento das "fontes legais ou regulatórias"? Há especialistas na área de Direito que apoiam o entendimento e a definição do que deve ser realmente implementado?
7. Há profissionais que auxiliem a compreensão ou a definição de fontes legais ou regulatórias aplicadas ao domínio do sistema a ser desenvolvido/mantido? Quem seria esta pessoa um especialista em Direito, uma consultoria contratada, alguém que seja parte da equipe de desenvolvimento ou alguém dentre os stakeholders na instituição/equipe? Se sim, como eles atuam?
8. Como é a relação da CTI com os procuradores?
9. Como são priorizados os requisitos legais ou regulatórios dentro dos projetos?
10. Já presenciou ou participou de alguma situação em que um requisito legal ou regulatório não foi atendido propositalmente? Por qual motivo esta situação aconteceu?
11. Considerando, os diferentes estágios de sistemas (desenvolvimento, manutenção e evolução), como é tratada a transição de estados da vigência da lei? (norma publicada, vacância, vigente, prorrogada, revogada, alterada, convertida, rejeitada, por exemplo)
12. Como são identificados nas fontes legais ou regulatórias o que se referem a direitos, obrigações, promulgação, publicação e vigência/revogação? Como são tratados?

13. Considerando a preocupação nacional e internacional com o direito de privacidade e segurança, o que tem sido feito neste sentido pela CTI?
14. A manutenção da conformidade legal ou regulatória está em maior ou menor grau de importância, quando solicitada uma alteração no sistema?
15. Como é documentada e verificada a conformidade legal e regulatória de um sistema computacional, na instituição?
16. Há alguma sistemática definida para essa documentação ou verificação? Se sim, há alguma periodicidade pré-definida?
17. Hoje, é possível garantir ou evidenciar a conformidade legal e regulatória nos sistemas, na infraestrutura de TI, nos processos, nos contratos ou qualquer outro artefato que seja de responsabilidade da CTI? Como?
18. Quais são as evidências legais possíveis de serem apresentadas ou produzidas em um determinado tempo estipulado para demonstrar a conformidade?
19. Quais são as evidências legais planejadas para uma futura auditoria do sistema desenvolvido?
20. Como é feito o alinhamento da conformidade dos processos de negócio com a conformidade legal dos sistemas computacionais e serviços de TI institucionais?
21. Quais seriam os possíveis órgãos fiscalizadores ou instituições reguladoras interessadas na verificação da conformidade legal do sistema desenvolvido/utilizado?
22. Em algum momento houve alguma auditoria interna/externa relacionada à conformidade legal dos sistemas computacionais (softwares, documentação, infraestrutura, processos, por exemplo)? Como foi a experiência?
23. As auditorias são aplicadas em quais fases do ciclo de desenvolvimento?
24. Os auditores, ou área responsável por tratar do tema, possuem autonomia para a atuação?

Requisitos legais ou regulatórios

1. Quais são as estratégias adotadas para identificar as leis, as normas ou toda e qualquer fonte legal ou regulatória relacionada a um novo requisito?
2. Como é identificado que há um novo requisito legal? Quais artefatos são utilizados para alertar a presença de requisitos legais, quando são necessárias manutenções ou evoluções dos sistemas computacionais junto a CTI?
3. Como são feitas as extrações das informações legais da fonte legal ou regulatória? Onde são armazenadas/refinadas/especificadas antes de serem implementadas? (por exemplo, na especificação, na tarefa no sistema de gerenciamento de projeto)
4. Há alguma diferença de tratamento do requisito legal?
5. Quais são as principais dificuldades em trabalhar com os requisitos legais: **i)** identificar as "fontes legais ou regulatórias"; **ii)** escolher quais as "fontes legais ou regulatórias" são aplicáveis ao domínio; **iii)** extrair os direitos e as obrigações relevantes desses “textos legais”; **iv)** conciliar as "fontes legais ou regulatórias" aplicáveis e as tecnologias disponíveis; ou **v)** tratar a dinamicidade das "fontes legais ou regulatórias"?
6. O senhor já teve problemas internos/externos ou processos administrativos relacionados com requisitos legais não atendidos ou atendidos de forma incorreta?
7. Que tipo de problemas, comumente, são encontrados na engenharia de requisitos legais feita pela CTI? Saberia dizer a origem destes problemas? (imperfeição, imprecisão, dinâmica, ambiguidade dos requisitos ou das "fontes legais ou regulatórias")
8. Como é entendida a “evidência legal”, quando nos referimos a implementação de requisitos legais?

Metodologia de desenvolvimento e gerenciamento de requisitos (verificados, validados, rastreabilidade, testes, monitoramento e visualização)

1. Qual é a natureza dos sistemas computacionais desenvolvidos por sua instituição?
2. Você classificaria a sua instituição como: **i)** é puramente ágil; **ii)** está em processo de transformação ágil; ou, **iii)** por conta da natureza dos sistemas envolvidos, os profissionais precisam utilizar os dois paradigmas?
3. Há quanto tempo vocês optaram pela transformação/adoção de metodologias ágeis?
4. A maior barreira para transformar-se/adotar-se as metodologias ágeis foi:
5. A maior preocupação para transformar-se/adotar-se as metodologias ágeis foi:
6. Motivos pelos quais optaram em transformar/adotar as metodologias ágeis?
7. Quais foram os benefícios dessa transformação/adoção de metodologias ágeis?
8. Quais foram os malefícios dessa transformação/adoção de metodologias ágeis?
9. Como foi essa transformação/adoção de metodologias ágeis?
10. O que facilitou essa transformação/adoção de metodologias ágeis?
11. O que dificultou essa transformação/adoção de metodologias ágeis?
12. Quais metodologias de desenvolvimento são utilizadas em sua equipe?
13. Quais são as práticas e as ferramentas utilizadas, que não estão relacionadas diretamente com as metodologias ágeis?
14. Você sugeriria alguma outra prática ou ferramenta, que não está dentre as utilizadas?
15. Quem decide quais práticas e ferramentas das metodologias ágeis serão utilizadas ou não, no projeto?
16. Qual é o número de sistemas atendidos pela instituição?
17. Qual é o número de projetos em manutenção no momento?
18. Qual é o número de projetos em evolução atualmente?
19. Qual é o número de projetos futuros (demanda reprimida)?
20. Qual é o número de equipes ágeis dentro da sua diretoria? Quantas pessoas há por cada uma dessas equipes?
21. Como são medidos os sucessos ou fracassos nos projetos, que utilizarem metodologias ágeis?
22. Quais seriam os resultados, que você poderia mencionar, para comprovar o sucesso ou o fracasso do projeto, que fez uso de metodologias ágeis?
23. Quais foram as causas dos defeitos/erros/falhas nos projetos, que adotaram metodologias ágeis?
24. O/em que você melhorou ou ganhou com a transformação/adoção de metodologias ágeis?
25. O que foi mais importante nesse processo de transformação/adoção ágil?
26. O que foi menos importante nesse processo de transformação/adoção ágil?

    --- RASTREABILIDADE ---
27. É possível saber quem são as pessoas envolvidas na produção do requisito legal? É importante ter essa informação? Por quê?
28. Como essas pessoas são envolvidas? Isso é importante pra você? Por quê?
29. Se houver mudança de responsável, você teria como saber quem foi o responsável, quem é atualmente, e quando houve a mudança no requisito legal? Como é o processo? Seria relevante ter essa informação? Por quê?
30. Quem precisa ser envolvido ou informado na mudança ou produção do requisito legal? Como você verificaria isso (documentação definida informalmente pelo *stakeholder*)? É importante ter essa informação? Por qual motivo?
31. Quem usa os requisitos legais levantados? Como utilizam? Saber isso é relevante para você? Por quê? Isso altera sua forma de tratar os requisitos legais?
32. Quais os papéis são desempenhados? Ter essa informação é importante? Por quê?

