



Universidade de Brasília

Instituto de Ciências Exatas
Departamento de Ciência da Computação

Gestão de Riscos no Processo de Terceirização de TI do IDP

Thabata Helen Macedo Granja

Dissertação apresentada como requisito parcial para conclusão do
Mestrado Profissional em Computação Aplicada

Orientador

Prof. Dr. Edgard Costa Oliveira

Coorientadora

Prof.a Dr.a Rejane Maria da Costa Figueiredo

Brasília
2022

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

HG759g Helen Macedo Granja, Thabata
Gestão de Riscos no Processo de Terceirização de TI do
IDP / Thabata Helen Macedo Granja; orientador Edgard Costa
Oliveira; co-orientador Rejane Maria da Costa Figueiredo. -
Brasília, 2022.
200 p.

Dissertação (Mestrado - Mestrado Profissional em
Computação Aplicada) -- Universidade de Brasília, 2022.

1. Terceirização de TI. 2. Gestão de riscos. 3. Elicitação
de requisitos de software. I. Costa Oliveira, Edgard,
orient. II. Maria da Costa Figueiredo, Rejane, co-orient.
III. Título.

Dedicatória

Dedico esta dissertação à minha família, especialmente à minha avó, Neuza Marlene Fabricio Macedo, pois tenho nela meu maior exemplo de dedicação e resiliência, características necessárias para conseguir finalizar este mestrado.

Agradecimentos

Agradeço primeiramente ao meu orientador Prof.Dr.Edgard Costa Oliveira e à minha coorientadora Prof.Dr.^a Rejane Maria da Costa Figueiredo, por todo apoio, parceria, acolhimento e paciência.

À minha mãe, Taís Helene Macedo, a maior mestra da minha vida, de quem sempre tive como inspiração de força e determinação: sigo tentando alcançar metade de sua grandeza. À minha irmã, Karoline Louize Macedo Granja, que me ensina todos os dias o poder da organização, planejamento, calma e diálogo. Amo vocês mais que tudo!

Rô, Cacá, Mari e Livinha, por mostrarem a importância de mergulhar de cabeça em tudo que eu fizer, do trabalho à diversão. Vocês são um grande tesouro redescoberto.

Ao meu parceiro de vida, Igor de Oliveira Martins, que mesmo conhecendo todas as minhas fraquezas, continuou acreditando na minha força, quando nem mesmo eu a enxergava, seja do meu lado ou a mais de 7 mil km de distância.

Aos meus colegas da turma do PPCA/2019, pois juntos fomos mais longe. Em especial ao Vitor Lopes, presente do mestrado que me ensinou a jogar os dados da vida, ao Maxwell Carvalho, por todas as risadas em sala, ao Raniere Magalhães e à Daniele Oliveira: pessoas queridas que sei que posso contar para o que der e vier.

Aos meus amigos, especialmente ao meu melhor amigo, Daniel Filippe da Silva Lameira, por ser o alívio cômico nos tempos difíceis e por sempre estar comigo, sendo meu ouvido amigo. Ao Sargento Lucas, meu mestre treinador, por me ensinar a nunca baixar a guarda nos momentos de luta. Aos mestres "raiz" que me encorajaram a enfrentar o desafio do mestrado, Prof. Me. Eduardo Pires Fernandes e Prof. Me. Clayton Lobato.

Ao IDP, instituição que vive a evolução por meio da educação, com destaque para o Prof. Dr. Francisco Schertel Ferreira Mendes, que tanto agregou a este trabalho, ao Hugo de Paula Franco Teixeira, profissional que respeito e admiro, ao Marcelo Henrique da Silva e sua equipe, e por fim, à equipe do EAD, parceiros de perrengues e conquistas.

Aos alunos do "Grupo 1" de PSP2: João, Isaac, Eduardo e Willian, que foram essenciais para a realização deste trabalho. Formamos uma bela equipe!

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES), por meio do Acesso ao Portal de Periódicos.

Resumo

As empresas são ecossistemas complexos e precisam se adaptar a mudanças, simultaneamente ao enfrentamento de diversas incertezas. A terceirização de TI tem se tornado uma opção, pois nas organizações o atendimento às demandas internas tem sido dado por produtos e serviços de terceiros. Dada a complexidade do processo de terceirização, devido à intangibilidade das soluções de TI, a gestão de riscos pode ser uma aliada na busca do aumento das chances de sucesso da terceirização. O presente trabalho tem por objetivo propor uma ferramenta computacional para identificação, análise e avaliação dos riscos na terceirização de TI, por meio de estudo de caso em uma instituição de nível superior. O estudo de caso foi estruturado em etapas, que foram executadas de forma cíclica, visando obter os dados necessários para a análise e o relato da pesquisa. A partir do COBIT 5, das normas ISO 31000 e ISO 37500, foram extraídas 33 boas práticas devidamente caracterizadas e ordenadas. Em seguida foi feito o mapeamento do processo atual de terceirização de TI do IDP, cujo entendimento e diagramação foram realizados por meio de entrevistas semi-estruturadas e pesquisa documental, resultando na proposta de um novo processo de terceirização para a instituição, aderente às práticas anteriormente extraídas. Com base no novo processo, foi realizado um levantamento de ferramentas de avaliação de riscos existentes, as quais foram analisadas frente às boas práticas levantadas. Foi verificada baixa aderência às boas práticas e ao processo mapeado, levando a uma nova proposta de especificação de requisitos de um software para avaliação de riscos de processos de terceirização de TI da instituição, usando-se como método as técnicas extraídas do *Lean Inception*. A especificação foi validada através da prototipação das telas que foram analisadas por colaboradores da instituição que participam do processo de terceirização de TI na empresa. Desta forma, o IDP tem, doravante, uma proposta de um novo processo de terceirização mais alinhado às boas práticas, bem como a especificação de um sistema computacional que auxiliará sua execução. Como proposta de trabalhos futuros, é sugerida a implantação do novo processo de terceirização de TI com base nas boas práticas, assim como o desenvolvimento do software especificado, ambos propostos neste trabalho.

Palavras-chave: terceirização de TI, gestão de riscos, elicitação de requisitos de software

Abstract

Business organizations, regardless of their area of activity or size, are complex ecosystems that need to constantly adapt to changes, while facing the most diverse uncertainties. The outsourcing of Information Technology (IT) has become a frequent resource, as in organizations the fulfillment of internal demands has been given by third-party products and services. Given the complexity of the outsourcing process, due to the intangibility of IT solutions, risk management can be an ally in the search to increase the chances of outsourcing success. The present work aims to propose a computational tool for the identification, analysis and assessment of risks in IT outsourcing, through a case study in a higher education institution. The case study was structured in stages, which in turn were performed in a cyclical way, aiming to obtain the necessary data for the analysis and for the research report. From COBIT 5, ISO 31000 and ISO 37500, 33 good practices were extracted, duly characterized and ordered. The result of the extraction together with the mapping of the current process of IT outsourcing of the IDP, whose understanding and mapping was carried out through semi-structured interviews and documental research, a proposal was made for a new process for the institution, by adhering to the practices previously extracted. Based on the proposed new process, a survey of existing tools was carried out and, after verifying their low adherence to good practices, a proposal was made for a specification of the requirements of a software for risk assessment of IT outsourcing processes by using techniques extracted from Lean Inception. The specification had its practical validation carried out through the prototyping of screens that were evaluated by employees who actively participate in the current IT outsourcing process in the company. In this way, the IDP has, from now on, a proposal for a new outsourcing process more aligned with good practices, as well as the specification of a computer system that can help its execution. As a proposal for future works, it is suggested the implementation of this new proposed process of IT outsourcing based on good practices, as well as the development of the specified software.

Keywords: IT outsourcing, risk management, software requirements elicitation

Sumário

1	Introdução	1
1.1	Contexto	1
1.2	Questão de pesquisa	3
1.3	Objetivos	4
1.4	Metodologia da pesquisa	4
1.5	Estrutura do trabalho	5
2	Revisão de Literatura	7
2.1	Considerações iniciais do capítulo	7
2.2	Gestão de riscos	7
2.2.1	Softwares de gestão de riscos	12
2.2.2	Gestão de riscos de TI	16
2.3	Conceito de terceirização	19
2.3.1	Terceirização de TI	19
2.4	Gestão de Riscos na terceirização de TI	22
2.5	Gestão de Processos de Negócios	23
2.6	Gestão de escopo de projeto utilizando Estrutura Analítica do Projeto (EAP)	26
2.7	Considerações finais do capítulo	30
3	Metodologia da pesquisa	31
3.1	Considerações iniciais do capítulo	31
3.2	Fase de planejamento da pesquisa	31
3.3	Fase de coleta de dados	32
3.3.1	Entrevistas semiestruturadas	33
3.3.2	Pesquisa documental	33
3.3.3	Estudo de caso	34
3.3.4	Prototipação	37
3.4	Fases de análise de dados e relato dos resultados	38
3.5	Considerações finais do capítulo	39

4	Seleção de boas práticas para a terceirização de TI e a gestão de riscos	41
4.1	Considerações iniciais do capítulo	41
4.2	Seleção de boas práticas	41
4.2.1	COBIT 5	43
4.2.2	A norma ISO 37500	46
4.2.3	A norma ISO 31000	50
4.3	Análise de boas práticas e respectivas atividades	56
4.4	Validação da extração das práticas	64
4.5	Considerações finais do capítulo	65
5	Descrição do processo de terceirização de TI no IDP	66
5.1	Considerações Iniciais do Capítulo	66
5.2	História da instituição	66
5.3	Cardeia de valor do IDP	68
5.4	Descrição da TI no IDP	69
5.4.1	Processo de terceirização de TI no IDP	71
5.5	Validação do processo atual de terceirização de TI	75
5.6	Considerações finais do capítulo	76
6	Proposta de novo processo de terceirização de TI para o IDP	77
6.1	Considerações iniciais do capítulo	77
6.2	Proposta de novo processo de terceirização de TI para o IDP	77
6.3	Processo de análise estratégica da solicitação	80
6.4	Processo de avaliação e decisão	82
6.5	Processo de especificação das necessidades	84
6.6	Processo de análise e seleção de fornecedor(es)	84
6.7	Processo de preparação para implantação da terceirização	86
6.8	Processo de gerenciamento da terceirização	89
6.8.1	Processo administrar terceirização	92
6.9	Validação do novo processo proposto	93
6.10	Considerações finais do capítulo	94
7	Especificação da ferramenta	95
7.1	Considerações iniciais do capítulo	95
7.2	Planejamento das atividades	96
7.3	Análise de ferramentas existentes	98
7.4	Elicitação dos requisitos de software de gestão de riscos no processo de terceirização de TI do IDP	102

7.4.1	Visão do produto	105
7.4.2	O produto É - NÃO É - FAZ - NÃO FAZ	107
7.4.3	Objetivos do produto	108
7.4.4	Técnica descreva <i>personas</i>	108
7.4.5	<i>Técnica de brainstorming</i> de funcionalidades	109
7.5	Protótipo das telas do software de avaliação de riscos da terceirização de TI no IDP	112
7.6	Validação dos resultados finais	127
7.7	Considerações Finais do Capítulo	128
8	Conclusão	129
8.1	Proposta de trabalhos futuros	131
	Referências	133
	Apêndice	140
	A Documento de visão elaborado em PSP2	141
	Anexo	167
	I Atividades extraídas das boas práticas	167
	II Comparativo das ferramentas de gestão de riscos existentes	188
	III Primeira versão das funcionalidades e protótipos	191

Lista de Figuras

1.1	Protocolo de estudo de caso. Fonte: [1]	5
2.1	Linha do tempo das publicações relevantes sobre riscos. Fonte: [2]	8
2.2	Princípios, estrutura e processo de gestão de riscos segundo a ISO 31000. Fonte: [3]	10
2.3	Modelo de gestão de riscos do HM Treasury/Orange Book. Fonte: [4]	11
2.4	Processo de gestão de riscos de segurança da informação segundo a ABNT NBR ISO/IEC 27005. Fonte: [5]	18
2.5	Fases do ciclo de vida BPM. Fonte: [6]	24
2.6	Principais componentes do BPMN e representação simples de um processo. Fonte: adaptado de [7]	26
2.7	Fluxo de Processos do Guia PMBOK. Fonte: [8]	28
2.8	Exemplo de EAP ilustrativa com Entregas Principais. Fonte: [8]	29
3.1	Planejamento da pesquisa. Fonte: autora	31
3.2	Plano metodológico adotado. Fonte: autora	32
3.3	Coleta de dados. Fonte: autora	32
3.4	Ciclo das etapas do estudo de caso. Fonte: [1]	34
3.5	Ciclos unificados do estudo de caso. Fonte: autora	35
3.6	Associação dos objetivos específicos com os métodos e ciclos do estudo de caso. Fonte: autora	36
4.1	Primeiro ciclo do estudo de caso. Fonte: autora	41
4.2	Cobertura de outros frameworks no COBIT 5. Fonte: [9]	42
4.3	Cobertura de outros frameworks pela ISO 37500. Fonte: [10]	43
4.4	: Modelo de Referência de Processo do COBIT 5. Fonte: [9]	45
4.5	Modelo contextual de terceirização. Fonte: [10]	47
4.6	Ciclo de vida da terceirização. Fonte: [10]	48
4.7	Ações definidas e resultados esperados da gestão de riscos. Fonte: [3]	52
4.8	Passos para implementação da estrutura de gestão de riscos. Fonte: [3]	53

4.9	Processo de gestão de riscos. Fonte: [3]	54
5.1	Segundo ciclo do estudo de caso. Fonte: Autora	66
5.2	Cadeia de valor do IDP. Fonte: autora	68
5.3	Diagrama do Processo de Terceirização de TI no IDP: visão macro. Fonte: Autora	72
6.1	Terceiro ciclo do estudo de caso. Fonte: Autora	77
6.2	Novo processo de terceirização de TI proposto. Fonte: autora	78
6.3	Processo de análise estratégica da solicitação. Fonte: Autora	81
6.4	Processo de avaliação e decisão. Fonte: Autora	83
6.5	Processo de especificação das necessidades. Fonte: Autora	84
6.6	Processo de análise e seleção de fornecedor(es). Fonte: Autora	85
6.7	Processo de preparação para implantação da terceirização. Fonte: Autora	87
6.8	Processo de gerenciamento da terceirização. Fonte: Autora	91
6.9	Processo administrar terceirização. Fonte: Autora	92
7.1	Quarto ciclo do estudo de caso. Fonte: autora	95
7.2	Quinto e último ciclo do estudo de caso. Fonte: Autora	96
7.3	EAP do Projeto de PSP2. Fonte: Autora	97
7.4	Exemplo agenda do <i>Lean Inception</i> . Fonte: [11]	103
7.5	Visão do produto. Fonte: autora	106
7.6	Definição de é/não é, faz/não faz. Fonte: Autora	107
7.7	Definição dos objetivos do produto. Fonte: Autora	108
7.8	Definição das personas. Fonte: autora	109
7.9	Definição das funcionalidades. Fonte: Autora	110
7.10	Modelagem do sistema proposto. Fonte: Autora	113
7.11	Protótipo da tela de login. Fonte: Autora	114
7.12	Protótipo da tela de menu principal. Fonte: Autora	115
7.13	Protótipo da tela de cadastro dos projetos de terceirização. Fonte: Autora	116
7.14	Protótipo da tela de cadastro dos fornecedores. Fonte: Autora	118
7.15	Protótipo da tela de cadastro dos usuários. Fonte: Autora	119
7.16	Protótipo da tela de cadastro e avaliação de riscos. Fonte: Autora	120
7.17	Protótipo da tela de monitorar riscos. Fonte: Autora	121
7.18	Protótipo da tela de monitoramento da execução do processo de terceiri- zação em projetos. Fonte: Autora	122
7.19	Protótipo da tela de acompanhamento dos projetos. Fonte: Autora	123
7.20	Protótipo da tela de relatórios. Fonte: Autora	124
7.21	Protótipo da tela de consultar projetos. Fonte: Autora	125

7.22	Protótipo da tela de configuração de API. Fonte: Autora	126
II.1	Tabela comparativa entre ferramentas de gestão de riscos baseadas em categorias genéricas. Fonte: [12] [13] [14]	189
II.2	Tabela comparativa das ferramentas em relação às práticas. Fonte: autora	190
III.1	Tela de Login. Fonte: autora	194
III.2	Tela do Menu. Fonte: autora	194
III.3	Tela de lista de projetos. Fonte: autora	195
III.4	Tela de informações sobre o projetos. Fonte: autora	195
III.5	Tela de histórico de projetos. Fonte: autora	196
III.6	Tela de acompanhamento de projetos. Fonte: autora	196
III.7	Tela de cadastro de riscos. Fonte: autora	197
III.8	Tela de cadastro de projetos. Fonte: autora	197
III.9	Tela de cadastro de fornecedores. Fonte: autora	198
III.10	Tela de monitoramento de riscos. Fonte: autora	198
III.11	Tela da visão do solicitante da terceirização. Fonte: autora	199
III.12	Tela de cadastro de usuários. Fonte: autora	199
III.13	Tela de acompanhamento de atividades do projeto. Fonte: autora	200
III.14	Tela de integração por API. Fonte: autora	200

Lista de Tabelas

4.1	Princípios ISO 31000. Fonte: [3]	51
4.2	Práticas do COBIT 5 [15] ordenadas por peso	57
4.3	Peso médio da prática por repetição de referência	60
4.4	Compilação das boas práticas de gestão de riscos e terceirização de TI	61
7.1	Ordenação e pontuação das ferramentas por categorias. Fonte: Autora	100
7.2	Ordenação e pontuação das ferramentas por prática adotada. Fonte: autora	102
7.3	Técnicas do <i>Lean Inception</i> e seus resultados. Fonte: [11]	104
7.4	Funcionalidades identificadas e descritas	110
I.1	Atividades extraídas do COBIT 5 [15]	167
I.2	Fases e atividades extraídas da ISO 37500 [10]	172
I.3	Atividades, descrições e referências das boas práticas	178
I.4	Peso de cada fase baseado no peso médio das práticas	187
III.1	Funcionalidades identificadas e descritas	191

Lista de Abreviaturas e Siglas

ABPMP *Association of Business Process Management Professionals.*

BPM *Business Process Management.*

BPMI *Business Process Management Initiative.*

BPMN *Business Process Model and Notation.*

CAPES *Coordenação de Aperfeiçoamento de Pessoal de Nível Superior.*

CMMI *Capability Maturity Model Integration.*

COBIT *Control Objectives for Information and Related Technologies.*

COSO *Committee of Sponsoring Organizations of the Treadway Commission.*

EAP *Estrutura Analítica do Projeto.*

ERM *Enterprise Risk Management.*

ERP *Enterprise Resource Planning.*

FERMA *Federation of European Risk Management Associations.*

GP *Gente e Performance.*

IBM *International Business Machines Corporation.*

IDP *Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa.*

IES *Instituição de Ensino Superior.*

ISACA *Information Systems Audit and Control Associatio.*

ISO *International Organization for Standardization.*

MBA *Master of Business Administration.*

MVP *Minimum viable product.*

PMBOK *Project Management Body of Knowledge.*

PMI *Project Management Institute.*

PSP2 *Projeto de Sistemas de Produção 2.*

PTA *Practical Threat Analysis.*

RIMS *Risk and Insurance Management Society.*

SaaS *Software as a Service.*

SIEP *Sistemas de Informação para Engenharia de Produção.*

TEMAC *Teoria do Enfoque Meta Analítico.*

TI *Tecnologia da Informação.*

UX *User experience.*

Capítulo 1

Introdução

Neste capítulo, apresenta-se o contexto deste trabalho, que leva à questão de pesquisa. Uma vez que o objeto desta pesquisa trata da gestão de riscos do processo de terceirização de Tecnologia da Informação (TI), contextualizou-se aqui o cenário da terceirização no Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP), por meio da revisão bibliográfica sobre os assuntos citados. Em seguida, caracterizou-se o problema e foram apresentados o objetivo de pesquisa definido e a metodologia de pesquisa adotada e ao final foi apresentada a estrutura deste documento.

1.1 Contexto

As organizações empresariais são sistemas complexos e sofrem constantes pressões do mercado para se adaptarem continuamente às mudanças e demandas externas. Frente a este cenário de constante mudança, a estratégia de terceirização é uma das soluções potenciais, pois ela representa, no geral, um modelo de negócio que visa atender a demanda de clientes por meio da entrega de um dado produto ou serviço por um fornecedor [10].

Quando se trata da terceirização de TI, Mu e Pei [16] indicam que os principais motivos podem ser precedidos pela necessidade de melhoria na área de TI, pela melhoria do desempenho organizacional ou de seu impacto, assim como para garantir ganhos comerciais. Mostrando com isso uma importância estratégica e afeta fortemente no desempenho da organização. McIvor [17] apresenta a pesquisa realizada pela PA Consultoria (*PA Consulting Group*) em que apenas 5% das empresas entrevistadas indicam altos índices de satisfação a partir das terceirizações realizadas.

Porém, o processo de terceirização de Tecnologia da Informação (TI) tem se mostrado cada vez mais complexo devido ao fato da aquisição de TI ser um bem intangível para a instituição [18], seja pela dificuldade na mensuração de custos e na visibilidade dos

benefícios e resultados, assim como pelas dificuldades oriundas das constantes mudanças no campo da tecnologia [19].

Faz-se necessário compreender as ameaças para reduzir incertezas, possibilitando o alcance dos objetivos estratégicos da TI. Para isso, o uso da gestão de riscos no processo de contratação de TI é oportuno [20]. Apesar de não eliminar todas as incertezas, aumentam-se as chances de sucesso [21].

A gestão de riscos, como uma abordagem mais abrangente, tem sido empregada em diversos outros contextos. No setor público, ganhou destaque após um movimento fomentado pelo Centro Canadense para o Desenvolvimento da Gestão (*Canadian Centre for Management Development*), que conforme Ávila [22], impulsionou o desenvolvimento da área não apenas o próprio país, mas também em várias outras partes do mundo.

No Brasil, o impacto do cenário mundial frente à gestão de riscos foi sentido com a publicação a Lei nº 13.303/2016 [23], que é o principal parâmetro nacional no que se refere a Gestão de Riscos, Auditoria e Controles Internos, reforçada pela Instrução Normativa Conjunta CGU/MP nº 01 publicada em maio de 2016 [24].

No âmbito do Distrito Federal, em conformidade com as tendências federais brasileiras, no ano de 2016 foi publicado o Decreto nº 37.302 [25], em que são estabelecidos os modelos e boas práticas de Gestão de Riscos e Controle Interno a serem implantados no âmbito do Distrito Federal, sob responsabilidade da Controladoria-Geral do Distrito Federal para apoio, monitoramento e normatização da implementação do decreto.

Porém, em pesquisas livres nos principais sites de busca não é possível observar o mesmo movimento significativo e padronizado do serviço público no âmbito das empresas privadas, seja no Distrito Federal ou no Brasil como um todo. Situação que se torna mais escassa no contexto de empresas privadas da área de ensino, assim como o Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP), objeto de estudo desta pesquisa.

A terceirização é uma tradução da palavra de origem inglesa "*outsourcing*", e pode ser entendida como a contratação de organizações de fora da empresa, para que seja executada toda ou parte de atividades e funções da rotina geralmente executado internamente na instituição em troca de uma determinada remuneração [26] [27] [28] [29] [30].

Seu início se deu no século 18 e até a década de 80 não era bem recebida, passando a ganhar grande força somente nos anos 90 [31]. Mesma década onde a terceirização de TI também ganhou um grande destaque, passando a ser uma escolha estratégica que viria a definir o sucesso e sobrevivência das empresas [32].

A terceirização de TI é definida como “*a sub-contratação da responsabilidade no fornecimento de serviços de TI para uma entrega, solução ou produto tecnológico específico e pré-definido*” [16].

A motivação da terceirização pode ocorrer por diversos fatores: falta de habilidade na equipe atual; necessidade da redução de esforço; ganho de eficiência e identificação de *gaps* organizacionais, e principalmente entre as áreas de negócio e a tecnologia da informação [16].

Além disso, os autores Fusiripong, Baharom e Yusof [33] indicam que as falhas de projetos de terceirização são resultantes de decisões pouco fundamentadas, tomadas a partir de incertezas e informações incompletas, tornando a decisão em si, arriscada.

Frente a este cenário de incertezas, a gestão de riscos aparece como um grande aliado, gerando a proteção de valor para uma instituição e auxiliando no controle eficiente frente às incertezas, sendo ferramenta importante no estabelecimento de estratégias e tomada de decisões fundamentais que visem o alcance dos objetivos da organização [3].

O gerenciamento de riscos faz parte de todas as atividades em qualquer nível da organização. Realizá-lo de forma padronizada, utilizando boas práticas em modelos reconhecidos evita desde o excesso de burocracia até desordem das atividades, que podem resultar na falsa impressão de uma gestão de riscos eficiente que na prática não garante os benefícios desejados [2].

No que tange a gestão de riscos relacionados a terceirização de TI, duas grandes questões se mostram relevantes para os profissionais: quais são os riscos e como mitigá-los. Porém ao consolidar essas informações percebe-se que, devido a grande quantidade de práticas específicas projetadas para reduzir cada risco, a complexidade na redução dos riscos, muitas empresas podem questionar os reais benefícios na terceirização de TI. [34].

1.2 Questão de pesquisa

No cenário atual de gestão de riscos no processo de terceirização de TI apresentado, se encontra o Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP) o qual situa-se em um momento de grande crescimento recente, com aumento das ofertas de cursos em diferentes áreas de atuação.

Porém, a instituição não possui um processo definido de terceirização de TI, nem aplicação de nenhuma das atividades estruturadas relacionadas ao processo de gestão de riscos. No momento, cada área segue diferentes procedimentos de contratação e são responsáveis pelo controle das mesmas. Observa-se também a falta de insumos documentados para a decisão e gestão da terceirização de TI e seus riscos associados.

A partir das lacunas encontradas, a questão de pesquisa que se buscou responder neste trabalho é:

Como avaliar os riscos no processo de terceirização de TI em uma instituição privada de ensino superior?

1.3 Objetivos

O objetivo geral da pesquisa é: *propor uma ferramenta computacional para avaliação dos riscos na terceirização de Tecnologia da Informação (TI) do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP), alinhada às boas práticas.*

Para alcançar o objetivo geral, foram definidos os seguintes objetivos específicos:

- Sistematizar os conhecimentos sobre terceirização de TI e gestão de riscos a partir da orientação de boas práticas;
- Descrever o processo de terceirização de TI no IDP;
- Propor um novo processo de terceirização TI alinhado às boas práticas sistematizadas;
- Elicitar os requisitos de um software para avaliação de riscos de processos de terceirização de TI.

1.4 Metodologia da pesquisa

O plano metodológico adotado nesta pesquisa, detalhado no *Capítulo 3 - Metodologia da Pesquisa*, compreende quatro fases básicas: planejamento da pesquisa; coleta de dados; análise dos dados; e relato dos resultados. A metodologia foi selecionada e classificada quanto a natureza, abordagem, tipologia, e procedimentos e técnicas de coleta de dados.

Quanto à natureza, a pesquisa é aplicada dado o cunho prático em um contexto definido. A abordagem selecionada é a qualitativa, pois não fez uso de métodos e técnicas estatísticas, visto que o objetivo deste trabalho é de fazer uma análise intuitiva dos resultados pelo pesquisador e não o de provar estatisticamente o sucesso ou fracasso das especificações, atividades, tarefas e artefatos [35] [36].

Quanto ao tipo, a pesquisa é classificada como descritiva, pois evidencia as características de um dado fenômeno por meio do estudo, análise, registro e interpretação dos fatos [37] [36]. Quanto à Coleta de dados, foram selecionadas as técnicas de entrevistas semiestruturadas, reuniões, pesquisa documental e estudo de caso.

A técnica de estudo de caso se caracteriza como um método empírico que investiga fenômenos contemporâneos. A técnica é largamente empregada na área de engenharia de software, e se baseia em múltiplas fontes de evidências para investigar uma instância dentro do seu contexto da vida real, quando não há fronteira clara entre o fenômeno e o contexto [1].

O protocolo do estudo de caso definido foi uma adaptação da proposta de Runeson [1], cuja composição se divide em 3 etapas. A primeira etapa é a *coleta de evidências*, quando

são executados os procedimentos de coleta de dados, seguido pela etapa de *análise dos dados coletados*, em que o procedimento de análise é aplicado nos dados coletados, e por fim a etapa de *reporte*, quando as conclusões são compiladas em relatórios [1].

As etapas são realizadas de forma cíclica até o momento em que todos os objetivos específicos e, por consequência, o objetivo geral forem atingidos, conforme demonstrado na Figura 1.1



Figura 1.1: Protocolo de estudo de caso. Fonte: [1]

1.5 Estrutura do trabalho

Este trabalho está organizado em oito capítulos, incluindo este, o qual compreende o contexto, a revisão de literatura, o problema, os objetivos e a metodologia da pesquisa adotada.

No *Capítulo 2 - Revisão de Literatura*, inicia-se um estudo sobre a terceirização de TI, a gestão de riscos e sua correlação, abordando ali os principais trabalhos publicados sobre os temas da pesquisa, com o objetivo de se ter uma melhor compreensão do assunto.

No *Capítulo 3 - Metodologia da Pesquisa*, dado o objetivo da pesquisa, apresenta-se o plano metodológico adotados. Em seguida, o planejamento das fases.

No *Capítulo 4 - Seleção de boas práticas para a terceirização de TI e gestão de riscos*, são realizados os procedimentos de busca, seleção, extração e análise das melhores práticas aplicadas a terceirização de TI e gestão de riscos, com objetivo de realizar sua caracterização, pontuação e ordenação por relevância.

No *Capítulo 5 - Descrição do processo de terceirização de TI no IDP*, dado que o objeto de pesquisa é o Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP), apresenta-se uma breve contextualização da instituição, seu histórico e a caracterização do processo de terceirização de TI existente na instituição.

No *Capítulo 6 - Proposta de novo processo de terceirização de TI para o IDP*, a partir da junção dos procedimentos internos da instituição já caracterizados e nas atividades retiradas das boas práticas é apresentada a proposta de um novo processo de terceirização de TI para o IDP.

No *Capítulo 7 – Especificação da ferramenta*, a partir do processo de terceirização de TI proposto para o IDP baseado nas boas práticas, apresentam-se a elicitação e prototipação de uma ferramenta de avaliação de riscos.

No *Capítulo 8 – Conclusão*, apresentam-se as conclusões deste trabalho e possíveis trabalhos futuros.

Finalizando, as *Referências Bibliográficas*.

Capítulo 2

Revisão de Literatura

2.1 Considerações iniciais do capítulo

Neste capítulo é apresentada uma revisão bibliográfica relacionada aos principais temas abordados neste trabalho, a saber: terceirização de TI, gestão de riscos e, gestão de riscos na terceirização de TI.

Tendo em vista o caráter exploratório deste capítulo, no início de cada seção sobre os temas foi realizada uma contextualização das publicações relacionadas. Esse trabalho foi resultado de um processo de revisão bibliográfica realizado em duas etapas, as quais foram feitas com base no método de revisão de literatura denominado Teoria do Enfoque Meta Analítico (TEMAC) [38].

Na primeira etapa, foram definidas as palavras-chaves para cada tema. A base de dados utilizada foi a do *Web of Science*. Na segunda etapa, foi realizada uma verificação da quantidade de trabalhos publicados, os trabalhos mais antigos, as publicações mais citadas e o ano com maior ocorrência de publicações.

2.2 Gestão de riscos

Toda e qualquer organização, independentemente de seu tamanho ou área de atuação, enfrenta incertezas constantemente. Incertezas essas que podem ser oportunidades para se agregar valor ou podem ser riscos de impacto negativo para a instituição [39].

A gestão de riscos não é um assunto recente na história da humanidade, porém a primeira publicação acadêmica que utilizou o termo, seus conceitos, princípios e que sistematizou o tema para as organizações, surgiu em 1921, na obra *Risk, Uncertainty and Profit de Frank Knight*. Desde então, o tema vem sendo cada vez mais discutido, gerando mais publicações sobre o tema, conforme linha do tempo apresentada na Figura 2.1 [2]:



Figura 2.1: Linha do tempo das publicações relevantes sobre riscos. Fonte: [2].

O propósito da gestão de riscos é a criação e proteção de valor para uma instituição e o auxílio no alcance dos objetivos frente às incertezas. Ela é uma ferramenta importante no estabelecimento de estratégias e tomada de decisões fundamentais que visem o alcance dos objetivos da organização [3].

De acordo com o Instituto Brasileiro de Governança Corporativa [40], o planejamento estratégico é composto por uma governança corporativa e por processos contínuos e estruturados, que unidos tem o objetivo de manter o sistema vivo e em pleno funcionamento. A gestão de riscos é um sistema intrínseco a esse planejamento, pois pretende conduzir o gerenciamento dos riscos existentes no ambiente de negócios, visando o alcance dos objetivos definidos no planejamento estratégico.

Ao se tratar da gestão de riscos, é relevante destacar a diferença entre incerteza e riscos. A incerteza é uma situação em que não há informações reais ou precisas, impedindo assim o entendimento de probabilidades acerca do alcance dos objetivos, e por consequência não há como se gerirem riscos no contexto [41]. Os riscos são o efeito da incerteza sobre os objetivos, o qual é mensurado em termos da probabilidade de algo acontecer, a partir

de informações necessárias para avaliação da chance de algo ocorrer e suas respectivas consequências [42].

As organizações que operam sem levar em conta os riscos a que estão sujeitas, estão em constante situação de incerteza quanto aos seus objetivos. Portanto, é uma questão crítica implementar a gestão de riscos para aumentar a probabilidade de sucesso dos negócios. Para isso é necessário identificar, avaliar e tratar os riscos [43].

A gestão de riscos é parte integrante de todas as atividades em qualquer nível da organização, uma vez que as mesmas podem afetar direta ou indiretamente no alcance dos objetivos de uma instituição. Portanto, para se alcançar os objetivos definidos, a gestão de riscos precisa ser completamente integrada aos processos e sistemas de gestão da instituição [44].

Cabe ressaltar a importância da realização da gestão de riscos de forma estruturada, utilizando-se para tanto de boas práticas oriundas de modelos reconhecidos. Assim, podem ser evitadas situações extremas como o excesso de burocracia ou a falta de organização das atividades na organização. Isso pode resultar na falsa impressão de que há uma gestão de riscos eficiente mas que na prática não garante o alcance dos benefícios desejados [2].

No intuito de padronizar, melhorar e orientar a realização da gestão de riscos, foi criada a norma ISO/ABNT 31000 [3], publicada pela *International Organization for Standardization* (ISO) que tem como objetivo estabelecer princípios e diretrizes sobre a gestão de riscos para sua aplicação a todos os tipos e tamanhos de organizações, em uma ampla gama de atividades, sejam elas estratégias, decisões, operações, processos, funções, projetos, produtos, serviços e ativos. Seus princípios, estrutura e processo são apresentados a seguir na Figura 2.2 [3]:

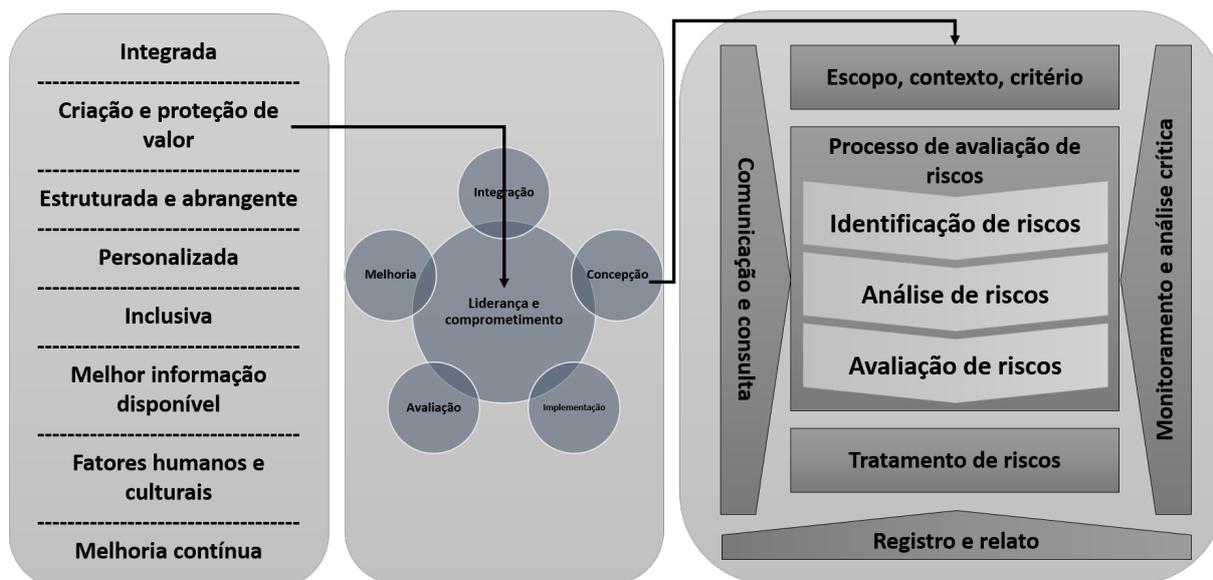


Figura 2.2: Princípios, estrutura e processo de gestão de riscos segundo a ISO 31000. Fonte: [3].

Por ser uma norma genérica e independente de contexto, foram criadas diversas outras referências em gestão de riscos, oriundas de instituições e consultores especializados na publicação de referências temáticas que buscam unificar terminologias e definir padrões de aplicação.

Dentre as referências existentes, destaca-se o *Enterprise Risk Management* (ERM) [45], ou na tradução literal Gerenciamento de Riscos Corporativos, é um modelo proposto pelo *Committee of Sponsoring Organizations of the Treadway Commission* (COSO), que amplia os controles internos com foco em riscos. Esse modelo representa uma estruturação da gestão de riscos, proporcionando sua evolução e aprimoramento. Ele é uma ferramenta para identificação de eventos que possam afetar a entidade, ou que permite identificar oportunidades relacionadas com a execução dos objetivos. A partir desse modelo, a organização pode avaliar se o gerenciamento de riscos está sendo eficaz ou não e o que fazer para torná-lo eficaz.

Outro exemplo de abordagem sistematizada da gestão de riscos é o modelo usado pelo Departamento do Tesouro Britânico [4], o qual é apresentado na Figura 2.3. Neste modelo, é possível observar claramente no centro da imagem a adoção das atividades constantes do processo de gestão de riscos apresentado na ISO/IEC 31000 [3], as setas representando entradas e saídas de *insights* e informações internas e externas ao contexto. Na parte mais externa, estão os princípios que devem ser aplicados para que a gestão de riscos seja considerada eficaz, e nas laterais as atividades de comunicação e consulta.