33. Em quais tipos requisitos os stakeholders colaboram? É importante ter essa informação? Por quê?
34. Como e em que momento o cliente é envolvido? É relevante saber essa informação? Por quê?
35. No seu projeto há preocupação com a rastreabilidade?
36. Quais tipos de rastreabilidade vocês usam? Por qual motivo?
37. Que tipos de rastros são verificados?
38. Qual a dificuldade de se manter a rastreabilidade dos requisitos legais? Por quê?
39. É importante para você saber a origem do requisito legal? Como documenta(ria)?
40. Quando é necessário refinar o requisito legal, é criado um relacionamento com o requisito de origem?
41. A modificação das ferramentas, processos e procedimentos feita no último ano trouxe alguma melhoria ou dificuldade? Quais seriam?
    ---- VISUALIZAÇÃO ---
42. Essas modificações trouxeram-lhe algum tipo de visualização de dados para verificar rastros? Quais? (Por exemplo, pessoas envolvidas, papéis desempenhados, mudanças de responsabilidade)
43. Quais visualizações são importantes para você? Por qual motivo?
44. Você faz uso de alguma estratégia ou ferramenta de visualização dos relacionamentos entre os artefatos do projeto? Qual o papel e em quais momentos são/foram importantes no gerenciamento do projeto? Alguma experiência para relatar? Caso contrário, ter uma visualização dos relacionamentos entre os artefatos seria útil no seu dia-a-dia? Por que?
45. A visualização poderia ser relevante para lhe ajudar a identificar problemas, impacto das mudanças ou soluções? Por quê? Se sim, quais tipos de visualização seriam mais adequadas nas classes indicadas por você?
46. Você gostaria de ter algum tipo de visualização sobre alguns dados que não tem hoje, e não foi perguntado sobre?

Expansão da instituição (pessoal, infraestrutura e sistemas)

1. Como aconteceu a expansão da instituição considerando os sistemas e a infraestrutura? Vocês foram consultados? Houve algum planejamento junto à CTI?
2. Como isso vem afetando os serviços, a infraestrutura e os sistemas dentro instituição?
3. Quantos são os sistemas, módulos, centros, aplicativos, ativos, por exemplo, de responsabilidade da CTI? Como é feito este controle?
4. Como são as tomadas de decisão para alteração de tecnologia, evolução ou descontinuidade de módulos ou serviços?
5. Como são feitas as comunicações de mudanças tanto para equipe, como para a comunidade interna e externa? Qual é a hierarquia desta comunicação de mudanças?

Finalização

1. Quais foram as lições aprendidas?
2. Você teria alguma sugestão que melhoraria sua gestão, considerando os aspectos legais envolvidos, mas que ainda não conseguiu implementar? (Por exemplo, comportamento mais proativo, repositório oficial das "fontes legais ou regulatórias" classificado, com mecanismos de busca de novos processos ou fluxos de trabalho, especialistas no domínio, melhor rastreabilidade da informação, outros tipos de visualização)
3. Você teria alguma observação adicional?
4. Você teria alguma sugestão a mais com relação a este estudo?

5. Quanto à comissão externa, seria possível o repasse dos documentos da comissão de priorização e definição do conteúdo das *sprints*?
6. Você aceitaria receber algumas questões por *e-mail*? ( ) sim ( ) não

Apêndice A.13 – Roteiro para entrevista sobre gestão e governança digital e estratégias de governança digital

- Parte 1 - Alinhamento geral

Os princípios do PDTIC foram definidos de forma alinhada aos princípios da EGD?
(1. foco nas necessidades da sociedade; 2. abertura e transparência; 3. compartilhamento da capacidade de serviço; 4. compartilhamento de dados; 5. simplicidade; 6. priorização de serviços públicos disponibilizados em meio digital; 7. segurança e privacidade; 8. participação e controle social; 9. governo como plataforma; 10. inovação)

( ) não Por quê? _____ ( ) sim

As diretrizes do PDTIC foram definidas de forma alinhadas às diretrizes da EGD?
(participação cidadã; melhoria do gerenciamento interno do Estado; e integração com parceiros e fornecedores)

( ) não Por quê? _____ ( ) sim

O referencial estratégico de TI do PDTIC - missão, visão e valores - remete aos eixos da EGD?

( ) não Por quê? _____ ( ) sim

Os objetivos estratégicos de TIC do PDTIC estão aptos a implementarem os preceitos da EGD?

( ) não Por quê? _____ ( ) sim

Os critérios de priorização das demandas foram relacionados à EGD?

( ) não Por quê? _____ ( ) sim

A EGD consta na lista dos documentos de referência?

( ) não Por quê? _____ ( ) sim

Foram definidas metas, com indicadores e prazos, ações e iniciativas relativas à governança digital que contribuam para o alcance dos objetivos da EGD?

( ) não ( ) sim Quais foram as metas? _____

Foram definidas necessidades alinhadas à implementação da EGD?

( ) não ( ) sim Quais? _____

- Parte 2 - Alinhamento das necessidades

Foram identificadas necessidades de TI e ações para disponibilizar bases de dados com seus respectivos artefatos no Portal Brasileiro de Dados Abertos?

( ) não ( ) sim Quais? _____

Foram previstas necessidades de TI e ações para ampliar a prestação de serviços públicos por meios digitais?

( ) não ( ) sim Quais? _____

Foram previstas necessidades de TI e ações para expandir os serviços publicados no Portal de Serviços Públicos?

( ) não ( ) sim Quais? _____

Foram previstas necessidades de TI e ações para aprimorar a qualidade da informação sobre os serviços públicos cadastrados no Portal de Serviços?

( ) não ( ) sim Quais? _____

Foram previstas necessidades de TI e ações para ampliar o uso de serviços públicos digitais pela sociedade?

( ) não ( ) sim Quais? _____

Foram previstas necessidades de TI e ações com o objetivo de aumentar a quantidade de serviços públicos avaliados pela sociedade?

( ) não ( ) sim Quais? _____

Foram previstas necessidades de TI e ações com o objetivo de aumentar a quantidade de serviços públicos utilizando solução unificada de autenticação do cidadão?

( ) não ( ) sim Quais? _____

Foram identificadas necessidades de TI e ações com o objetivo de aumentar o número de APIs disponibilizadas na Plataforma de Interoperabilidade de sistemas e dados do Governo Federal?

( ) não ( ) sim Quais? _____

Foram identificadas necessidades de TI e ações para ampliação da realização de consultas públicas por meios digitais?

( ) não ( ) sim Quais? _____

Apêndice A.14 – Roteiro para entrevista com *Chief Product Officer* (*CPO*) e *Chief Technical Officer* (*CTO*)

ID: _____.

Formação e Experiência acadêmica

- Qual é a sua formação?
- Quais foram as temáticas que você trabalhou na academia?

Experiência profissional

- Instituição em que trabalha?
- Cargo que ocupa?
- Função que desempenha?
- Tempo de experiência profissional neste cargo?
- Quais são as suas atribuições?
- Trabalhou em outro cargo? ( ) Não ( ) Sim
    - Se sim, qual(is)?
- Quais temáticas dos sistemas que você já trabalhou?

Atuação

- Fale-me um pouco da sua experiência:
    - Na área de desenvolvimento.
    - Na gestão de equipes.

- Teve alguma experiência com a Engenharia de Requisitos?
    - Se sim, conte-me um pouco sobre essa experiência.

Documentação de requisitos

- O que você entende sobre documentação de requisitos?
- Quais são os artefatos definidos para a documentação?
    - Por que motivos estes foram os artefatos escolhidos?
    - Esses artefatos atualmente atendem ao propósito para o qual foi definido?
- Em quais momentos a documentação mostrou-se importante no ciclo de vida dos sistemas?
- Para quais papéis (gerência, desenvolvimento, testes, outros) você acredita que a documentação de requisitos é mais importante?
- Quais dificuldades você acredita que a equipe tenha na elaboração da documentação? E por quê isso acontece?
- A quem você pretende atender com documentação? e por quê?
- Quais critérios foram levados em conta para elaborar a estrutura do modelo de artefato utilizado?
- Como é verificada a conformidade legal dos sistemas desenvolvidos ou mantidos pela CTI?
    - Quais são as evidências buscadas?