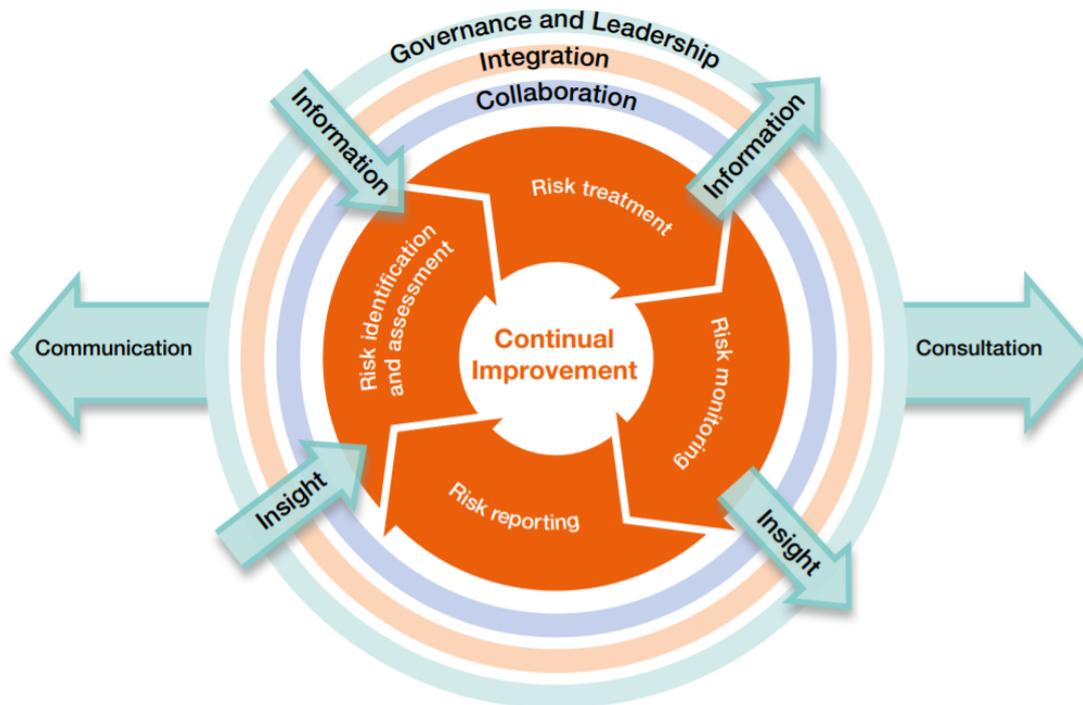


Figura 2.3: Modelo de gestão de riscos do HM Treasury/Orange Book. Fonte: [4]

Vale destacar outros modelos de gestão de riscos como os seguintes: o *FERMA - A Risk Management Standard* [46], o qual é um modelo criado pela *Federation of European Risk Management Associations* (FERMA), o *Standard and Poor's Risk Management Framework* [47], que aborda a cultura do risco, o gerenciamento e exposição, e por fim a sua otimização, o *OCEG "Red Book" 3.0: 2015 - A Governance, Risk and Compliance Capability Model* [48], que apresenta uma proposta de acesso aberto que integra governança, risco, auditoria, conformidade, ética/cultura de TI em uma abordagem unificada. Outro exemplo é o *Risk Management Framework - RMF do Department of Defense (DoD)* [49], utilizado pelo governo federal americano. Estes são alguns dos principais modelos de gestão de riscos elaborados e utilizados em outros países.

A *Risk and Insurance Management Society* (RIMS) ou Sociedade de Gestão de Riscos e Seguros (tradução livre), realizou uma revisão dos diversos modelos, normativos, guias, *frameworks*, entre outros documentos, e concluiu que existem características comuns entre eles. Dentre elas, destacam-se: a estruturação de etapas e atividades de processos, relatórios e supervisão da identificação de riscos, necessidade de patrocínio da alta gestão, definição clara de responsabilidades, compreensão da responsabilidade da definição de apetite aos riscos e seus limites e tolerâncias aceitáveis, estabelecimento de metas e atividades, formalização documental das avaliações de riscos, monitoramento dos planos e tratamentos dos riscos [50].

As iniciativas de padronização da gestão de riscos buscam auxiliar sua execução de

forma eficiente. No entanto, isso não torna sua aplicação mais simples, pois a adoção da gestão de riscos difere de uma organização para outra, revelando particularidades, práticas únicas e distintas que não podem ser descritas em manuais genéricos. Essas particularidades são justificadas pelas necessidades das instituições e pela percepção dos gestores, os quais são influenciados por diferentes contextos organizacionais, sejam eles políticos, econômicos ou sociais [51].

Enfim, visando identificar a ocorrência de trabalhos acadêmicos publicados sobre o tema em outros contextos, foi realizada uma pesquisa bibliográfica na base da *Web of Science* com a palavra-chave "*risk management*" (gestão de riscos em inglês), a qual retornou um grande número de publicações que, até o momento da pesquisa, somavam 51.584 trabalhos publicados.

Observando-se os resultados obtidos, ainda foi possível perceber que o autor com mais publicações na área é LI Y, com 100 publicações. O trabalho mais citado dentro do assunto é o "*2016 European Guidelines on cardiovascular disease prevention in clinical practice*" dos autores Piepoli, et al. [52], que somam um total de 2.947 citações.

Outro dado relevante é que o ano com a maior quantidade de publicações, até o momento, foi o ano de 2020, com 4.880. Observa-se que esse é um assunto em alta e cada vez mais abordado, nas mais diversas áreas de aplicação, e não somente na área de Tecnologia da Informação (TI).

2.2.1 Softwares de gestão de riscos

A gestão de riscos, nas instituições, pode ser aplicada de maneira transversal e necessita de integração com os demais processos existentes na empresa, para seu pleno funcionamento. [44]. Assim, pode-se afirmar que a gestão de riscos é de fato uma abordagem de suma importância para qualquer organização, principalmente quando é realizada utilizando-se de modelos e padrões reconhecidos [2].

Nesta pesquisa, foi realizado um levantamento das ferramentas de software existentes para auxiliar as atividades da gestão de riscos. Para esse propósito, foram utilizados os sites *GetApp*[12], *SourceForge*[13] e *Capterra*[14] os quais visam realizar busca e classificação de softwares. Por meio de pesquisa de softwares e fornecedores, nos sites mencionados, foram coletadas informações de vinte e quatro diferentes ferramentas de gestão de riscos, as quais estão descritas a seguir.

O *Donasafe* [53] é uma plataforma comercial multifuncional que abarca questões de saúde, segurança, meio ambiente, risco e fornecedor. Ele é composto por mais de 30 aplicativos que podem ser utilizado via *web* ou por aplicativos compatíveis com *IOS* e *Android*. O foco desta ferramenta está na diversidade e facilidade de uso. O módulo de

gestão de riscos baseia-se na norma ISO 31000 e é utilizado para auxiliar na conformidade com qualquer norma e regulamentação sobre segurança [3].

O software comercial *Onspring* [54] é voltado para a automatização de processos de negócios com foco na transparência, eficiência e controle. É disponibilizado como uma solução *Software as a Service* (SaaS), possui suítes específicas, sendo a uma de governança, risco e conformidade, outra de gerenciamento de serviços de TI e por último um pacote de operações de negócios. O módulo de riscos gerencia as responsabilidades para a tomada de decisões, adoção e adesão a protocolos.

O *Risk Secure Watch* [55] é uma plataforma comercial inteligente via *Software as a Service* (SaaS) para avaliação de riscos e segurança, que visa gerenciar riscos, monitorar e manter a segurança, bem como acompanhar a melhoria contínua. Propõe-se a ser um software personalizável, que possa se adaptar às necessidades do contexto utilizado.

O *IBM OpenPages com IBM Watson* [56] é uma solução comercial de governança, risco e conformidade escalável e tem como principal diferencial uso de inteligência artificial. A proposta da plataforma é centralizar as atividades da gestão de riscos em um único ambiente de forma intuitiva, onde qualquer pessoa, mesmo que não seja especialista na área de riscos, poderá utilizá-la.

O *Fusion Risk Management* [57] é um software comercial pertencente ao conjunto de sistemas da *Fusion Framework System*. A plataforma propõe uma melhora na resposta aos riscos por meio da simplificação das operações, juntamente com a melhora de sua visibilidade frente aos dados de toda a empresa. Para isto permite o mapeamento de processos críticos, planejamento e avaliação das atividades do gerenciamento de riscos, entre outras atividades de forma automática, reduzindo a carga de tarefas manuais.

O *Soft Expert* [58] é uma empresa com mais de 10 produtos para as mais diversas finalidades empresariais. Dentre eles oferece um produto específico para gerenciar governança, riscos e conformidade. O software comercial integra as estratégias de negócios com as práticas de conformidade e gerenciamento de riscos, aplicando elementos como riscos, políticas internas, leis/regulamentos, eventos de perda, indicadores de risco, indicadores de desempenho, problemas, avaliações, planos de ação e auditorias.

A *Soft Expert* também apresenta um software voltado exclusivamente para a gestão de riscos. Com um módulo denominado *SoftExpert ERM* [59] permite realizar a identificação, análise, avaliação, monitoramento e gerenciamento dos riscos de uma forma integrada. Esta solução serve como uma base para iniciativas de gestão de riscos visto que possui uma vasta biblioteca reutilizável de riscos e seus respectivos controles, avaliações e eventos, tais como perdas e não conformidades, indicadores de desempenho e planos de tratamento.

O software comercial *INTERISK* [60], é inteiramente focado na inteligência em riscos, integrando soluções de automação de gestão de riscos, tecnologia cibernética, processo

otimizado para a organização e aplicação da Lei Geral de Proteção de Dados, auditoria baseada em riscos, gestão de perdas, gestão de não conformidades, gestão de riscos tributários bem como seus impactos financeiros, entre outras.

O *RISKID* [59] é um software comercial que realiza a gestão de riscos inteligente por meio da cultura de conscientização e participação de todos os envolvidos, adotando uma abordagem focada na colaboração e facilidade de uso. A plataforma apresenta em suas funcionalidades um processo bem definido com papéis e atividades claras e sequenciais que buscam auxiliar os usuários.

Dos softwares apresentados até o momento o *TRAC governance cloud* [61] é o primeiro que tem o seu foco no gerenciamento da terceirização. Ele permite o gerenciamento eficaz de processos de governança críticos, em uma única ferramenta, abarcando também o gerenciamento de riscos e de problemas. Ele possui um foco direcionado ao auxílio na tomada de decisão e o envolvimento, colaborações e comunicação entre o fornecedor e o cliente.

O *A1 Tracker* [59] é um software comercial de gerenciamento de riscos que auxilia em questões relacionadas a riscos em contrato, reclamações, seguro, incidente, conformidade, segurança, aquisição e questões legais, fazendo uso de painéis personalizáveis, relatórios de métricas, portais para usuários, integrações com outros sistemas e treinamentos. O *A1 Tracker* apoia as empresas que buscam melhor gerenciar os riscos independentemente do tipo de negócio.

O software de governança, risco e conformidade baseado em nuvem da *ZenGRC* [62] auxilia na gestão de riscos da organização, de terceiros e de segurança cibernética. O software comercial realiza uma gestão de riscos operacionalizada, permite cálculos de riscos personalizáveis, e auxilia no monitoramento contínuo de riscos por meio de relatórios gerados pela plataforma.

O *FORM OpX* [63] é um software comercial, cuja aplicação é voltada para empresas grandes ou em crescimento, e se propõe a ser uma plataforma que combina coleta de dados e fluxos de trabalho avançados com *insights* operacionais para aumentar a produtividade em tempo real. A redução de risco é realizada por meio do gerenciamento dinâmico das tarefas, por meio da capacitação de equipes e digitalização do gerenciamento de incidentes.

O *Resolver* [64] é uma plataforma comercial utilizada em vários setores e áreas de negócios. A gestão de riscos conecta os riscos com os incidentes, de modo que sejam feitas avaliações tanto das prevenções quanto do entendimento de eventos passados. Tem como foco uma tecnologia fácil de usar aliada a um software altamente configurável que faz uso de dados e relatórios para quantificar e comunicar claramente o impacto dos eventos de risco e de segurança para a organização.

O *Módulo Risk Manager* [65] é uma solução de propriedade da empresa brasileira

Módulo, que realiza a automatização da governança, riscos e *compliance*, por meio da aplicação de uma metodologia proprietária desenvolvida que se baseou em normas e padrões internacionais de gestão de riscos. Com ele é possível implementar um processo eficaz, automatizado e integrado nas empresas.

A *FLOWTI* [66] é uma solução provida por um conjunto de empresas que prestam serviços e consultorias de TI. O escopo extrapola a gestão de riscos e propõe realizar o acompanhamento das empresas nos processos de planejamento, aquisição e implantação dos ativos de TI.

O software comercial *SimpleRisk* [67] apresenta funcionalidades abrangentes no que tange às necessidades de governança, gestão de riscos e conformidade. Seu funcionamento consiste em módulos, iniciando por um básico chamado *SimpleRisk Core* que é gratuito e apresenta funcionalidades simples, e os demais módulos são adquiridos à medida em que a organização, amadurece e precisa de funcionalidades mais avançadas.

Das ferramentas analisadas, a *Open Source Risk Engine* [68] é a primeira ferramenta de código aberto, que permite usar e modificar a base de código, bem como incorporá-la em aplicativos comerciais. O foco de seu uso está na análise de produtos financeiros e sua estruturação.

A *Practical Threat Analysis* (PTA) é uma metodologia desenvolvida para modelar as ameaças calculadas. Esta metodologia é utilizada pela *PTA Professional* [69], uma ferramenta comercial de avaliação de riscos que visa auxiliar analistas de segurança e consultores, identificando as vulnerabilidades e os riscos e definindo um plano de mitigação de risco eficaz.

Dentro da categoria de software de código aberto, o *Eramba* [70] surgiu da insatisfação de profissionais de governança, risco e *compliance* que lidavam com a falta de acessibilidade de ferramentas simples, gratuitas e que atuam em nível empresarial. O software surgiu com o objetivo de ser escalável, aberto e acessível. Até o momento da pesquisa, esta ferramenta contava com 11504 usuários da comunidade, 379 usuários corporativos e 3689 downloads no ano de 2021 [70]. Apesar de ter um código aberto sua distribuição é proibida e é cobrado um valor dos custos operacionais.

Outro software aberto é o *RA Risk Coverage Software* [71], o qual resultou de um projeto desenvolvido pelas empresas *Kostadin Taneski* e *A1 Telekom Austria*. Esse software é um projeto de ferramenta padrão e aberta que apoia uma abordagem baseada em riscos e tem como características: modelagem de fluxo de dados, catálogo de riscos, modelagem da avaliação dos riscos e a visualização e análise de cobertura de riscos.

OpenVAS [72] foi desenvolvido pela empresa *Greenbone Networks* e faz parte da família de produtos de gerenciamento de vulnerabilidade comercial juntamente com outros módulos *Open Source*. Seu foco extrapola gestão de riscos, e tem como recursos testes

não autenticados e autenticados, vários protocolos industriais e de Internet de alto e baixo nível, visando detectar vulnerabilidades nas empresas.

Por fim é apresentada a ferramenta *Project Risk Manager* [73] fornecida pela empresa de mesmo nome que é especializada em gerenciamento de riscos de projetos e fornece consultoria, treinamento, facilitação de *workshops* e serviços de software. O software é apresentado em uma versão gratuita e outra paga, cuja diferença entre elas são algumas limitações de uso. A ferramenta propõe-se a gerenciar com eficiência os riscos inerentes a cada projeto, identificando-os, quantificando-os e mitigando-os com precisão.

Após o um entendimento específico de cada das ferramentas apresentadas neste item, foi possível observar em todas elas uma estruturação do processo de gestão de riscos baseado na ISO 31000 [3]. Mesmo naquelas que não apresentam esta referência de forma clara em suas documentações.

Outra percepção é que das vinte e quatro ferramentas analisadas, apenas três tem seu código aberto: ([72]; *RA Risk Coverage Software* e; *Eramba*).

A maioria das ferramentas tem uma abordagem generalistas, sendo que somente cinco delas focadas na gestão de riscos: *RA Risk Coverage Software*; *PTA Professional*; [64]; *RISKID* e; *SoftExpert ERM*.

Apenas as ferramentas *FLOWTI* e *TRAC governance cloud* tem suas atividades centralizadas na terceirização de TI, tratando questões específicas como gestão de fornecedores.

Quatro ferramentas apresentam claramente uma possibilidade de modelagem e acompanhamento dos processos de negócios que podem ser adaptados de acordo com a necessidades. São elas: *Onspring*; *Fusion Risk Management*; *RISKID* e; *FORM OpX*

Por fim, destaca-se as seguintes ferramentas por apresentarem funcionalidades específicas que não foram identificadas nos outros softwares analisados. *IBM OpenPages com IBM Watson* por ter a utilização da inteligência artificial para auxílio nas atividades de gestão de riscos. E *SoftExpert ERM* por possuir uma biblioteca reutilizável que contém riscos, seus controles, avaliações e eventos, entre outros elementos associados.

2.2.2 Gestão de riscos de TI

A gestão de riscos, quando vista sob a ótica da tecnologia da informação em geral, e na engenharia de software em particular, é uma questão crítica a ser considerada em projetos de desenvolvimento e implantação. Em cenários onde os riscos não são entendidos, identificados e gerenciados, é possível observar a incidência de diversos problemas como não cumprimento de cronogramas, aumento dos custos, problemas nos requisitos e também na entrega de produtos que não agregam valor ao negócio [74].

Os riscos de TI estão associados aos objetivos de uso, propriedade, operação, envolvimento e influência da adoção de TI na organização, os quais podem causar impactos à TI e afetar o negócio das organizações [15].

O gerenciamento de riscos de TI é abordado em vários *frameworks* de gestão de projetos de TI. Ele é considerado um processo de apoio para o gerenciamento de vários tipos de riscos, otimizando assim o valor associado aos investimento de TI, buscando o equilíbrio dos custos envolvidos, as medidas de segurança e a obtenção de ganhos, ao mesmo tempo em que protege os sistemas e as informações. [75].

Uma pesquisa realizada pela *Deloitte* com a participação de 100 empresas mostrou que apenas 54% das empresas brasileiras pesquisadas não possuem estrutura de gestão de riscos operacional, e que 61% desse percentual não realizam análises de riscos relacionados à TI. Porém, esse resultado muda quando é analisada a gestão de riscos de segurança da informação, passando representar 72% das empresas respondentes [76].

O normativo que começou a tratar da gestão de riscos junto à TI foi a ISO/IEC 13335-3 [77], apresentando a avaliação de riscos como parte importante da gestão da segurança da informação, focando na diminuição das vulnerabilidades de forma alinhada com o nível de tolerância da organização em correr riscos.

A ABNT NBR ISO/IEC 27005 [5] apresenta a gestão de riscos para segurança de TI e complementa o processo apresentado na ABNT NBR ISO/IEC 31000 com um nível maior de detalhes das atividades, principalmente no que tange o tratamento dos riscos, conforme apresentado na Figura 2.4.

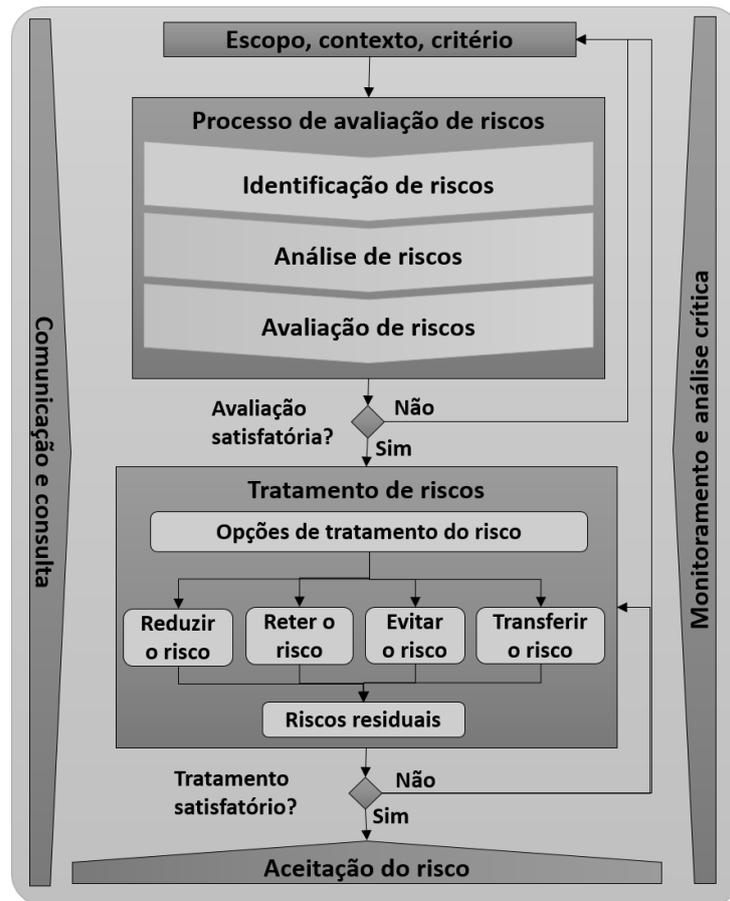


Figura 2.4: Processo de gestão de riscos de segurança da informação segundo a ABNT NBR ISO/IEC 27005. Fonte: [5]

A gestão dos riscos de TI integrada nas práticas de gestão das empresas é fundamental, pois riscos sempre existirão, mesmo que não sejam identificados ou conhecidos [15]. Portanto essa integração incentiva a compreensão das prioridades de negócios e a proteção de serviços mais críticos por parte da TI, além de ser essencial o apoio e adesão das partes interessadas, a implantação das política e a cultura de riscos que envolva treinamento e comunicação na instituição [75].

O *Project Management Body of Knowledge* (PMBOK) apresenta o gerenciamento de riscos de projetos como uma das áreas de conhecimento de sua estrutura e portanto parte fundamental na gestão de projetos. Essa área de conhecimento tem como objetivo a busca por maximizar a exposição aos eventos positivos e minimizar a exposição aos eventos negativos. É composta pelos seguintes processos: Planejamento da gerência de riscos; identificação dos riscos; Análise qualitativa dos riscos; Análise quantitativa dos riscos; Planejamento das respostas aos riscos; Implementação das respostas aos riscos; e Monitoramento dos riscos [8]. Vale ressaltar as semelhanças entre sua estrutura com o processo da ISO 31000 [3].

Outro exemplo de *framework* que aborda o assunto é o COBIT 5 para risco, o qual fornece um conjunto de 111 exemplos em 20 diferentes categorias de cenários. Ele indica como aplicar os processos do COBIT 5 para responder aos riscos de forma eficaz e eficiente a fim de dar suporte ao valor atribuído pelas partes interessadas [15].

Para muitas organizações, os riscos de TI são frequentemente subestimados, mesmo quando há práticas de gestão de riscos da TI disponíveis e há o entendimento da necessidade e importância da gestão de riscos. Este é um cenário preocupante pois a crescente transformação do setor de TI traz consigo a exposição das organizações a maiores níveis de probabilidade de eventos indesejados e seus impactos, como de vazamento de dados, roubo de ativos e danos à reputação [75].

2.3 Conceito de terceirização

O termo "terceirização" é uma tradução da palavra de origem inglesa "*outsourcing*" e sua definição é abordada por diversos autores. Ele é uma abreviatura do termo "*outside resource using*", que em tradução livre significa "uso de recursos externos", e pode ser entendido como a contratação de organizações de fora da empresa para que seja executada toda ou parte de atividades e funções da rotina, geralmente executada internamente na instituição em troca de uma determinada remuneração [26] [27] [28] [29] [30]. Esta ação de terceirização é realizada para cortar custos internos, ou, visando um crescimento competitivo no mercado, melhorar a qualidade de produtos ofertados [26].

O início da terceirização se deu no século 18 e até a década de 80 não era bem recebida, passando a ganhar grande força somente nos anos 90 [31]. Desde então, a terceirização mostra-se como uma prática da organização e da gestão empresarial, resultando em uma vantagem competitiva frente à disponibilização de produtos e serviços de forma mais eficaz e eficiente por fornecedores externos [78]. Assim, é possível concluir que a terceirização pode ser entendida como um modelo de negócio que visa a entrega de um produto ou serviço realizado por um fornecedor, como alternativa ao seu desenvolvimento interno na própria empresa [10].

2.3.1 Terceirização de TI

Na pesquisa por trabalhos publicados sobre o tema terceirização de TI, foi necessária a aplicação de uma *string* de busca mais complexa na base do *Web of Science*, pois esse termo pode ser citado de diversas formas. Portanto, o termo buscado usado na busca foi ("*IT*" OR "*information technology*") OR ("*IS*" OR "*information system**") AND ("*outsourc**").

A pesquisa resultou, até o momento em que foi realizada, num total de 15.956 publicações, sendo a publicação mais citada "*Competing models of entrepreneurial intentions*" dos autores Krueger, NF, Reilly, MD e Carsrud, AL [79] que totaliza 1.901 citações. O ano com a maior quantidade de publicações foi 2019 com 1.438 registros e o autor com maior número de publicações nesse assunto foi LI J, com um total de 96 trabalhos publicados.

A primeira publicação é datada de 1991, em um trabalho intitulado "*GLOBAL OUTSOURCING OF INFORMATION-SYSTEMS FUNCTIONS - OPPORTUNITIES AND CHALLENGES*", dos autores Uday M Apte e MaryAnne Winniford [80]. É possível observar com isso que o início das pesquisas sobre a terceirização de TI acompanhou o crescimento da terceirização em geral, há 30 anos.

Um grande impulso na terceirização de TI ocorreu na área de infraestrutura, quando foi anunciado um acordo em que a empresa *International Business Machines Corporation* (IBM) assumiria o *Data Center* da empresa Kodak. Esse acordo visava cortar os custos de operações internas em até 50%, através do repasse de quatro centros da Kodak e cerca de 300 funcionários para a IBM. O impacto do acordo citado foi tão profundo que a terceirização de TI passou a ser uma escolha estratégica que viria a definir o sucesso e sobrevivência das empresas na década de 1990 [32].

Com o aumento da utilização da terceirização como uma parte amplamente aceita do negócio, sua atuação passa a ser realizada de forma transversal no departamento de TI, desde *help desk* até desenvolvimento e manutenção. Isso resultou no acesso a uma gama ampla de recursos qualificados, permitindo às empresas focarem em suas atividades internas essenciais e em seus pontos fortes, acelerando o tempo de entrega com a redução de custos operacionais [81].

As pesquisas sobre o tema terceirização também aumentaram, acompanhando o crescimento da terceirização nas empresas. Essas pesquisas abordam o entendimento sobre suas questões, focando no porquê das empresas terceirizarem, como se beneficiam disso, o que se terceiriza, e como o fazem, além dos resultados da terceirização, mensurados por meio da percepção de expectativa, satisfação e performance [34].

Mesmo sendo um tema crescente em pesquisas e publicações, ainda é um assunto recente, se comparado, por exemplo aos 100 anos de estudos publicados sobre a gestão de riscos. Outro fator importante é a complexidade desse campo de estudo, devido ao crescimento da quantidade de tipos de terceirização que surgem com o avanço da TI e as mudanças dinâmicas do cenário de negócios, gerando assim um variedade de abordagens sobre os estudos da terceirização [82].

No que se refere ao termo "terceirização de TI", este pode ser entendido como a transferência parcial ou total de atividades internas e serviços de TI para fornecedores externos, que tem suas atividades regidas por acordos contratuais estabelecido entre as partes [83].

Um ponto relevante a se observar é que ao se transferir uma atividade interna para uma execução externa, a empresa que adere à terceirização perde, pelo menos, algum controle sobre tal atividade, além da necessidade de reorganizar a forma de gestão e operação na instituição [84].

No que se refere aos resultados esperados com a terceirização de TI, as declarações são otimistas sobre os ganhos associados. Porém, as consequências podem ser tanto positivas como negativas, levando ao seu fracasso ou sucesso [85]. Os motivos pelos quais os projetos de terceirização falham são resultantes de decisões pouco fundamentadas feitas a partir de incertezas e informações incompletas, tornando a decisão de terceirização em si arriscada por natureza [21].

Por outro lado, Cristofoli [85] apresenta uma lista de fatores, com base na literatura, que influenciam o sucesso da terceirização de TI:

- Alinhamento estratégico: é de grande importância que a terceirização de TI esteja alinhada com a estratégia global da empresa;
- Valor para o negócio: contribuindo com a melhoria da execução do negócio, a terceirização de TI influencia positivamente o crescimento do valor do negócio;
- Economias de escala: tem influência direta da falta de capacidade do fornecedor em realizar economias de escala;
- Estrutura de custo: a terceirização de TI sendo um agente transformador de custos fixos em custos variáveis;
- Gestão de riscos: a adoção de práticas da gestão de riscos como um fator determinante para o resultado positivo da terceirização de TI;
- Controle e monitoramento: são executados visando o aumento das chances de sucesso da terceirização, por meio de normas e controles gerais que fortalecem os relacionamentos e que se tornam fatores essenciais para o êxito do negócio.

Os principais desafios organizacionais trazidos pela terceirização permeiam dois principais temas. O primeiro é a garantia da entrega de valor, em que é analisado o desempenho e os benefícios que a terceirização trouxe. O segundo tema é o controle e a diminuição do risco atrelado, quando busca-se atender à necessidade de terceirizar os serviços certos de maneira correta [84].

Frente a esse cenário da terceirização de TI, a gestão de riscos se mostra, claramente, como um dos fatores críticos de sucesso para uma terceirização eficaz que, apesar de não eliminar todas as incertezas, aumentam as chances de sucesso [83].

2.4 Gestão de Riscos na terceirização de TI

Na busca do entendimento do contexto das pesquisas referentes à gestão de riscos na terceirização de TI foi utilizada na base científica *Web of Science* a junção das *strings* de pesquisa sobre gestão de riscos e terceirização de TI, resultando na seguinte expressão: *((("IT"OR "information technology") OR ("IS"OR "information system*")) AND ("outsourc*") AND ("risk management"))*

Obteve-se um número de 309 trabalhos publicados, iniciando no ano de 1995 com o trabalho "*FRAUD - THE ROOT CAUSES*" do autor POMERANZ, F [86]. As publicações anuais não são expressivas, em que foi observado um pico maior nos anos de 2014 e 2017 com 25 publicações anuais cada ano. Observa-se então que esse é um tema ainda mais novo do que a própria terceirização de TI e se mostra ainda pouco explorado no meio acadêmico.

A baixa quantidade de pesquisas sobre o assunto (se comparado a outros temas deste trabalho) alinhada ao fato da gestão de riscos, que abrange em seu processo a identificação, análise, controle e gerenciamento dos riscos, ao ser aplicada no contexto de terceirização tem sua complexidade aumentada devido à ampliação de partes e ambientes envolvidos [83] [3].

Os riscos podem variar de setor para setor, bem como seus impactos. A gestão deve avaliar o valor pretendido e seus riscos associados antes de tomar decisões referentes à terceirização [10].

No que tange aos riscos relacionados à terceirização de TI, duas grandes questões se mostram relevantes para os profissionais: quais são os riscos e como mitigá-los. Porém, ao se consolidar essas informações, percebe-se que, devido à grande quantidade de práticas específicas projetadas para reduzir cada risco, a complexidade na redução dos riscos, muitas empresas podem questionar os reais benefícios na terceirização de TI. [34].

Lacity, Khan e Willcocks [34] sugerem que a curva de aprendizado resultante das experiências não pode ser substituída por observação e estudo da mitigação realizada por outras empresas. Deste modo, a vivência anterior na terceirização é vital para o sucesso da terceirização da TI. Para isso, busca-se gerenciar a aprendizagem por meio de teste-piloto, além de contemplar no planejamento da terceirização um momento para possíveis erros.

A responsabilidade sobre o êxito da terceirização é, em sua maioria, daquele que a contrata, devendo se atentar às questões críticas de incertezas como possibilidade de gestão fraca, equipe inexperiente, incerteza nos negócios, habilidades tecnológicas desatualizadas, incerteza naturais, custos ocultos, falta de aprendizado organizacional, perda de capacidade inovadora, perigos de um triângulo eterno de dependência, indivisibilidade da tecnologia e foco difuso. Portanto, o sucesso da terceirização está ligado diretamente

à capacidade da empresa em gerir os serviços de TI já existentes [87]. Essa gestão e controle devem ser estendidos a qualquer atividade de terceirização, visando o auxílio no gerenciamento dos riscos. Para isso, é crucial estabelecer um processo de terceirização bem definido que considere as necessidades da organização do que tange ao controle e conformidade financeira, relacionamento, desempenho e a gestão proativa dos riscos [84].

Entendendo que a gestão de riscos envolve um processo de identificação, análise, controle e gerenciamento dos riscos ao longo do ciclo de vida de um projeto, ao ser aplicada ao contexto de terceirização sua complexidade é aumentada devido ao aumento de partes e contextos envolvidos [86] [3].

2.5 Gestão de Processos de Negócios

Define-se processo como uma agregação de atividades e comportamentos inter-relacionados que visam converter entradas e saídas, através de uma série de ações realizadas em uma ordem específica que podem ser executados por pessoas ou máquinas e são voltadas para atingir um resultado que soluciona uma questão específica [6] [88] [89] [90].

Negócio é definido como interações entre pessoas que executam um conjunto de atividades visando a entrega de valor e geração de um retorno [6]. Processo de negócio, por sua vez, é um trabalho que tem como principal objetivo entregar valor para os clientes ou gerenciar outros processos [6].

A Gestão de Processos de Negócio, ou *Business Process Management* (BPM), é uma disciplina gerencial que realiza a integração entre as expectativas e necessidades dos clientes e as estratégias e objetivos da organização [6]. Permitindo que os usuários monitorem a execução de processos individuais e analisem o comportamento geral de operações de ponta a ponta [91] [88]. O BPM engloba desde estratégias, objetivos e cultura, até o gerenciamento de desempenho e estabelecimento da governança de processos [6].

Seu surgimento ocorreu em um contexto de mercado altamente competitivo, onde as empresas buscaram o entendimento e agilidade essenciais para ter uma resposta eficaz com uma maior eficiência no trabalho [92]. Desta forma transformou a visão do funcionamento das instituições de um conjunto de áreas funcionais, para uma combinação de processos integrados, não sendo mais divididas por departamentos específicos e sim responsabilidades dentro dos processos de trabalho [93] [94].

O principal objetivo de seu uso é estruturar uma arquitetura de processos bem definida, mostrando o valor entregue para as partes envolvidas, mensuração de desempenho dos processos, possibilitando assim esclarecer as metas da instituição e descrever como alcançá-las detalhando as atividades dos processos de negócio [6] [95].

Apesar da literatura apresentar diferentes etapas e atividades que constituem a execução do ciclo de vida de funcionamento do BPM [7]. Porém, um dos modelos mais completos e mais difundidos é o ciclo proposto pela *Association of Business Process Management Professionals* (ABPMP) [6]. O ciclo em questão é composto por seis fases conforme é apresentado na Figura 2.5.

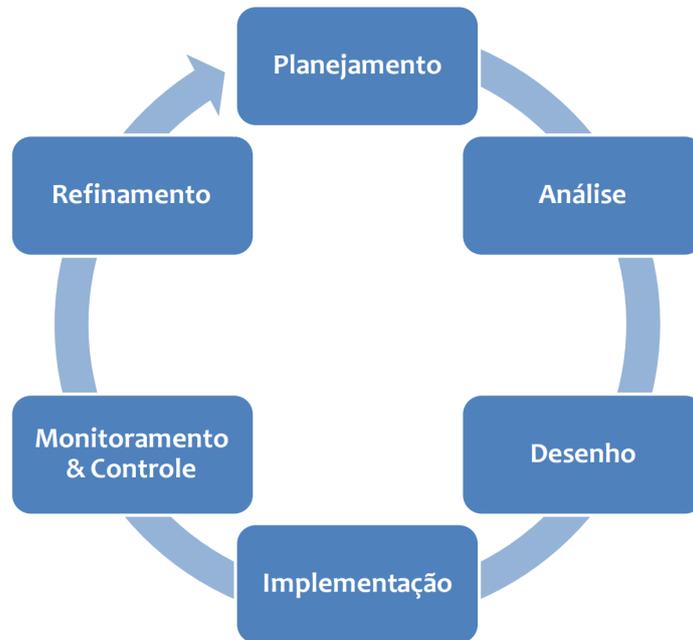


Figura 2.5: Fases do ciclo de vida BPM. Fonte: [6]

A primeira é a fase de planejamento, onde é estabelecido uma estratégia e planejamento para a execução das ações do BPM. Em seguida é realizada a fase de diagnóstico, onde o processo de negócio é diagnosticado, ou seja, é feito um entendimento do processo atual de ponta a ponta, bem como seu alinhamento aos objetivos e metas negociais. Neste momento é possível se utilizar de recursos visuais como mapeamento do processo atual, que pode ser chamado de AS-IS [6].

A terceira fase é o desenho, momento em que é feito o mapeamento do novo processo e toda suas especificações, o modelo mapeado também pode ser chamado de TO-BE. Na fase seguinte é realizada a implementação do novo modelo, bem como os desafios e relacionados a mudança e otimização do processo. Em seguida é executada a fase de monitoramento e controle, onde os todos os resultados são registrados para servirem de insumos para tomadas de decisões futuras. Por fim, a na última fase é realizado o refinamento, momento em que são feitos os ajustes e melhorias necessários para contribuir de forma cíclica com o BPM [6].

A notação denominada *Business Process Model and Notation* (BPMN), criada pela *Business Process Management Initiative* (BPMI), é um padrão que apresenta um conjunto

de símbolos que padronizam a modelagem de processos e está presente nas principais ferramentas de modelagem existentes[6].

Os componentes dos diagramas BPMN são divididos em raias paralelas, onde cada uma representa o papel realizado por um ator que realiza uma atividade seguindo o fluxo de trabalho [6]. Os principais componentes são [7]:

- Atividades, apresenta os trabalhos realizados em um processo;
- Subprocessos, são utilizados para ocultar níveis de abstração de trabalho;
- Eventos, representa algum acontecimento que interfere no fluxo do processo;
- Associação, serve para ligar artefatos com elementos do diagrama;
- Fluxo de sequência, indica ordem das atividades;
- Fluxo de mensagem, indica fluxo de mensagem entre os atores;
- *Gateway*, controla divergências e convergências do fluxo, podendo ser do tipo exclusivo, baseado em evento, inclusivo, complexo ou paralelo.

A Figura 2.6 apresenta um exemplo simplificado de um modelo de processo utilizando a notação BPMN bem como os principais componentes de diagramas listados anteriormente.

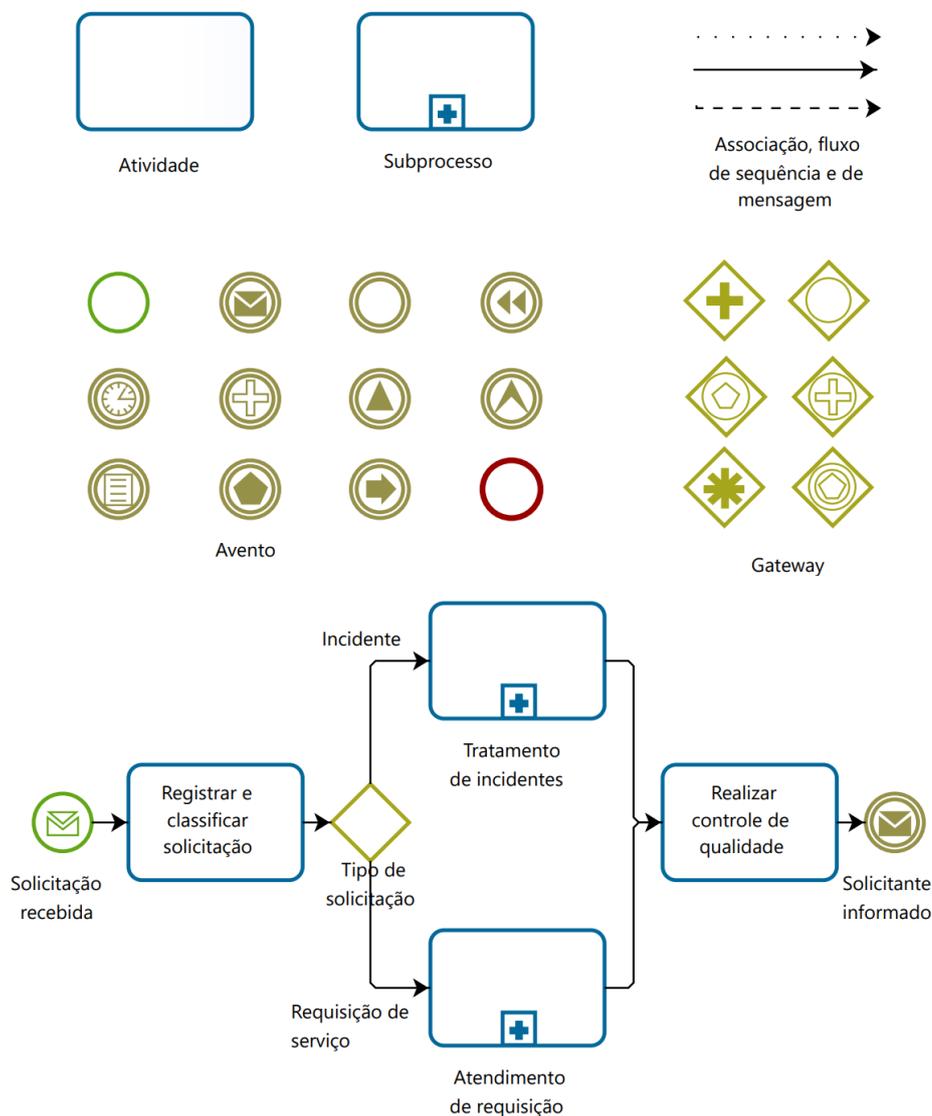


Figura 2.6: Principais componentes do BPMN e representação simples de um processo. Fonte: adaptado de [7]

2.6 Gestão de escopo de projeto utilizando Estrutura Analítica do Projeto (EAP)

Projetos podem ser entendidos como conjunto de atividades que geram um esforço temporário, com início e fim definidos para criação de um produto, serviço ou resultado exclusivo. O gerenciamento de projetos busca, dentro contexto de cada projeto, criar um equilíbrio entre tempo, custo, comunicação entre os envolvidos, qualidade e escopo, permitindo que as instituições executem seus projetos de forma eficiente e eficaz [8].