Decisões

- Quais estratégias você utiliza para:
    - Definir quais artefatos de requisitos serão utilizados?
    - Estimular a colaboração entre os membros das equipes?
    - Estimular a cooperação entre as instituições parceiras?
- Quais são os artefatos utilizados para sua gerência?
- Como você monitora o uso dos artefatos definidos?

Desafios da Gestão

- Dentro da sua gestão e considerando sua experiência, qual a importância do analista de requisitos?
- Considerando os papéis existentes nas equipes de desenvolvimento, por qual motivo as atribuições de um analista de requisitos foram acumuladas ao analista de negócios?
- Como você vê a colaboração entre os analistas de requisitos?
- Como funciona o relacionamento com as cooperadas?
    - No entendimento dos sistemas, das dúvidas?
    - Algo tem sido relatado como dificuldade?

- Como funciona a questão do versionamento dos sistemas para as cooperadas?

Descontinuidade de soluções e sistemas legados

- Como você vê a descontinuidade no uso dos sistemas?
- Existe um plano de gestão de risco:
    - Ações associadas a entrada e saída de analista de requisitos?
        - Se sim, como funciona (contingenciamento)?
        - Instituições cooperadas (entrada e saída)?

Encerramento

Você teria alguma sugestão a mais? algo que gostaria de comentar?
Quais são os seus planos futuros para sua gestão a pequeno, médio e longo prazo?

Apêndice A.16 – Roteiro para entrevista por *e-mail* para *Chief Product Officer* (*CPO*) e *Chief Technical Officer* (*CTO*)

Ser *Chief Product Officer - (CPO) ou Chief Technical Officer (CTO)*

1. Qual foi a sua maior dificuldade?
2. Qual era o organograma antes da sua chegada? Como está esse organograma depois inclusive com as últimas demissões, realocações, rescisões de contratos?
3. Como você gerencia e controla todas as atividades da diretoria? Quais são as estratégias utilizadas? Quais são as ferramentas utilizadas? Quais são as estratégias utilizadas para relacionar (rastrear) todas as informações das equipes e da diretoria?
4. Você participa de quais grupos de auditoria, controle, gestão ou gerenciamento estratégicos, de tomada de decisão ou consultivos, como por exemplo comitês/comissões/grupos de trabalho? Saberia informar por quais motivos foi escolhida?
5. Você poderia enviar/compartilhar documentos, decisões, fluxos, "textos legais" ou qualquer outro material, mesmo que sejam tarjadas as informações sigilosas e confidenciais?

Sua equipe e interseções

1. Como é solicitado um novo membro? Como é justificada a solicitação?
2. Como são distribuídos os membros pelas equipes?
3. Como são divididas essas pessoas dentre as equipes existentes?
4. Existe alguma interseção clara entre as equipes de sistemas e infraestrutura? Inclusive considerando atividades, necessidades, prioridades e cronogramas?
5. Como é feita a integração entre estas equipes?
6. Quais foram/são as iniciativas para melhorar esta integração?
7. Quais são os indicadores de produtividade, qualidade e competências utilizados?
8. Como são promovidas e retribuídas aquisição de maior produtividade, qualidade e competências nos recursos humanos da CTI? E como são penalizados nos casos contrários?
9. Você acredita que é conhecida a hierarquia de comando e as responsabilidades de cada cargo? Como são decididos os conflitos? Quem é o árbitro final?
10. Para você seria relevante ter a sistematização dos desdobramentos relacionados à perda de um membro da equipe? (Lembrando que a perda de um membro na equipe pode levar a perda de conhecimento) É importante ter essa informação? Por quê?

Apêndice A.17 – Roteiro para entrevista com Analista/Engenheiro(a) de Requisitos

Feito em parceria com Souza (2019).

ID: _____.

Formação e Experiência acadêmica

- Formação
- Tem alguma experiência em pesquisa(s) acadêmica(s)? ( ) Não ( ) Sim
    - Se sim, de que tipo(s): [ ] iniciação científica [ ] trabalho de conclusão de curso [ ] dissertação de mestrado [ ] tese de doutorado
        - Qual(is) temáticas?
- Cursos de extensão (qualquer) ou aperfeiçoamento (voltado para profissão atual).

Experiência profissional

- Instituição em que trabalha?
- Cargo que ocupa?
- Função que desempenha?
- Tempo de experiência profissional neste cargo?
- Quais são as suas atribuições?
- Trabalhou em outro cargo? ( ) Não ( ) Sim
    - Se sim, qual(is)?

Estratégias de atualização

- Quais são as formas que você utiliza para se atualizar?
- Você tem interesse por quais áreas de conhecimento?

Atuação

- Qual é a sua experiência com a Engenharia de Requisitos nas metodologias/técnicas de:
    - Elicitação de requisitos:
        - Realização de entrevistas ou aplicação de questionários (**técnicas de pesquisa**)?
        - Utilização de *brainstorming*, *brainstorming paradox*, mudança de perspectiva ou técnicas de analogia (**técnicas de criatividade**)?
        - Realização de arqueologia de sistema, leitura baseada em perspectiva ou reutilização (**técnicas baseadas em documentos**)?
        - Observação de campo ou *apprenticing* (**técnicas de observação**)?
        - Protótipos, mapas mentais, *workshops*, cartões CRC, gravações de áudio e vídeo, modelagem de casos de uso ou "*user stories*" (**técnicas de apoio**)?
    - Documentação
        - Realização de modelagem conceitual - como uso dos diagramas da UML?

        - Uso de estruturas de documentos - estruturas padronizadas ou conteúdo padrão customizados?
        - Criação de glossário?
    - Validação
        - Emissão de parecer de especialista?
        - Realização de inspeção?
        - Realização de *walkthrough*?
        - Feitura de leitura baseada em perspectiva?
        - Validação por protótipos?
        - Utilização de checklists?
    - Gerenciamento de requisitos
        - Designação de atributos para requisitos?
        - Visualização de requisitos?
        - Priorização de requisitos?
        - Implementação da rastreabilidade de requisitos?
        - Versionamento de requisitos?
        - Gerenciamento de mudança de requisitos?
- Você já utilizou alguma outra técnica não mencionada?
- Em que sua atuação profissional influencia no trabalho da sua equipe?
    - Como?
- Existem iniciativas de colaboração entre os analistas de requisitos?
    - Se sim, fale-nos um pouco sobre elas?
- Existem iniciativas de colaboração entre os demais cargos?
    - Se sim, fale-nos um pouco sobre elas?
- Entre as instituições parceiras, como é realizada a cooperação técnica?

Organização e Recuperação da Informação

- Qual a importância que você atribui às suas atividades?
- Qual o papel que você atribuiria aos requisitos dentro do ciclo de vida dos sistemas?
- Em relação a definição de uma estratégia de documentação:
    - (1. quanto ao conteúdo)
        - Como são definidas as categorias de informação (estrutura do documento) prioritárias?
    - (2. quanto à forma)
        - Como são definidos os artefatos prioritários?
    - (3. quanto ao estilo)
        - Como são definidos os critérios de estilo de escrita para artefatos "documentalmente escritos"? (por exemplo: simplicidade ou detalhamento das regras)
    - (4. quanto ao público-alvo)
        - Como é definido o público-alvo da documentação? (por exemplo: foco no entendimento usuário final ou no entendimento do corpo técnico?)
- De que forma as necessidades da manutenção do sistema impactam a documentação dos requisitos?
- Como são criados, gerenciados e preservados as definições e os artefatos produzidos?
- Existem políticas ou modelos disponíveis para auxiliar a construção e manutenção dos artefatos?
- De alguma forma, há uma base de conhecimento produzido?

    - Se sim, há o reuso ou reaproveitamento do que foi produzido?
- Quais são as atividades executadas com o objetivo de recuperação da informação?
    - (Por exemplo, tomada de decisão para alteração de tecnologia, evolução ou descontinuidade de módulos)
    - Nesse mesmo contexto, quais são os instrumentos e artefatos utilizados?
- Em quais momentos os artefatos existentes já foram utilizados como evidência legal? (por exemplo, para dirimir dúvidas com clientes ou na equipe, comprovar a implementação ou a conformidade com o que definido ou exigido)

Fechamento

Como a sua prática pode ser melhorada?

Você teria alguma sugestão a mais?

Apêndice A.18 – Roteiro para entrevista com Desenvolvedor(a), Analista e Engenheiro(a) de Requisitos (primeira fase)

Feito em parceria com Santos (2017) e Trindade (2018).

ID: _____.

Gerenciamento de requisitos

1. Existe alguma estratégia definida que permite o acompanhamento, evolução ou gerenciamento dos requisitos do *software*?
2. Vocês utilizam alguma ferramenta de gerenciamento de requisitos?
3. Você poderia descrever o fluxo padrão de trabalho, normalmente utilizado, do processo de definição de requisitos (elicitação, modelagem, análise)?
4. Alguma técnica específica de priorização dos requisitos é utilizada durante o processo de definição dos requisitos? Se existe, quem é o responsável?

Rastreabilidade e testes

1. Principais dificuldades para manter os requisitos atualizados e integrados com os outros dados (código, banco, testes) gerados durante o desenvolvimento e manutenção?
2. Existe algum mecanismo que permita a verificação de relacionamentos existentes entre os diversos artefatos do sistema?
3. É utilizada alguma metodologia de planejamento e realização dos testes (unitário, integração)?
4. Você poderia descrever o fluxo padrão do processo de testes?
5. É possível estabelecer algum tipo de ligação entre os testes, o código-fonte da funcionalidade implementada e os requisitos que deram origem a funcionalidade?

Requisitos legais

1. Na fase de elicitação de requisitos, a equipe se preocupa com as leis do sistema?
2. Como vocês sabem que há uma nova "fonte legal ou regulatória" a ser atendida?
3. Algum profissional auxilia no entendimento das leis? Preparação da equipe?
4. É conhecida a hierarquia das fontes legais ou regulatórias (Constituição Federal, Emendas, Tratados Internacionais, lei complementar, lei específica ou especial, lei ordinária, medida provisória, lei delegada, decreto legislativo, resolução, decreto, portaria, contratos, normas, regimentos, regulamentos, por exemplo) pelos membros da equipe?
5. É possível identificar quais requisitos têm relação com as leis (quantificar)?
6. Existe alguma forma de saber quais partes do sistema (código, banco, relatórios) estão relacionados com os requisitos legais?
7. Quando é alterada uma norma, quais os procedimentos realizados?

Monitoramento e conformidade legal

1. Como é feito o acompanhamento e a evolução das leis?
2. É feita validação dos requisitos legais?
3. Após a implementação, os *stakeholders* são comunicados para validar os requisitos legais implementados?
4. Como é feito o monitoramento da conformidade legal dos sistemas?
5. O sistema está em conformidade atualmente? Seria possível afirmar isso?!

6. Como é feita a avaliação do risco de inconformidade legal do sistema? E das possíveis sanções de má implementação do requisito legal?
7. Quando é necessário realizar uma manutenção ou a evolução de um sistema, como é garantida que a conformidade legal será mantida?
8. O que você entende por visualização de rastros/links entre artefatos?
9. Utiliza algum tipo de visualização de dados para verificar rastros? Como: pessoas envolvidas, papéis desempenhados, mudanças de responsabilidades…
10. Gostaria de ter algum tipo de visualização sobre alguns dados que não tem hoje e não foi perguntado sobre?

Você aceitaria receber algumas questões por e-mail? ( ) sim ( ) não

Entrevistador(a): _____ Data: ____/____/_____

Apêndice B – *Template* para criação de documentação de um requisito

Apêndice B.1 – *Template* para criação de documentação de um requisito inspirado nos atributos de um requisito preconizado por Pohl (2010)

Origem	**Identificador**
<Código da origem>	<Código do requisito>
Nome	
<Nome único a ser dado ao requisito>	
Descrição	
<Descrição do requisito em si>	
Versão	**Autor**
<Versão atual do requisito>	<Autor do requisito>
Criticalidade	**Prioridade**
<Estimativa da extensão de perdas e danos, e de possível ocorrência>	<Prioridade do requisito frente a outro para sua implementação>
Responsável	**Tipo de requisito**
<Responsável pela especificação do conteúdo do requisito>	<Especifica o tipo de requisito>
Status de validação	**Status de acordo**
<Indica o status atual da validação>	<Indica o status atual da negociação de acordo>
Esforço	**Release**
<Esforço estimado/efetivo para implementar o requisito>	<Designa a release na qual o requisito deverá ser implementado>
Obrigatoriedade legal ou regulatória	**Referências cruzadas**
<Especifica o grau de obrigatoriedade legal ou regulatória do requisito>	<Especifica os relacionamentos com outros requisitos>

Informações gerais	
<Inclui quaisquer informações consideradas relevantes>	
Fontes Legais ou Regulatórias - FLR	
<Origem da fonte legal ou regulatória>	<Detalhamento da fonte legal ou regulatória>

Apêndice C – Exemplos da transformação de história de usuário em requisito legal ou regulatório e sua relação com a legislação aplicável

Apêndice C.1 – Exemplo 01 da transformação de história de usuário em requisito legal ou regulatório e sua relação com a legislação aplicável

Origens	**Identificador**
HU00078	RLR00056
O Sistema deverá solicitar ao usuário a confirmação da leitura das políticas de privacidade e de segurança.	
Fonte Legal ou Regulatória - FLR	
FLR001 - Lei 8.078, de 11 de setembro de 1990 dispõe sobre a proteção do consumidor e dá outras providências. (Código de Defesa do Consumidor)	FLR001.1 - Art. 43, parágrafo primeiro. Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
FLR002 - Decreto nº 7.962, de 15 de março de 2013 regulamenta a Lei no 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico (Lei do e-Commerce)	FLR002.1 - Art 4o, inciso VII. utilizar mecanismos de segurança eficazes para pagamento e para tratamento de dados do consumidor.
FLR003 - Lei 12.965, de abril de 2014 estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. (Marco Civil da Internet)	FLR003.1 - Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

FLR004 - Lei 13.709, de agosto de 2018 dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (Lei Geral de Proteção de Dados Pessoais - LGPD)	FLR004.1 - Art. 2o. inciso I. o respeito à privacidade.
	FLR004.2 - Art. 2o. inciso IV. a inviolabilidade da intimidade, da honra e da imagem.
	FLR004.3 - Art. 7o. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses. inciso I - mediante o fornecimento de consentimento pelo titular.
	FLR004.4 - Art. 7o. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses. inciso II - para o cumprimento de obrigação legal ou regulatória pelo controlador.
	FLR004.5 - Art. 7o. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses. inciso X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.
	FLR004.6 - Art. 8o. O consentimento previsto no inciso I do Art. 7o. desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

Apêndice C.2 – Exemplo 02 da transformação de história de usuário em requisito legal ou regulatório e sua relação com a legislação aplicável

Origens	**Identificador**
HU00078	RLR00057
O Sistema deverá solicitar ao usuário a confirmação da leitura do termo de serviços.	
Fonte Legal ou Regulatória - FLR	
FLR001 - Lei 8.078, de 11 de setembro de 1990 dispõe sobre a proteção do consumidor e dá outras providências. (Código de Defesa do Consumidor)	FLR001.1 - Art. 43, parágrafo primeiro. Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
FLR002 - Decreto nº 7.962, de 15 de março de 2013 regulamenta a Lei no 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico (Lei do e-Commerce).	FLR002.1 - Art 4o, inciso VII. utilizar mecanismos de segurança eficazes para pagamento e para tratamento de dados do consumidor.
FLR003 - Lei 12.965, de abril de 2014 estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. (Marco Civil da Internet)	FLR003.1 - Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
FLR004 - Lei 13.709, de agosto de 2018	FLR004.1 - Art. 2o. inciso I. o respeito à

dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (Lei Geral de Proteção de Dados Pessoais - LGPD)	privacidade.
	FLR004.2 - Art. 2o. inciso IV. a inviolabilidade da intimidade, da honra e da imagem.
	FLR004.3 - Art. 7o. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses. inciso I - mediante o fornecimento de consentimento pelo titular.
	FLR004.4 - Art. 7o. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses. inciso II - para o cumprimento de obrigação legal ou regulatória pelo controlador.
	FLR004.5 - Art. 7o. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: inciso X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.
	FLR004.6 - Art. 8o. O consentimento previsto no inciso I do Art. 7o. desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