Frente a isto foi criado nos Estados Unidos em 1969 o *Project Management Institute* (PMI), uma instituição focada em promover a gestão de projetos, se tornando a organização referência no assunto. Posteriormente, em 1987, a instituição publicou o *Project Management Body of Knowledge* (PMBOK), que consiste em um conjunto de práticas organizadas em 49 processos e grupos de processos que são agrupados em um fluxo composto por 5 grupos: iniciação; planejamento; execução; monitoramento e controle e; encerramento [8]. Conforme apresentado na Figura 2.7.

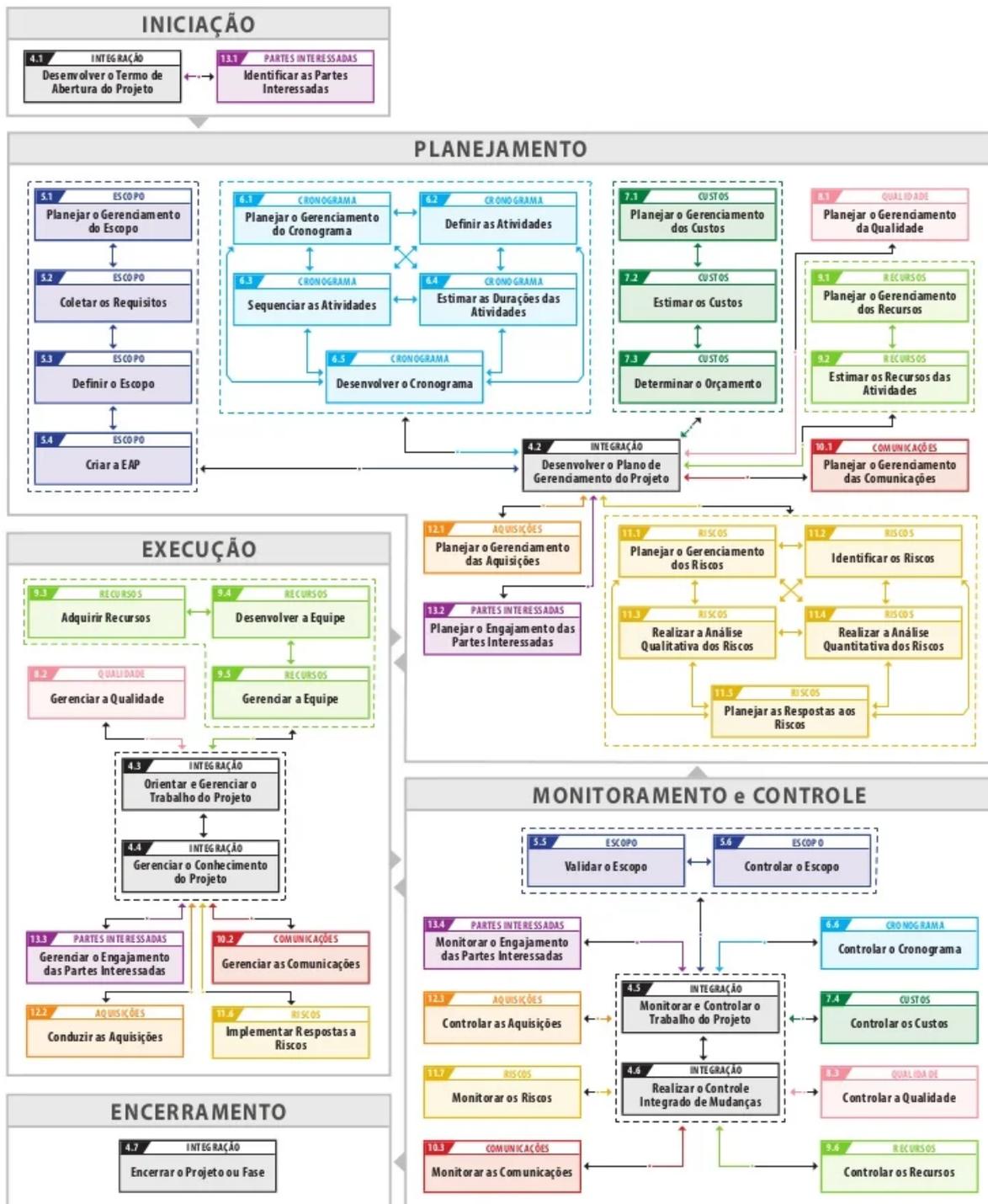


Figura 2.7: Fluxo de Processos do Guia PMBOK. Fonte: [8]

Dentro da execução do gerenciamento do projeto, um grande desafio encontrado é a definição clara do produto e/ou serviço que deverão ser entregues para o cliente, estabelecendo assim o escopo do trabalho que deverá ser realizado [96].

O PMBOK aborda esta questão através do gerenciamento do escopo do projeto, composto pelos processos necessários para definir e controlar o que está e o que não está incluído no projeto. Dos seis processos que o compõe destaca-se o processo denominado “Criar Estrutura Analítica do Projeto (EAP),” ou seja, processo de decompor as entregas do projeto em componentes menores os quais devem ser dispostos em um diagrama com níveis hierárquicos de ações sequenciadas [8].

Fazendo uso do plano de gerenciamento do escopo, juntamente com a especificação do escopo do projeto a EAP define e organiza o escopo total do projeto, bem como seu trabalho planejado que são denominados pacotes de trabalho que podem ser produtos de trabalho ou entregas resultante de atividades [8].

A estrutura de EAP pode ser elaborada usando uma abordagem descendente (textit top-down), onde os níveis mais altos dos componentes são detalhados em níveis menores, ou abordagem ascendente (textit bottom-up), utilizada para agrupar subcomponentes. Com esta decomposição o planejamento, gerenciamento e controle dos componentes aumenta [8]. É apresentado na Figura 2.8 um exemplo de construção de EAP.

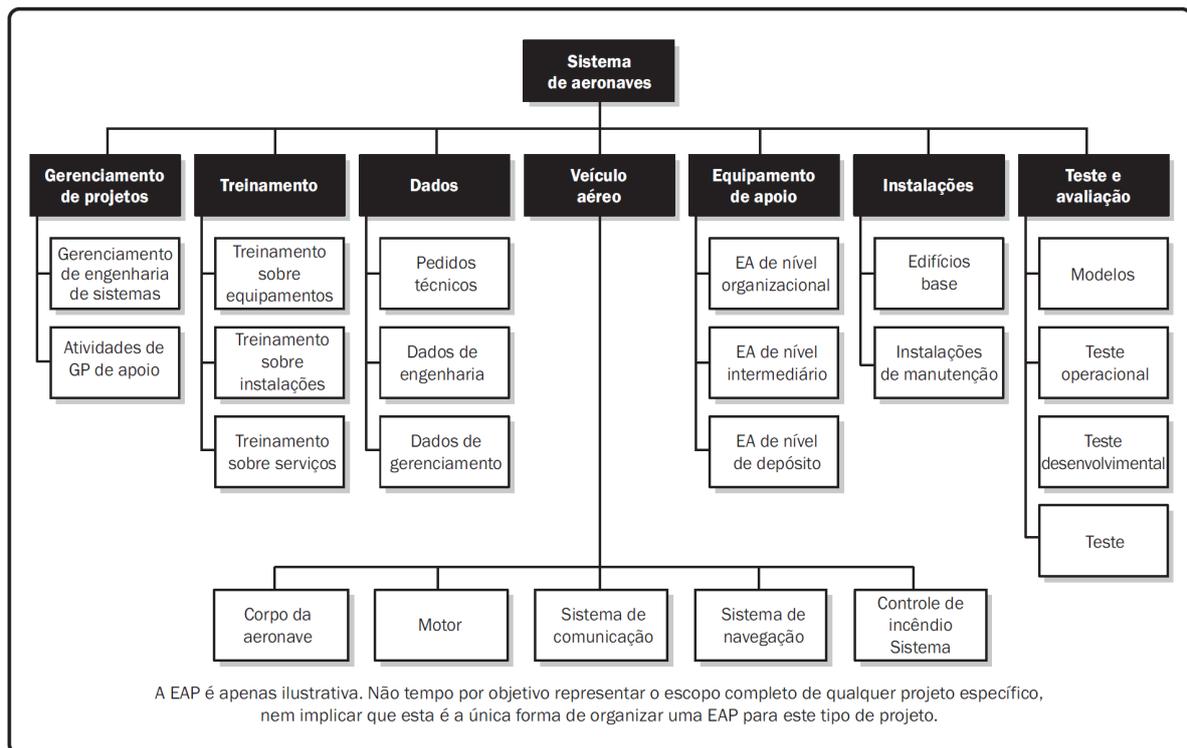


Figura 2.8: Exemplo de EAP ilustrativa com Entregas Principais. Fonte: [8]

2.7 Considerações finais do capítulo

Neste capítulo, foi apresentada uma revisão bibliográfica dos principais temas abordados na pesquisa, e foram identificadas as publicações necessárias para fundamentação da pesquisa. Com isso foi possível obter um melhor entendimento sobre a gestão de riscos, sua aplicação específica na TI, a terceirização de TI e por fim a gestão de riscos na terceirização de TI. Dando continuidade, *Capítulo 3 – Metodologia da pesquisa* tem a apresentação e descrição da metodologia empregada nesta pesquisa, com a descrição do planejamento, dos procedimentos e das ações adotadas.

Capítulo 3

Metodologia da pesquisa

3.1 Considerações iniciais do capítulo

Dado o objetivo desta pesquisa, propor uma *solução de gestão de riscos para o processo de terceirização de TI*, neste capítulo apresentam-se os materiais e os métodos empregados. No *capítulo 1 - Introdução* foi apresentada a classificação metodológica e neste capítulo é apresentado e descrito o plano metodológico adotado, com as quatro fases básicas: planejamento da pesquisa; coleta de dados; análise dos dados; e relato dos resultados.

3.2 Fase de planejamento da pesquisa

A primeira fase, Planejamento da Pesquisa, inicia-se com o entendimento do problema organizacional e a definição do objetivo da pesquisa. Na fase seguinte, *Coleta de Dados*, foram empregados os procedimentos e técnicas de coleta de dados. Na fase *Análise de Dados*, foram analisados os dados coletados de forma qualitativa. Na fase final, *Relato dos Resultados*, se caracteriza por este documento como relato deste trabalho.

O planejamento da pesquisa, representada na Figura 3.1, é a primeira fase do plano metodológico.

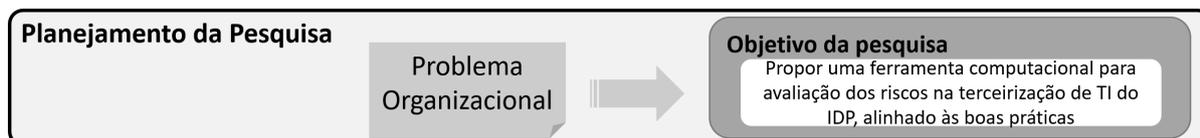


Figura 3.1: Planejamento da pesquisa. Fonte: autora

Essa fase tem como resultado a definição do tema de pesquisa, o problema organizacional a ser resolvido, o objetivo geral e os específicos, assim como a metodologia de pesquisa selecionada e empregada nesta pesquisa.

O plano metodológico adotado é detalhado na Figura 3.2:

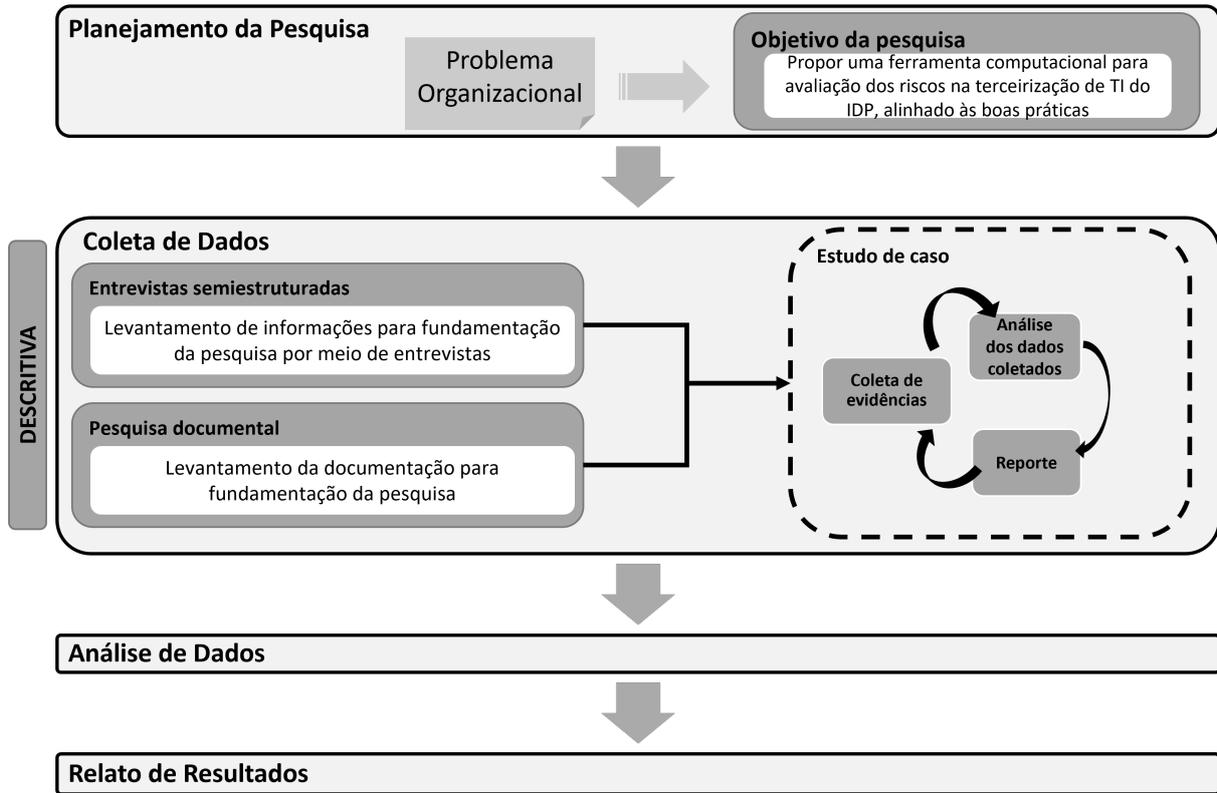


Figura 3.2: Plano metodológico adotado. Fonte: autora

3.3 Fase de coleta de dados

Na fase de coleta de dados, conforme ilustra a Figura 3.3, foram utilizadas as seguintes técnicas de coleta de dados: a entrevista semiestruturada; a pesquisa documental; e a técnica estudo de caso, em que foram adotadas as etapas *coleta de evidências*; *análise dos dados coletados*; e *reporte*.

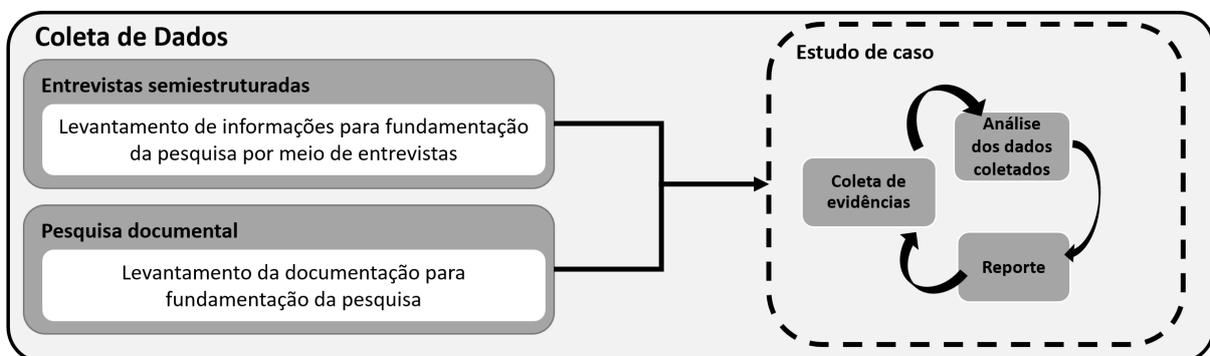


Figura 3.3: Coleta de dados. Fonte: autora

3.3.1 Entrevistas semiestruturadas

A entrevista semiestruturada pode ser definida como uma técnica em que o investigador, fazendo uso de teorias e pressupostos previamente definidos, apresenta frente ao investigado perguntas com o objetivo de recolher respostas que de interesse para a investigação [36] [97].

Quando segue um nível semiestruturado, este recurso metodológico tem uma característica mais flexível, permitindo que o entrevistado tenha uma liberdade de expressão, mantendo o foco no tema determinado pelo entrevistador. Este por sua vez formula um roteiro de perguntas principais iniciais que podem ser complementadas oportunamente por outras questões momentâneas na própria entrevista [36] [97].

Nesta pesquisa, a aplicação da entrevista ocorreu no momento da descrição do processo de terceirização de TI do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP). A amostra definida para a realização das entrevistas constou de pessoas que possuem envolvimento direto com o processo estudado. Foram selecionados então os gerentes de cada área e um colaborador da área demandante.

A amostra escolhida para ser entrevistado equivale a proporção de 62,5% do total de colaboradores envolvidos a cada ciclo de processo. Foram entrevistados os gestores das áreas de tecnologia da informação, financeira, *facilities*, diretoria e Organização e Método.

O tempo de duração foi delimitado em 2 horas e todas as entrevistas foram iniciadas com uma breve explicação sobre o objetivo da pesquisa, seguida pela pergunta inicial que guiou toda a interação entre a pesquisadora e o entrevistado: "Como ocorre o processo de aquisição desde o início do interesse e planejamento e até o seu fim, levando em consideração a participação da sua área no processo como um todo?".

As entrevistas foram realizadas, gravadas e depois consolidadas, auxiliando tanto na caracterização do IDP quando na descrição do processo de terceirização em execução no momento da pesquisa.

Como as entrevistas foram realizadas em momentos específicos da pesquisa fazendo parte da execução de objetivos específicos, os maiores detalhes como a quantidade de entrevistas, roteiro, tempo e participantes, é descrito no capítulo em que houve sua execução.

3.3.2 Pesquisa documental

A pesquisa documental, apesar de se assemelhar à pesquisa bibliográfica, tem como principal diferença a natureza de suas fontes, que são mais diversificadas e dispersas, além de não receberem tratamento analítico e serem reelaboradas de acordo como os objetos

da pesquisa. Ela pode ser composta por guias, modelos, instruções, relatórios, e-mails, manuais, entre outros [36].

A pesquisa documental ocorreu em vários momentos da pesquisa. Primeiramente na análise e extração de boas práticas de terceirização e gestão de riscos, oriundos do COBIT 5, ISO 37500 e ISO 31000. Em seguida foi utilizada no estudo de documentos internos do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP) para se ter um diagnóstico do processo de terceirização de TI existente. E por fim, juntamente com a revisão bibliográfica realizada no *capítulo 2*, a pesquisa documental foi utilizada na busca de ferramentas existentes que se alinhavam com as boas práticas e as necessidades de um novo processo de terceirização de TI, ora proposto.

3.3.3 Estudo de caso

A técnica de estudo de caso adotada está alinhada com o conceito que Yin [98], que define estudo de caso como a observação empírica que busca investigar um fenômeno dentro do seu contexto da vida real, especialmente quando os limites entre o contexto e o fenômeno não estão definidos de forma clara. O protocolo de estudo de caso adotado segue a proposta de Runesson [1]. Foram definidas 3 etapas: coleta de dados; análise dos dados; e relato dos resultados. As etapas foram realizadas de forma cíclica, conforme apresentado na Figura 3.4.

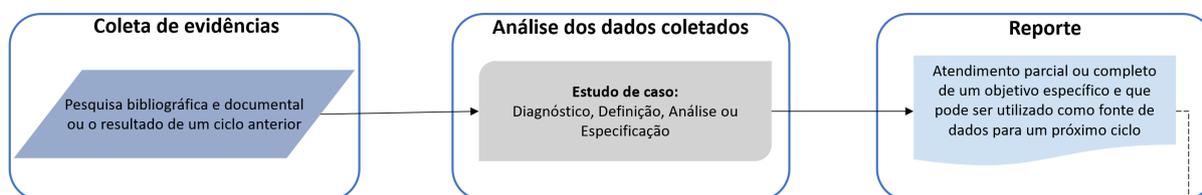


Figura 3.4: Ciclo das etapas do estudo de caso. Fonte: [1]

A etapa de coleta dos dados, ou coleta de evidências, é o procedimento de extração das informações necessárias para a etapa seguinte, a de análise [1]. Essa etapa está diretamente ligada aos demais procedimentos de coleta, como pesquisa documental e entrevista semiestruturada, mas também pode fazer uso de resultados obtidos em ciclos anteriores.

Na *análise dos dados coletados* é realizado todo o procedimento de análise, diagnóstico, definição ou especificação dos dados extraídos na etapa anterior [1]. Nessa etapa ocorre a investigação do fenômeno estudado. Por fim, o reporte consolida todas as conclusões de forma compilada e viável para utilização, seja para um próximo ciclo ou para a elaboração do documento final da pesquisa [1].

Ciclos do estudo de caso

O planejamento da execução dos ciclos do estudo de caso foi orientado pelos objetivos específicos, resultando em um total de cinco ciclos, conforme apresentado na Figura 3.5.

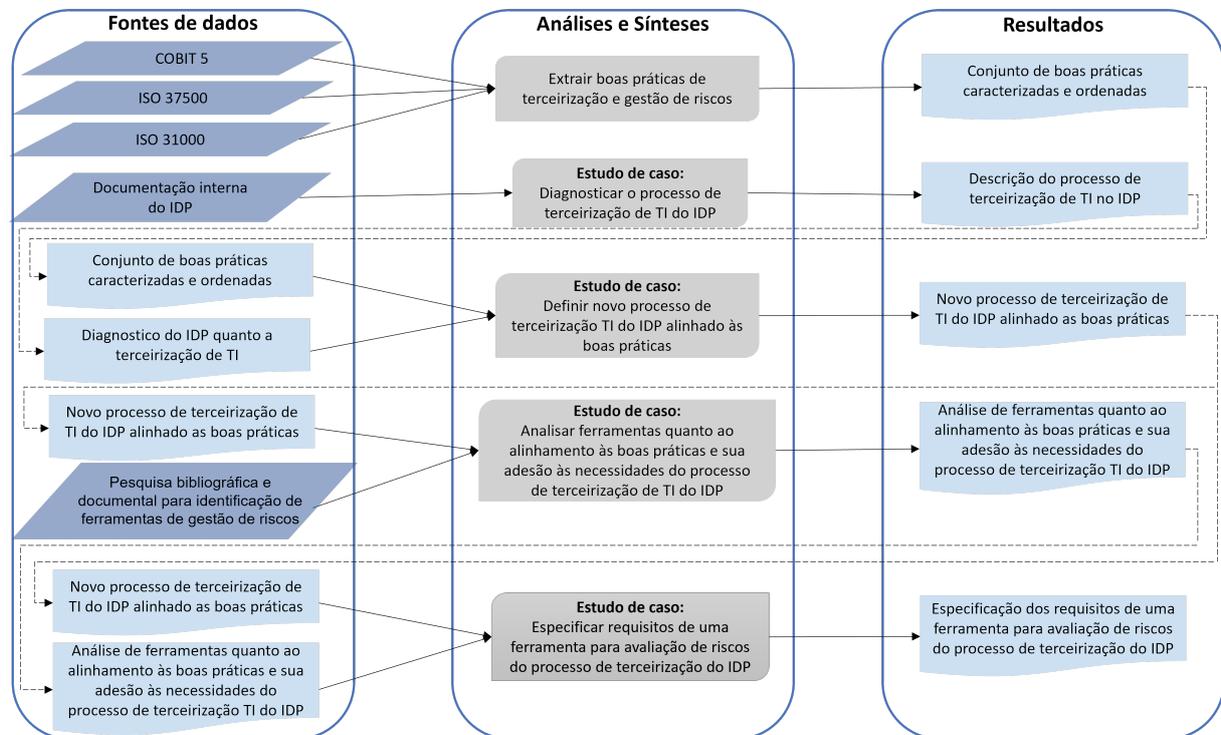


Figura 3.5: Ciclos unificados do estudo de caso. Fonte: autora

O primeiro ciclo teve início na busca de fonte de dados, tendo como escopo: COBIT 5, ISO 37500 e ISO 31000. Onde foram extraídas fases, práticas e atividades, devidamente caracterizadas, pontuadas e ordenadas. O resultado foi compilado e descrito no *capítulo 4 - seleção de boas práticas para a terceirização de TI e gestão de riscos*.

O segundo ciclo iniciou-se com o levantamento de informações sobre a organização onde se deu a pesquisa, o Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP). Foi feito o uso da pesquisa documental juntamente com entrevistas semi-estruturadas para caracterizar o objeto de estudo e seu histórico. Essa atividade resultou no diagnóstico de terceirização de TI atual da instituição, bem como o mapeamento do processo atual (AS-IS) realizado, utilizando a notação *Business Process Model and Notation* (BPMN), descrito no *capítulo 5 – Descrição do processo de terceirização de TI no IDP*

O resultado do segundo ciclo somado à extração de boas práticas, realizada no primeiro ciclo, serviram de fonte de dados para o terceiro ciclo. A partir da análise dos dados, foi possível realizar a proposta de um *novo processo de terceirização de TI para o IDP, alinhado às boas práticas de terceirização de TI e à gestão de riscos*. O resultado foi um

novo mapeamento proposto (TO-BE) também fez uso da notação BPMN e está descrito e detalhado no *capítulo 6 – Proposta de novo processo de terceirização de TI para o IDP*.

No quarto ciclo, a fonte de dados foi o *novo processo de terceirização de TI definido*, somado à busca bibliográfica e documental de ferramentas de gestão de riscos. Para a etapa de análise, foi empregado um trabalho em conjunto com alunos da disciplina de Projeto de Sistemas de Produção 2 (PSP2), do Curso de Graduação em Engenharia de Produção EPR/FT/UnB. As ferramentas foram analisadas quanto ao atendimento das necessidades do novo processo definido e suas finalidades foram descritas e ordenadas.

O quinto e último ciclo fez uso dos resultados dos dois últimos ciclos: do novo processo, e da análise de ferramentas, como fonte de dados. Dando seguimento ao trabalho em conjunto com a disciplina de Projeto de Sistemas de Produção 2 (PSP2), foi realizada a especificação dos requisitos para a construção de uma ferramenta para avaliação dos riscos no processo de terceirização de TI do IDP.

O resultado do quinto ciclo compõe o relato descrito no *capítulo 7 – Especificação da ferramenta*, resultado assim no alcance do objetivo geral da pesquisa. É possível observar que cada ciclo está associado à execução de um objetivo específico, com exceção do quarto e quinto ciclos, os últimos, que juntos formam um objetivo específico. Por fim, na Figura 3.6, é realizada uma apresentação geral, associando-se cada objetivo específico, definido com os métodos utilizados para sua realização, a seus respectivos ciclos executados do estudo de caso.

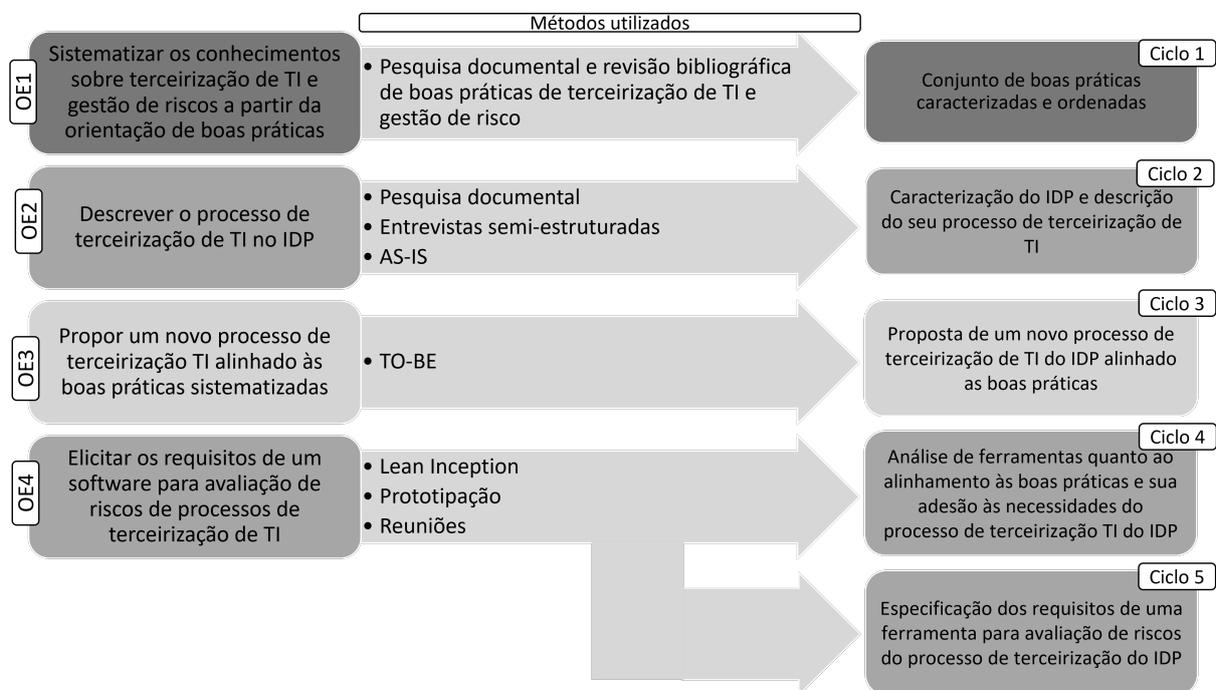


Figura 3.6: Associação dos objetivos específicos com os métodos e ciclos do estudo de caso. Fonte: autora

3.3.4 Prototipação

A prototipação é um recurso utilizado na especificação da ferramenta proposta, portanto faz-se necessário realizar uma descrição prévia dos seus conceitos e entendimentos. A prototipação é uma representação visual do design de um produto que pode ser realizada por meio de um esboço desenhado em um papel, ou até por meio de uma apresentação fiel e executável das telas do produto final [99]. Ela é usada como meio de comunicação entre equipes para validação de definições ou teste de ideias [100], e pode ser categorizada como de baixa fidelidade (o foco maior é na estrutura geral do sistema), de alta fidelidade (o foco é na reprodução fidedigna do sistema), e protótipos funcionais (que utilizam de linguagem de programação para reproduzir a navegação no sistema, ainda sem implementação das regras de negócio) [101].

O uso da prototipação de baixa fidelidade pode apoiar a elicitação de requisitos, pois aumenta a satisfação do usuário final juntamente com uma otimização dos recursos utilizados, pois a criatividade é canalizada para o desenho de uma solução efetiva [102].

Quanto aos seus objetivos, a prototipagem pode ser categorizada como exploratória, cuja função é esclarecer os requisitos dos usuários e da administração com relação ao sistema futuro a partir das ideias iniciais. A prototipação experimental se concentra na implementação técnica dos objetivos do desenvolvimento do sistema. Por fim, a evolutiva, que é usada como uma ferramenta de adaptação do processo de evolução contínuo de adaptação, aproximando ao máximo o protótipo do sistema em questão [103].

Os protótipos também são separados por tipos: protótipo próprio, que descreve um sistema visando a análise dos requisitos. *Breadboard* é focado em ajudar no esclarecimento técnico do sistema e geralmente tem o envolvimento restrito à equipe de desenvolvimento. O último tipo é chamado de sistema piloto e não é usado apenas como um recurso ilustrativo e sim projetado para uso real do sistema [103]. Ao ser definido o objetivo da prototipação e seu tipo, é necessário entender qual é a técnica de construção que melhor se adequa ao contexto que será aplicado. Frequentemente as duas principais abordagens estão relacionadas com o desenvolvimento de software [104].

A primeira é chamada de prototipagem horizontal, em que camadas específicas do sistema são construídas, especificando-se os *layouts* de tela e os diálogos do usuário. A outra abordagem é denominada abordagem vertical, onde é selecionada uma parte do sistema para ser implementada de forma completa [104] [103].

Nesta pesquisa foi utilizado o protótipo de baixa fidelidade, classificado como próprio e exploratório, com uma construção horizontal.

3.4 Fases de análise de dados e relato dos resultados

A fase de análise de dados partiu dos dados coletados em cada ciclo e seu objetivo foi analisar e validar esses dados, conforme apresentado na Figura 3.5. A validação de boas práticas ora selecionadas foi planejada e organizada em uma *tabela* contendo fases, práticas e atividades, devidamente associadas entre si e ordenadas de acordo com pesos extraídos das próprias práticas selecionadas. Isso resultou em insumos para a construção de um processo de terceirização de TI baseado nas boas práticas, e na rastreabilidade de cada um dos seus componentes relacionados a suas referências.

A análise dos dados e a validação da descrição do processo atual do IDP foi realizada a partir de reuniões virtuais, por meio do *Microsoft Teams*, com cada um dos gestores das áreas: de TI, Organização e Método, Financeiro e Acadêmico, ou seja, os gestores das áreas envolvidas no processo de terceirização, de forma individual, visando obter uma percepção de cada área de atuação separadamente, sem interferências das demais.

A reunião teve duração limitada em até 1 hora, tendo como pauta a apresentação do processo AS-IS mapeado, bem como sua descrição. O objetivo foi buscar a validação das atividades e seus resultados, além dos papéis responsáveis por cada atividade. A validação ocorreu por meio da apresentação do processo mapeado de forma detalhada, atividade por atividade. O principal aspecto observado foi a correspondência do processo AS-IS com a realidade observada no momento do mapeamento. Após cada atividade apresentada, o participante da reunião podia concordar com o que foi apresentado ou discordar e, juntamente, propor melhorias ou correções no processo. Correções estas que eram realizadas durante a reunião.

O terceiro ciclo do estudo de caso teve como resultado a proposta de um novo processo de terceirização de TI para o IDP. A validação do estudo ocorreu em reuniões virtuais junto aos gerentes das áreas de TI, Organização e Método, Financeiro e Acadêmico, sendo o último o representante da área demandante.

A representatividade das pessoas selecionadas para a reunião de validação foi de 52% do total de colaboradores envolvidos no processo de terceirização. A duração média da reunião foi de 45 minutos e ocorreu via plataforma *Microsoft Teams*. O roteiro de validação se assemelha ao usado na reunião de validação do processo AS-IS, porém, devido à quantidade de atividades, os pontos de pausa para captação da percepção das pessoas envolvidas na reunião ocorriam a cada análise de processo.

Os participantes verbalmente expressavam se concordavam ou não com o que foi apresentado ou, no caso negativo, apontavam os ajustes necessários. O principal aspecto observado nessa validação foi a viabilidade da execução do processo apresentado no IDP e o atendimento às necessidades de negócios internos da instituição.

A análise e validação da busca por ferramentas existentes, adequadas às boas práticas extraídas, ocorreu pela elaboração de uma tabela comparativa, ordenada por ferramentas que tinham mais funcionalidades e que estavam mais aderentes às boas práticas. Para tanto, foi utilizada a mesma pontuação feita na validação das boas práticas. Assim foi possível verificar quais as ferramentas estavam mais aderentes às boas práticas e o respectivo percentual de aderência.

Por fim, foi realizada uma análise e validação dos requisitos elicitados assim como das telas prototipadas, resultante do último ciclo do estudo de caso. Essa validação ocorreu junto ao IDP e também foi feita por meio de reuniões via plataforma *Microsoft Teams*.

A duração média de cada reunião foi de 45 minutos e contou com a participação dos mesmos colaboradores do IDP que participaram das validações anteriores, assim como dos gerentes das áreas de TI, Organização e Método, Financeiro e um representante da área demandante, nesse caso o representante da área acadêmica, de forma individual.

A reunião foi realizada em dois momentos: inicialmente foi apresentada uma lista de funcionalidades, onde cada uma delas foi descrita. Em seguida, os envolvidos nas reuniões poderiam concordar com as funcionalidades apresentadas, ou sugerir alterações.

No segundo momento da reunião, os participantes foram apresentados a cada uma das telas prototipadas, juntamente com as funcionalidades anteriormente apresentadas, associadas às boas práticas que serviram como referência. Após a apresentação de cada protótipo de tela, o participante poderia concordar ou apontar ajustes a serem feitos.

Tendo em vista que essa validação ocorreu após a apresentação do novo processo proposto, o principal aspecto nela observado foi a percepção da aderência da ferramenta ao processo que será implantado no contexto do IDP. Dessa forma, a coleta de dados foi analisada e validada. Na fase *relato dos resultados*, foi feita a consolidação e organização de todas as informações e resultados de forma resumida, resultando, por fim, na escrita desta dissertação.

3.5 Considerações finais do capítulo

Neste capítulo foi apresentada a metodologia de estudo utilizada no trabalho, a qual teve como principal objetivo contribuir para a avaliação de riscos dos processos de terceirização de TI do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP). Foram descritas e detalhadas as atividades realizadas em cada etapa do plano metodológico proposto, sua estratégia de execução e todos os passos, desde a definição do objetivo da pesquisa, passando pelos procedimentos de coletas de dados, a análise e consolidação dos resultados, os quais serão apresentados nos capítulos seguintes. Em seguida, no *capítulo 4 - Seleção de boas práticas para a terceirização de TI e gestão de riscos* apresentou-se uma

busca, seleção, extração e análise das melhores práticas aplicadas à terceirização de TI e à gestão de riscos, com o objetivo de realizar sua caracterização, pontuação e ordenação por relevância.

Capítulo 4

Seleção de boas práticas para a terceirização de TI e a gestão de riscos

4.1 Considerações iniciais do capítulo

Este capítulo apresenta a execução do primeiro ciclo do estudo de caso, conforme a Figura 4.1. Com isso, foi possível atender o segundo objetivo específico definido "*sistematizar os conhecimentos para a terceirização de TI e gestão de riscos a partir da orientação de melhores práticas*".

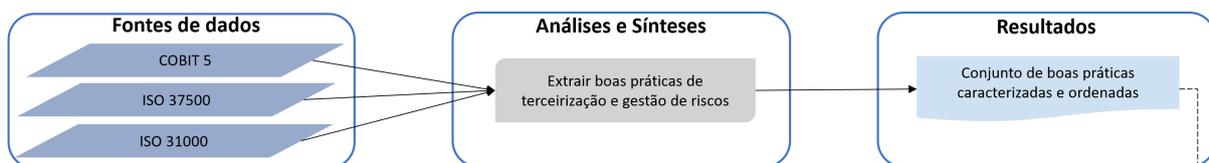


Figura 4.1: Primeiro ciclo do estudo de caso. Fonte: autora

A seleção de boas práticas para a terceirização de TI e gestão de riscos foi feita por meio de pesquisas documentais e revisão bibliográfica, na qual foi realizada uma seleção e descrição sobre as fontes consultadas. Como resultado, tem-se um conjunto de fases, práticas e atividades, devidamente caracterizadas e critérios para ordenação das mesmas.

4.2 Seleção de boas práticas

Tendo em vista o tempo limitado de pesquisa e buscando selecionar normativos e *frameworks* que tenham a maior abrangência em relação a outras boas práticas, foram es-

colhidas 3 fontes, ISO 31000, ISO 37500 e COBIT 5. A escolha da norma ISO 31000 [3] se deu em função dessa norma ser a referência de base quando se trata de boas práticas relacionadas à gestão de riscos. Conforme foi apresentado no *capítulo 2*, as pesquisas relacionadas à gestão de riscos e à gestão de riscos de TI mostram que todas as publicações sobre o tema utilizam da mesma estrutura básica do processo apresentado no normativo.