Apêndice C.3 – Exemplo 03 da transformação de história de usuário em requisito legal ou regulatório e sua relação com a legislação aplicável

Origens	**Identificador**
HU00078; RLR00056; RLR00057	RLR00098
O Sistema deverá solicitar que o usuário demonstre a manifestação de consentimento do tratamento de seus dados pessoais.	
Fonte Legal ou Regulatória - FLR	
FLR001 - Lei 8.078, de 11 de setembro de 1990 dispõe sobre a proteção do consumidor e dá outras providências. (Código de Defesa do Consumidor)	FLR001.1 - Art. 43, parágrafo primeiro. Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
FLR002 - Decreto nº 7.962, de 15 de março de 2013 regulamenta a Lei no 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico (Lei do e-Commerce)	FLR002.1 - Art 4o, inciso VII. utilizar mecanismos de segurança eficazes para pagamento e para tratamento de dados do consumidor.
FLR003 - Lei 12.965, de abril de 2014 estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. (Marco Civil da Internet)	FLR003.1 - Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

FLR004 - Lei 13.709, de agosto de 2018 dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (Lei Geral de Proteção de Dados Pessoais - LGPD)	FLR004.1 - Art. 2o. inciso I. o respeito à privacidade.
	FLR004.2 - Art. 2o. inciso IV. a inviolabilidade da intimidade, da honra e da imagem.
	FLR004.3 - Art. 7o. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: inciso I - mediante o fornecimento de consentimento pelo titular.
	FLR004.4 - Art. 7o. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: inciso II - para o cumprimento de obrigação legal ou regulatória pelo controlador.
	FLR004.5 - Art. 7o. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: inciso X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.
	FLR004.6 - Art. 8o. O consentimento previsto no inciso I do Art. 7o. desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

Apêndice D – Instrumentos de Apoio à Avaliação do *Framework* Proposto

Apêndice D.1 – Planejamento das entrevistas e do questionário

Proposta do estudo e seu objetivo:

Apresentar aos participantes o *Framework*, e apreender suas impressões frente suas responsabilidades cotidianas na implementação e na manutenção da conformidade legal e regulatória de sistemas computacionais. Além disso, descobrir os desafios não vencidos pelo *Framework* com o objetivo de mitigá-los.

Público-alvo:

Gestores, líderes de equipe e analistas/engenheiros de requisitos

Candidato(a) para piloto:

Lista de candidatos a respondentes:

Prazos:

Piloto:
Entrevista com participantes:
Análise preliminar:
Resultados preliminares:
Análise final:
Resultados:

Metodologia:

Abordagem de seleção e contato
Técnicas e processos a serem utilizados
Tipos de questões e objetivos a serem alcançados
Instrumentos a serem utilizados

***E-mails*:**

Convite
Roteiro de entrevista pré-abordagem da aplicação do *Framework*
Agradecimento

Equipamentos a serem utilizados:

Gravador de áudio ou vídeo
Formulário *online*

Ambientes

Online
Espaço sugerido pelo participante

Formulário

Autorização
TCLE
TCUIAV
Mensagem inicial

Execução

Informar o próprio nome
Comentar um pouco sobre o projeto
Informar qual é a proposta deste estudo
Falar sobre o tempo estimado para execução das atividades propostas
Pedir leitura e assinatura (ou consentimento) dos TCLE e TCUIAV
Pedir autorização para gravação
Iniciar a gravação
Confirmar o consentimento a partir do início da gravação ou confirmar o consentimento a partir da "mensagem" com um ponteiro para TCLE
Avisar que a integridade e a privacidade do(a) participante será totalmente preservada como descrito nos Termos
Perguntar se ficou alguma dúvida com relação ao preenchimento do questionário
Tirar dúvidas
Iniciar apresentação
Apresentar os conceitos, o *Framework* e os exemplos do tratamento de fonte e requisito legais ou regulatórios utilizando o *Framework*
Finalizar apresentação
Questionar se ficou alguma dúvida
Tirar dúvidas
Iniciar as perguntas do roteiro para entrevista pós-abordagem do *framework*
Questionar se ficou alguma dúvida
Tirar dúvidas
Finalizar entrevista

Finalização

Agradecimento pela participação e pela colaboração
Confirmação da possibilidade de envio de um *e-mail*

Apêndice D.2 – Modelos de *e-mails*

1. *E-mail* de convite para participação de entrevista

Assunto: Conformidade legal e regulatória de sistemas computacionais - convite

Olá, <Nome do(a) convidado(a)>.

Eu me chamo Erica Miranda, e sou aluna do curso de doutorado em Ciência da Computação, da Universidade Federal do Rio Grande do Norte (UFRN). Meu projeto de pesquisa está relacionado com a investigação, proposta e validação de um *framework* para conformidade legal e regulatória de sistemas computacionais.

Para esta fase da pesquisa, convido você a participar de uma entrevista sobre o uso deste framework para gerenciamento de requisitos e fontes legais ou regulatórias. Estimamos que essa entrevista deverá levar em torno de 1 h. Assim, peço que escolha o melhor dia/horário para você dentro das opções disponíveis na planilha no endereço a seguir, e me informe, para que dia/horário sejam reservados para uma videoconferência (Google Meet):

<link>

Desde já, agradeço a sua colaboração.

Fico no aguardo do seu retorno.
Erica Miranda.

2. *E-mail* de encaminhamento do formulário de pré-entrevista

Assunto: Confirmação de agendamento da participação na entrevista

Olá, <Nome do(a) convidado(a)>.

Agradeço seu aceite em participar da entrevista por videoconferência (Google Meet), no dia <data - horário >, para meu projeto de pesquisa sobre um *framework* para conformidade legal e regulatória de sistemas computacionais.

Antes desta data e deste horário, preciso que você preencha um formulário disponível neste endereço:

<link>

Cordialmente,

Erica Miranda.

3. *E-mail* de reiteração de convite ao preenchimento do formulário online (pré-entrevista)

Assunto: Preenchimento do formulário online

Olá, <Nome do(a) convidado(a)>.

Tudo bem?

Observei que você ainda não preencheu o formulário. Quando puder, mas antes do dia e do horário da entrevista, preciso que você preencha este formulário, que está disponível no endereço:

<*link*>

Cordialmente,
Erica Miranda.

4. *E-mail* de informação da sala ao participante

Assunto: Sala no Google Meet para nossa entrevista.

Olá, <Nome do(a) convidado(a)>.

Hoje, é o dia da nossa entrevista, que ocorrerá através do Google Meet, na sala:
<Endereço da sala no Google Meet>

Aguardo por você no horário combinado (<horário marcado>).
Erica Miranda.

5. *E-mail* de agradecimento pela participação

Assunto: Agradecimento pela participação na entrevista

Olá, <Nome do(a) convidado(a)>.

Agradeço sua participação na entrevista para meu projeto de pesquisa sobre um framework para conformidade legal e regulatória de sistemas computacionais. Sua colaboração permitirá maior entendimento dos objetos desta pesquisa.

Cordialmente,
Erica Miranda.

6. *E-mail* de reiteração de convite à entrevista (INFORMAL)

Assunto: Convite para participação de entrevista

Olá, <Nome do(a) convidado(a)>.

Bem sei, que na correria cotidiana, algumas atividades ficam para depois. Entretanto, como a mensagem também pode ter ido para sua caixa de spam, reencaminho meu convite para participação de uma entrevista enviada anteriormente.

Conto com a sua colaboração,
Erica Miranda.

7. *E-mail* de reiteração de convite à participação de entrevista após a falta

Assunto: Ausência no horário marcado para entrevista

Olá, <Nome do(a) convidado(a)>.

Tudo bem?

Imprevistos acontecem. Você gostaria de marcar um novo dia/horário para nossa entrevista?

Se sua resposta foi sim, ficaria muito grata se você verificasse os dias/horários disponíveis, no link a seguir, ou me informasse sua disponibilidade para agendarmos nossa entrevista.

<link>

Desde já, agradeço a sua colaboração.

Fico no aguardo do seu retorno.
Erica Miranda.

8. *E-mail* de reiteração de convite à participação de entrevista após segunda chamada

Assunto: Conformidade legal e regulatória de sistemas computacionais - convite

Olá, <Nome do(a) convidado(a)>.

Tudo bem?

Sua participação é muito importante para meu projeto de pesquisa, que está relacionado com a investigação, proposta e validação de um framework para conformidade legal e regulatória de sistemas computacionais. Por este motivo, apresento minha insistência na sua participação.

Peço que escolha o melhor dia/horário para você dentro de sua disponibilidade para uma videoconferência (Google Meet) e, assim, sincronizarmos um dia/horário para uma entrevista.

Desde já, agradeço a sua colaboração.

Fico no aguardo do seu retorno.
Erica Miranda.

Apêndice D.3 – Termo de Consentimento Livre e Esclarecido (TCLE)

Fui convidado(a) a participar de um estudo relacionado como o projeto de pesquisa nomeado "Documentação e Rastreabilidade de Artefatos para Evolução Sustentável de Sistemas Computacionais", cujo objetivo é oferecer subsídios adequados à documentação e à rastreabilidade dos artefatos do ciclo de vida de sistemas para equipes na indústria de desenvolvimento de sistemas. Sendo que, nesta fase do projeto, o foco está na conformidade legal e regulatória desses sistemas.

A minha participação no referido estudo acontece no sentido de auxiliar a investigação sobre as dificuldades e as estratégias utilizadas na documentação e na rastreabilidade de artefatos para evolução sustentável de sistemas computacionais visando a implementação ou manutenção da conformidade legal e regulatória desses sistemas computacionais.

Fui alertado(a) de que, da pesquisa a se realizar, posso esperar alguns benefícios, tais como: aprendizagem da abordagem, estratégias e dos artefatos oriundos da pesquisa em si. Recebi, por outro lado, os esclarecimentos necessários sobre os possíveis desconfortos e riscos decorrentes do estudo, levando-se em conta que é uma pesquisa, e os resultados positivos ou negativos somente serão obtidos após a sua realização. Assim, poderei sentir cansaço ou fadiga pelo número de horas dispensadas na realização do estudo.

Estou ciente de que minha privacidade será respeitada, ou seja, meu nome ou qualquer outro dado ou elemento que possa, de qualquer forma, identificar-me, será mantido em sigilo. Além disso, saliento que tenho conhecimento de que a documentação produzida será mantida por até dois anos para fins legais. Também fui informado(a) de que posso me recusar a participar do estudo, ou retirar meu consentimento até a finalização da execução das atividades deste estudo, sem precisar justificar, e de, por desejar sair da pesquisa, não sofrerei qualquer prejuízo à assistência que venho recebendo.

É assegurada a assistência durante toda pesquisa, bem como o livre acesso a todas as informações e os esclarecimentos adicionais sobre o estudo e suas consequências, enfim, tudo o que eu queira saber antes, durante e depois da minha participação. Enfim, tendo sido orientado(a) quanto ao teor de todo o aqui mencionado e compreendido a natureza e o objetivo do já referido estudo, manifesto meu livre consentimento em participar, estando totalmente ciente de que não há nenhum valor econômico, a receber ou a pagar, por minha participação.

A saber, as pesquisadoras envolvidas com o referido estudo são:
Profa. Márcia Jacyntha Nunes Rodrigues Lucena (coordenadora) - e-mail: marciaj@dimap.ufrn.br.
Erica Esteves Cunha de Miranda - e-mail: erica@ppgsc.ufrn.br.

Por esta ser a expressão da minha vontade, darei continuidade ao preenchimento dos formulários e da minha participação em entrevistas realizadas de maneira online ou presenciais de acordo com a minha disponibilidade.

Apêndice D.4 – Roteiro para questionário pré-abordagem da apresentação do *Framework*

Conformidade Legal e Regulatória

Você foi convidado(a) a participar de uma entrevista. Para darmos o primeiro passo, precisamos saber um pouco mais de você e do seu cotidiano, e para isso pedimos que preencha este formulário com toda sua atenção. O tempo de preenchimento é de 10 a 15 minutos.

Leia o Termo de Consentimento Livre e Esclarecido (TCLE), que explica um pouco mais sobre a pesquisa, e define como será sua participação. Sinta-se à vontade para contatar-nos.

O TCLE está disponível no endereço: <*link*>

1. Id do(a) participante: _____. (e-mail no formulário)
2. Você concorda com os termos estabelecidos no TCLE?
    a. Não
    b. Sim

Informações pessoais e acadêmicas

3. Qual é a sua idade?
4. Qual é o seu sexo?
    a. Feminino
    b. Masculino
    c. Prefiro não declarar
5. Qual é a sua formação acadêmica?

Informações profissionais

6. Em que área você atua?
    a. Analista de Requisitos
    b. Analista de Sistemas
    c. Auditor(a)
    d. Desenvolvedor(a)
    e. Gerente de Equipe
    f. Gestor(a) de Infraestrutura
    g. Gestor(a) de Sistemas
    h. Testador(a)
    i. Outro: _____
7. Há quanto tempo você atua nesta área?
    a. Menos de um ano

    b. Entre um e três anos
    c. Entre quatro e seis anos
    d. Outro
8. Quais são as suas principais atribuições?
9. Quais são as suas principais dificuldades e desafios nas suas atividades diárias?
10. O reuso e a sustentabilidade são práticas na instituição?
    a. Não
    b. Sim
11. Quais os tipos de rastreabilidade que são feitas na sua instituição?
    a. Pré-especificação de requisitos
    b. Pós-especificações de requisitos
    c. Entre requisitos
    d. Não é feito nenhum tipo de rastreabilidade
    e. Desconheço o que venha ser rastreabilidade
12. Quais são os tipos de visualização da informação em diferentes contextos e níveis praticados na sua instituição?

Requisitos legais ou regulatórios

Os requisitos legais ou regulatórios estão relacionados com leis, normas, regimentos, regulamentos; e não podem deixar de ser atendidos sob pena de alguma sanção.

13. Você utiliza alguma ferramenta para gerenciamento de requisitos?
    a. Não
    b. Sim
14. Esta ferramenta oferece recursos como rastreamento, visualização da informação, atualização dos dados, como seu refinamento, por exemplo?
15. Há presença de requisitos legais ou regulatórios nos sistemas sob sua gestão?
    a. Não
    b. Sim
16. Fale um pouco desses requisitos legais ou regulatórios, que estejam presentes nos sistemas computacionais com que você trabalha?

Implementação e manutenção da conformidade legal e regulatória

17. Nos sistemas de informação sob sua gestão, quais são os instrumentos e evidências de conformidade legal e regulatória?
18. Você já sofreu ou participou de alguma auditoria no âmbito dos sistemas computacionais em que trabalha ou trabalhou? Se sim, conte-nos como foi.

Agradecemos, e aguardamos por sua participação na entrevista.