O COBIT 5 [9] foi selecionado primeiramente por ter uma proposta de *framework*, isso é, uma estrutura abrangente, podendo ser usado como uma estrutura geral. Segundo os documentos do Cobit, um dos seus princípios é ser um modelo único e integrado que busca unificar o diversos padrões de tecnologia como ITIL, CMMI, COSO e algumas normas ISO, conforme é apresentado na Figura 4.2. Cabe destacar o fato de que o COBIT 5 traz em uma de suas publicações uma pontuação baseada no grau em que terceirização, aquisição e gestão de riscos influenciam cada prática descrita.

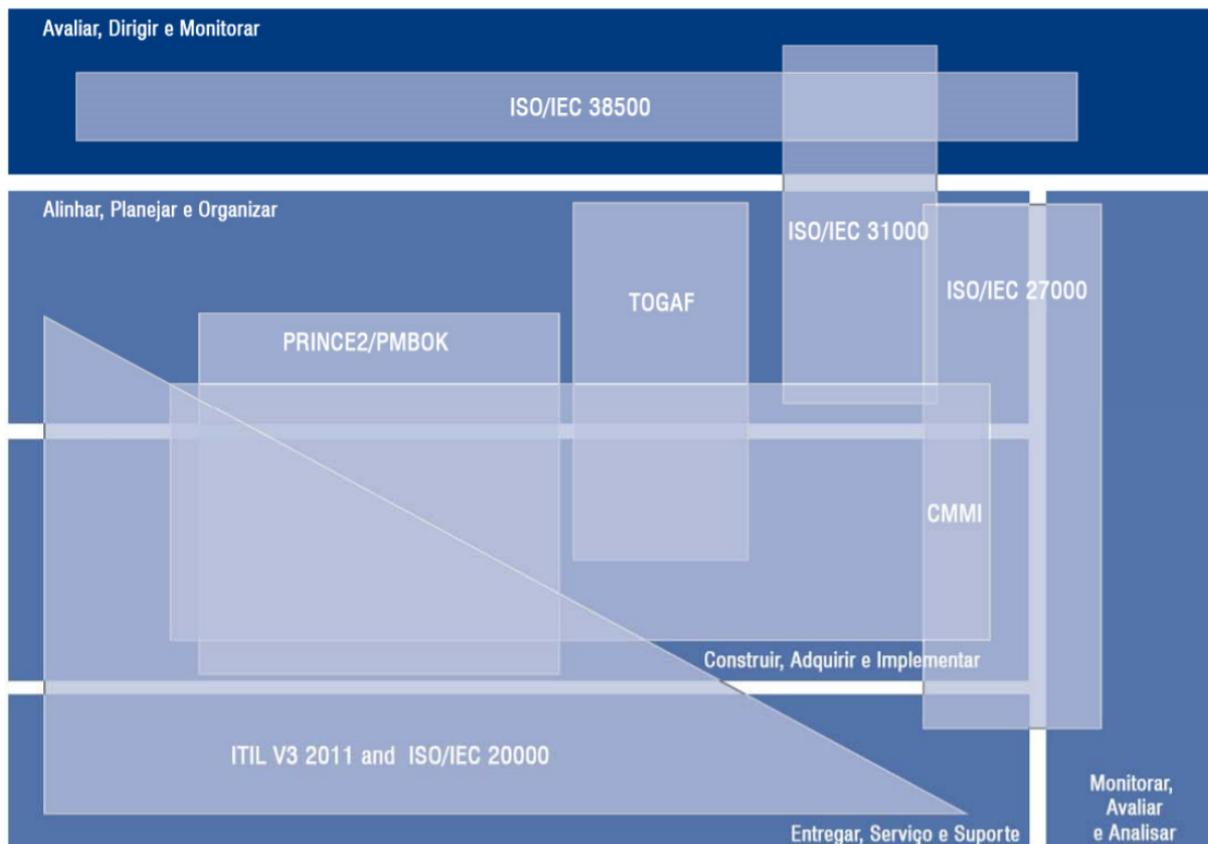


Figura 4.2: Cobertura de outros frameworks no COBIT 5. Fonte: [9]

A ISO 37500 [10], além de ser a norma publicada pela *International Organization for Standardization* (ISO) para ser o guia completo sobre terceirização, assim como o COBIT 5, também abrange outros *frameworks*, conforme apresentado na Figura 4.3.

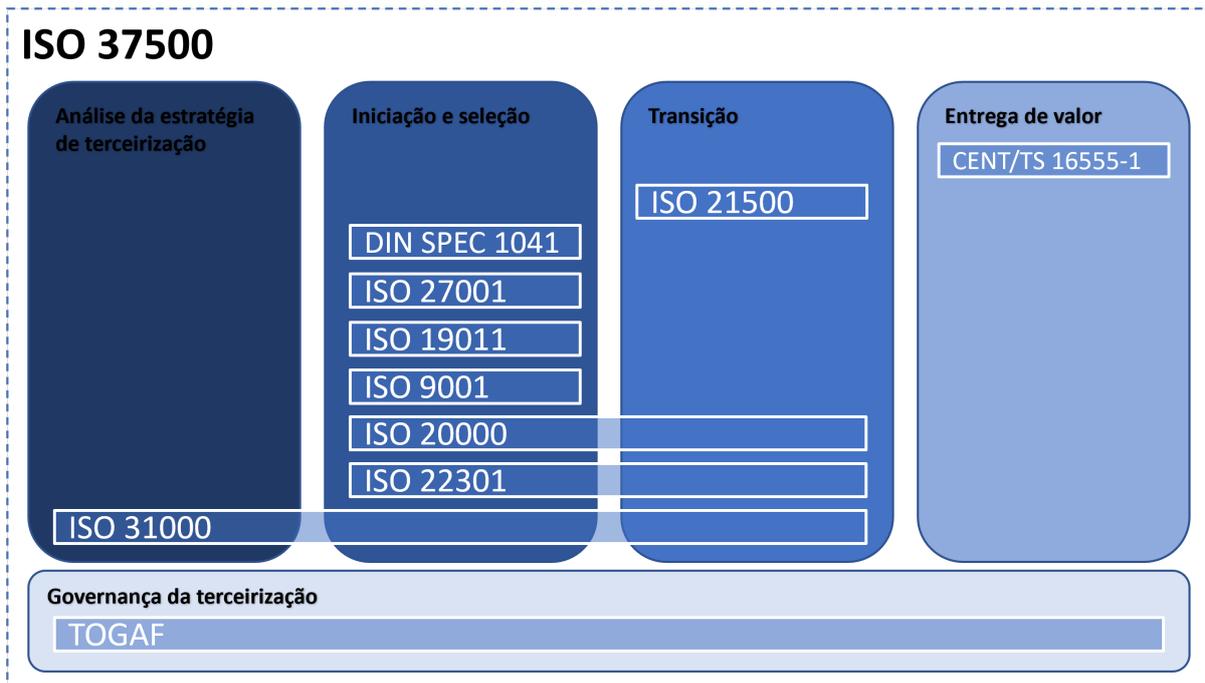


Figura 4.3: Cobertura de outros frameworks pela ISO 37500. Fonte: [10]

Com isso, tem-se um conjunto de boas práticas selecionadas para orientar os próximos passos desta pesquisa. Nas seções a seguir, as práticas selecionadas são apresentadas e descritas, contendo estrutura, processos, fases e atividades relacionadas.

4.2.1 COBIT 5

O *Information Systems Audit and Control Association* (ISACA), em 1994, visando apresentar um conjunto de objetivos para auxiliar a auditoria de TI, publicou o *Control Objectives for Information and Related Technologies* (COBIT). Desde então ele tem evoluído e atualizado de forma incremental para englobar cada vez mais áreas e contemplar outras normas, *frameworks* e guias [105].

Em 2012 ocorreu a última atualização do *framework* Cobit na versão 5, que integrou a versão anterior (4.1) ao Risk IT e os modelos de processo do Val IT 2.0, tornando-se numa ferramenta robusta que unifica os padrões de tecnologia da informação como: ITIL, CMMI, COSO e algumas normas ISO [105].

O COBIT 5 é composto por um Modelo de Referência de Processos, um Guia de implementação do ciclo de vida e uma Cascata de Objetivos. Ele é sustentado por cinco princípios fundamentais [106]:

- Atender às necessidades das partes interessadas;
- Abranger toda a organização;

- Aplicar um modelo único integrado de governança e gestão de TI na organização;
- Permitir uma abordagem holística;
- Distinguir a governança da gestão.

O COBIT 5 apresenta a necessidade de se abordarem questões gerais sobre a TI, como o envolvimento de partes interessadas, dependência de parceiros externos, grande quantidade de informação, ambiente de TI cada vez mais pervasivo, necessidade de orientações sobre tecnologias emergentes, cobrir negócios de ponta a ponta, maior controle sobre as soluções de TI, conexão e alinhamento com importantes padrões e modelos de mercado e a integração de dados.

De forma prescritiva, o COBIT 5 demonstra que cada organização deve organizar seus processos conforme julgar conveniente, contanto que todos os objetivos de governança e gestão necessários sejam cobertos e integrados. A governança avalia, dirige e monitora enquanto que a gestão planeja, constrói, entrega e também monitora.

Este *framework* apresenta um modelo de referência organizando os processos por domínio, resultado da junção do modelo já proposto na versão anterior, 4.1, com o processo do *Risk IT* e *Val IT*, os quais são documentos complementares anteriormente criados.

A Figura 4.4 apresenta um conjunto de 37 processos agrupados em 5 domínios.

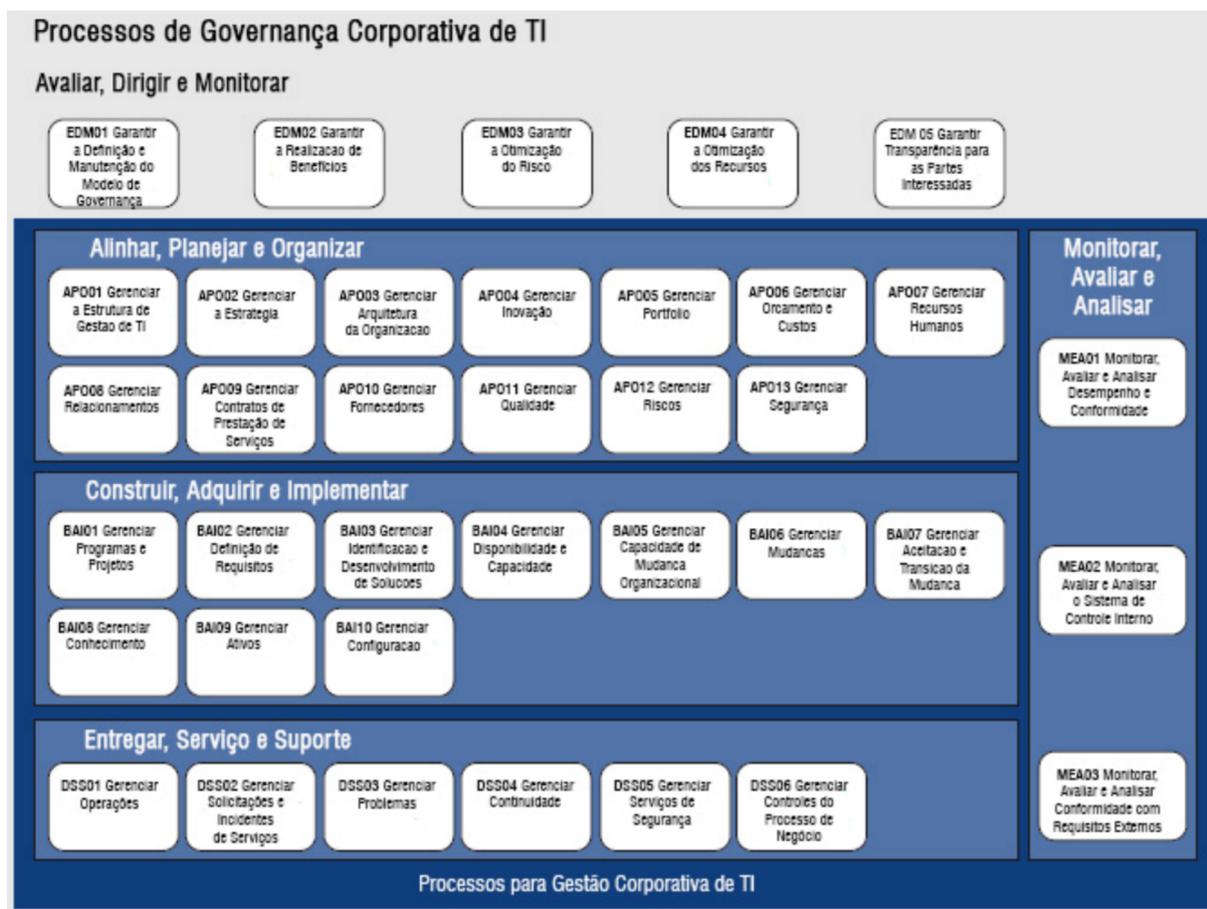


Figura 4.4: : Modelo de Referência de Processo do COBIT 5. Fonte: [9]

O COBIT 5 é uma ferramenta robusta e completa, visando dar uma maior abrangência de informações. Ele é composto por uma família de produtos publicados nas seguintes partes:

- ***COBIT® 2019 Framework: Introduction and Methodology***
 - Introdução e metodologia — detalha os princípios de governança, oferece conceitos e exemplos básicos e lança a construção da estrutura geral, incluindo o COBIT Core Model [9].
- ***COBIT® 2019 Framework: Governance and Management Objectives***
 - Objetivos de gestão e governança - oferece descrição detalhada do COBIT Core Model e seus 40 objetivos de gestão e governança, que são definidos e combinados com o processo relacionado, metas da empresa e práticas de governança e gestão [15].
- ***COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution***

- Guia de design: desenhando uma solução de governança de informação e tecnologia - Oferece informação sobre como fazer para desenhar um sistema de governança sob medida para as organizações [107].
- ***COBIT® 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution***
 - Guia de implementação: implementando e otimizando uma solução de governança de informação e tecnologia - oferece um roteiro para a contínua melhoria da governança [108].

Dentre as publicações listadas acima, vale destacar o "Guia de Design"[107] que apresenta em seu apêndice uma tabela com o mapeamento do grau que cada fator possui, ou seja, os valores dos fatores de design que influenciam na importância de um processo específico. Os pesos usam uma escala de zero (0) a quatro (4): 4 indica a maior influência e 0 indica a ausência de qualquer relacionamento.

Na publicação "Objetivos da Governança e Gestão"[15], cada um dos processos são detalhadamente descritos. São apresentados o domínio associado, descrição, propósito, objetivos associados, sugestão de métricas, descrição das práticas associadas (as fontes de referência de cada uma), atividades que compõem essas práticas, áreas organizacionais envolvidas e suas responsabilidades, insumos, resultados, e outras informações. Com isso é possível ter um material completo de todas as práticas e atividades, bem como a avaliação do grau de cada um com elementos específicos de design.

4.2.2 A norma ISO 37500

A norma ISO 37500 tem como objetivo fornecer uma orientação geral sobre terceirização, incluindo conceitos básicos de terceirização para melhorar a compreensão das partes interessadas, fornecendo um conjunto de práticas que podem ser usadas para gerenciar o ciclo de vida, podendo ser aplicada para qualquer organização em qualquer setor de atuação [10]. Ela parte do princípio de que a organização já estabeleceu uma estratégia de terceirização, ou seja, se inicia quando o caso de negócio foi válido e sua opção viável.

O escopo da norma abarca as principais fases, processos e aspectos da governança da terceirização, visando fornecer uma boa base para realização de acordos bem sucedidos. Sua aplicação não é rígida e pode ser adaptada e estendida às necessidades específicas do contexto em que esteja sendo aplicada, em todos os seus aspectos como leis e regulamentos vigentes, tamanho do acordo, maturidade e tipo do setor. Outro aspecto importante é quanto ao reconhecimento do trabalho integrado de diversas áreas como partes interessa-

das no processo de terceirização, considerando-se que a cada acordo, a responsabilidade das partes do ciclo de vida deve ser interpretada e ajustada.

A norma caracteriza a busca pela terceirização, justificada pela necessidade de se estar continuamente alinhado com as estratégias de negócios, construindo a capacidade de mudanças desde o início do ciclo de vida da terceirização, sendo possível por meio de uma estrutura de governança de terceirização conjunta. Para isto, é apresentado um modelo contextual de terceirização, ilustrado na Figura 4.5 a seguir:

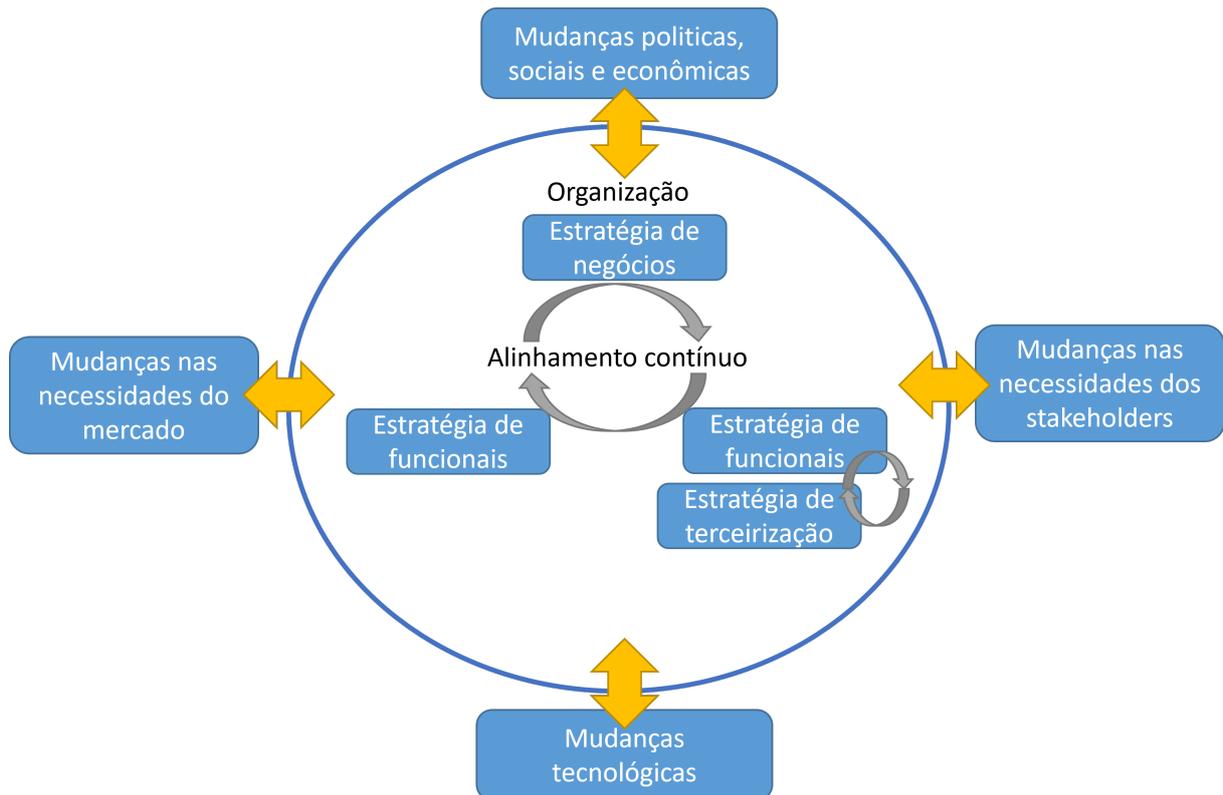


Figura 4.5: Modelo contextual de terceirização. Fonte: [10]

Visando auxiliar na procura para obter valor agregado durante a identificação e tratamento dos riscos, a norma fornece um processo de alto nível para terceirização. Nele é abordado o ciclo de vida da terceirização, os processos conjuntos (cliente e fornecedor), flexibilidade para mudanças, formas de garantir a entrega de valor e relacionamento colaborativo entre as partes.

A Figura 4.6 a seguir apresenta o macroprocesso do ciclo de vida da terceirização, destacando as funções de monitorar, avaliar e direcionar continuamente todas as fases do ciclo de vida da terceirização, que podem ser adaptados para atender os requisitos de acordo com cada tipo de terceirização.



Figura 4.6: Ciclo de vida da terceirização. Fonte: [10]

A Governança da terceirização está no centro do modelo e tem como finalidade ser um capacitador para liderança estratégica eficaz. O ciclo de vida envolve o desenvolvimento do processo, reunindo um nível apropriado de gestão do cliente e do fornecedor, realizando o trabalho de forma conjunta e contínua.

As atividades relacionadas a esta fase estão presentes em todas as demais fases com o intuito de monitorar, avaliar e direcionar o ciclo de vida da terceirização.

A segunda fase denominada "Análise da estratégia de terceirização" tem o foco predominante no cliente e visa iniciar e avaliar as oportunidades de terceirização, bem como manter um alinhamento entre elas e os objetivos e requisitos do negócio. Somente após essa fase a empresa poderá avaliar o real valor que a terceirização pode trazer para seu negócio. Nesta fase será decidido se a contratação da terceirização continuará ou será cancelada. As principais atividades dessa fase são listadas a seguir.

- Verificar os pré-requisitos da terceirização;
- Compreender os serviços elegíveis para terceirização;
- Avaliar o impacto organizacional da terceirização de serviços;
- Definir estratégia de terceirização;
- Desenvolver business case(s) inicial(is) para terceirização;
- Avaliar e decidir;
- Montar o projeto de terceirização.

O objetivo da próxima fase, denominada "Iniciação e seleção", onde todos os requisitos que envolvem a terceirização são identificados e descritos da forma mais completa. É nesta fase em que é selecionado o fornecedor, com a assinatura dos acordos e ciência e aprovação da alta gestão. Suas atividades são listadas a seguir.

- Detalhar os serviços necessários;
- Detalhar do modelo de terceirização;
- Definir os requisitos e estrutura do contrato;
- Identificar provedores potenciais;
- Fornecedores da lista restrita;
- Contratos básicos;
- Negociar e estabelecer acordos.

"Transição" é o nome da terceira fase que tem como foco o cuidado do estabelecimento de recursos para que o fornecedor possa entregar o acordado da melhor forma. Ela pode incluir a transferência de ativos, procedimentos, pessoas e quaisquer outras questões que envolvem a contratação.

Por meio do trabalho em conjunto do cliente e o fornecedor é realizado um projeto piloto, possibilitando o cumprimento das responsabilidades de prestação de serviço com qualidade e desempenho necessários. A seguir, a lista de suas atividades:

- Estabelecer a equipe do projeto de transição;
- Estabelecer governança de terceirização;
- Refinar a estrutura de entrega e o plano de transição;
- Refinar a aquisição de conhecimento;
- Realizar a transição de conhecimentos, pessoas, processos e tecnologia;
- Implantar as estruturas de qualidade, risco, auditoria e conformidade;
- Implantar a estrutura de gerenciamento de ativos e conhecimento;
- Implantar estruturas de tipo de entrega;
- Testar a capacidade de entrega do serviço;
- Piloto e transferência.

A última fase é denominada "Entrega de valor", e tem como principal objetivo garantir que a terceirização está sustentando o valor do acordo realizado. As atividades do cliente são voltadas para o monitoramento do fornecedor. Ela termina com a preparação para uma análise e avaliação dos resultados da terceirização, visando auxiliar na decisão de renová-la ou finalizá-la. São listadas a seguir as atividades da fase:

- Prestar serviço;
- Monitorar e revisar o desempenho do serviço;
- Gerenciar e resolver problemas;
- Entregar e gerenciar mudanças;
- Entregar inovação (opcional);
- Entregar transformação (opcional);
- Administrar as finanças;
- Gerenciar relacionamentos;
- Gerir o contrato;
- Garantia de valor e business case;
- Continuação ou término da preparação do contrato.

No normativo, todas as atividades são descritas, seus objetivos destacados, os pontos para realização bem sucedida são apresentados, suas fontes de referências citadas e por fim todos os insumos e resultados são apresentados. Após a explicação minuciosa de todas as atividades de todas as fases, o documento apresenta um conjunto de anexos que visam complementar as orientações apresentadas, materiais como exemplos de estruturas, listas, templates e processos complementares.

4.2.3 A norma ISO 31000

A ISO 31000 [3] é um documento basilar da família de normas de gestão de riscos, criada pela *International Organization for Standardization* (ISO). Ela apresenta os princípios, estrutura e processo de gestão de riscos, os quais servem como diretrizes para a gestão de riscos, considerando contextos externo e interno, visando a melhoria do sistema de gestão. A aplicação de suas diretrizes não tem limitações de contexto ou organização, oferecendo uma abordagem geral para qualquer indústria e setor, abordando qualquer tipo de risco, podendo ser utilizado em qualquer atividade da organização.

No que se refere aos princípios, a norma os utiliza como base da gestão de riscos da organização possibilitando o gerenciamento eficaz e eficiente das incertezas de seus objetivos, deixando claro sua intenção, propósito e seu valor. É apresentada a seguir a Tabela 4.1 consolidada dos princípios contidos na norma e suas respectivas explicações:

Tabela 4.1: Princípios ISO 31000. Fonte: [3]

Princípio	Explicação
Integrada	Parte integrante de todas as atividades organizacionais.
Estruturada e abrangente	Para resultados consistentes e comparáveis é necessária a utilização de uma abordagem estruturada e abrangente.
Personalizada	A estrutura do processo de gestão de risco é única e proporcional para cada contexto organizacional, seja ele interno ou externo.
Inclusiva	A gestão de riscos necessita ser inclusiva, possibilitando a ponderação de diferentes conhecimentos, pontos de vistas e percepções, o que resulta em uma maior conscientização fundamentada.
Dinâmica	Os riscos devem refletir os contextos, internos e externos de uma organização, e conseqüentemente acompanhar suas mudanças de maneira apropriada e oportuna.
Melhor informação disponível	A gestão de riscos se utiliza de informações oportunas, claras e disponíveis de bases históricas, atuais e expectativas futuras, além de considerar limitações e incertezas associadas.
Fatores humanos e culturais	Os fatores humanos e culturais impactam diretamente em todo e qualquer aspecto da gestão de riscos, independentemente do nível e estágio.
Melhoria contínua	A melhoria contínua deve estar presente na gestão de riscos, possibilitando seu aperfeiçoamento por meio de aprendizados e experiências.

Após definir e explicar os princípios, o documento apresenta a estrutura de gestão de riscos, que tem como propósito o apoio na integração entre as atividades e funções da organização com a gestão de riscos. O apoio das partes interessadas, principalmente da alta gestão, em todas as atividades, inclusive na tomada de decisão é fator crítico de sucesso na eficácia da gestão de riscos. Convém que os componentes da estrutura e seu modo de funcionamento sejam específicos para a necessidade da organização e aborde as lacunas resultantes de avaliações de práticas e processos já existentes.

O normativo primeiramente apresenta a estrutura de liderança e comprometimento, diretamente relacionada à alta gestão e órgãos de supervisão, os quais devem demonstrar liderança e comprometimento em suas ações. É claramente separado o papel da alta

gestão, a qual é responsável por gerenciar os riscos, e os órgãos de supervisão, os quais monitoram a gestão de riscos em aspectos específicos.

A supervisão consiste na compreensão dos riscos associados à busca dos objetivos da organização e conseqüentemente em assegurar o alinhamento dos riscos com os objetivos estratégicos da organização, bem como a operabilidade e implantação eficaz dos sistemas de gestão de riscos, além da comunicação apropriada sobre informações associadas aos riscos e sua gestão. Nela são definidas ações e apresentados os resultados esperados, conforme informações consolidadas na Figura 4.7 apresentada a seguir.

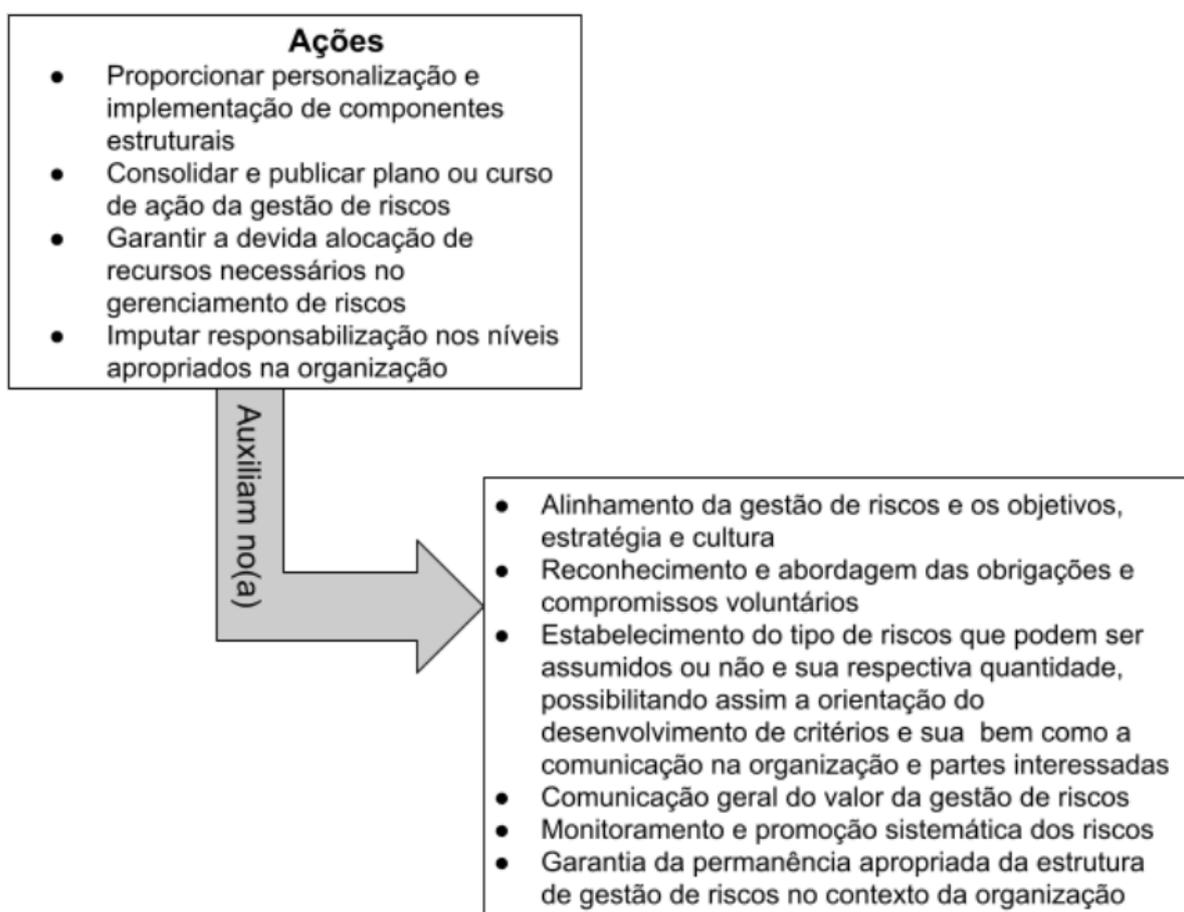


Figura 4.7: Ações definidas e resultados esperados da gestão de riscos. Fonte: [3]

A integração dinamiza a gestão de riscos, garantindo que não seja apenas uma parte separada da organização e que esteja alinhada com o propósito da organização, sua governança, liderança e comprometimento, estratégia e operações.

Para a concepção da estrutura de gestão de riscos, é necessário inicialmente entender toda a organização e seu contexto, incluindo os seus fatores relacionados, direcionadores e tendências que possam afetar a organização, relacionamentos e necessidades, internas e externas e sua complexidade e dependência. Isso se faz ao se examinar internamente a

organização, definições, estratégias, políticas, objetivos, cultura, normas, modelos, diretrizes, capacidades, dados relações e interdependências devem ser consideradas.

Como já apresentado anteriormente, o comprometimento contínuo com a gestão de riscos, reforçado por meio de formas claras de comunicação de objetivos, é fator crucial de sucesso, portanto sua articulação é necessária. Visando uma gestão de riscos coordenada, é necessária a atribuição de papéis, responsabilidades e responsabilizações para indivíduos ou unidades que possuam autoridade ou responsabilidade sobre os riscos. Cabe à alta gestão e aos órgãos de supervisão a alocação de recursos, considerando pessoas, habilidades, experiências e competências, associadas a processos, métodos e ferramentas utilizadas na gestão de riscos da organização, sua documentação, a gestão de conhecimento e treinamento.

Uma vez feita a preparação inicial, a organização estará apta a implementar a estrutura de gestão de riscos a partir dos passos apresentados na Figura 4.8 a seguir:

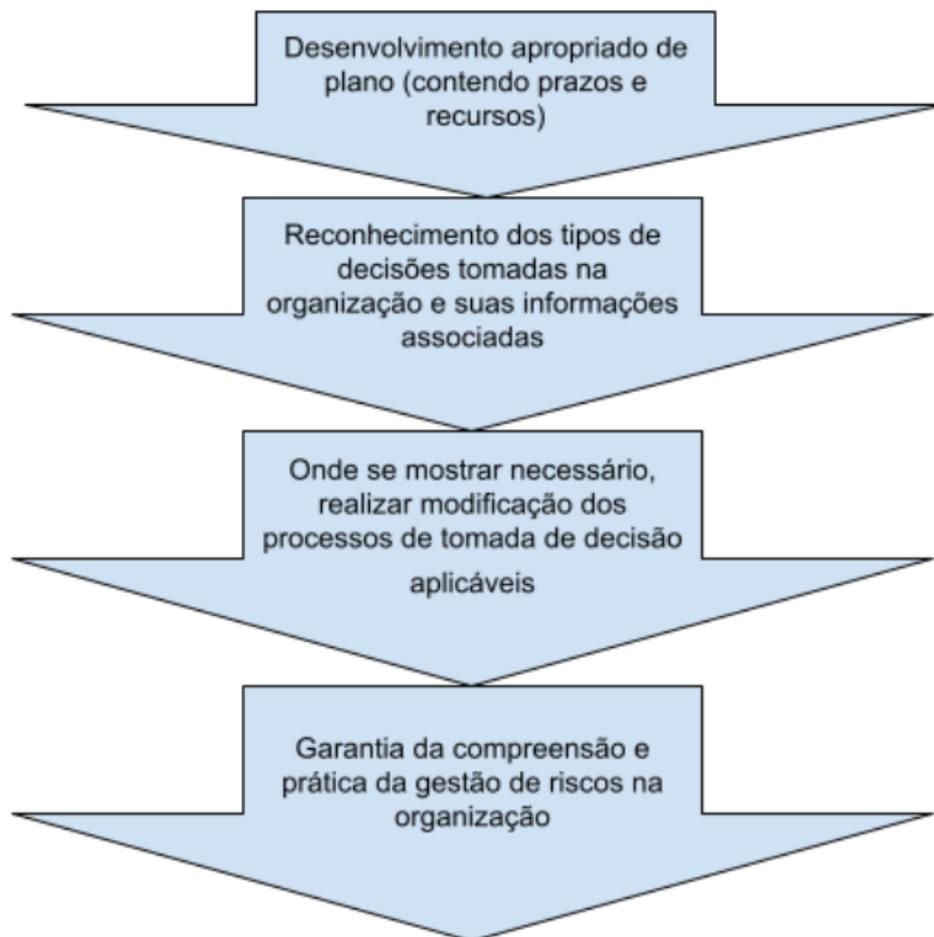


Figura 4.8: Passos para implementação da estrutura de gestão de riscos. Fonte: [3]

A constante avaliação da eficácia da estrutura implementada consiste na mensuração periódica de seu desempenho, e na validação da sua adequação aos objetivos da organi-

zação. Esta ação é de suma importância para o monitoramento e adaptação da estrutura de gestão de riscos, visando a melhoria contínua, à medida que lacunas e oportunidades são identificadas.

Após a explicação da estrutura da gestão de riscos, o normativo apresenta o processo de gestão de riscos, conforme Figura 4.9 a seguir.

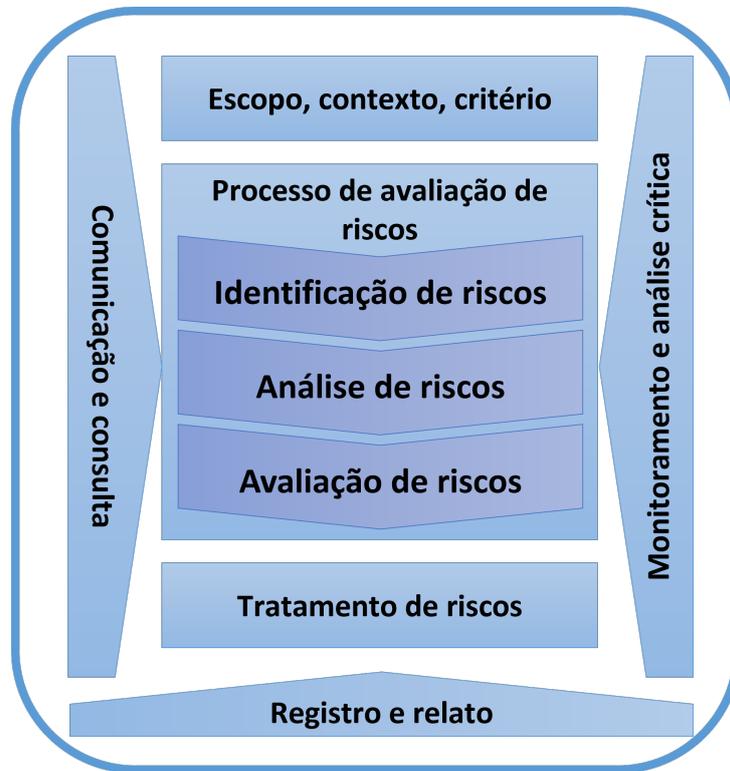


Figura 4.9: Processo de gestão de riscos. Fonte: [3]

Vale destacar que o processo tem várias aplicações na organização, e apesar de ser mostrado de forma sequenciada, na prática deve ser utilizado de forma iterativa. São apresentadas a seguir, de forma sucinta, cada uma das atividades presentes no processo de gestão de riscos.

- Comunicação e consulta
 - Atividade associada à comunicação do risco, reunindo áreas envolvidas no processo de gestão de riscos para assegurar e fornecer informações para facilitar o entendimento dos riscos e apoiar a tomada de decisões, visando incluir as partes envolvidas e as pessoas afetados pelo risco.
- Escopo, contexto e critérios
 - A necessidade de definição do escopo e delimitação do contexto, interno e externo, se dá pois a gestão de riscos pode ser aplicada em diferentes níveis,

e é importante a clareza sobre os objetivos pertinentes que devem ser considerados. Está associada a essa atividade a definição dos critérios de riscos, definindo quantidade e tipo de riscos que podem assumir, ou não, e sua respectiva avaliação da sua significância.

- Processo de avaliação de riscos
 - Identificação dos riscos
 - * A identificação dos riscos é a primeira atividade do processo de avaliação de riscos e consiste em encontrar, reconhecer e descrever os riscos (sejam eles oportunidades ou impedimentos no alcance dos objetivos da organização).
 - Análise de riscos
 - * Depois que é feita a identificação de riscos, é necessário compreender a natureza, características, fontes, consequências, e todos os demais aspectos que tangem o risco. O grau de detalhamento e complexidade dependerá do propósito da análise, da disponibilidade e confiabilidade da informação.
 - Avaliação de riscos
 - * Por fim a avaliação de riscos deve apoiar as decisões, comparando resultados da análise e gerando insumos para a decisão de como se agir frente ao risco, desde a aceitação do risco até a reconsideração dos objetivos da organização.
- Tratamento de riscos
 - Essa atividade se inicia com o levantamento de opções de tratamento de riscos, balanceando os benefícios, custos, esforços, vantagens e desvantagens. O tratamento pode gerar outros riscos que devem ser gerenciados e caso não haja opções de tratamento disponíveis, convém o registro e acompanhamento do risco. A preparação do plano de tratamento de riscos deverá identificar claramente a ordem de tratamento. Sua implementação deve ser integrada aos planos e processos de gestão da organização.
- Monitoramento e análise crítica
 - No monitoramento e análise crítica se assegura a melhoria da qualidade e eficácia da concepção, implementação e conseqüentemente o resultado do processo. Essa atividade deve estar presente em todos os estágios do processo, e seus resultados incorporados nas atividades de gestão de desempenho.
- Registro e relato

- Todo processo de gestão de risco deverá ser devidamente documentado, com isso tem-se a viabilização da comunicação das atividades e os resultados na organização, gerando informações para a tomada de decisão, a melhoria nas atividades de gestão de riscos e na interação com partes interessadas, resultando por fim na melhoria da qualidade do diálogo das partes interessadas, apoiando a alta gestão e os órgãos de supervisão cumprindo suas respectivas responsabilidades.

4.3 Análise de boas práticas e respectivas atividades

Partindo do escopo definido, primeiramente foi realizado um estudo aprofundado do COBIT 5, versão 2019, especificamente de seus domínios, as respectivas práticas e atividades que os compõem. Foi feita a análise da descrição, finalidade e demais informações pertencentes aos processos, selecionando-se aquelas que apresentavam relação com a terceirização de TI.

Inicialmente cada prática do COBIT foi analisada individualmente, seu domínio associado, sua descrição e atividades, possibilitando assim uma seleção daquelas que apresentam relação com o contexto estudado. Para isto foi utilizado o livro do Guia de Design [107], onde foram selecionados os fatores de design relacionados com terceirização, aquisição e gestão de riscos. Foram selecionados os seguintes fatores:

- **Mapeamento de estratégias empresariais na aquisição e crescimento:** fatores que influenciam o sucesso no uso da TI com foco na aquisição e crescimento.
- **Mapeamento da Terceirização:** classificação do modelo de uso da TI, focado nos serviços de terceiros para disponibilização de serviços de TI.
- **Maturidade:** Capacidade do processo baseado no *Capability Maturity Model Integration* (CMMI), o qual opera em níveis de capacidade variando de 0 (ausência de qualquer capacidade básica) até 5 (atinge o objetivo, foco na melhoria contínua). Portanto o nível reflete quão bem um processo é implementado e executado.
- **Gestão de riscos:** perfil de risco da empresa no que tange à TI, dividido nas seguintes áreas:
 - Tomada de decisão de investimento em TI, definição e manutenção de portfólio
 - Gerenciamento de ciclo de vida de programas e projetos
 - Custo e supervisão de TI
 - Experiência, habilidades e comportamento de TI

- Arquitetura empresarial / TI
- Incidentes de infraestrutura operacional de TI
- Ações não autorizadas
- Problemas de adoção / uso de software
- Incidentes de hardware
- Falhas de software
- Ataques lógicos (*hacking, malware, etc.*)
- Incidentes de terceiros / fornecedores
- Não conformidade
- Questões geopolíticas
- Ação industrial
- Atos da natureza
- Inovação baseada em tecnologia
- Ambiental
- Gerenciamento de dados e informações

Uma vez feita a seleção dos fatores e verificada a atribuição do grau de relevância para cada fator de design, somado para cada prática, o resultado gerou a atribuição de um peso por prática. Com o peso foi possível definir uma ordenação das práticas, iniciando-se pela prática que apresenta maior influência até a menor, consolidadas na Tabela 4.3:

Tabela 4.2: Práticas do COBIT 5 [15] ordenadas por peso

Referência Prática	Prática	Peso terceirização	Peso riscos	Peso total
APO10.01	Identifique e avalie relacionamentos e contratos com fornecedores	5	24	29
APO10.02	Selecione fornecedores	5	24	29
APO10.03	Gerenciar relacionamentos e contratos com fornecedores	5	24	29
APO10.04	Gerenciar o risco do fornecedor	5	24	29
APO10.05	Monitore o desempenho e a conformidade do fornecedor	5	24	29

Tabela 4.2 – Continuação das Práticas do COBIT 5 [15] ordenadas por peso

Referência Prática	Prática	Peso terceirização	Peso riscos	Peso total
MEA02.01	Monitore os controles internos	2	27	29
DSS04.01	Definir a política de continuidade de negócios, objetivos e escopo	2	24	26
DSS04.03	Desenvolva e implemente uma resposta de continuidade de negócios	2	24	26
APO03.01	Desenvolva a visão da arquitetura corporativa	5	19	24
EDM05.01	Avalie o envolvimento das partes interessadas e os requisitos de relatórios	2,5	21	23,5
APO02.02	Avalie as capacidades atuais, desempenho e maturidade da empresa	4,5	16	20,5
APO06.01	Gerenciar finanças e contabilidade	2,5	17	19,5
APO09.01	Identifique os serviços de TI	5	13	18
APO09.04	Monitore e relate os níveis de serviço	5	13	18
APO09.05	Revise os acordos e contratos de serviço	5	13	18
EDM02.01	Estabeleça o mix de investimento alvo	2,5	15	17,5
DSS01.02	Gerenciar serviços terceirizados de TI	2	15	17
BAI02.01	Definir e manter o negócio funcional e técnico requisitos	2	13	15
BAI02.02	Realizar um estudo de viabilidade e formular soluções alternativas	2	13	15
BAI02.04	Obtenha a aprovação de requisitos e soluções	2	13	15
BAI03.04	Adquira componentes da solução	2	13	15
BAI03.05	Soluções de construção	2	13	15
BAI03.09	Gerenciar mudanças nos requisitos	2	13	15
BAI01.03	Gerenciar o engajamento das partes interessadas	5	9	14
BAI01.04	Desenvolver e manter o plano do programa	5	9	14
BAI01.05	Inicie e execute o programa	5	9	14
BAI01.06	Monitorar, controlar e relatar os resultados do programa	5	9	14
BAI01.09	Fechar um programa	5	9	14
APO04.01	Crie um ambiente propício à inovação	2	5	7

Tabela 4.2 – *Continuação das Práticas do COBIT 5 [15] ordenadas por peso*

Referência Prática	Prática	Peso terceirização	Peso riscos	Peso total
APO04.02	Mantenha uma compreensão do ambiente corporativo	2	5	7
APO04.03	Monitore e analise o ambiente de tecnologia	2	5	7

Em seguida, todas as atividades relacionadas às práticas foram refinadas, visando a união de atividades semelhantes, buscando eliminar ações redundantes, e principalmente definir um nível de aplicação no processo, resultando em um conjunto de atividades descritas, listadas e associadas com as práticas. Este resultado pode ser observado no *anexo I*.

Em seguida a norma ISO 37500 foi analisada, da qual foram extraídas as fases do ciclo de vida da terceirização e suas atividades relacionadas, que foram refinadas, resultando em uma lista de atividades por fase. Esta lista também pode ser observada no *anexo I*.

O último normativo a ser integrado a este trabalho foi a ISO 31000. Foi realizada uma abordagem diferente, pois conforme é apresentado na Figura 4.2 e na Figura 4.3, este normativo já encontra-se contemplado nas duas referências anteriores. Portanto, o trabalho realizado foi no sentido da identificação do processo de gestão de riscos nas atividades extraídas e refinadas.

Com todas as fases, práticas e atividades extraídas e refinadas, o próximo passo foi realizar a unificação das boas práticas. Tendo em vista que do COBIT 5 foram retiradas as práticas e o seu peso, o resultado da sua extração e refinamento serviu como base para a classificação das demais práticas. A junção foi realizada e como resultado foi possível, a partir das referências do COBIT 5, ISO 37500 e ISO 31000, obter um documento consolidado com todas as fases, práticas e atividades extraídas das boas práticas, sua descrição detalhada, bem como as referências de cada uma delas, apresentadas no *anexo I*.

Tendo em vista que as práticas foram pontuadas e ordenadas de acordo com os critérios do COBIT 5, conforme apresentado na Tabela 4.3, e todas as demais referências das boas práticas foram unificadas em uma estrutura única, conforme Tabela I, foi possível distribuir os pesos nas fases e atividades respectivas.

Antes de realizar a atribuição de peso foi necessário fazer um balanceamento, uma vez que cada prática pode estar associada a uma ou mais atividades. Para equalizar os

valores e o peso de cada prática, eles foram divididos pela quantidade de vezes que em ela era referenciada nas atividades, e este número gerou a média individual por prática. O resultado é a Tabela 4.3 onde é utilizado como referência das práticas as siglas utilizadas pelo próprio COBIT 5.

Tabela 4.3: Peso médio da prática por repetição de referência

Referência Prática	Quantidade de vezes que a prática foi referenciada	Peso total	Peso médio por repetições
APO02.02	1	20,5	20,5
APO03.01	2	24,0	12,0
APO04.01	1	7,0	7,0
APO04.02	2	7,0	3,5
APO04.03	1	7,0	7,0
APO06.01	1	19,5	19,5
APO09.01	2	18,0	9,0
APO09.04	2	18,0	9,0
APO09.05	1	18,0	18,0
APO10.01	1	29,0	29,0
APO10.02	6	29,0	4,8
APO10.03	3	29,0	9,7
APO10.04	2	29,0	14,5
APO10.05	2	29,0	14,5
BAI01.03	1	14,0	14,0
BAI01.04	3	14,0	4,7
BAI01.05	2	14,0	7,0
BAI01.06	1	14,0	14,0
BAI01.09	2	14,0	7,0
BAI02.01	3	15,0	5,0
BAI02.02	9	15,0	1,7
BAI02.04	1	15,0	15,0
BAI03.04	2	15,0	7,5
BAI03.05	2	15,0	7,5
BAI03.09	1	15,0	15,0
DSS01.02	2	17,0	8,5

Tabela 4.3 – *Peso médio da prática por repetição de referência*

Referência Prática	Quantidade de vezes que a prática foi referenciada	Peso total	Peso médio por repetições
DSS04.01	3	26,0	8,7
DSS04.03	1	26,0	26,0
EDM02.01	2	17,5	8,8
EDM05.01	1	23,5	23,5

Com o valor do peso médio das práticas por repetição foi possível mensurar o peso de cada fase, apresentado no *anexo I*, e conseqüentemente de cada atividade. Como insumo final é apresentada uma estrutura que apresenta um compilado das boas práticas de gestão de riscos e terceirização de TI composta por fases, práticas e atividades, respectivamente com seus pesos atribuídos e referências do COBIT 5, ISO 31000 e ISO 37500, apresentado na Tabela 4.3.

Tabela 4.4: Compilação das boas práticas de gestão de riscos e terceirização de TI

Fase (ISO 37500)	Prática (COBIT 5)	Atividade (31000 + 37500 + COBIT)	Peso
Análise de estratégia de terceirização	Avalie as capacidades atuais, desempenho e maturidade da empresa	verificar os pré-requisitos da terceirização	44,8
	Definir a política de continuidade de negócios, objetivos e escopo	Identificar serviços impactados	17,4
		Avaliar o impacto organizacional da terceirização	8,7
		Definir estratégia de terceirização	8,7
	Identifique os serviços de TI	Consultar catálogo base de TI	9,0
	Gerenciar o engajamento das partes interessadas	Gerenciar partes interessadas	49,5

Tabela 4.4 – Continuação do compilado das boas práticas de gestão de riscos e terceirização de TI

Fase (ISO 37500)	Prática (COBIT 5)	Atividade (31000 + 37500 + COBIT)	Peso
	Desenvolver e manter o plano do programa	Descrever contexto de riscos, prazos e custos da solicitação	4,7
		Deliberar sobre a realização da terceirização	4,7
		Montar projeto base de terceirização	4,7
Iniciação e Seleção	Definir e manter o negócio funcional e técnico requisitados	Detalhar os serviços necessários	5,0
		Definir os requisitos e estrutura do contrato	5,0
	Identifique e avalie relacionamentos e contratos com fornecedores	Identificar provedores potenciais	29,0
	Selecione fornecedores	Solicitar propostas	4,8
		Analisar e ordenar as propostas recebidas	4,8
		Obter aconselhamento jurídico	4,8
	Adquira componentes da solução	Estabelecer acordos	7,5
	Selecione fornecedores	Selecionar provedor	21,5
		Realizar avaliação dos riscos	19,3
		Assinar o contrato	4,8
Transição	Gerenciar relacionamentos e contratos com fornecedores	Estabelecer a equipe do projeto de transição	9,7
	Gerenciar o risco do fornecedor	Monitorar riscos durante a implantação	14,5

Tabela 4.4 – Continuação do compilado das boas práticas de gestão de riscos e terceirização de TI

Fase (ISO 37500)	Prática (COBIT 5)	Atividade (31000 + 37500 + COBIT)	Peso
	Desenvolva e implemente uma resposta de continuidade de negócios	Avaliar plano de continuidade dos fornecedores	26,0
	Realizar um estudo de viabilidade e formular soluções alternativas	Estabelecer governança de terceirização	1,7
		Refinar a estrutura de entrega e o plano de transição	1,7
		Refinar a aquisição de conhecimento	1,7
		Realizar a transição de conhecimentos, pessoas, processos e tecnologia	1,7
		Implantar as estruturas de qualidade, risco, auditoria e conformidade	1,7
		Implantar a estrutura de gerenciamento de ativos e conhecimento	1,7
		Implantar estruturas de tipo de entrega	1,7
		Finalizar transferência	1,7
Entrega de valor	Inicie e execute o programa	Iniciar terceirização	7,0
	Soluções de construção	Configurar ferramenta/serviço	7,5
		Realizar treinamentos necessários	7,5
	Definir e manter o negócio funcional e técnico requisitos	Gerenciar escopo da terceirização	5,0
	Monitore e relate os níveis de serviço	Monitorar a terceirização	27,0

Tabela 4.4 – Continuação do compilado das boas práticas de gestão de riscos e terceirização de TI

Fase (ISO 37500)	Prática (COBIT 5)	Atividade (31000 + 37500 + COBIT)	Peso
		Gerenciar e resolver problemas	9,0
	Monitore o desempenho e a conformidade do fornecedor	Monitorar e revisar o desempenho da terceirização	21,5
	Gerenciar serviços terceirizados de TI	Gerir o contrato	8,5
		Analisar terceirização	14,5
		Documentar informações sobre a terceirização	8,5
	Adquira componentes da solução	Gerenciar recursos de TI durante a terceirização	21,5
	Gerenciar mudanças nos requisitos	Gerenciar mudanças	15,0
	Gerenciar relacionamentos e contratos com fornecedores	Definir funções e responsabilidades	9,7
		Alinhar expectativas	9,7
	Gerenciar finanças e contabilidade	Administrar custos da terceirização	19,5
	Crie um ambiente propício à inovação	Incentivar inovações	26,5
	Fechar um programa	Analisar renovação da terceirização	7,0
		Finalizar terceirização	7,0

4.4 Validação da extração das práticas

A tabela final ora apresentada consolida os insumos necessários para a construção de um processo de terceirização de TI alinhado às boas práticas e à gestão de riscos. É apresentado também o grau de importância de cada atividade para o processo, definida

de forma quantitativa por meio dos pesos atribuídos. Esta classificação se torna relevante para o processo pois apresenta quantitativamente o impacto de cada atividade para o processo como um todo. Por fim o último aspecto relevante da tabela é a indicação das referências, associando cada atividade à fonte da qual foi retirada, possibilitando uma rastreabilidade dos componentes apresentados na tabela.

4.5 Considerações finais do capítulo

Após a seleção das boas práticas, levando em consideração a busca de uma maior abrangência, foi realizada a extração das informações, e posteriormente sua análise, unificação e ordenação, resultando no atendimento do primeiro objetivo específico proposto no trabalho.

No *capítulo 5 – Descrição do processo de terceirização de TI no IDP*, apresenta-se a caracterização do objeto estudado, bem como sua história, estrutura, focando no processo de terceirização de TI existente.

Capítulo 5

Descrição do processo de terceirização de TI no IDP

5.1 Considerações Iniciais do Capítulo

Neste capítulo apresenta-se a execução do segundo ciclo do estudo de caso, isto é, o diagnóstico do processo de terceirização do IDP, conforme a Figura 5.1. Este capítulo apresenta o segundo objetivo específico definido "*Descrever o processo de terceirização de TI no IDP*".

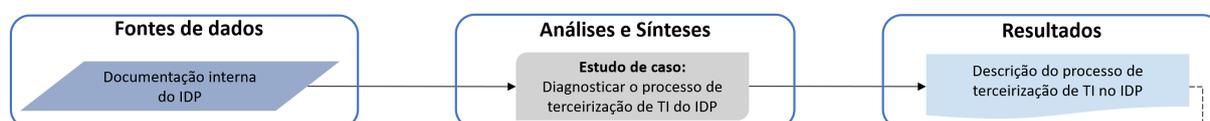


Figura 5.1: Segundo ciclo do estudo de caso. Fonte: Autora

A partir da pesquisa documental sobre o Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP), foi gerado um breve histórico das informações sobre a instituição, além do levantamento da cadeia de valor e a realização do mapeamento do processo existente (*AS-IS*), fazendo uso do *Business Process Management* (BPM) [6]. Como resultados, tem-se a caracterização atual da TI e o mapeamento do processo de terceirização do IDP atual.

5.2 História da instituição

O Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP) é uma Instituição de Ensino Superior (IES) de natureza privada, com fins lucrativos, cuja sede está localizada em Brasília. Idealizado em 1990 e fundada em 1998, originalmente era denominado

Instituto Brasiliense de Direito Público e tinha como oferta cursos de extensão que se iniciaram com o curso de Hermenêutica Constitucional e Direitos Fundamentais e, em seguida, cursos de especialização focados em Direito Constitucional.

A partir desta experiência foi adquirida a *expertise* necessária para receber junto ao MEC, no início dos anos 2000, o credenciamento para ofertas de cursos pós-graduação lato sensu voltados a formar especialistas em direito público. Com o aumento constante da notoriedade e importância da instituição, endossada pelo público constante, sentiu-se a necessidade de se expandirem as atividades acadêmicas. Houve então, durante dois anos, o preparo e desenvolvimento do projeto de pós-graduação stricto sensu junto à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), o qual obteve sucesso em seu credenciamento.

O IDP teve uma caminhada um tanto quanto singular se comparada com outras instituições de ensino, visto que teve seu início com cursos de extensão, passando para a especialização e, posteriormente, o mestrado. Este processo resultou na expansão física da sede, que teve sua construção finalizada no ano de 2007, seguida pelo credenciamento do curso de graduação, obtido no ano de 2010.

Em paralelo ao crescimento e diversificação dos níveis acadêmicos ofertados, desde o princípio do instituto foram realizados seminários, congressos, palestras e congressos nacionais e internacionais que reuniram lideranças do cenário político, jurídico, empresarial e acadêmico do país e do exterior.

Nele sempre houve uma preocupação com o diálogo no plano internacional, por meio da presença dos grandes nomes do Direito. Esse diálogo foi essencial para a abertura de portas para a cooperação com centros de ensino e instituições de outros países, bem como para a realização de atividades conjuntas, como pesquisas e convênios.

Desde sua fundação, a organização ganhou mercado e ficou conhecida pela qualidade de capacitações ofertadas na área de Direito, inicialmente, em Brasília, e depois em âmbito nacional. Com sua reputação consolidada no Direito, em 2016, houve um movimento para a diversificação da área atuante de ensino, passando a ofertar graduação e mestrado em administração pública. Este pode ser considerado um marco importante na história da instituição, que desde então vem expandindo cada vez mais a sua diversidade de cursos.

De 2020 até o momento, foram lançados mais de 8 novos cursos de graduação, dois novos programas de mestrado, um programa de doutorado, três novos *Master of Business Administration* (MBA)s, dez novos cursos de especialização, além de cursos de pós-graduação lato sensu à distância focados na área do direito.

O IDP atualmente conta com 12 cursos de graduação, em áreas diversas. No nível de pós-graduação são 29 cursos de *lato sensu* na área do direito e 4 cursos de *stricto* nas áreas de administração pública, economia e direito. Além de uma estrutura física que

conta com 2 sedes em Brasília e uma filial em São Paulo.

5.3 Cardeia de valor do IDP

O IDP é uma instituição voltada a fazer um trabalho diferenciado, de qualidade, inovador, adaptativo e com pluralismo, o que é refletido em sua cultura. O grupo de colaboradores da empresa é composto por profissionais que compõem uma estrutura organizacional horizontalizada, sem uma representação formal hierarquizada de um organograma institucional. Assim, o IDP está organizado em áreas generalistas voltadas para as necessidades de suas atividades. Para um melhor entendimento do seu funcionamento atual, foi elaborada uma cadeia de valor constituída pelas principais áreas e seus respectivos macroprocessos, conforme Figura 5.2.

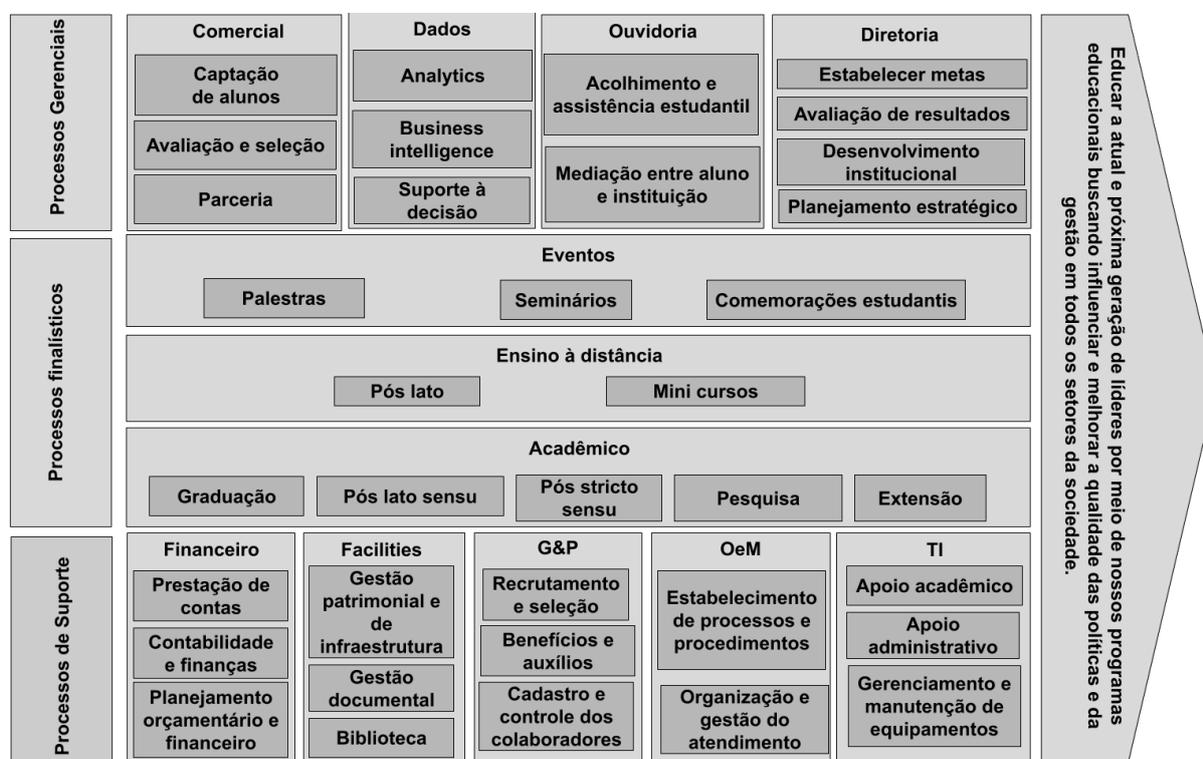


Figura 5.2: Cadeia de valor do IDP. Fonte: autora

O valor da empresa está pautado em *"Educar a atual e próxima geração de líderes por meio de nossos programas educacionais, buscando influenciar e melhorar a qualidade das políticas e da gestão em todos os setores da sociedade"*. Esta é a diretriz principal que serve como um guia, uma missão para a instituição. Os processos finalísticos do IDP estão diretamente ligados à prestação de serviços para os discentes, sejam eventos, ensino à distância ou atividades acadêmicas, como pesquisas, extensões assim como os cursos de graduação e de pós-graduação.

Os processos gerenciais envolvem ações relativas à captação de novos alunos por meio da área comercial. A área de dados realiza a consolidação e análise de dados para apoio à tomada de decisão. A ouvidoria tem o papel de contato direto com os alunos, e por fim a diretoria é a área estratégica da instituição. Os processos de suporte compreendem atividades de sustentação, como o financeiro, que cuida na prestação de contas, contabilidade e finanças, frente de *facilities*, responsável pelas atividades patrimoniais e estruturais, Gente e Performance (GP), responsável pelos recursos humanos da empresa, Organização e Método, que visa pela organização de procedimentos e processos internos e, por fim, a Tecnologia da Informação (TI), responsável por todo apoio tecnológico, seja ele na área acadêmica ou administrativa, bem como o gerenciamento e manutenção dos equipamentos tecnológicos.

O IDP possui uma cultura organizacional que facilita e incentiva as modificações estruturais para atender aos objetivos e projetos vigentes, podendo executar ações de criação, dissolução e fusão de áreas de trabalho. O seu funcionamento por meio de fluxos de trabalho possibilita o acompanhamento e adaptação institucional aos crescimentos e mudanças internas sem muitos problemas em um primeiro momento. Porém, como foi possível observar na história da instituição, seu crescimento ocorreu de forma exponencial desde 2016, tendo um aumento abrupto de serviços prestados do ano de 2020 até hoje. Os processos internos, anteriormente adequados para um contexto de menor complexidade, tiveram que rapidamente se adequar à nova realidade do instituto.

A pandemia do novo coronavírus demandou rápidas tomadas de decisões, novas adaptações de processos, principalmente no que tange à tecnologia, além de uma rápida aprendizagem sobre as novas ferramentas e modelos de ensino online. Os processos e atividades, antes bem executados passaram a apresentar novas dificuldades para realização.

5.4 Descrição da TI no IDP

As ações executadas pela área de TI no Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP) ocorrem de maneira transversal, atendendo desde o nível estratégico até o operacional. A área busca constantemente a otimização de tempo, eficiência e produtividade nos métodos e formas de trabalho, além de redução de custos da TI. O macroprocesso de "Apoio acadêmico" é composto por subprocessos relacionados às atividades dos docentes e dos discentes, listados a seguir.

- Cadastro de docentes e discentes;
- Orientação sobre utilização de equipamentos ou ferramentas;

- Verificação rotineira dos recursos tecnológicos utilizados nas aulas (inclusive dos laboratórios de informática);
- Pedido de equipamentos computacionais;
- Auxílio para transmissões online de aulas ou eventos;
- Preparação de rede para aulas e eventos.

A frente de TI também realiza o macroprocesso de "Gerenciamento e manutenção de equipamentos". Este é composto pelos seguintes subprocessos:

- Manutenção de impressoras e scanners;
- Montagem e movimentação de estações de trabalho;
- Solicitações de compra ou reparo de equipamentos computacionais;
- Manutenção e troca de equipamentos computacionais e periféricos;
- Manutenção da rede sem fio na instituição.

O macroprocesso "Apoio administrativo" refere-se o suporte tecnológico para a área administrativa e abrange os seguintes subprocessos:

- Gerenciamento de acessos para colaboradores;
- Cadastro de colaboradores na rede;
- Esclarecimento de dúvidas sobre utilização de equipamentos ou ferramentas;
- Gestão das pastas na rede interna;
- Formatação de computadores;
- Solicitação de instalação de ferramentas computacionais;
- Implementação e monitoramento de infraestrutura de TI;
- Gerenciamento das máquinas servidores;
- Gestão da segurança da informação na instituição;
- Terceirização de TI.

Ao analisar os macroprocessos e subprocessos da frente de TI do IDP, é possível observar que sua atuação é essencial para o alcance dos objetivos gerais da instituição. A maturidade relacionada à infraestrutura de TI se mostra mais consistente, porém no que se refere ao desenvolvimento de soluções tecnológicas ainda se tem uma participação tímida da área.

A falta de capacidade para desenvolvimento interno de soluções de TI vai na direção oposta do aumento da necessidades de ferramentas computacionais, seja pelo crescimento da instituição e conseqüentemente pelo aumento da complexidade dos seus processos internos, seja pela situação imposta pela pandemia, citada anteriormente. Dessa forma, tem-se a terceirização de TI como a solução para este *gap*, atendendo assim a demandas internas relacionadas à tecnologia. Apesar de se mostrar como um recurso poderoso para a empresa, este também passa ser o subprocesso mais crítico da frente de TI, dada a sua alta relevância não só para a área de TI, mas para todas as demais, pois atende todo o ecossistema tecnológico do instituto.

5.4.1 Processo de terceirização de TI no IDP

O processo de terceirização de TI no IDP envolve diretamente cinco áreas do órgão, sendo quatro dessas áreas fixas e uma variável, representada pela área demandante. Entre as áreas fixas, em que há diferentes níveis de participação, têm-se as equipes de tecnologia da informação (três colaboradores), equipe financeira (quatro colaboradores), equipe de *facilities* (quatro colaboradores) e a diretoria (três diretores). A cada ciclo do processo são envolvidos: um colaborador de cada área e seu respectivo gestor, desta forma, ao total, oito colaboradores participam do processo de aquisição já considerando a área demandante.

Buscando compreender esse processo, as entrevistas foram conduzidas com os gerentes de cada área e com um colaborador da área demandante, totalizando cinco colaboradores e representando uma proporção de 62,5% do total de colaboradores envolvidos a cada ciclo de processo.

As entrevista ocorreram de forma semi-estruturada, com uma duração variando de 30 minutos a 2 horas onde foi realizada uma pergunta aberta principal “Como ocorre o processo de aquisição desde o início do interesse e planejamento e até o seu fim, levando em consideração a participação da sua área no processo como um todo?”

Ao final das entrevistas os entrevistadores extraíram um consolidado de informações visando obter respostas para os seguintes pontos:

- Como é feita a solicitação de aquisições?
- A área possui um planejamento das aquisições de interesse? Se sim, como ele é feito?
- Qual a participação e as responsabilidades da área no processo como um todo?
- Como ocorre o acompanhamento do contrato após o seu início?

Com auxílio de informações resultantes de entrevistas, foi elaborado o macroprocesso de terceirização de TI apresentado na Figura 5.3:

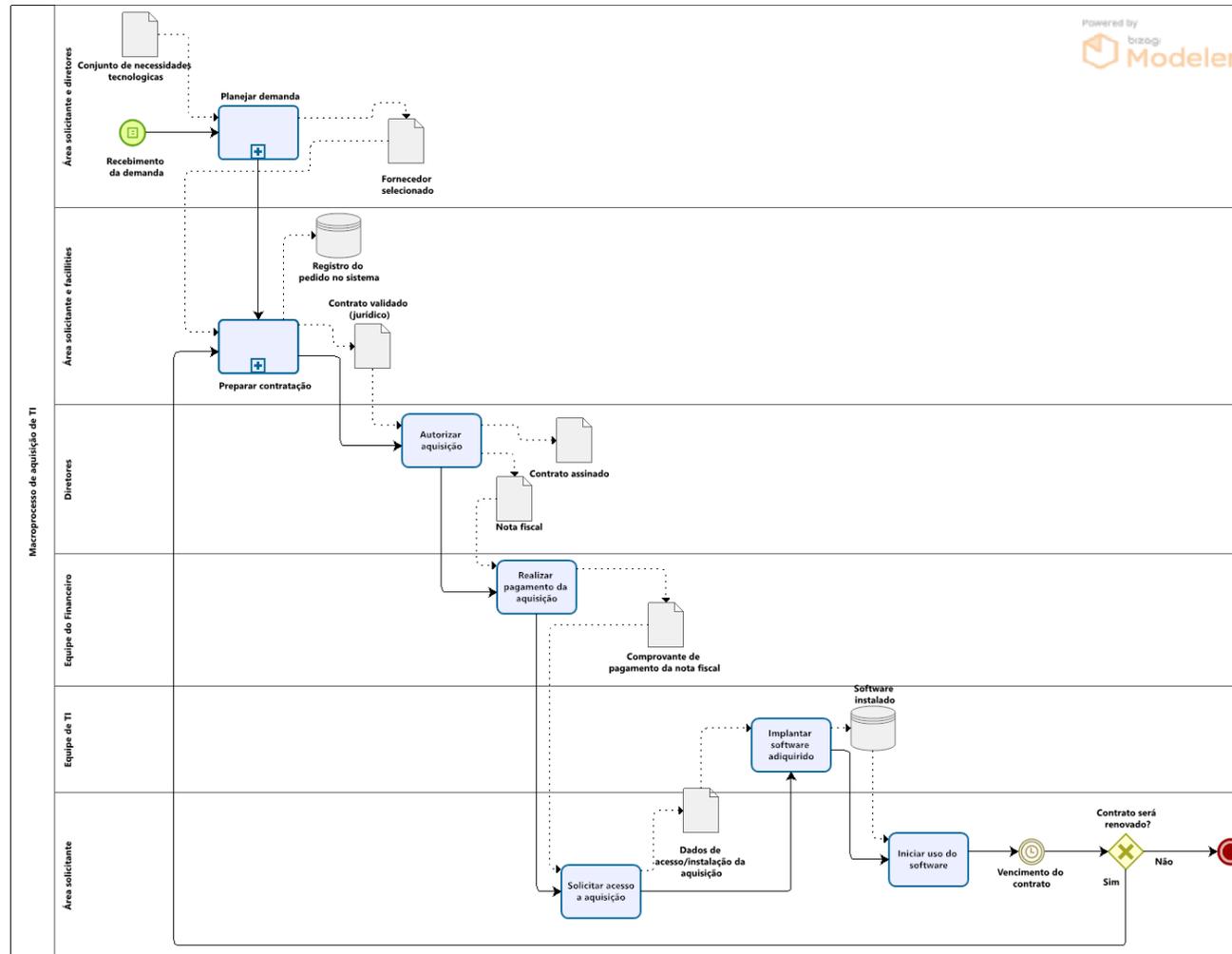


Figura 5.3: Diagrama do Processo de Terceirização de TI no IDP: visão macro. Fonte: Autora

Tendo em vista o macroprocesso apresentado acima, na Figura 5.3, foram identificados alguns pontos críticos que podem gerar problemas no processo descrito.

O processo não faz parte integrante de todas as áreas organizacionais, podendo ter alterações dependendo da área que o executa. Outra questão é a falta de inclusão de suas atividades, pois não possibilita a ponderação de diferentes conhecimentos, pontos de vistas e percepções, o que resulta na dificuldade de obtenção de um consenso. Adicionalmente, não é observado um aperfeiçoamento do processo, que poderia advir de aprendizados e experiências na execução das atividades do processo.

Foi identificada a falta de integração das atividades realizadas pelas áreas envolvidas no processo, para assegurar e fornecer informações, o que dificulta a sua supervisão e a tomada de decisões relacionada a ele, além de não gerar um senso de inclusão aos afetados pelas atividades, desestimulando sua execução por parte dos colaboradores.

Outro ponto relacionado à falta de integração das atividades se refere à ausência de comunicação entre os envolvidos durante todo o processo, ou seja, não há fluidez de informações, principalmente quando o processo segue para outra área. Como exemplo, a área solicitante inicia a conversa com o fornecedor do software antes da certeza se a área financeira realizou o pagamento da nota fiscal.

Há uma grande necessidade de definição mais clara e objetiva do escopo, seu impacto e delimitação do contexto em que o software será aplicado. Principalmente da parte dos diretores sobre a definição orçamentária da aquisição em questão. Em paralelo, existe a falta da gestão dos softwares anteriormente adquiridos, em que é possível observar casos de aquisições de soluções semelhantes, feitas por áreas distintas.

Também pode-se destacar a falta da definição dos critérios de risco relacionados à aquisição, sua respectiva identificação, análise e avaliação, gerando uma incerteza sobre os tipos de riscos que podem assumir, ou não, e seus impactos para a instituição.

No que tange ao monitoramento e análise crítica, o processo visa assegurar a melhoria da qualidade e eficácia das fases de planejamento, execução, gestão do processo e conseqüentemente o resultado do processo. No entanto este se apresenta burocrático e centralizador, deixando a cargo da direção do órgão a seleção do software, que por sua vez deverá em seguida aprovar a escolha. Isso ocorre sem o envolvimento da área técnica de TI, que somente terá envolvimento após a finalização da aquisição, tendo o papel final de integração e configuração para o uso pela área solicitante do software.

Ao final, após a conclusão da aquisição, principalmente nos casos de contratos na modalidade software como serviço, ou *Software as a Service* (SaaS), o acompanhamento da terceirização não é padronizado e depende da área solicitante, correndo o risco de possíveis perdas de prazo para renovação, renovações automáticas sem autorização, entre outros problemas. Portanto é possível destacar como principais problemas da terceirização

de TI no IDP a falta de um processo padronizado com atividades, papéis, áreas envolvidas, insumos e resultados, bem como a necessidade de um controle maior das terceirizações já realizadas e seu respectivo monitoramento.

Outra necessidade observada no contexto da terceirização de TI do IDP se refere ao entendimento das atividades do processo e sua importância. Tendo em vista seu ambiente que está em constante mudança e transformação, os envolvidos precisam de uma orientação maior quais são as atividades que mais impactam no processo, para, caso necessário, consiga adaptar o processo minimizando as consequências para a terceirização.

Atualmente não existe um processo formal de planejamento, execução ou gestão das terceirizações de TI. A falta de uma padronização alinhada à criticidade envolvida resultam em contratações de TI problemáticas, desde o momento da concepção até sua implantação.

Um exemplo recente disso ocorreu em 2019 com a ferramenta *TOTVS Protheus*, uma ferramenta de *Enterprise Resource Planning* (ERP), Planejamento de Recursos Empresariais ou Sistema Integrado de Gestão. Este sistema tem como objetivo interligar todos os dados e processos de uma organização em uma plataforma integrada. Sua contratação foi realizada sem um estudo de viabilidade prévio, o qual foi elaborado apenas depois da assinatura do contrato.

A contratação dessa solução foi composta por 2 contratos que totalizavam R\$70.371,60. O primeiro consistia em um valor total de R\$33.258,00, sendo R\$12.000,00 relacionados à implantação e o restante dividido em um ano de mensalidades no valor de R\$1.771,50. O segundo era relacionado ao aplicativo e tinha o valor total de R\$37.113,6, onde o valor de R\$8.550,00 era referente a implantação e o restante dividido em parcelas mensais de R\$2.380,30 com duração de um ano.

Visto o equívoco, foi feita solicitação de rescisão contratual junto a empresa contratada, porém o valor da multa rescisória era maior do que contrato (o qual não foi divulgado). Com isso foi decidido manter o contrato, mesmo sem a utilização da ferramenta.

Há também casos de terceirizações duplicadas, ou seja, contratação de diferentes softwares por diferentes áreas da instituição, mas que tem o mesmo objetivo. Como a utilização do *OTRS* e o *Desk Manager*, ambas ferramentas de gestão de chamados, ou o *RD Station* e *Hubspot*, ambos softwares para marketing de entrada, vendas e atendimento ao cliente.

Por fim, outro exemplo de uma terceirização que não teve um planejamento e preparação adequada foi a aquisição do software *DocXpress*, uma ferramenta que serve como repositório de documentos dos alunos com a ferramenta de administração. Sua contratação ocorreu em meados de 2019, porém sua utilização era condicionada a integração com a ferramenta de gestão acadêmica já existente na instituição, *TOTVS RM*.

As condições de implantação não ficaram claras no contrato, com isso a empresa não realizou a sua integração conforme necessário, e por falta de equipe interna qualificada a ferramenta ficou sem utilização até meados de 2020, quando foi realizado um projeto com contratação de equipe técnica que solucionou o problema relacionado a integração possibilitando seu uso.

Frente aos problemas referentes a terceirização exemplificados e com a falta um processo formal de contratação de TI, conforme citado anteriormente. Buscou-se realizar o mapeamento de um processo unificado visando ter um entendimento dos procedimentos internos e observação de possíveis pontos críticos.

5.5 Validação do processo atual de terceirização de TI

Assim como previsto na fase de análise dos dados, o resultado do mapeamento do processo atual de terceirização de TI do IDP foi validado. Essa validação ocorreu com cada um dos gestores estratégicos que participam ativamente das contratações de TI da instituição.

A primeira reunião ocorreu com o gestor da TI, papel importante no processo estudado, tendo em vista que sua área é diretamente impactada pelas terceirizações. A reunião teve duração de 56 minutos, e não foi apontado nenhum ajuste necessário. O único ponto levantado foi de que o processo validado estava sendo modificado e um novo protocolo com maior participação da TI entraria em vigor. No momento da reunião essa atualização ainda não estava definida claramente e não tinha data para ser implementada.

Em seguida, de forma sequencial, ocorreram as reuniões com o gestor do financeiro, que teve uma duração de 1 hora, e o representante da área solicitante, com duração de 49 minutos. As reuniões ocorreram separadamente e os dois concordaram com o processo apresentado. O representante da área solicitante atua na equipe de cursos de pós-graduação *stricto sensu*. A sua participação deu-se em função dele ter acabado de passar de forma completa pelo processo de terceirização de TI em sua área, realizando a contratação de um sistema que realiza o serviço de detecção de plágio de forma.