Apêndice D.5 – Apresentação sobre o *Framework* realizada antes das entrevistas

Framework

Conformidade Legal e Regulatória

Agenda

- Problema
- Objetivo geral
- Direcionamento para conformidade legal e regulatória
- Hierarquia legal e regulatória
- Vigência legal
- Visão geral do Framework
- Exemplos

2

Problema

- A **falta da observação** de leis, normas, regulamentação, regimentos, estatutos, em suma **"fontes legais ou regulatórias"**, presentes na sociedade moderna, resulta na inconformidade legal ou regulatória em todos e quaisquer sistemas, independente de sua natureza, seu propósito, ou sua classificação
- A conformidade legal e regulatória não é algo, simplesmente, a ser atingida e, sim, regularmente a ser **verificada e mantida**

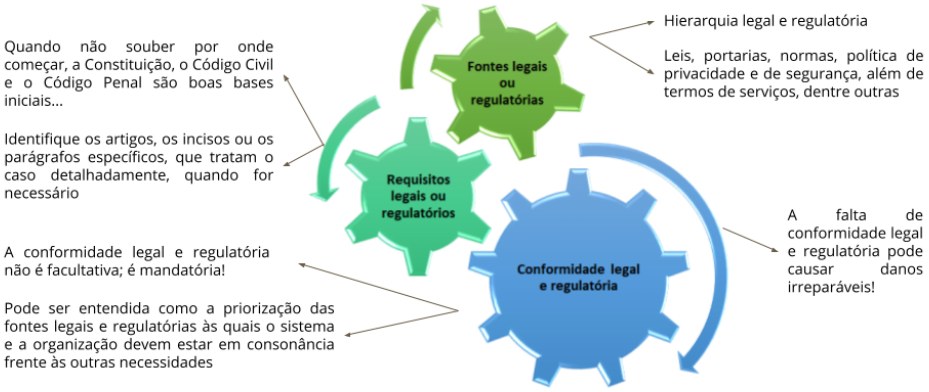
3

Objetivo geral

- O objetivo geral desta pesquisa é propor uma **sistemática para melhorar a conformidade legal e regulatória dos sistemas computacionais** a partir da evolução do sistema, das fontes legais ou regulatórias aplicáveis ao contexto do sistema e dos requisitos legais ou regulatórios elicitados ou atualizados

4

Direcionamento para conformidade legal e regulatória



5

Hierarquia legal e regulatória

1. Constituição Federal e emendas constitucionais promulgadas
2. Tratados internacionais e direitos humanos
3. Leis complementares
4. Leis ordinárias
5. Leis delegadas
6. Medidas provisórias
7. Decretos legislativos e resoluções
8. Decretos autônomos
9. Legislação estadual
10. Atos normativos secundários
11. Leis anteriores à Constituição em vigor
12. Leis que tenham sido revogada
13. Leis municipais em face da Constituição Federal
14. Propostas de emenda constitucional ou projetos de lei
15. Súmulas
16. Contratos

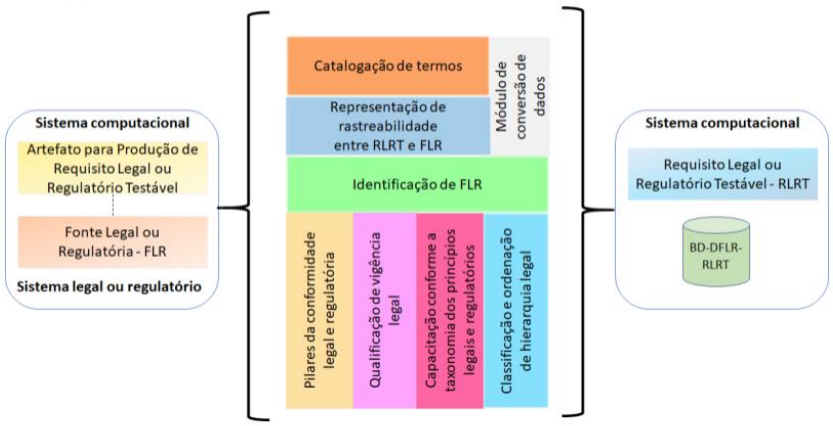
6

Vigência legal

- Alterada
- Convertida
- Declarada insubsistente
- Declarada perempta
- Decurso de prazo
- Em vacância
- Não vigente
- Prejudicada
- Prorrogada (prorrogação de vigência)
- Publicada
- Rejeitada
- Revogada
- Suprimida (no sentido de revogação) x supressão de dispositivo
- Vigente

7

Visão geral do Framework

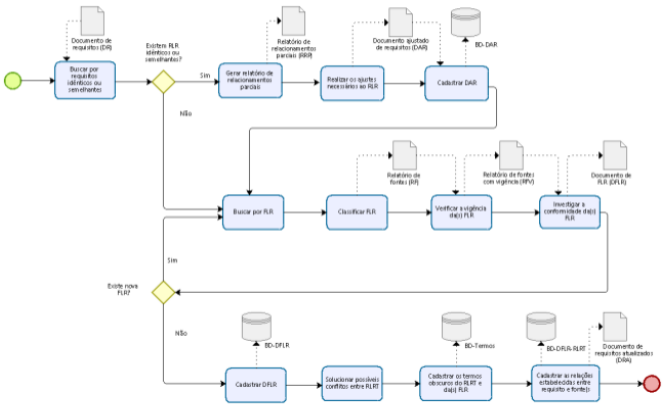


8

Fundamentação de RLRT a partir de FLR

9

Fluxo de atividades para fundamentação RLRT com FLR



Fundamentação de RLRT a partir de FLR 1/5

Raça/Cor → História

- Constituição
  - "Art. 3º Constituem objetivos fundamentais da República Federativa do Brasil: (...)
    - IV - **promover o bem de todos**, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação."
  - "Art. 5º Todos são **iguais perante a lei**, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade (...)"
- UERJ 2000 (cotas sociais), UnB 2004 (cotas raciais)
- Censo da Educação Superior de 1997 e 2009
  - "não declarada", "não dispõe de informação"
  - Lei 12288/2010 → delibera sobre questões étnicos-raciais
  - Portaria Normativa MEC nº 21, 28 de agosto de 2013 → igualdade

Fundamentação de RLRT a partir de FLR 2/5

História do usuário

ID: HU05941
Desejo saber a raça dos usuários do sistema
[Observações]

Requisito legal ou regulatório

Origem	**Identificador**
HU05941	RLR001589
O Sistema deverá solicitar que o usuário selecione a raça/cor dentre as opções oferecidas: amarela, branca, indígena, parda, preta, prefiro não declarar.	

Fundamentação de RLRT a partir de FLR 3/5

Raça/Cor → "Classificação e Ordenação de Hierarquia Legal" → Documento da Hierarquia Legal e Regulatória (DHLR)

- Constituição
  - "Art. 3º Constituem objetivos fundamentais da República Federativa do Brasil: (...)
    - IV - **promover o bem de todos**, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação."
  - "Art. 5º Todos são **iguais perante a lei**, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade (...)"
- Lei 12.711, de 29 de agosto de 2012
  - Dispõe sobre o ingresso nas universidades federais e nas instituições federais de ensino técnico de nível médio e dá outras providências

13

Fundamentação de RLRT a partir de FLR 4/5

Raça/Cor → "Classificação e Ordenação de Hierarquia Legal" → Documento da Hierarquia Legal e Regulatória (DHLR)

- Decreto 7.824, de 11 de outubro de 2012
  - Regulamenta a Lei nº 12.711, de 29 de agosto de 2012, que dispõe sobre o ingresso nas universidades federais e nas instituições federais de ensino técnico de nível médio
- Portaria Normativa do MEC nº 18, 11 de outubro de 2012
  - Dispõe sobre a implementação das reservas de vagas em instituições federais de ensino de que tratam a Lei nº 12.711, de 29 de agosto de 2012, e o Decreto nº 7.824, de 11 de outubro de 2012
- **Portaria Normativa do MEC nº 21, de 28 de agosto de 2013**
  - **Dispõe sobre a inclusão da educação para as relações étnico-raciais, do ensino de História e Cultura Afro-Brasileira e Africana, promoção da igualdade racial e enfrentamento ao racismo nos programas e ações do Ministério da Educação, e dá outras providências**