Por fim, a última reunião ocorreu com o gestor da equipe Organização e Método, sua seleção ocorreu devido a sua participação estratégica do seu setor para a instituição, possibilitando ter uma visão transversal do funcionamento do IDP. Com duração de 1 hora, o gestor não apresentou nenhum ponto a ser ajustado, e apenas reforçou as dificuldades enfrentadas em função da falta de estruturação do processo de terceirização de TI. Assim, a caracterização do processo de terceirização de TI do IDP foi devidamente validado.

5.6 Considerações finais do capítulo

Após a apresentação do contexto estudado, a instituição de ensino Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP), sua história, caracterização e descrição, foi então alcançado o segundo objetivo específico proposto no trabalho, o qual teve como resultado o entendimento e mapeamento do processo de terceirização de TI existente na instituição.

Partindo do resultado deste capítulo, juntamente com os resultado do *capítulo 4 - Seleção de boas práticas para a terceirização de TI e gestão de riscos*, no capítulo seguinte apresenta-se uma proposta de um novo processo de terceirização de TI para o IDP.

Capítulo 6

Proposta de novo processo de terceirização de TI para o IDP

6.1 Considerações iniciais do capítulo

Este capítulo apresenta os resultados da execução do terceiro ciclo do estudo de caso, conforme a Figura 6.1. Com isso, foi possível atender o terceiro objetivo específico definido "*Propor novo processo de terceirização TI alinhado às boas práticas*".

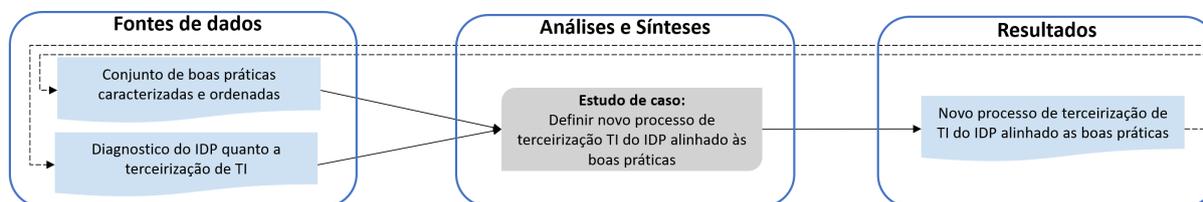


Figura 6.1: Terceiro ciclo do estudo de caso. Fonte: Autora

Este capítulo apresenta os resultados oriundos da análise das boas práticas de gestão de riscos e de terceirização de TI, juntamente com o entendimento e mapeamento do processo de terceirização de TI existente no IDP. As informações foram compiladas e unificadas, resultando na proposta de um novo processo de terceirização que atenda às demandas internas e que esteja alinhado às boas práticas.

6.2 Proposta de novo processo de terceirização de TI para o IDP

Buscando uma melhor organização das atividades no processo, este foi separado por fases e suas atividades agrupadas por finalidade comum, conforme mostra a Figura 6.2:

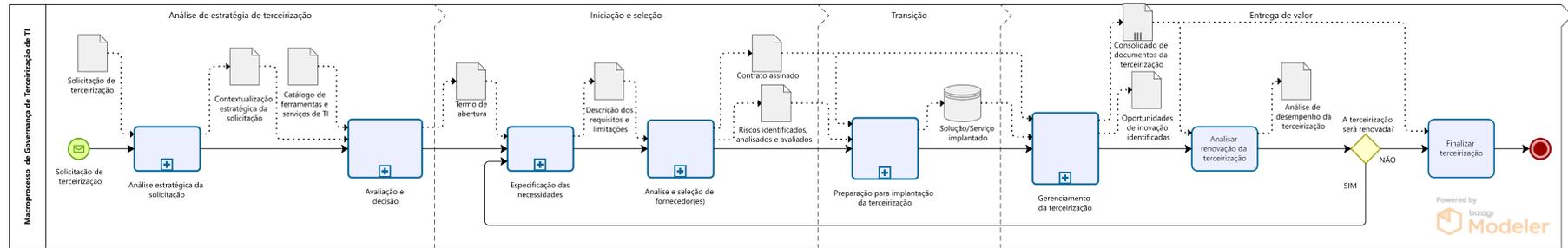


Figura 6.2: Novo processo de terceirização de TI proposto. Fonte: autora

As fases do processo seguem os mesmos objetivos que apresentadas na ISO 37500 [10]. A análise de estratégia é a primeira fase do processo de terceirização, buscando iniciar e avaliar a solicitação da terceirização quanto aos impactos estratégicos da organização, ação esta que é realizada na "Análise estratégica da solicitação" gerando um entendimento da contextualização da ação de forma estratégica. Esta atividade gera um insumo para a "Avaliação e decisão" onde será decidido, a partir das informações coletadas, se a terceirização ocorrerá ou não, finalizando assim esta fase.

A fase seguinte, de iniciação e seleção, parte do princípio de que a terceirização será iniciada, portanto na "especificação das necessidades" o estudo macro que é feito na fase anterior é aprofundado e os requisitos e limitações são definidos para que seja realizada a "análise e seleção de fornecedor(es)" onde é feito um trabalho de busca e seleção de fornecedores para a necessidade de terceirização descrita, e que finaliza com a formalização do acordo.

Na transição dá-se a "preparação para implantação da terceirização", ou seja a implantação do serviço ou solução, com todos os repasses necessários para que o fornecedor estabeleça os recursos necessários para cumprir a sua responsabilidade de prestação de serviço acordada com o cliente.

Na última fase, denominada entrega de valor, é realizado o "gerenciamento da terceirização", tendo como principal objetivo a sustentação da entrega de valor conforme o acordado. Nesta fase o cliente monitora a prestação de serviço ou a utilização da solução para que ao fim do contrato possa realizar a análise para decisão sobre sua renovação.

Neste momento, fazendo uso do consolidado dos documentos da terceirização, é realizada a análise da renovação, em que as partes interessadas identificam os critérios para tomar a decisão de continuação ou não da terceirização.

Se a decisão for pela continuidade da terceirização, então o fluxo retorna para o processo de especificação das necessidades, tendo em vista que os requisitos podem ter sido alterados ao longo da execução da terceirização, bem como pode ser encontrado um fornecedor mais adequado e vantajoso para a instituição.

Porém, se a decisão for pela finalização da terceirização, será executada a atividade de finalizar a terceirização, onde haverá um encerramento ordenado, incluindo aprovação formal, revisão e arquivamento de toda documentação, inclusive das lições aprendidas. Em seguida o processo é encerrado.

Cada um dos processos descritos acima e apresentados na Figura 6.2 serão descritos de forma detalhada nas seções seguintes.

6.3 Processo de análise estratégica da solicitação

A análise estratégica da solicitação é iniciada pela área solicitante, que representa qualquer área ou colaborador que envia a solicitação de terceirização para a equipe de Organização e Método, unidade responsável por ações estratégicas no IDP. Esta equipe, por sua vez, utiliza da descrição da solicitação enviada pela área solicitante para verificar os pré-requisitos da terceirização, identificando suas funções juntamente como alinhamento com as estratégias e objetivos da instituição. Isso se dá para garantir que as funções sejam específicas o suficiente para ser capaz de julgar e direcionar se as iniciativas de terceirização contribuirão para os objetivos estratégicos e considerar os serviços, desafios e mercados atuais e futuros.

Como resultado, é obtida uma descrição dos negócios e das funções atreladas à solicitação de terceirização, que por sua vez se torna insumo para a identificação de serviços impactados pela terceirização, entendendo seu papel na cadeia de valor da organização, sua importância estratégica, seus elementos, recursos e ativos, custos, riscos e restrições.

Toda esta análise é consolidada e documentada como serviços impactados, identificados e descritos. Com este entendimento geral é possível definir a estratégia de terceirização, onde é determinada a abordagem do risco, seleção de fornecedores, transferência dos envolvidos (internos e externos) e transformação da terceirização na organização, gerando assim um registro completo da contextualização estratégica da solicitação de terceirização na instituição. Com isso, o processo de análise estratégica da solicitação é finalizado. Seu mapeamento está representado na Figura 6.3:

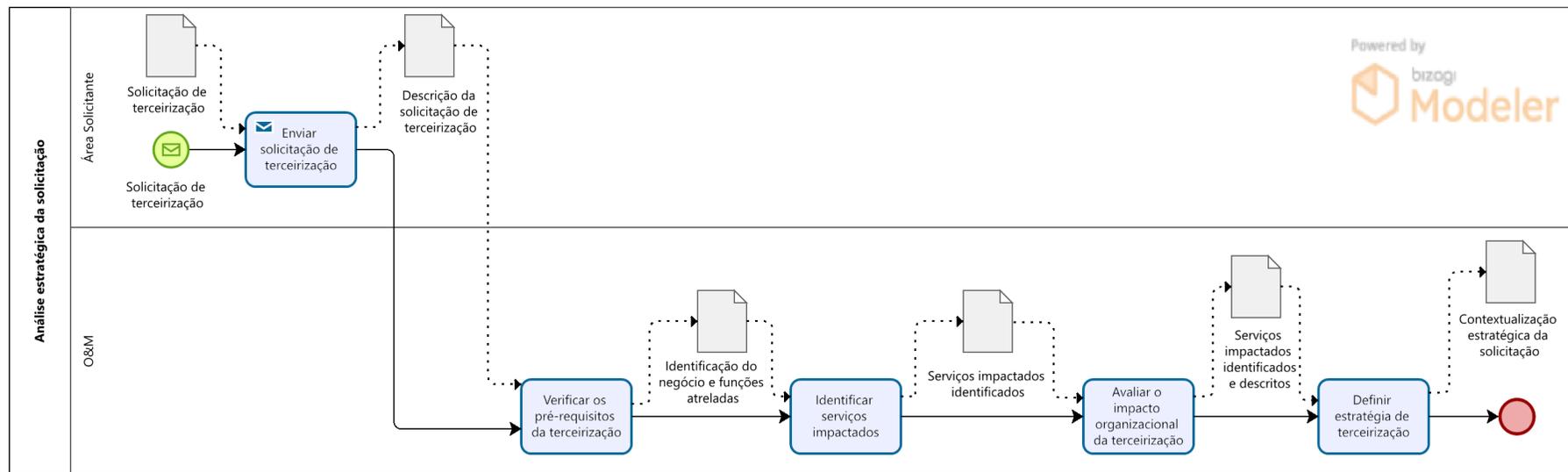


Figura 6.3: Processo de análise estratégica da solicitação. Fonte: Autora

6.4 Processo de avaliação e decisão

O processo de avaliação e decisão é iniciado pela TI com a atividade de consulta ao catálogo da base de TI, onde, fazendo uso da contextualização resultante do processo anterior juntamente com o catálogo de ferramentas e serviços de TI do IDP. A análise dos serviços e níveis de serviço atuais de TI serve para identificar lacunas entre os serviços existentes e as atividades de negócios que eles suportam. São identificadas e documentadas as áreas para melhoria dos serviços existentes e as opções de nível de serviço.

Em seguida, a área da TI se junta com a área solicitante para realizar o gerenciamento das partes interessadas, onde todas as áreas ou colaboradores envolvidos na contratação são identificados e registrados, bem como suas preocupações e objetivos, e incluídos no processo de terceirização, sejam essas pessoas de dentro ou de fora da empresa. A identificação das partes interessadas e a análise das lacunas e áreas de melhoria são utilizados pelas partes interessadas para elaborar o planejamento básico da terceirização, onde são descritos os contextos de risco, os prazos e custos da solicitação.

Por fim, com o planejamento resultante da atividade anterior, a diretoria, representando a alta gestão, junto com a área de TI, área técnica, e de Organização e Método, área estratégica, fazem a deliberação sobre a realização da terceirização, momento em que será decidido pela terceirização ou não, a partir das informações consolidadas.

Nesse momento o processo toma rumos diferentes, dependendo da decisão sobre aceitar ou não a solicitação de terceirização. Se a solicitação for recusada, todo o macroprocesso de governança da terceirização é encerrado. Caso a solicitação seja aceita, é montado o projeto base da terceirização, que a partir do planejamento é criado um termo de abertura do projeto, determinam-se os limites do projeto em termos de custos, escopo, tempo, etc., finalizando assim o processo de avaliação e decisão, cujo mapeamento é apresentado na Figura 6.4. Aqui é também finalizada a fase de análise estratégica da terceirização.

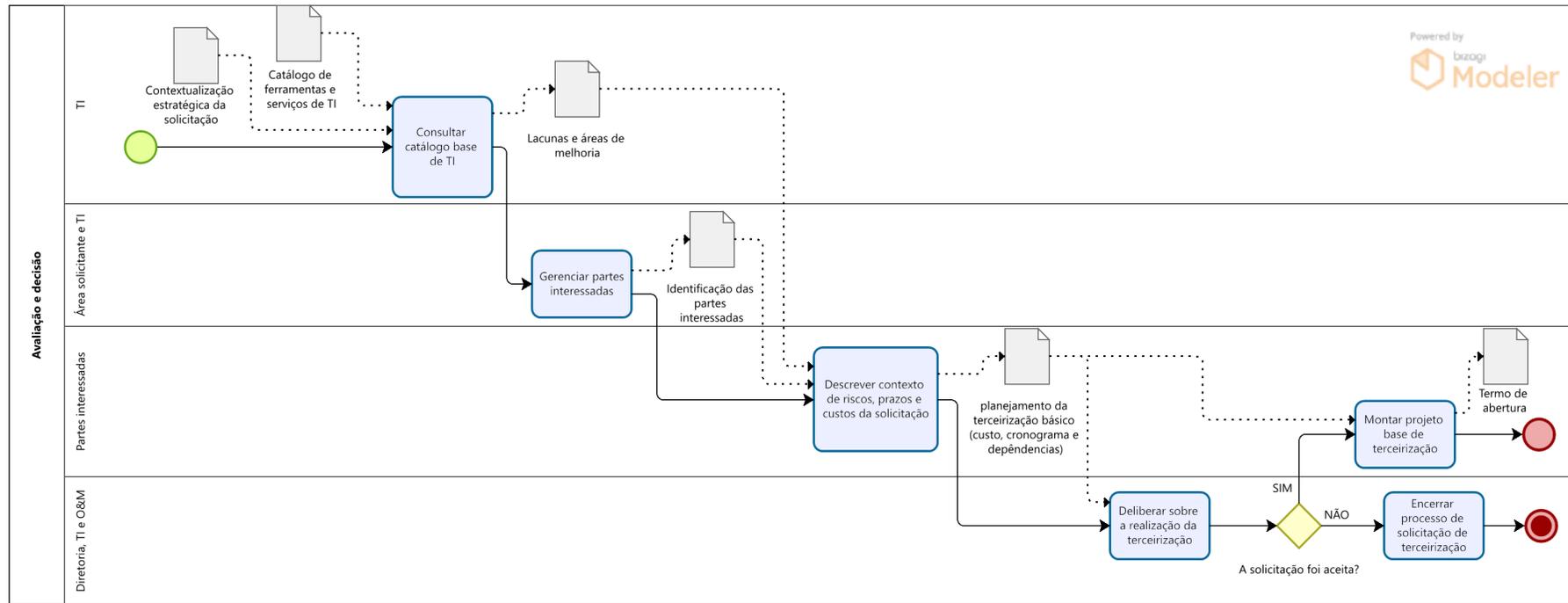


Figura 6.4: Processo de avaliação e decisão. Fonte: Autora

6.5 Processo de especificação das necessidades

A especificação das necessidades é o próximo processo que vem depois da decisão por aceitar a solicitação de terceirização. É um processo simples, conforme pode ser observado na Figura 6.5, se comparado com os demais, porém é muito importante, pois é neste momento que é realizado um entendimento detalhado do serviço/solução solicitado.

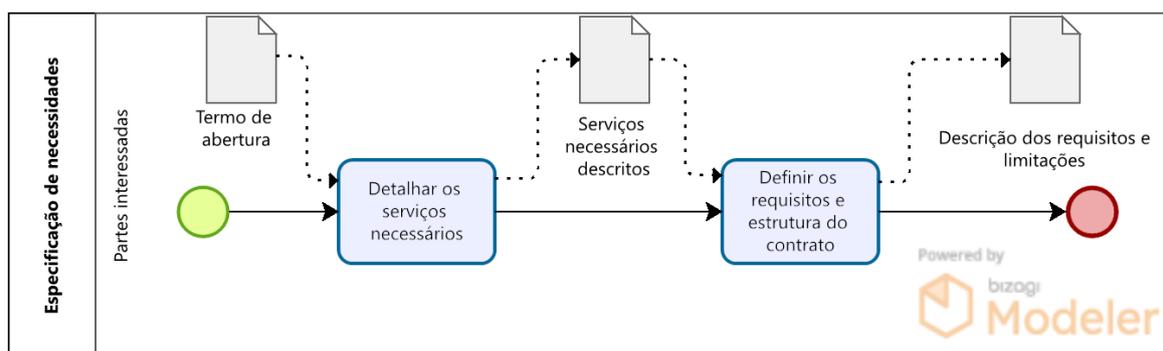


Figura 6.5: Processo de especificação das necessidades. Fonte: Autora

A execução deste processo é de responsabilidade das partes interessadas definidas na fase anterior, fazendo uso do termo de abertura, também elaborado na fase anterior. Esse processo tem como primeira atividade detalhar os serviços necessários, onde são descritas todas as informações possíveis sobre os serviços necessários como: qualidade, quantidade, preço, indicadores de medição de desempenho e limites do serviço. Este processo resulta na documentação dos serviços necessários descritos, que por sua vez será utilizada para definir os requisitos e estrutura do contrato, onde são definidos, ou analisados, os requisitos incluindo os direitos e obrigações de todas as partes. O término do processo é uma descrição detalhada dos requisitos e das limitações da terceirização de TI.

6.6 Processo de análise e seleção de fornecedor(es)

O processo seguinte, de análise e seleção de fornecedor(es), faz uso da descrição dos requisitos e limitações para buscar o(s) fornecedor(es) que melhor atenda(m) as necessidades definidas, e estabelecer o acordo de terceirização e avaliar os riscos associados. O mapeamento do processo é apresentado na Figura 6.6:

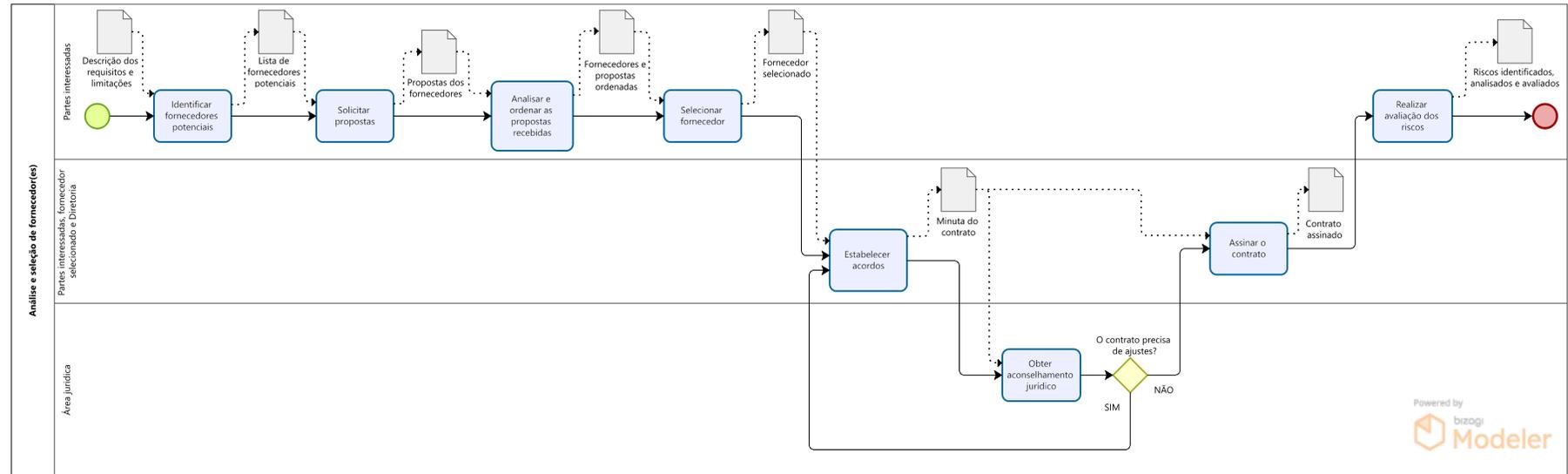


Figura 6.6: Processo de análise e seleção de fornecedor(es). Fonte: Autora

A primeira atividade do processo é realizada pelas partes interessadas, que utilizando a descrição dos requisitos e limitações, busca, identifica, registra e categoriza os possíveis fornecedores que podem atender à solicitação. Com a lista de potenciais fornecedores, as partes interessadas entram em contato com cada um, solicitando as propostas de acordo com requisitos definidos, que depois de consolidadas são reunidas, revisadas e ordenadas de acordo com o atendimento dos requisitos da área solicitante.

Com esta ordenação, as partes interessadas tem insumos suficientes para realizar a escolha do fornecedor. Esta seleção é feita pelo modo mais adequado, com base em critérios de viabilidade, incluindo risco e custo, resultando no fornecedor que melhor atenda aos requisitos. É importante ter o envolvimento de todas as partes interessadas na escolha do fornecedor.

Uma vez que o fornecedor foi selecionado, é iniciado então o estabelecimento do acordo. Essa atividade tem o envolvimento das partes interessadas, do fornecedor selecionado e da diretoria, os quais seguem com os acordos e aprovações necessárias nos principais pontos de decisão no processo de terceirização. Como resultado, é obtida a minuta do contrato que deverá ser analisada pela área jurídica e, caso necessário, pode retornar para estabelecimento de novos acordos. Caso não precise de ajustes, o contrato segue para assinatura das partes interessadas, fornecedor e diretoria. Neste momento a minuta se torna o contrato oficialmente assinado.

Apos ter sido selecionado o fornecedor, os acordos terem sido realizados e documentados no contrato, as partes interessadas já podem realizar a avaliação dos riscos da terceirização, assim os riscos são identificados, analisados, avaliados e todo o resultado dessa avaliação é documentado.

Com o fim do processo, o contrato assinado e os requisitos identificados, analisados e avaliados, é então finalizada a fase de iniciação e seleção. A fase seguinte, de transição, é iniciada com o foco na preparação dos recursos para a entrega de valor da terceirização.

6.7 Processo de preparação para implantação da terceirização

O processo de preparação para implantação da terceirização é o único processo da fase de transição. Ele ocorre logo após a definição do fornecedor, da assinatura do contrato e da avaliação dos riscos, e tem como saída a solução ou serviço implantados no ambiente da organização, e esse mapeamento é apresentado Figura 6.7:

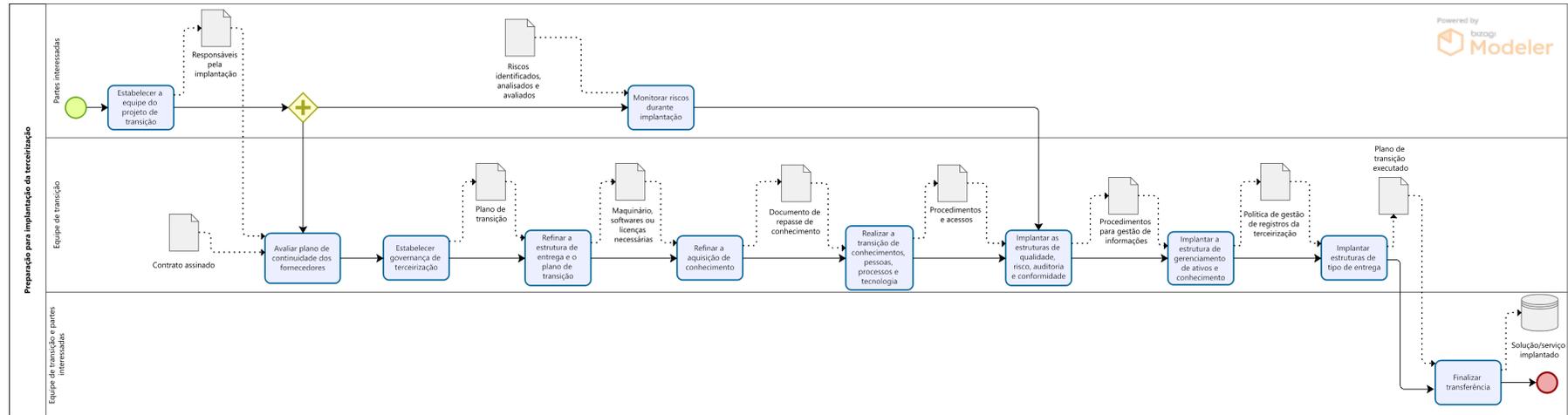


Figura 6.7: Processo de preparação para implantação da terceirização. Fonte: Autora

A primeira atividade é realizada pelas partes interessadas, no momento de definir, atribuir funções e responsabilidades aos membros individuais da equipe do cliente e do provedor, a qual é denominada equipe de transição. Esta equipe pode ser semelhante aos colaboradores definidos como partes interessadas. A separação das equipes é necessária pois se mostra como uma atividade interna do IDP, onde colaboradores específicos auxiliam apenas no momento da implantação de terceirização.

Com a definição da equipe de transição, duas atividades ocorrem em paralelo. Uma realizada pelas partes interessadas, fazendo uso do riscos identificados, analisados e avaliados, em que monitoram-se os riscos relacionados à capacidade do fornecedor de entregar o serviço contratado durante a implantação. Este é um dos momentos mais críticos, pois caso não ocorra da melhor forma, ele pode influenciar o resto da terceirização. A outra atividade paralela é realizada pela equipe de transição que, munida do contrato assinado, analisa o plano de continuidade do(s) fornecedor(es) contratados, verificando se estes apresentam planos de continuidade eficazes em vigor.

Em seguida é estabelecida a governança da terceirização, pela equipe de transição, onde é definido o processo de avaliação do progresso do projeto e a revisão dos principais documentos e entregas do projeto. Com o plano de transição resultante, a equipe realiza o refinamento da estrutura de entrega e o plano elaborado, levantando as necessidades de aquisições paralelas, como aquisição e/ou configuração de maquinários, softwares e licenças regulatórias, e outras atividades que tenham prazo de entrega.

Com toda a preparação da estrutura e suas possíveis dependências de aquisições paralelas, a aquisição de conhecimento é refinada pela equipe de transição, que terá todo o repasse de conhecimento sobre a ferramenta, visando a apropriação do conhecimento sobre a terceirização e elaboração de documentos de repasse de conhecimento.

A equipe de transição, agora munida do conhecimento necessário sobre a solução/serviço, inicia o processo de transição de conhecimento, pessoas, processos e tecnologias por meio de estabelecimento de procedimentos internos e da liberação de acessos necessários.

Neste momento todos os procedimentos e monitoramentos documentados nas atividades anteriores visam implantar a estrutura de qualidade, riscos, auditoria e conformidade, gerando assim procedimentos gerais para implementar mecanismo de obtenção de informações das equipes de gestão de qualidade, riscos, conformidade e desempenho de um fornecedor.

Com os procedimentos definidos, a equipe de transição implanta em seguida a estrutura de gerenciamento de ativos e dos conhecimentos que envolvem a terceirização, resultando na política de gestão de registros para a manutenção da atualidade dos registros. Em seguida é realizada a última implantação da equipe de transição, e a mais significativa, que é a definição da estrutura de tipo de entrega. São atribuídos recursos de acordo com

o plano de capacidade e introduzidas tarefas e responsabilidades, ou seja, é finalizado o plano de transição definido inicialmente no processo.

A última atividade deste processo é a finalização da transferência, onde todo o processo, procedimentos e documentações gerados na preparação para implantação da terceirização são repassadas da equipe de transição para as partes interessadas, e a solução/serviço, bem como as estruturas que os envolvem tem sua implantação finalizada, encerrando tanto o processo quanto a fase de transição.

6.8 Processo de gerenciamento da terceirização

Este processo é iniciado em seguida à fase de entrega de valor, composta pelo processo de gerenciamento da terceirização. Com a solução/serviço implantado, a TI junto com as partes interessadas, o configuram para uso, visando atender aos requisitos e processamentos de negócio, deixando-o pronto para utilização dos usuários finais. Feito isso, é realizado o processo de administrar a terceirização, executado pela equipe do financeiro, TI e o gestor do contrato, que fazendo uso do contrato assinado e a solução/serviço, tratam das questões administrativas que serão descritas e seu mapeamento apresentado na seção seguinte.

De forma paralela, as partes interessadas, a área solicitante da terceirização e os usuários finais são treinados para que todos possam obter o melhor da terceirização, gerando assim guias e manuais de uso que possam ser consultados a qualquer momento. Após o treinamento de todos, as partes interessadas realizam a definição das funções e responsabilidades na solução/serviço, deixando todos os envolvidos alinhados.

Porém, como não há a participação de todos os usuários desde o início do processo, é preciso garantir que as expectativas de desempenho estejam alinhadas com os requisitos acordados por meio de interações regulares. Por meio deste alinhamento, tem-se um acordo formal da entrega de valor alinhado com todos os envolvidos, e a partir deste ponto a terceirização é analisada quanto ao monitoramento e análise da entrega do serviço/solução, visando garantir que o fornecedor está oferecendo uma qualidade de serviço/solução aceitável, atendendo aos requisitos e com aderência às condições do contrato.

A análise da entrega de valor auxilia no gerenciamento do escopo da terceirização, que é executado pelas partes interessadas. Este é controlado, bem como seus requisitos e solicitações de mudanças ao longo do ciclo de vida da terceirização.

Em conjunto com o gerenciamento do escopo, também é realizado o gerenciamento e resolução de problemas. As questões e problemas são registrados, classificados, escalados e comunicados com base em na gravidade de cada um deles. Em paralelo, também é realizado o gerenciamento das mudanças solicitadas no gerenciamento do escopo. Este

é um procedimento que registra, classifica, avalia e aprova solicitações de mudança que devem levar em consideração os riscos, os impactos potenciais aos serviços, o cliente, os requisitos do serviço, os benefícios do negócio, a viabilidade técnica e o impacto financeiro.

Esses gerenciamentos geram os registros da terceirização que são insumos para o monitoramento e revisão do empenho realizado também pelas partes interessadas. Isso tudo gera uma análise sobre o desempenho que por sua vez, junto com os documentos administrativos, compõem a atividade de documentar as informações sobre a terceirização, resultando em um relatório que consolida os documentos da terceirização.

Neste momento é realizado o incentivo por inovações, reunindo toda a experiência em volta do ciclo de vida da terceirização. Esta atividade contribui para o processo de compreensão da estratégia empresarial e TI, operações empresariais e atuais desafios, de modo a aplicar o conhecimento para identificar a tecnologia potencial de valor agregado e inovar a TI. Assim clientes, fornecedores e parceiros de negócios podem identificar oportunidades de inovação internas ou externas.

Todo este processo foi mapeado e está representado na Figura 6.8:

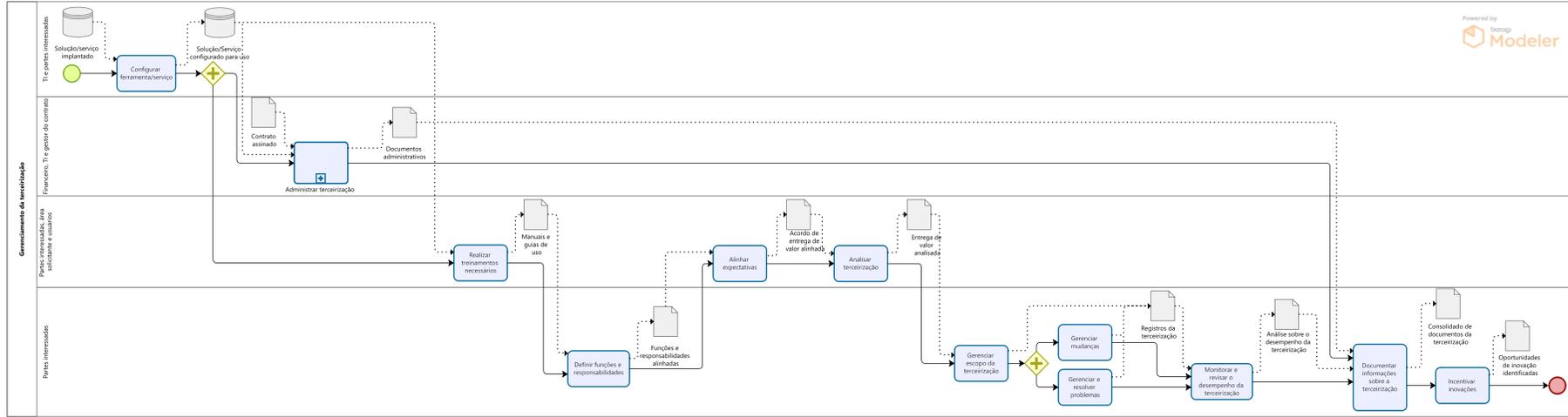


Figura 6.8: Processo de gerenciamento da terceirização. Fonte: Autora

6.8.1 Processo administrar terceirização

Por fim, o processo de administrar terceirização aparece dentro do processo de gerenciamento da terceirização, o qual está representado na Figura 6.9:

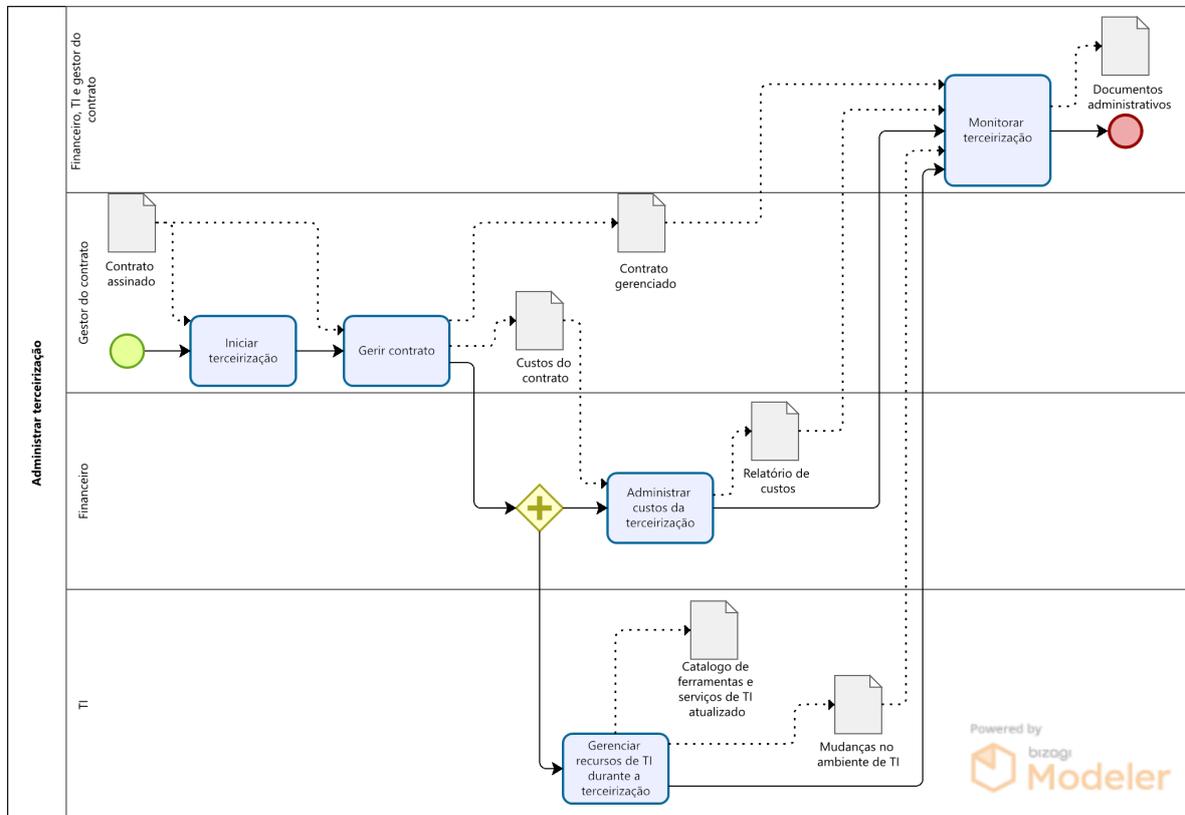


Figura 6.9: Processo administrar terceirização. Fonte: Autora

Este processo é iniciado pelo gestor do contrato, que utiliza o contrato assinado para iniciar a terceirização, que tem como objetivo garantir que as atividades de tomada de decisão e entrega sejam focadas no valor, abordando os riscos e atendendo aos requisitos das partes interessadas. Após o início da terceirização, é iniciado também o gerenciamento do contrato, onde o gestor do contrato visa garantir que os requisitos cumpram o contrato, bem como a segurança dos processos de informação, as prioridades de processamentos e os negócios operacionais.

Na gestão do contrato são gerados os custos relacionados que são enviados para o financeiro realizar a sua administração, executando a administração financeira para o contrato, criação, validação e processamento de notas fiscais, bem como gerenciamento de problemas de pagamento e gerenciamento de preços, resultando no relatório de custos. Em paralelo a área de TI realiza o gerenciamento dos recursos da TI durante a terceirização.

Tendo em vista os impactos que podem ocorrer na área, os serviços, ativos e recursos de TI são monitorados e controlados, criados ou alterados. Juntamente com o recebimento e gestão de todas as aquisições de infraestrutura e software, realizando a atualização do catálogo de ferramentas e serviços de TI. As mudanças são registradas a fim de constarem na documentação da terceirização.

Por fim, a última atividade do processo é o monitoramento da terceirização, realizado pelo financeiro, TI e gestor do contrato, fazendo uso de todos os resultados das atividades anteriores. Esta atividade visa monitorar e coletar dados de nível de serviço para avaliar o desempenho dos contratos de serviço de acordo com os termos acordados para garantir que estejam em vigor e atualizados, assim como fornecer relatórios regulares e formais do desempenho do contrato de serviço. Se necessário, podem ser realizados acordos sobre planos de ação, remediações e revisão do contrato de serviço existente para quaisquer problemas de desempenho ou tendências negativas.

Nesta ação é gerado um documento consolidando todo o monitoramento e análise, avaliação, documentações, e relatórios do processo administrativo que por sua vez servirá de insumo para o gerenciamento dos registros da terceirização, no processo de gerenciamento da terceirização.

Desta forma, finaliza-se a apresentação do mapeamento de todos os processos do macroprocesso de governança da terceirização de TI, bem como sua descrição, apresentação dos envolvidos e resultados gerados.

6.9 Validação do novo processo proposto

Com intuito de validar a viabilidade de implantação do mapeamento do novo processo de terceirização de TI no contexto do IDP, foram realizadas reuniões, onde o novo processo proposto foi apresentado, atividade por atividade de forma descritiva. Após a apresentação de cada uma das fases do processo foi feita uma pausa para captar a percepção dos participantes quanto ao que foi apresentado.

A primeira reunião ocorreu com o gestor de Organização e Método e em seguida com o financeiro, de forma individual, e a duração de ambas as reuniões foi de 40 minutos. Não houve nenhuma solicitação de alteração ou adaptação do processo.

Apenas foi destacado pelo gestor de Organização e Método a necessidade de aplicação do processo para o entendimento de seu funcionamento prático na instituição. Outro ponto levantado pelo gestor foi a imprescindibilidade de atualização constante do processo, em acompanhamento às mudanças internas da instituição. A reunião seguinte teve uma duração de 50 minutos e ocorreu com o gestor de TI da instituição. A percepção do processo apresentado foi muito positiva, sem pontos de ajustes solicitados.

Ao ser finalizada a apresentação do processo, o participante expressou grande interesse em iniciar a implantação do processo o quanto antes, pois ele estruturava de forma clara as atividades e papéis envolvidos, o que ainda não está estruturado no IDP.

A última reunião ocorreu com o representante da área solicitante, que está alocado atualmente na unidade acadêmica da pós-graduação *stricto sensu*. A reunião teve duração de 38 minutos, na qual foram apontados dois ajustes. O primeiro ajuste solicitado foi no momento em que é decidido que a terceirização seria renovada, onde o processo iniciava novamente no gerenciamento da terceirização.

Porém, o participante apontou casos em que há mudanças nas necessidades por parte da área solicitante, portanto faria mais sentido reiniciar o processo de renovação no momento da especificação das necessidades. O outro ajuste foi em função da necessidade de alinhamento das expectativas no processo de gerenciamento da terceirização.

Esta atividade deve envolver principalmente os usuários da terceirização, pois estes muitas vezes não participam do processo desde o começo, e os impactos do início do uso da terceirização precisam ser alinhados, principalmente se os usuários foram os docentes ou discentes do IDP.

Os dois ajustes solicitados não apresentaram impacto na aderência do processo mapeado com as boas práticas referenciadas, portanto estes foram incorporados no resultado final do processo, finalizando-se assim a validação do novo processo de terceirização de TI para o IDP.

6.10 Considerações finais do capítulo

Como resultado deste capítulo, foi apresentada a proposta do novo processo estruturado em todos os níveis, suas atividades descritas, artefatos e envolvidos identificados, atendendo às demandas internas e às boas práticas. Com isto é possível ter um melhor entendimento das necessidades tecnológicas para a implantação do processo de terceirização na instituição.

A partir das informações dispostas neste capítulo, inicia-se o próximo capítulo, cujo objetivo é a elicitação de requisitos do software de avaliação de riscos de processos de terceirização de TI do IDP.

Capítulo 7

Especificação da ferramenta

7.1 Considerações iniciais do capítulo

Este capítulo apresenta os resultados da execução dos dois últimos ciclos do estudo de caso, visando atender o último objetivo específico definido "*Elicitar os requisitos de software de avaliação de riscos de processos de terceirização de TI*".

No quarto e penúltimo ciclo, foram realizadas a pesquisa bibliográfica e documental para identificação de ferramentas de gestão de riscos que tenham adesão às necessidades do novo processo de terceirização de TI proposto para o IDP, alinhado às boas práticas de gestão de riscos e terceirização de TI, conforme apresentado na Figura 7.1:

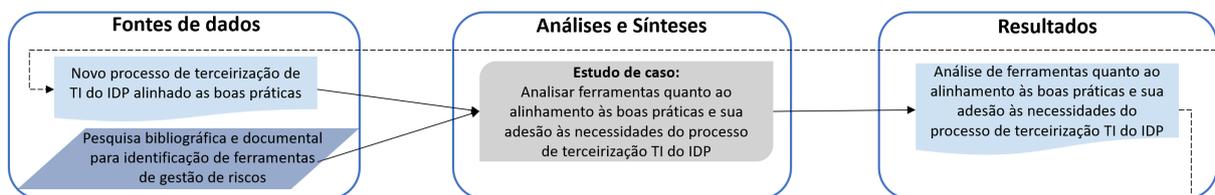


Figura 7.1: Quarto ciclo do estudo de caso. Fonte: autora

No último ciclo, apresentado na Figura 7.2, a partir da análise realizada das ferramentas existentes e do novo processo de terceirização de TI do IDP, alinhado às boas práticas, o objetivo buscado foi o de especificar os requisitos de uma ferramenta que tenha adesão à avaliação de riscos do processo de terceirização do IDP.

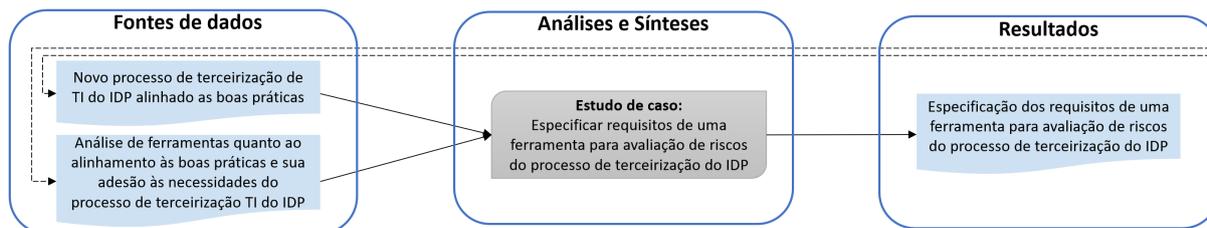


Figura 7.2: Quinto e último ciclo do estudo de caso. Fonte: Autora

7.2 Planejamento das atividades

As atividades relatadas nesse capítulo foram resultado de um projeto realizado dentro disciplina de Projeto de Sistemas de Produção 2 (PSP2), do Curso de Graduação em Engenharia de Produção EPR/FT/UnB. A disciplina tem como objetivo realizar o planejamento de um projeto de software, com ênfase na disciplina de Sistemas de Informação para Engenharia de Produção. Um grupo de 5 alunos foi designado para trabalhar em conjunto com a pesquisadora deste trabalho.

O curso de Engenharia de Produção da UnB oferece desde 2012 a oportunidade de integração entre os alunos de graduação e os de pós-graduação, por meio da colaboração pesquisas de Mestrado. Esta cooperação foi realizada por meio da oferta do objeto da pesquisa do mestrando como contexto para análise de problemas de planejamento de soluções de sistemas de informação, como opção de tema para grupos de alunos dentro de um projeto de sistemas de produção.

Esses trabalhos auxiliam tanto no envolvimento dos alunos de graduação com temas relevantes e oportunos para o entendimento de sistemas de informação, quanto possibilitam que pesquisadores do PPCA contem com o apoio dos alunos no desenvolvimento de artefatos da engenharia de software para a prototipação de ferramentas computacionais, podendo contribuir com um resultado mais aplicado de sua pesquisa.

As entregas foram alinhadas e refinadas entre os alunos, a pesquisadora e os orientadores, e organizadas visualmente por níveis hierárquicos, formando blocos de entregáveis do projeto, gerando uma Estrutura Analítica do Projeto (EAP), apresentada na Figura 7.3.

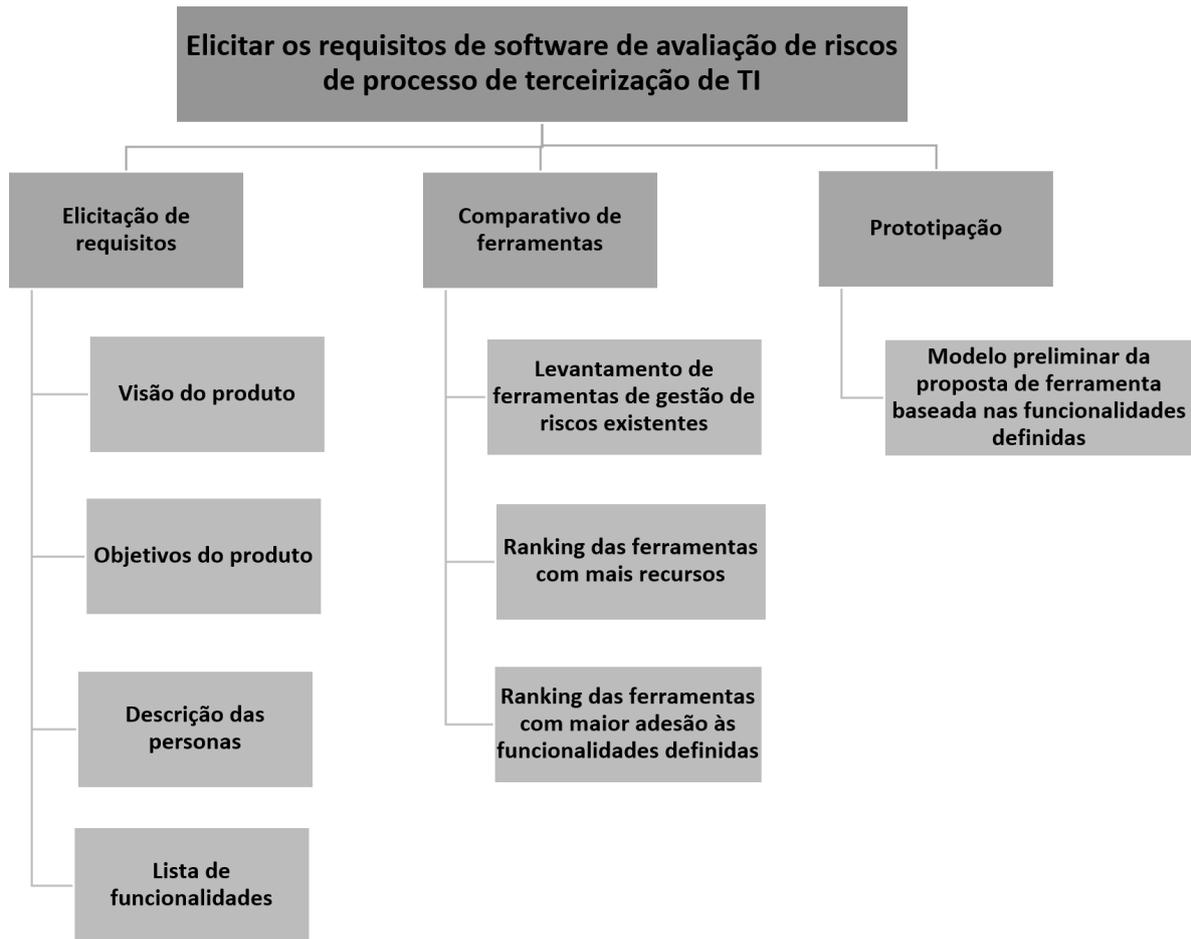


Figura 7.3: EAP do Projeto de PSP2. Fonte: Autora

A metodologia de trabalho dos alunos que formaram o "Grupo 1" da disciplina de PSP2 foi baseada em metodologias ágeis, com no mínimo 2 encontros semanais, a fim de garantir o alinhamento constante entre as partes, bem como a manutenção de uma solidez de entregas e validações constantes, conforme proposto na metodologia de pesquisa-ação. Os encontros foram realizados por pela plataforma de reuniões *Microsoft Teams*[109], devido à situação de pandemia que restringe os encontros presenciais.

A contribuição dos alunos ocorreu no tempo da disciplina, o início da interação entre a pesquisadora e os alunos, e se iniciou no dia 17/08/2021 com a apresentação da proposta da pesquisa. O projeto finalizou com a entrega e apresentação dos resultados, no fim da disciplina, que ocorreu no dia 26/10/2021. O trabalho foi avaliado e validado por uma banca avaliadora composta por professores da disciplina de Projeto de Sistemas de Produção 2 (PSP2) e Sistemas de Informação para Engenharia de Produção (SIEP).

De posse de todos os resultados obtidos e consolidados no documento de visão, que pode ser visto no *Apêndice A*, a pesquisadora realizou o refinamento para inclusão nos registros escritos na pesquisa.

7.3 Análise de ferramentas existentes

A primeira atividade foi buscar uma quantidade significativa de ferramentas de gestão de riscos, bem como suas especificações, funcionalidades e informações, a fim de realizar uma análise e refinamento inicial dos requisitos. Para tanto, a equipe aproveitou o levantamento realizado no Capítulo 2 sobre as ferramentas de gestão de riscos, juntamente com as informações disponibilizadas pelos sites utilizados para as pesquisas de revisão bibliográfica, *GetApp* [12], *SourceForge* [13] e *Capterra* [14], resultando na coleta de informações das 24 diferentes ferramentas identificadas. As informações sobre as ferramentas, disponibilizadas pelos sites de busca, foram extraídas e transformadas em 45 categorias de softwares, listadas a seguir:

- Gestão de risco de TI;
- Gerenciamento de serviços e objetivos de negócios;
- Obrigações de contrato / gerenciamento de métricas;
- Pesquisas de satisfação;
- Gerenciamento de reuniões;
- Gerenciamento de riscos e problemas;
- Relatórios e painéis;
- Fluxos de trabalho e os relatórios são automatizados;
- Única plataforma;
- Versão Mobile;
- Versão Gratuita;
- Assistência/ Consultoria;
- Interface simples, sem precisar de treinamento;
- Treinamento;
- Versão Web;
- *Buy Side* (fornecedores)/Gestão de fornecedores;
- Rastreamento de Conclusão;
- Gestão do ciclo de vida do contrato;
- Assinatura Eletrônica;

- Pesquisa de Texto Completo;
- Contratos Governamentais;
- ESG/ *Compliance*;
- Modelos pré-construídos;
- Lado de vendas (clientes);
- Contratos Especiais;
- Controle de versão;
- Gestão de fluxo de trabalho;
- Alertas/notificações;
- Controle do andamento;
- Rastreamento de conformidade;
- Relatórios e análise de dados;
- Análise de painel de detalhamento em tempo real, análise de tendências e análise comparativa;
- Monitoramento do progresso da avaliação e remediação do controle e a conclusão da tarefa em tempo real;
- Altamente/totalmente personalizável;
- *Third party*;
- Auditoria;
- Acompanhamento de despesas;
- Armazenamento de documentos;
- Controles de acesso ou permissões;
- Relatórios personalizáveis;
- Colaboração em equipe;
- Controle de processos de aprovação;
- Gestão de avaliação;
- Conformidade com os padrões ISO;

- Código Aberto.

Estas categorias foram utilizadas para realizar um comparativo inicial entre as ferramentas. O resultado da análise de cada ferramenta à luz das categorias foi binário: contém ou não contém. Por exemplo, categoria "Pesquisa de satisfação", se a ferramenta analisada apresenta, receberá a pontuação 1, se não, receberá 0. Ao final da análise cada ferramenta teve como resultado a soma da quantidade de categorias funcionais que apresenta. O consolidado das análises é apresentado na Figura II.1 presente no *Anexo II*. Portanto, quanto maior sua pontuação, mais funcionalidades a ferramenta tem. O resultado do comparativo gerou a seguinte ordenação apresentada na Tabela 7.1:

Tabela 7.1: Ordenação e pontuação das ferramentas por categorias. Fonte: Autora

Ordem	Ferramenta	Pontuação
1°	Donesafe	29
2°	Risk/Secure Watch	29
3°	TRAC governance cloud	29
4°	Módulo Risk Manager	29
5°	A1 Tracker	26
6°	Onspring	25
7°	Fusion Framework System	24
8°	INTERISK	22
9°	FORM Opx	22
10°	Resolver	21
11°	ZenGRC	19
12°	IBM OpenPages	17
13°	FLOWTI	17
14°	Soft e1pert	14
15°	SoftE1pert ERM	13
16°	Portal ISO	9
17°	Riskid	8
18°	SimpleRisk	7
19°	Eramba	7
20°	RA Risk Coverage Software	7
21°	PTA Professional	7
22°	Open Source Risk Engine	6
23°	OpenVAS	5
24°	Project Risk Manager	5

Dos resultados apresentados acima, foram extraídas as 10 primeiras soluções com melhor colocação: *Donesafe; Risk/Secure Watch; TRAC governance cloud; Módulo Risk Manager; A1 Tracker; Onspring; Fusion Framework System; INTERISK; FORM Opx e; Resolver*. Esta seleção inicial foi realizada a fim de restringir a abrangência da segunda análise que seria realizada, dada sua complexidade.

Feita a primeira seleção, as 10 ferramentas precisaram ser comparadas quanto a adesão às boas práticas, assim como a extração das boas práticas no *capítulo 4*, que serviu de insumo para a proposta do novo processo de terceirização de TI para o IDP apresentado no *capítulo 6*. As práticas extraídas do COBIT, bem como seus respectivos pesos, foram novamente utilizados. Desta forma, cada ferramenta seria analisada e comparada à luz das boas práticas, gerando assim uma ordenação, apresentando as que mais de aderem às necessidades propostas.

Para a análise das ferramentas foi utilizado como parâmetro a Tabela 4.3 com o peso de cada prática, suas respectivas fases, e atividades e descrições associadas. Tendo em vista que as ferramentas analisadas são de uso privado, a pesquisadora juntamente com os alunos de Projeto de Sistemas de Produção 2 (PSP2) entraram em contato com os fornecedores e fabricantes explicando o intuito da pesquisa e solicitando um acesso teste para a realização da análise.

Porém não obteve-se resposta de nenhum dos responsáveis pelas ferramentas. Portanto cada ferramenta foi analisada por meio do uso das informações contidas nos sites [12] [13] [14] citados acima, bem como seus guias e manuais disponibilizados nos sites das próprias ferramentas, referenciados no capítulo 2.

A comparação feita entre ferramentas em relação às práticas, resultou na Figura II.2 apresentada no *anexo II*. A ordenação resultante do comparativo é apresentada na Tabela 7.2.

Tabela 7.2: Ordenação e pontuação das ferramentas por prática adotada. Fonte: autora

Ordem	Ferramenta	Pontuação
1°	Onspring	472
2°	Resolver	466
3°	Donesafe	463,5
4°	A1 Tracker	457
5°	Risk Watch	454,5
6°	Módulo Risk Manager	449
7°	FORM OpX	419,5
8°	TRAC governance cloud	400
9°	INTERISK	336
10°	Fusion Framework System	238

É possível observar que a pontuação mudou a ordenação das ferramentas, logo, a ferramenta que apresenta maior quantidade de recursos não necessariamente é a ferramenta que está mais aderente às boas práticas. Mesmo com um resultado promissor da ferramenta com melhor pontuação *Onspring*, que apresenta um total de 472 pontos, quando comparado ao total de pontos das práticas (609,5 pontos) ela ainda tem uma defasagem de adesão de mais de 20% (ou seja de 137,5 pontos).

Portanto, a análise das ferramentas resultou na necessidade clara da proposta de uma ferramenta específica para o contexto que atenda o processo de avaliação dos riscos e terceirização de TI. Para isto, foi apresentada na próxima seção a elicitação dos requisitos desse software que está sendo proposto aqui.

7.4 Elicitação dos requisitos de software de gestão de riscos no processo de terceirização de TI do IDP

Para fins de elicitação de requisitos, foram utilizados como insumos a análise das ferramentas quanto ao alinhamento com as boas práticas e o novo processo de terceirização de TI do IDP, também alinhado com as boas práticas. Dado que as informações utilizadas para a elicitação são resultantes da pesquisa, o levantamento de requisitos foi um trabalho realizado em conjunto com os alunos de PSP2 e a pesquisadora, sem o envolvimento da equipe do IDP.

O objetivo final dessa elicitação foi o de descrever a visão geral do software, seus objetivos, características, usuários, e uma lista de requisitos funcionais. De forma que se possa ter um entendimento geral do software e obter insumos suficientes para a sua

prototipação. Buscou-se então uma forma de realizar a elicitação focando no valor vindo dos objetivos de negócios e das necessidades do IDP de forma rápida e objetiva, dado o tempo limitado da pesquisa.

O *Lean Inception*, é uma técnica de design de produto que surgiu como uma solução, por ser uma proposta disruptiva que tem ganhado força na comunidade da Engenharia de software. Essa proposta, de autoria de Paulo Caroli [11], apresenta um conjunto de técnicas que tem como objetivo a construção de um produto mínimo viável.

No contexto da TI, o produto mínimo viável pode ser entendido como um conjunto inicial de funcionalidades formando uma versão simplificada de um dado produto, para validação de hipóteses e aprendizagens sobre o negócio[11].A escolha se mostrou adequada neste trabalho pois o estilo *Lean* tem dois pontos fortes que atendem o contexto da pesquisa. Tem uma duração menor e deve eliminar tudo que não tem relação direta com o produto, e busca como resultado final a compreensão de um produto mínimo viável, *Minimum viable product* (MVP), que atenda às necessidades levantadas [11].

É importante ressaltar que o conjunto de técnicas tem como objetivo realizar o alinhamento sobre o produto mínimo viável para um grupo de pessoas, focado apenas no entendimento necessário para a construção de um dado produto [11].

Em sua proposta, Caroli[11] apresenta uma sugestão de uma lista de técnicas/atividades dispostas ao longo de uma semana, conforme apresentado na Figura 7.4. Porém deixa claro que é uma sugestão, um exemplo, e que cada analista pode fazer escolhas e variar as técnicas conforme a necessidade.



Figura 7.4: Exemplo agenda do *Lean Inception*. Fonte: [11]

Além das atividades apresentadas no exemplo de agenda, o autor também apresenta no seu livro[11] as técnicas: Esclarecendo o objetivo e entendendo os *trade-offs*.

As técnicas citadas organizam as ideias e os recursos, e sua execução permite que a equipe, a partir de técnicas e atividades ágeis e eficazes [11], realizem as entregas, conforme apresentado na Tabela7.3.

Tabela 7.3: Técnicas do *Lean Inception* e seus resultados. Fonte: [11]

Técnica	Resultado
Visão do produto	Descrição da visão do produto
Produto É - NÃO É - FAZ - NÃO FAZ	
Objetivos do produto	Priorização dos objetivos
<i>Personas</i>	Descrição dos principais usuários, seus perfis e suas necessidades
Lista de funcionalidades	Principais funcionalidades exploradas
Revisão técnica, de <i>User experience</i> (UX), ou experiência do usuário, e de negócio	Compreensão dos níveis de incerteza, esforço, valor para o usuário e valor de negócio por funcionalidade
<i>Trade-offs</i>	
Jornada dos usuários	Descrição da jornada de cada usuário
Sequenciador de funcionalidades	Plano de entrega incremental do produto, impulsionado pelo conceito do produto mínimo viável
CANVAS MVP	

Após realizar um estudo das técnicas, seus resultados associados, o contexto e o objetivo desta pesquisa foram selecionados. Tendo em vista que os resultados esperados foram a descrição da visão do produto, priorização dos objetivos, descrição dos principais usuários, seus perfis e necessidades e principais funcionalidades do sistema, as seguintes técnicas foram selecionadas: visão do produto; o produto É - NÃO É - FAZ - NÃO FAZ; objetivo do produto; descreva *personas* e; *brainstorming* de funcionalidades.

Devido à dificuldade de encontros presenciais devido a divergência de agendas dos participantes, foi decidido que a execução das técnicas seriam feitas durante as 2 reuniões semanais programadas, portanto, o tempo para sua realização foi de 2,5 semanas, tendo em vista que foram selecionadas 5 técnicas.

Para a realização das técnicas, o grupo junto com a pesquisadora, utilizou, como mencionado antes, a plataforma *Microsoft Teams*[109], como meio de comunicação, juntamente com o *Miro*[110], como ambiente de interação, que é uma plataforma de colaboração visual, que permite a realização das técnicas de forma colaborativa entre os participantes.

Assim, por meio da definição das técnicas, a agenda dos encontros e as plataformas de apoio, o *Lean Inception* foi iniciado. A explicação de cada técnica bem como sua aplicação na pesquisa e seus resultados, estão apresentados nas seções a seguir.

7.4.1 Visão do produto

Ter uma visão clara e unificada do produto define a essência do seu valor de negócio. Portanto esta é a primeira técnica realizada. Para tanto, foi disponibilizado um template para que cada participante preencha as lacunas de respostas individualmente, buscando uma percepção deles sobre a visão do produto. Feito isso, o resultado de cada participante foi apresentado e realizado um trabalho em conjunto unificando os *post-its*, gerando uma visão única do produto.

O resultado pode ser observado na figura 7.5.

VISÃO DO PRODUTO

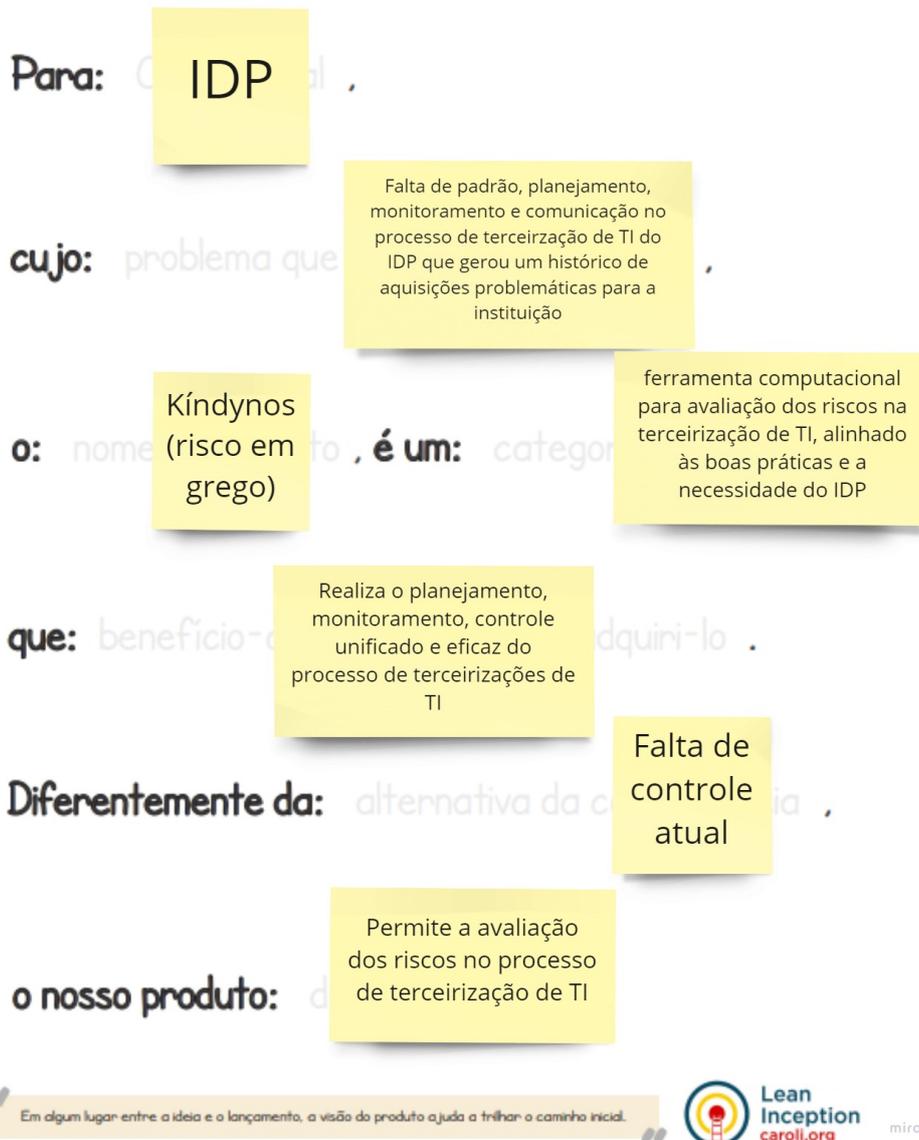


Figura 7.5: Visão do produto. Fonte: autora

O preenchimento dos campos pelos participantes não apresentaram muita divergência, mostrando que o alinhamento inicial do projeto teve grande impacto no alinhamento das informações. O único ponto discutido foi a lacuna sobre como deveria ser denominado o sistema em questão. Após votação foi escolhido o nome *Kíndynos*, versão grega da palavra "risco".

7.4.2 O produto É - NÃO É - FAZ - NÃO FAZ

A partir da ajuda na definição e do alinhamento da visão do produto, foi realizada a técnica de É - Não é - Faz - Não faz. Nela, o produto é classificado de forma a esclarecer mais o entendimento do produto. Assim como na técnica anterior, foi disponibilizado um *template* com os quatro quadrantes para que cada participante preenchesse de forma individual.

Foi dada a orientação de que os quadrantes referentes do "É" e "NÃO É" deveriam ser preenchidos com substantivo ou adjetivo, a fim de caracterizá-los. Já nos quadrantes "FAZ" e "NÃO FAZ" deveriam ser preenchidos com verbos indicando ações da ferramenta. Depois que todos preencheram os quadros, foi realizado o mesmo procedimento da técnica anterior, em que cada quadrante de cada participante foi apresentado e unificado, resultando em um quadro único mostrado na Figura 7.6.



Figura 7.6: Definição de é/não é, faz/não faz. Fonte: Autora

7.4.3 Objetivos do produto

Com o fechamento do entendimento da visão do produto, foi iniciado o entendimento de seus objetivos. Para a execução dessa técnica, foi solicitado que cada participante respondesse, de forma individual, a seguinte pergunta "Se você tiver que resumir o produto em três objetivos para o negócio, quais seriam eles?".

Quando todos os participantes finalizaram, as respostas foram expostas e agrupadas por similaridade. Depois disso foram escritos 3 objetivos que representassem todas as respostas. Os grupos de respostas que se mostraram muito divergentes dos objetivos principais escritos foram descartadas. Portanto o resultado é apresentado na Figura 7.7.

Se você tiver que resumir o produto em três objetivos para o negócio, quais seriam eles?

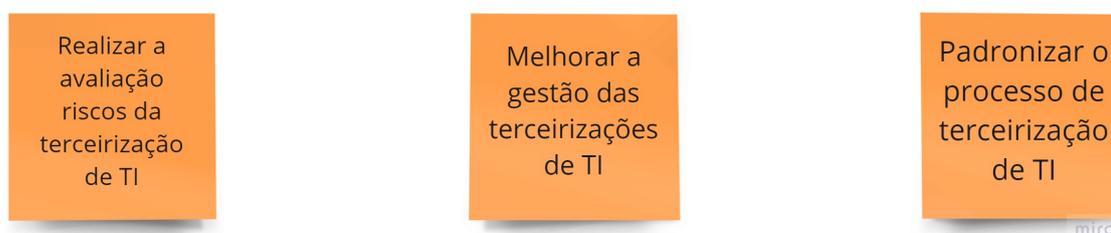


Figura 7.7: Definição dos objetivos do produto. Fonte: Autora

Com mais essa técnica, o entendimento dos objetivos do negócio foi alinhado, sendo possível chegar a um consenso entre os participantes sobre o que de fato é importante para o produto.

7.4.4 Técnica descreva *personas*

Esta técnica é utilizada para realizar a definição dos usuários do sistema e seus principais objetivos. Já que uma *persona* representa um perfil de usuário do produto ou serviço, é possível ter um entendimento do produto do ponto de vista de quem irá interagir diretamente com ele.

Para a realização desta técnica, foi solicitado que cada participante selecionasse um usuário do produto, e para essa seleção foi utilizado o desenho do macro processo onde os envolvidos já estavam definidos. Feito isso, cada participante apresentou a *persona* do produto que escolheu, descrevendo seu perfil e suas necessidades. Após a apresentação, a *persona* foi analisada pelo grupo a fim de preencher um quadro com sua identificação, perfil, comportamento e necessidades. Depois de realizar esta ação com todos os parti-

cipantes, as personas semelhantes foram unificadas e o resultado final foram 4 quadros apresentados na Figura 7.8.

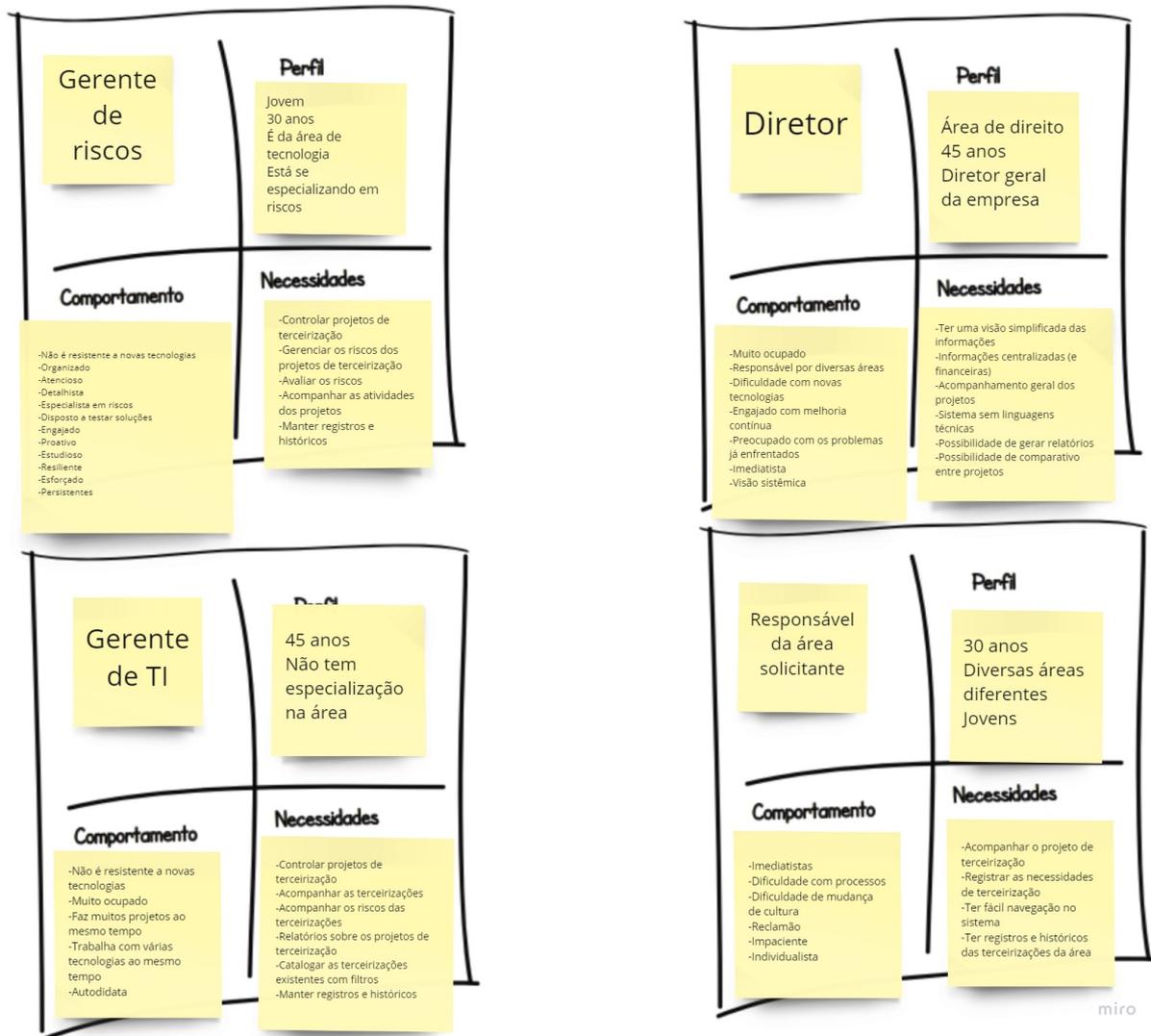


Figura 7.8: Definição das personas. Fonte: autora

É importante ressaltar que Caroli[11] enfatiza que o resultado dessa atividade não deve ser definitivo e sim atualizado e adaptado juntamente com a evolução do produto, principalmente depois do *feedback* sobre ele, pois é possível aprimorar a compreensão das personas envolvidas.

7.4.5 Técnica de *brainstorming* de funcionalidades

Por fim, a última atividade realizada foi a do *brainstorming* de funcionalidades. O entendimento de funcionalidades da solução neste contexto está associado a uma ação ou interação de um usuário com o produto em questão, onde sua descrição deve ser a mais

sucinta e direta possível. Sua realização consiste em dispor visualmente a definição dos objetivos elaborada e a descrição das personas juntamente com o novo processo de terceirização de TI do IDP.

Feito isso, foi realizado um *brainstorming* entre os participantes, guiado pelas perguntas *O que deve ter no produto para atender às necessidades da persona? Quais funcionalidades devemos construir para atingir esse objetivo do produto?*. As perguntas foram repetidas diversas vezes até se elencarem todas as necessidades das *personas* e de modo que todos os objetivos definidos fossem atendidos, resultando na Figura 7.9.



Figura 7.9: Definição das funcionalidades. Fonte: Autora

Ressalta-se que cada necessidade e objetivo podem gerar mais de uma funcionalidade atribuída, como também podem haver *personas* que não apresentam a necessidade de uma funcionalidade específica associada. As funcionalidades, depois de identificadas, foram organizadas, ordenadas e descritas em um trabalho em conjunto dos alunos com a pesquisadora, conforme apresentado na Tabela III no *anexo III*. A lista de funcionalidades foi posteriormente refinada pela pesquisadora, resultando assim na lista final apresentada na Tabela 7.4.5 a seguir.

Tabela 7.4: Funcionalidades identificadas e descritas

ID	Nome	Descrição
----	------	-----------

Tabela 7.4 – *Funcionalidades identificadas e descritas*

ID	Nome	Descrição
RF001	Cadastrar os projeto de terceirização	Cadastro de todas as informações da terceirização, desde a solicitação, como área solicitante, responsável, descrição da necessidade, negócios e funções associados, serviços impactados, e outras informações relevantes para a contextualização da terceirização de TI
RF002	Manter status do projeto de terceirização	Manter o status do projeto de terceirização de TI de acordo com andamento do processo
RF003	Adicionar/editar ou excluir informações do projeto	As informações do projeto podem ser adicionadas, editadas ou excluídas
RF004	Gestão de Fornecedores	Permite fazer a avaliação, acompanhamento, manter histórico dos fornecedores.
RF005	Associar fornecedor com projeto de terceirização	Realizar a associação dos fornecedores cadastrados com os projetos de terceirização cadastrados
RF006	Anexar documentos aos projetos	possibilidade de anexar documentos externos no projeto de terceirização
RF007	Manter listas de soluções alternativas em projetos	Permite salvar uma lista alternativas de soluções para as demandas de terceirização.
RF008	Cadastrar riscos da terceirização	Cadastrar todos os riscos identificados na terceirização
RF009	Avaliar e analisar os riscos do projeto de terceirização	Permite ao usuário classificar todos os riscos envolvidos no processo de terceirização, avaliando o risco em relação ao impacto do risco do desprezível ao extremo e a probabilidade dele, do raro ao muito provável.
RF010	Monitorar riscos do projeto	Permite monitorar os riscos da terceirização
RF011	Associar riscos com projetos	Os riscos cadastrados podem ser associados aos projetos de terceirização
RF012	Manter usuários	Realizar o cadastro, edição e exclusão de usuários na ferramenta
RF013	Manter permissões diferentes para cada usuário no projeto	Associar permissão de cada usuário para cada projeto
RF014	Consultar projetos de terceirização	Consultar projetos de terceirização, independentemente dos seus status

Tabela 7.4 – *Funcionalidades identificadas e descritas*

ID	Nome	Descrição
RF015	Acompanhar os projetos de terceirização	Permite o usuário acompanhar os status dos projetos de terceirização
RF016	Receber alertas sobre riscos	Emitir alertas quando sobre riscos que estão sendo monitorados
RF017	Gerar relatórios dos projetos	Emitir relatórios personalizados dos projetos
RF018	Gerar relatórios dos riscos	Emitir relatórios personalizados dos riscos
RF019	Configurar API	Permite a comunicação de serviços ou produtos sem a necessidade de saber como foram implementados, de forma que o trâmite de informação seja simplificado.
RF020	Monitorar projetos de terceirização	Permite ao usuário ter uma noção consolidada dos projetos que estão em execução pela instituição.
RF021	Monitorar riscos do projeto no processo	Monitorar riscos do projeto associados a execução das atividades do processo

Desta forma, foi finalizada a execução do *Lean Inception*, e todos os resultados necessários apontados no planejamento da sua realização foram atendidos. A partir de agora tem-se uma visão clara e unificada do produto, seus 3 objetivos principais, suas personas e por fim suas funcionalidades.

7.5 Protótipo das telas do software de avaliação de riscos da terceirização de TI no IDP

A partir da lista de funcionalidades apresentadas anteriormente, a prototipação das telas é um recurso de validação prática da estruturação inicial do software proposto. Na pesquisa atual, como a função da prototipação é a de apresentar a proposta da estrutura de um sistema de forma geral e suas funcionalidades definidas, a prototipação de baixa fidelidade atendeu tal demanda.

Uma vez que a prototipação do sistema teve como objetivo esclarecer, analisar e validar os requisitos levantados, a mesma pode ser classificada como um protótipo próprio e exploratório. Sua construção foi horizontal, tendo em vista que ela abrange todo o sistema especificando os *layouts* de suas telas. A prototipação das telas também foi realizada

em um trabalho conjunto entre a pesquisadora e a equipe de 4 alunos do "Grupo 1" da disciplina de Projeto de Sistemas de Produção 2 (PSP2) do curso de Engenharia de Produção.

A ferramenta utilizada para prototipação foi o *Miro* [110], tendo em vista a familiaridade que os alunos e a pesquisadora tinham, bem como sua facilidade de uso, sua função colaborativa e a possibilidade de utilização de um pacote da própria ferramenta denominado *Wireframe Library*, que apresenta elementos de telas para esse propósito.

O processo de prototipação ocorreu tendo como guia as funcionalidades levantadas e as práticas associadas. Por meio da realização de um trabalho em conjunto entre a pesquisadora e os alunos, as telas da ferramenta foram prototipadas e associadas a uma funcionalidade que por sua vez estava associada a uma ou mais práticas, as quais encontram-se no *anexo III*.