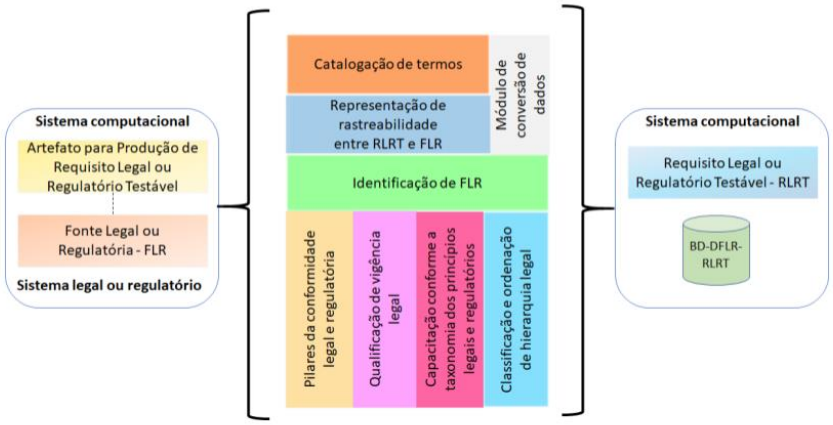
14

Fundamentação de RLRT a partir de FLR 5/5

Origem	**Identificador**
HU05941	RLR001589
O Sistema deverá solicitar que o usuário selecione a raça/cor dentre as opções oferecidas: amarela, branca, indígena, parda, preta, prefiro não declarar.	
Fontes Legais ou Regulatórias - FLR	
FLR000149 - Constituição Federal de 1988	FLR000149.1 - Art. 3o. inciso IV - promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação.
	FLR000149.2 - Art. 5o. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade (...)
FLR000150 - Portaria Normativa do MEC nº 21, de 28 de agosto de 2013 - dispõe sobre a inclusão da educação para as relações étnico-raciais, do ensino de História e Cultura Afro-Brasileira e Africana, promoção da igualdade racial e enfrentamento ao racismo nos programas e ações do Ministério da Educação, e dá outras providências	FLR000150.1 - Art. 2o. O Ministério da Educação instituirá a coleta do quesito raça/cor nos instrumentos de avaliação, coleta de dados do censo, bem como em suas ações e programas quando couber.

15

Visão geral do Framework

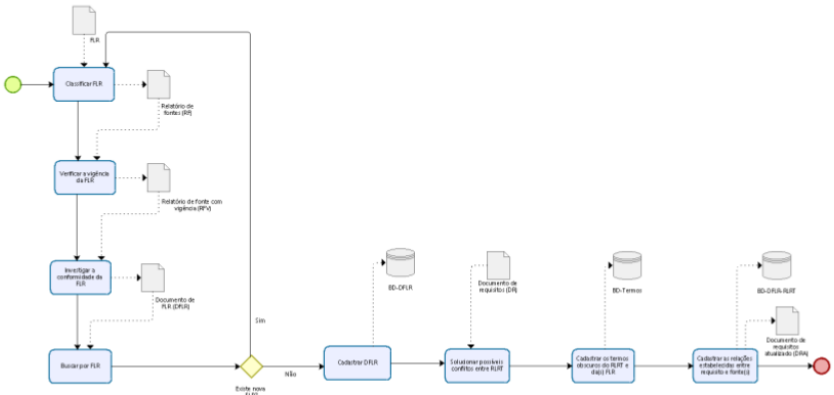


16

Transformação de uma FLR em RLRT

17

Fluxo de atividades de transformação de FLR em RLRT



18

Transformação de uma FLR em RLRT 1/5

Pseudoanonimato → "Classificação e Ordenação de Hierarquia Legal" → Documento da Hierarquia Legal e Regulatória (DHLR)

- Constituição Federal de 1988
  - Art. 5o., inciso IV - é livre a manifestação do pensamento, sendo vedado o anonimato
- Lei 8.078, de 11 de setembro de 1990
  - Dispõe sobre a proteção do consumidor e dá outras providências. (Código de Defesa do Consumidor)
- Decreto 7.962, de 15 de Março de 2013
  - Regulamenta a Lei no 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico (Lei do e-Commerce)

19

Transformação de uma FLR em RLRT 2/5

Pseudoanonimato → "Classificação e Ordenação de Hierarquia Legal" → Documento da hierarquia legal e regulatória (DHLR)

- Lei 12.965, de abril de 2014
  - Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. (Marco Civil da Internet)
- Lei 13.709, de Agosto de 2018
  - Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (Lei Geral de Proteção de Dados Pessoais - LGPD)

20

Transformação de uma FLR em RLRT 3/5

Origem	**Identificador**
FLR000000	RLR001590
O Sistema deverá solicitar ao usuário que demonstre seu consentimento no tratamento de seus dados pessoais a partir do aceite do termo de consentimento na ação de avançar para o próximo passo do processo de compra (pagamento).	
Fontes Legais ou Regulatórias - FLR	
FLR000123 - Constituição Federal de 1988	FLR000123.1 - Art. 5o., inciso IV - é livre a manifestação do pensamento, sendo vedado o anonimato;
FLR000124 - Lei 8.078, de 11 de setembro de 1990 dispõe sobre a proteção do consumidor e dá outras providências. (Código de Defesa do Consumidor)	FLR000124.1 - Art. 43, parágrafo primeiro. Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
FRL000128 - Decreto 7.962, de 15 de Março de 2013 regulamenta a Lei no 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico (Lei do e-Commerce)	FLR000128.1 - Art 4o., inciso VII - utilizar mecanismos de segurança eficazes para pagamento e para tratamento de dados do consumidor.

21

Transformação de uma FLR em RLRT 4/5

FLR000135 - Lei 12.965, de abril de 2014 estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. (Marco Civil da Internet)	FLR000135.1 - Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
FLR000185 - Lei 13.709, de Agosto de 2018 dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (Lei Geral de Proteção de Dados Pessoais - LGPD)	FLR000185.1 - Art. 2o. inciso I. o respeito à privacidade.
	FLR000185.2 - Art. 2o. inciso IV. a inviolabilidade da intimidade, da honra e da imagem.
	FLR000185.3 - Art. 7o. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses. Inciso I - mediante o fornecimento de consentimento pelo titular.
	FLR000185.4 - Art. 7o. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses. Inciso II - para o cumprimento de obrigação legal ou regulatória pelo controlador.

22

Transformação de uma FLR em RLRT 5/5

	FLR000185.5 - Art. 7o. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses. Inciso X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.
	FLR000185.6 - Art. 8o. O consentimento previsto no Inciso I do Art. 7o. desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

23

Apêndice D.6 – Roteiro para entrevista durante a abordagem do *Framework*

1. Id do(a) participante: _____. (*e-mail* no formulário)
2. O *framework* (através do componente "**Classificação e Ordenação de Hierarquia Legal**") facilita a identificação da hierarquia das fontes legais ou regulatórias a serem atendidas?
3. O componente "**Qualificação de Vigência Legal**" ajuda a planejar melhor as *sprints* de um projeto de um sistema computacional?
4. O componente "**Catalogação de Termos**" pode auxiliar a sua equipe a entender os termos utilizados nos documentos do ciclo de vida de um sistema computacional?
5. A criação de rastreabilidade entre todos os artefatos relacionados com os requisitos legais ou regulatórios e as fontes legais ou regulatórias é feita no componente "**Representação de rastreabilidade entre RLRT e FLR**". Isto pode lhe auxiliar de que forma no seu cotidiano?
6. O *framework* promove a sustentabilidade dos sistemas computacionais a partir do reuso das fontes legais ou regulatórias e dos requisitos legais e regulatórios a partir do componente "**Representação de rastreabilidade entre RLRT e FLR**". Isto pode lhe auxiliar de que forma no seu cotidiano?
7. Os componentes do *framework* podem melhorar seu planejamento e ações no dia a dia? Como?
8. O "**Módulo de Conversão de Dados**" será útil no seu dia a dia?
9. O componente "**Capacitação conforme a Taxonomia dos Princípios Legais e Regulatórios**" utilizado como base é capaz de resolver questões de privacidade e segurança?
10. Os componentes do *framework* são suficientes para atender a demanda atual de artefatos para planejamento, gerenciamento e manutenção da conformidade legal e regulatória?
11. A inserção do *framework* na rotina da equipe pode trazer quais benefícios ou malefícios?
12. Algo lhe decepcionou?
13. Algo lhe surpreendeu?
14. Em que momento houve maior dificuldade em entender o *framework*? A que pode ser atribuída esta dificuldade?
15. Você teria sugestões para o melhoramento do nosso *framework*?