Esses protótipos também foram avaliados por uma banca avaliadora composto por professores das disciplinas de Projeto de Sistemas de Produção 2 (PSP2) e Sistemas de Informação para Engenharia de Produção (SIEP) como entrega final das disciplinas. Depois disso, os protótipos ainda foram refinados pela pesquisadora. Antes de apresentar os protótipos das telas, visando um melhor entendimento sobre o funcionamento do software, é apresentado, na Figura 7.10, um modelo do funcionamento do sistema.

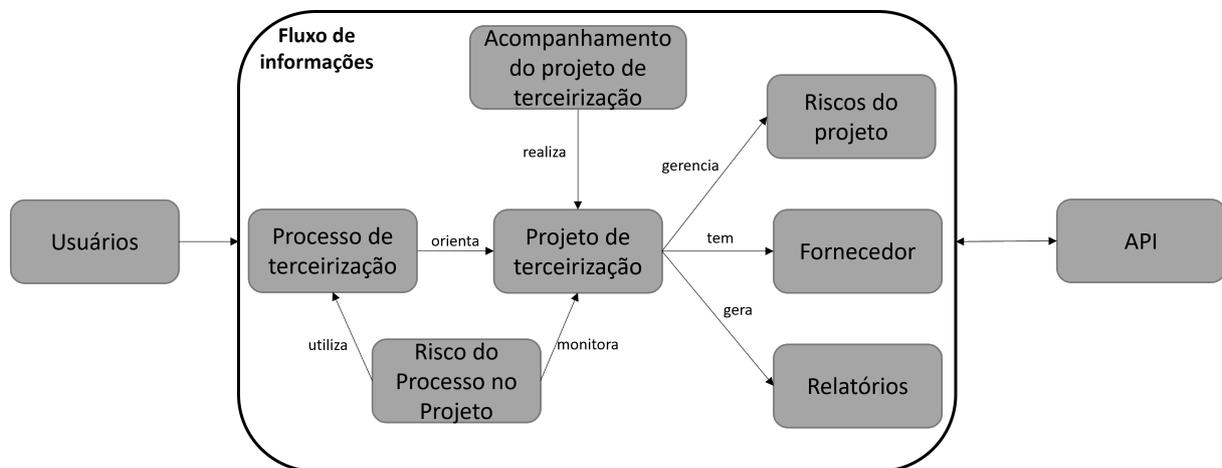


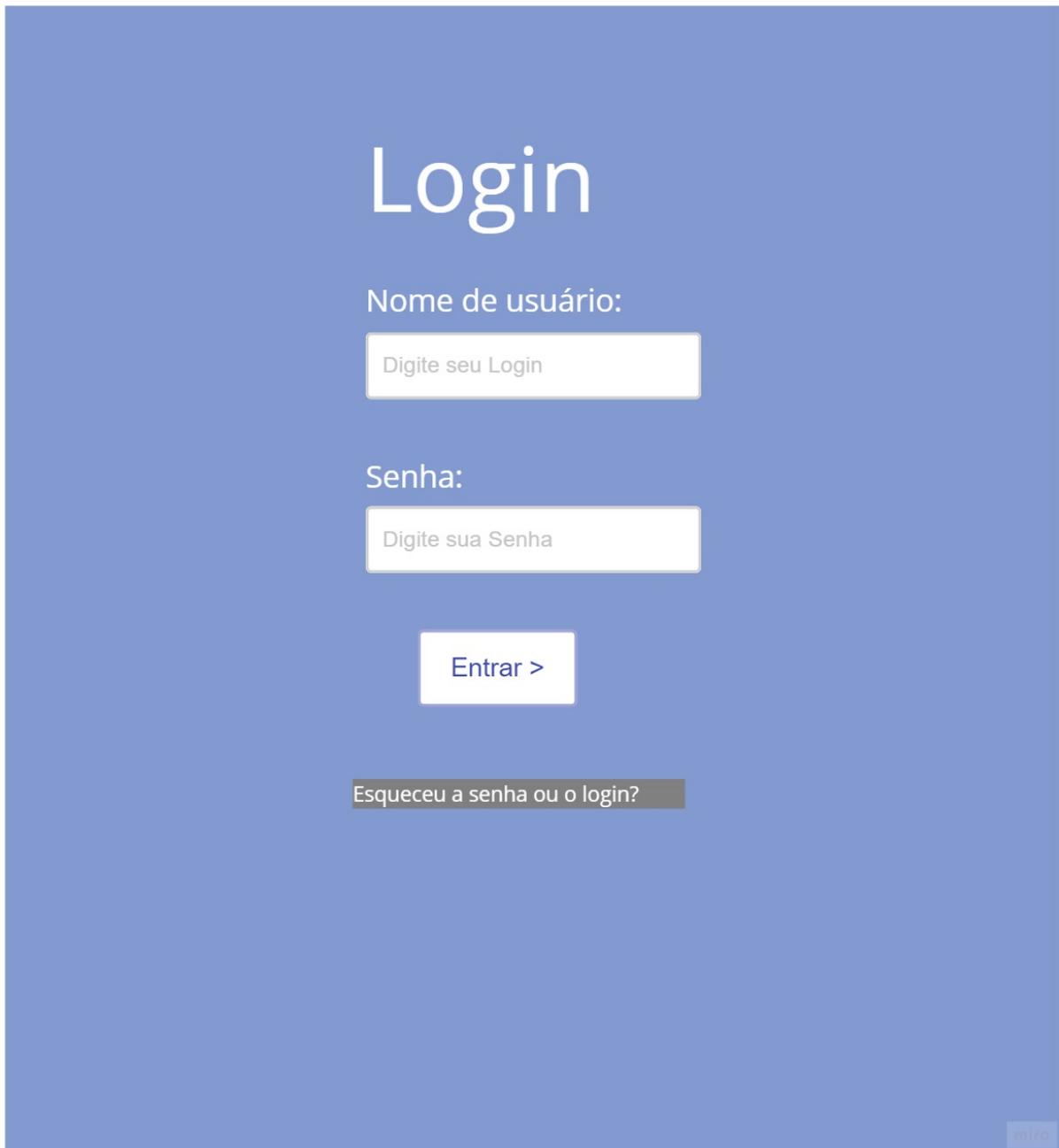
Figura 7.10: Modelagem do sistema proposto. Fonte: Autora

Como é possível observar, o centro do sistema é orbitado pelas informações do projeto de terceirização e, diferentemente das ferramentas existentes no mercado, a abordagem de riscos é dividida entre os riscos associados ao projeto específico, que seguem a execução do processo de avaliação de riscos (identificação, análise e avaliação), e os riscos do processo, que estão diretamente associados à execução das atividades extraídas das boas práticas. O sistema abarca também informações relacionadas aos fornecedores e à geração

de relatórios, além de permitir, por meio de API, integração com outras ferramentas, não limitando seu uso somente ao software sugerido.

A partir do entendimento geral dos módulos do sistema, são apresentados a seguir os protótipos das telas, bem como sua associação com as boas práticas e as funcionalidades especificadas.

A primeira tela é do Login, apresentada na Figura 7.11, onde o usuário irá acessar o sistema por meio de um nome e senha previamente registrados.



The image shows a login screen prototype with a solid blue background. At the top center, the word "Login" is written in a large, white, sans-serif font. Below this, the text "Nome de usuário:" is displayed in a smaller white font. Underneath is a white rectangular input field with rounded corners and a thin border, containing the placeholder text "Digite seu Login" in a light gray font. Below the first field, the text "Senha:" is displayed in the same white font. Underneath is another white rectangular input field with rounded corners and a thin border, containing the placeholder text "Digite sua Senha" in a light gray font. Below the second field, there is a white rectangular button with rounded corners and a thin border, containing the text "Entrar >" in a blue font. At the bottom of the form area, there is a dark gray rectangular button with rounded corners, containing the text "Esqueceu a senha ou o login?" in a white font. In the bottom right corner of the blue background, there is a small, faint white logo that appears to be "miso".

Figura 7.11: Protótipo da tela de login. Fonte: Autora

A funcionalidade associada é: *manter usuários*. A boa prática associada é: *gerenciar engajamento das partes interessadas*.

A tela seguinte, após o usuário fazer o login é a tela do menu principal, onde são apresentadas as principais funcionalidades do sistema, conforme Figura 7.12.

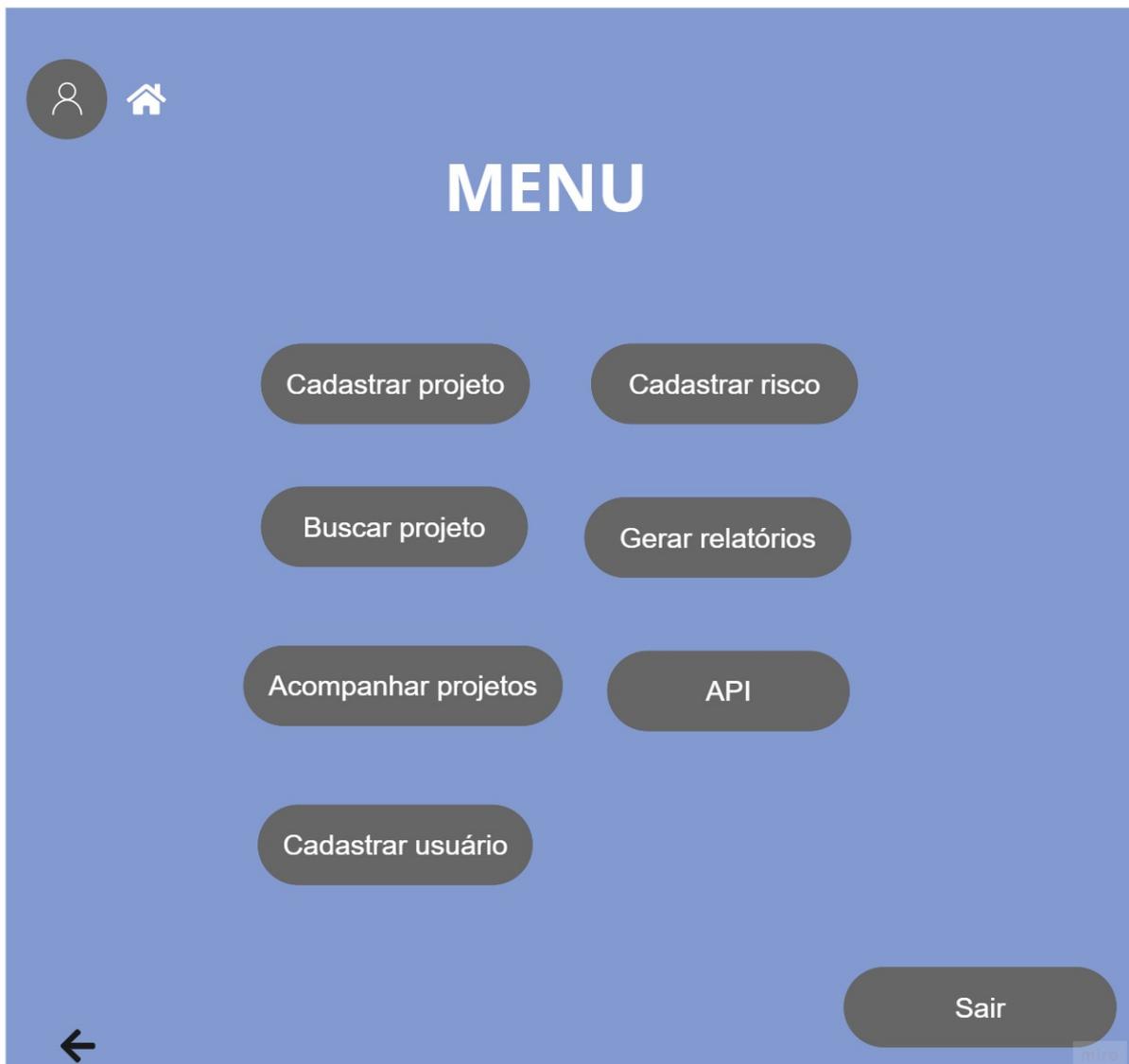


Figura 7.12: Protótipo da tela de menu principal. Fonte: Autora

A funcionalidade associada é: *manter permissões diferentes para cada usuário no projeto*. As boas práticas associadas são: *soluções de construção; gerenciar serviços terceirizados de TI; identificar serviços de TI e; iniciar e executar programa*.

A tela de cadastro dos projetos, apresentada na Figura 7.13, é a mais importante do sistema, pois é nela que serão consolidadas todas as informações referentes ao projeto de

terceirização. Cada campo representa entregáveis do processo de terceirização de TI e são agrupados para melhor visualização.

Cadastro do projeto STATUS

Nome

Descrição

Solicitação Concluído

Área solicitante ✓

Responsável ✓

Anexos

Estratégia Pendente

Negócios e funções ✓

Serviços impactados ✗

Contextualização da terceirização ✗

Termo de Abertura Pendente

Requisitos e limitações Pendente

Soluções alternativas Pendente

Riscos do projeto Pendente

Transição Pendente

Administrativo Pendente

Monitoramento da terceirização Pendente

← Encerrar Salvar Cancelar

Figura 7.13: Protótipo da tela de cadastro dos projetos de terceirização. Fonte: Autora

As funcionalidades associadas são: *cadastrar os projetos de terceirização; adicionar/editar ou excluir informações do projeto; anexar documentos aos projetos; manter lista de soluções alternativas nos projetos; associar fornecedor com projeto; manter status do projeto e; associar riscos do projeto.*

As boas práticas associadas são: *monitore o desempenho e a conformidade do fornecedor; fechar um programa; definir a política de continuidade de negócios, objetivos e escopo; avalie as capacidades atuais, desempenho e maturidade da empresa; selecione fornecedores; definir e manter o negócio funcional e técnico dos requisitos; gerenciar finanças e contabilidade; desenvolver e manter o plano do programa; monitorar e relatar os níveis de serviço; iniciar e executar um programa; gerenciar mudanças nos requisitos e; realizar um estudo de viabilidade e formular soluções alternativas.*

Na tela cadastro de fornecedores os mesmos são cadastrados e associados aos projetos de terceirização já cadastrados, conforme apresentado na Figura 7.13

Nome Add text

Responsável Add text

Contato Add text

Soluções Add text

Descrição Add text

Projetos associados

Tab 1 Tab 2 Tab 3

Quantidade de projetos encontrados: xx

← Cadastrar Cancelar

Figura 7.14: Protótipo da tela de cadastro dos fornecedores. Fonte: Autora

As funcionalidades associadas são: *gerenciar fornecedores; associar fornecedor com projeto de terceirização e; manter lista de soluções alternativas nos projetos.*

As boas práticas associadas são: gerenciar relacionamentos e contratos com fornecedores; selecione fornecedores e; identifique e avalie relacionamentos e contratos com fornecedores.

A tela apresentada na Figura 7.15 tem a função de cadastrar, ou excluir, usuários, atribuindo um perfil a eles, sendo possível assim delimitar o nível de acesso às áreas da ferramenta.

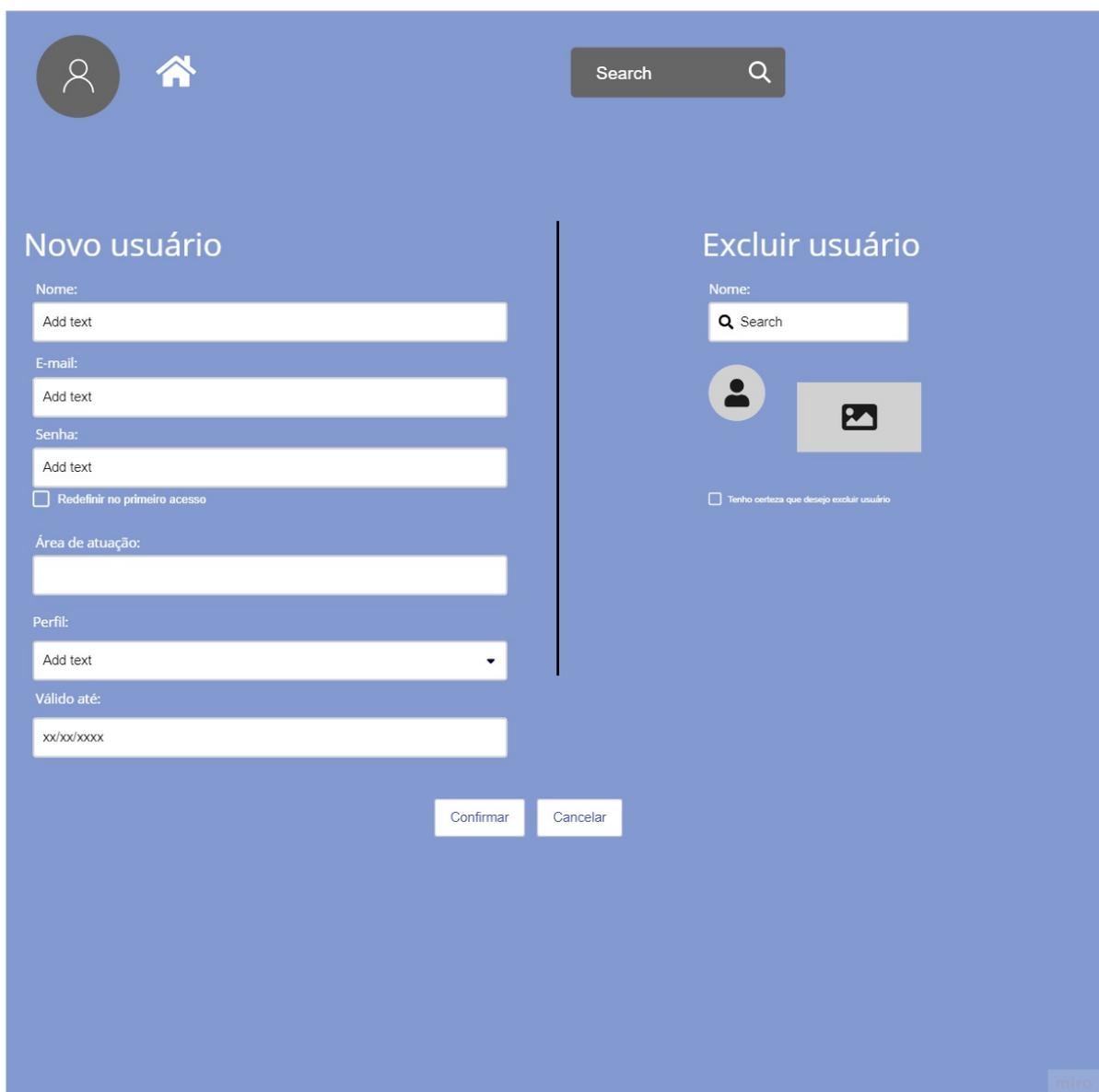


Figura 7.15: Protótipo da tela de cadastro dos usuários. Fonte: Autora

As funcionalidades associadas são: manter usuários e; manter permissões diferentes para cada usuário no projeto.

A boa prática associada é: gerenciar o engajamento das partes interessadas.

Na Figura 7.16 é apresentada a tela de cadastro e avaliação dos riscos no projeto. Aqui é importante fazer uma diferenciação entre os riscos do projeto e os riscos do projeto no processo. Os riscos do projeto, são riscos identificados, analisados e avaliados do projeto de terceirização em questão.



Figura 7.16: Protótipo da tela de cadastro e avaliação de riscos. Fonte: Autora

As funcionalidades associadas são: *cadastrar riscos da terceirização; avaliar e analisar os riscos do projeto de terceirização; associar riscos com projetos e; monitorar riscos do projeto.*

As boas práticas associadas são: *selecione fornecedores; desenvolver e manter o plano do programa e; gerenciar o risco do fornecedor.*

Para monitoramento dos riscos do projeto é apresentada a tela de monitoramento dos riscos nos projetos, Figura 7.17, informações essas que podem ser extraídas, caso necessário.



Figura 7.17: Protótipo da tela de monitorar riscos. Fonte: Autora

A funcionalidade associada é: monitorar riscos do projeto.

As boas práticas associadas são: gerenciar o risco do fornecedor e; desenvolver e manter o plano do programa.

Os riscos do projeto no processo de terceirização de TI são monitorados na tela de monitoramento dos riscos do projeto no processo, apresentada na Figura 7.18.

Esse monitoramento é referente à execução do projeto de acordo com o processo, definido conforme proposta realizada no capítulo 6, e que por sua vez apresenta o mapeamento

acompanhado por cada atividade separada por fase e as pontuações atreladas a cada uma delas, bem como um resumo da pontuação realizada e a porcentagem equivalente. Portanto, esta tela se refere à adesão do projeto ao processo de terceirização de TI definido e todas suas atividades respectivas.

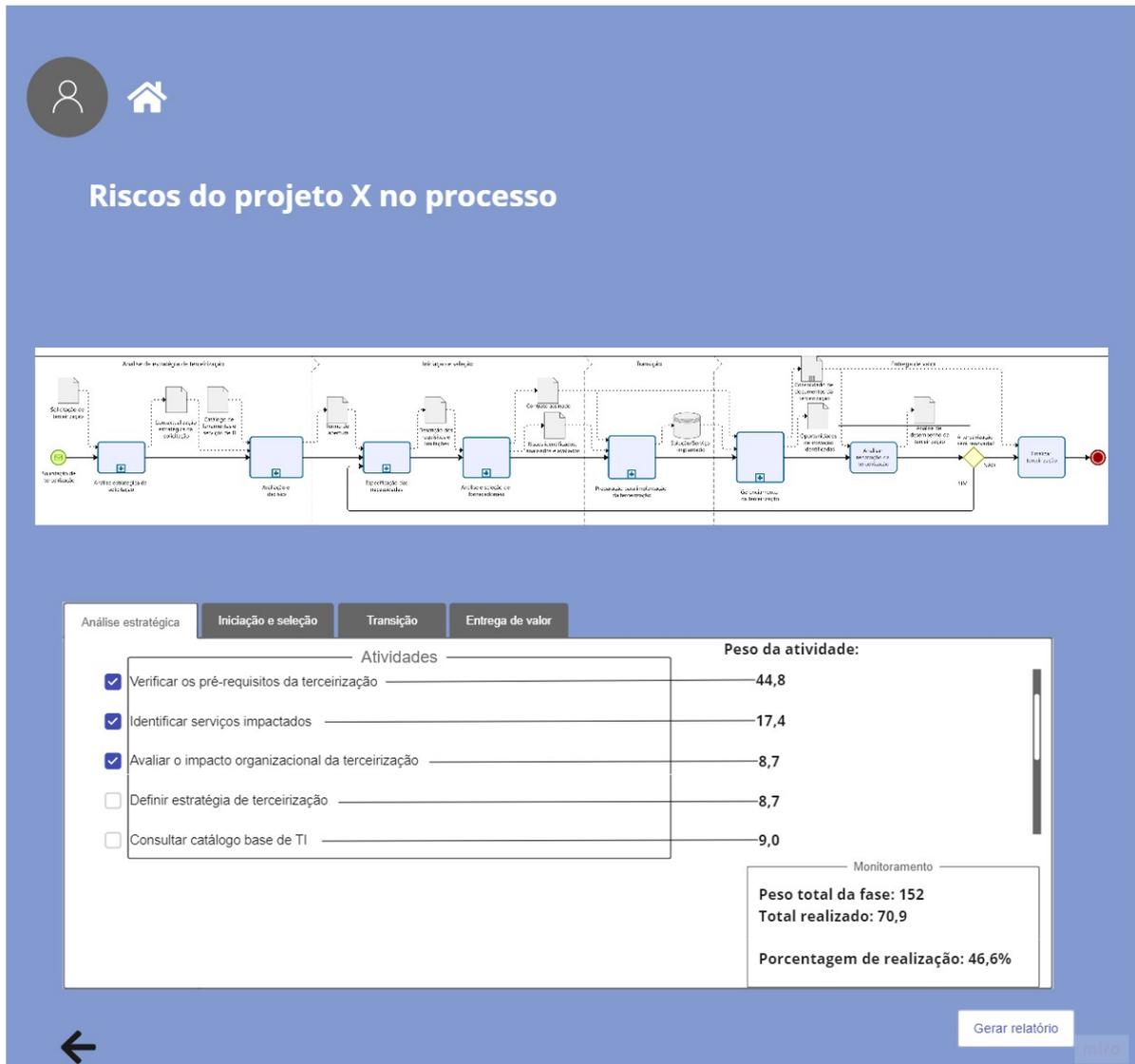


Figura 7.18: Protótipo da tela de monitoramento da execução do processo de terceirização em projetos. Fonte: Autora

As funcionalidades associadas são: *monitorar riscos do projeto no processo; monitorar projetos de terceirização; gerar relatórios dos projetos; consultar projetos de terceirização e; acompanhar os projetos de terceirização.*

As boas práticas associadas são: *gerenciar o risco do fornecedor e; desenvolver e manter o plano do programa.*

A Figura 7.19 apresenta a tela de monitoramento dos projetos de terceirização. Ela apresenta de forma resumida uma lista dos projetos de terceirização associados ao usuário, bem como os alertas de projetos em risco de execução, com base tanto nos riscos identificados para o projeto especificamente, quanto o risco de não realização das atividades extraídas das boas práticas.

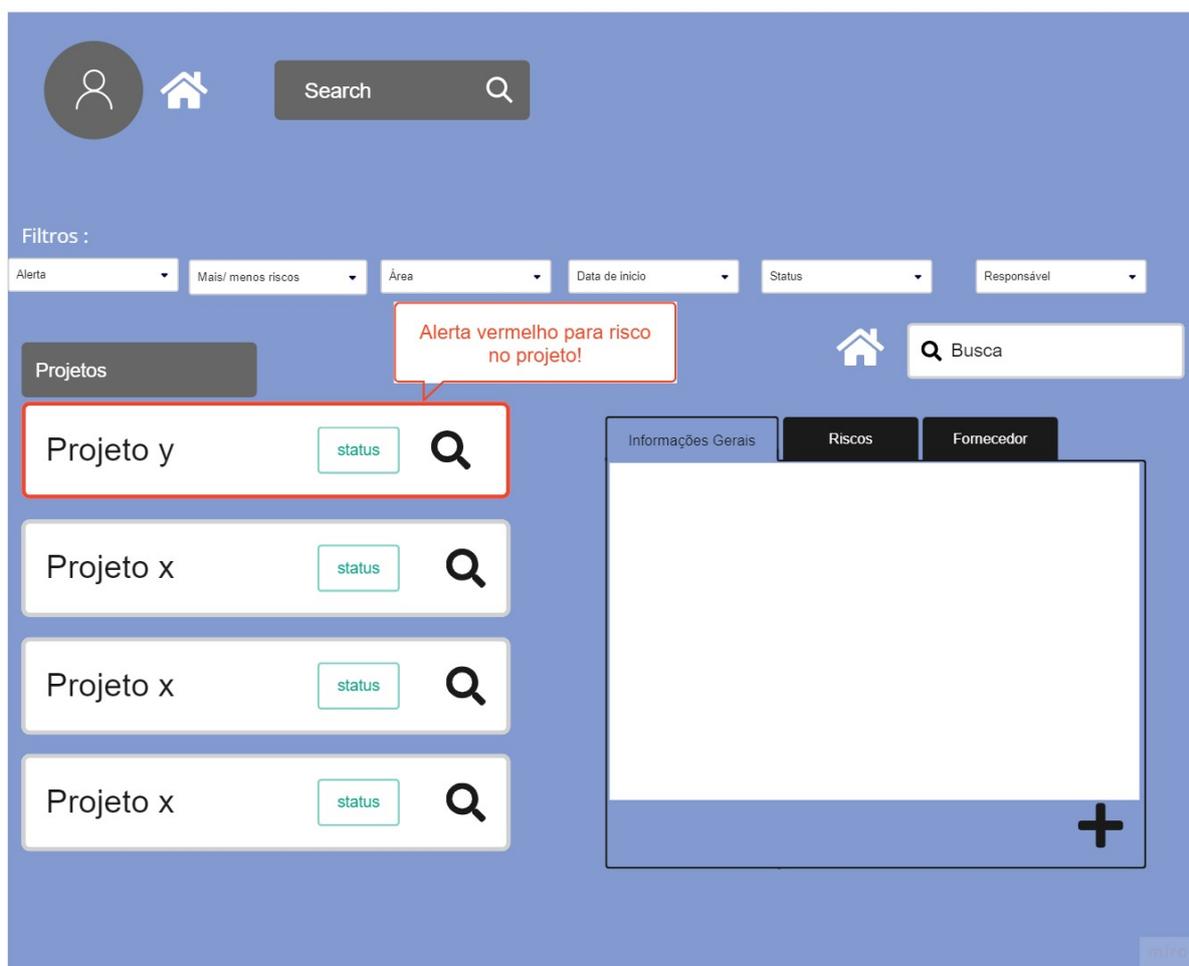


Figura 7.19: Protótipo da tela de acompanhamento dos projetos. Fonte: Autora

As funcionalidades associadas são: *monitorar projetos de terceirização; receber alertas sobre riscos e; acompanhar os projetos de terceirização.*

As boas práticas associadas são: *monitorar e relatar os níveis de serviço; definir e manter o negócio funcional e técnico dos requisitos; gerenciar serviços terceirizados de TI e; desenvolver e manter o plano do programa.*

A tela de relatórios, apresentada na Figura 7.20, é o espaço na ferramenta no qual os dados referente aos projetos, fornecedores e riscos podem ser obtidos analisados por meio

de relatórios. Os relatórios permitem fazer um cruzamentos dos dados selecionados pelos usuários.



Figura 7.20: Protótipo da tela de relatórios. Fonte: Autora

As funcionalidades associadas são: *gerar relatórios dos riscos e; gerar relatórios dos projetos.*

As boas práticas associadas são: *gerenciar o risco do fornecedor; monitore o desempenho e a conformidade do fornecedor; desenvolver e manter o plano do programa e; gerenciar serviços terceirizados de TI.*

A tela de lista de projetos de terceirização, apresentada na figura 7.21, apresenta uma lista todos os projetos de terceirização, tantos os que estão ativos quantos os que já foram finalizados, além de apresentar as informações de cada projeto.



Figura 7.21: Protótipo da tela de consultar projetos. Fonte: Autora

A funcionalidade associada é: consultar projetos de terceirização.

As boas práticas associadas são: *desenvolver e manter plano do programa; definir a política de continuidade de negócios, objetivos e escopo; monitorar o desempenho e a conformidade do fornecedor; avaliar as capacidades atuais, desempenho e maturidade da*

empresa; monitore e relate os níveis de serviço e; definir e manter o negócio funcional e técnico dos requisitos.

Por fim, a última tela apresentada na Figura 7.22 apresenta a configuração de APIs da ferramenta. Com isso o sistema pode ser integrado a outros sistemas existentes, ou pode ter suas informações extraídas para análises de dados dos projetos de terceirização de TI em outras plataformas. O propósito desta funcionalidade é permitir a interoperabilidade, a continuidade do seu uso, bem como a possibilidade de inovações e expansão de funcionalidades.

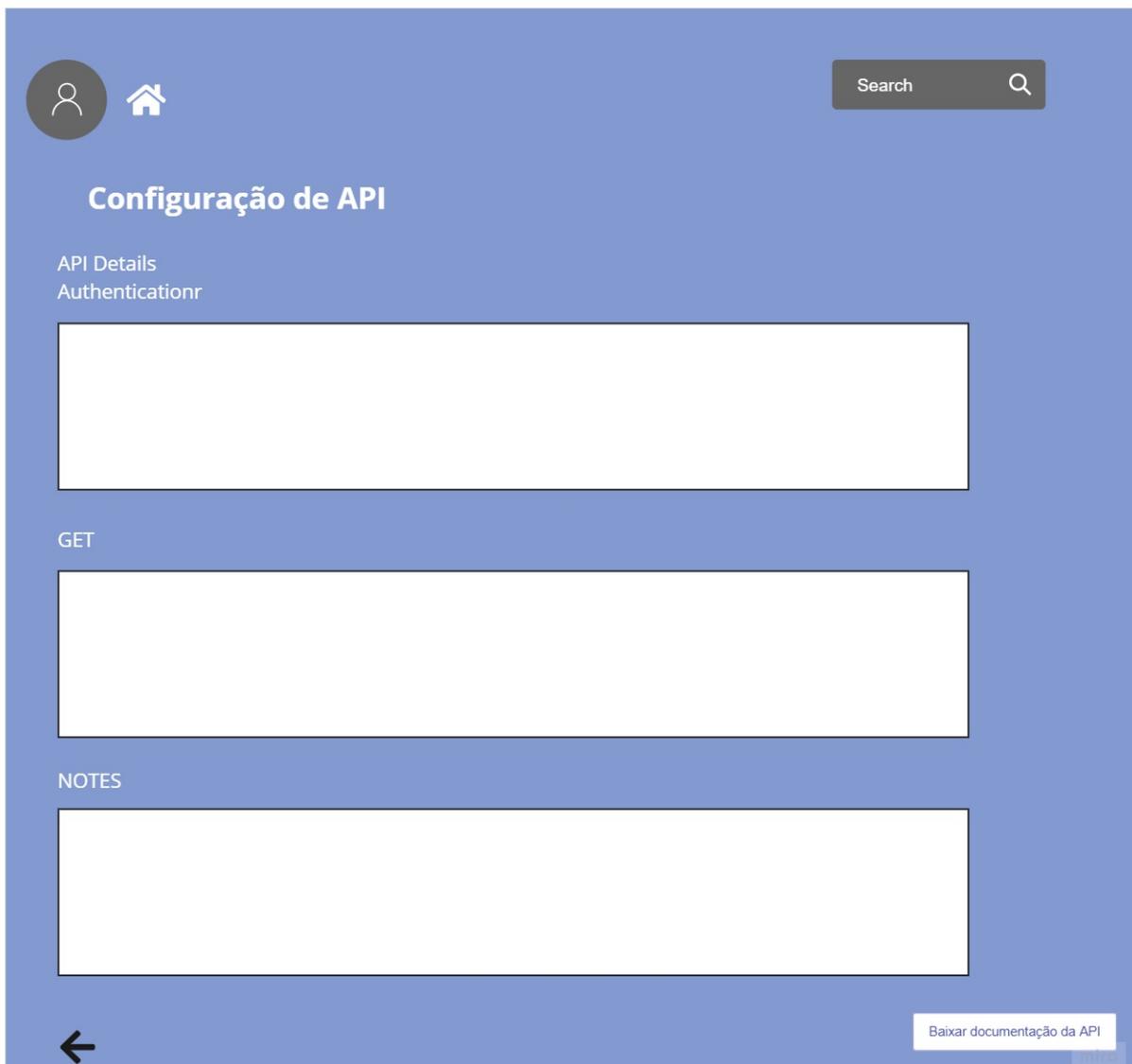


Figura 7.22: Protótipo da tela de configuração de API. Fonte: Autora

A funcionalidade associada é: configurar API.

As boas práticas associadas são: *desenvolver e implementar uma resposta de continuidade dos negócios e; crie um ambiente propício à inovação.*

Dessa forma a prototipação das telas baseadas no levantamento das funcionalidades juntamente com às boas práticas selecionadas foram finalizadas.

7.6 Validação dos resultados finais

Na busca por uma validação da sistematização do novo processo de terceirização de TI, juntamente com a viabilidade de utilização do software pela instituição, foram conduzidas reuniões com o intuito de validar as funcionalidades e as telas prototipadas do software proposto. Mantendo-se uma linearidade nas validações, os perfis selecionados para validar o resultado final da pesquisa foram os mesmos que validaram os resultados anteriores.

O gerente de TI, que é diretamente impactado pelas contratações e terá uma grande mudança nas atividades empenhadas por sua área, gerando um maior envolvimento da sua equipe. O gestor do financeiro, que apesar de não ter um envolvimento direto, é de um setor que sente os impactos econômicos que as mudanças podem trazer pra instituição como um todo. O gestor de Organização e Método, que por si é de uma área que trabalha transversalmente na instituição, e tem como uma de suas atividades o estabelecimento de processos e procedimentos internos, conforme apresentado na cadeia de valor do IDP, na Figura 5.2.

Por fim, o colaborador que trabalha na área acadêmica da pós-graduação stricto sensu, representando a área solicitante, foi selecionado pois, além de atuar diretamente com os processos finalísticos da instituição, também participou de um processo de terceirização desde seu início, levantando a necessidade até sua implantação e utilização.

As reuniões foram conduzidas via *Microsoft Teams* com os participantes citados anteriormente. Esta participação representa uma proporção de 52% do total de colaboradores envolvidos no processo de terceirização de TI para uma área específica.

A pauta da reunião consistiu em duas partes, sendo a primeira em uma apresentação da lista de funcionalidades com explicações breves de cada uma, ao final da apresentação da lista foi realizado um ponto de controle para entender se estavam de acordo com o que foi apresentado, ou tinham ajustes a serem realizados.

Na segunda parte foram apresentados os protótipos das telas juntamente com as funcionalidades listadas e as boas práticas associadas. Ao fim da apresentação de cada tela, bem como das funcionalidades e boas práticas associadas a ela, o participante tinha a oportunidade de concordar como que foi exposto ou, caso contrário apresentar os ajustes.

Uma questão levantada tanto pelo gestor de Organização e Método quanto pelo representante da área solicitante foi a necessidade de se realizar novamente a validação após

a implantação do novo processo, tendo em vista que ele pode sofrer alterações com sua aplicação prática.

A reunião com o gestor de TI teve duração de 40 minutos, com o gestor de Organização e Método foram 45 minutos, como financeiro teve uma duração de 30 e com representante da área solicitante foi um total de 45 minutos. Nenhum dos participantes apontou ajustes necessários, nem nas funcionalidades, nem nas telas prototipadas.

Desta forma, considera-se validado o resultado final da pesquisa por parte dos colaboradores que participam do processo atual de terceirização de TI do IDP.

7.7 Considerações Finais do Capítulo

Neste capítulo foram apresentados os resultados dos últimos ciclos do estudo de caso, com análise de ferramentas de gestão de riscos em relação às boas práticas de gestão de riscos e terceirização de TI, e em seguida a elicitação de requisitos da proposta de um software que atenda às boas práticas e ao novo processo de terceirização de TI do IDP, bem como a prototipação de suas telas com base nos requisitos elicitados.

Capítulo 8

Conclusão

Este trabalho discorreu sobre um projeto de software para fazer a gestão e a avaliação dos riscos da terceirizações de TI no IDP. Entende-se terceirização de TI como a transferência parcial ou total de atividades internas de tecnologia para terceiros, seja por meio de aquisição de recursos tecnológicos ou contratação de serviços [83].

Neste projeto foi alcançado o primeiro objetivo específico que visou, por meio de uma revisão de literatura e pesquisa documental, a extração de um conjunto de boas práticas, caracterizadas e ordenadas das principais referências e fontes de dados sobre terceirização de TI e gestão de riscos. Foram selecionadas boas práticas como o COBIT 5 [9], a ISO 37500 [10] e a ISO 31000 [3], e destas referências foram extraídos e consolidadas 48 atividades devidamente pontuadas e ordenadas, conforme as próprias práticas. Estas atividades foram por sua vez agrupadas em 4 fases.

O segundo objetivo específico foi alcançado por meio da descrição do processo de terceirização de TI do IDP. Ele teve como método pesquisas documentais para se obter um panorama geral da instituição, apresentando sua história e entendendo seu funcionamento. Feito isso, foi possível elaborar a cadeia de valor da instituição que é composta por 12 processos gerenciais, 10 processos finalísticos e 14 processos de suporte.

Para mapear o processo específico de terceirização de TI, entender todas suas atividades, insumos, papéis e, principalmente, as maiores dificuldades e erros observados, foram realizadas entrevistas semiestruturadas com 5 colaboradores que representavam no momento da entrevista uma proporção de de 62,5% do total de envolvidos nas terceirizações. Em seguida foi executada a proposta do terceiro objetivo específico de propor um novo processo de terceirização de TI para o IDP, baseado nas boas práticas, por meio do entendimento do processo de terceirização de TI vigente na instituição, juntamente com a extração das boas práticas, resultando assim na proposta de um novo processo de terceirização.

Este mapeamento é composto por um macroprocesso de Governança da Terceirização

de TI, que por sua vez é composto pelos processos de análise estratégica da solicitação, avaliação e decisão, especificação das necessidades, análise e seleção de fornecedor(es), preparação para implantação da terceirização e gerenciamento da terceirização.

O quarto e último objetivo específico buscou elicitar os requisitos de um software para avaliação de riscos do processo de terceirização de TI. A execução deste objetivo foi dividida em duas partes, a primeira buscou no mercado ferramentas existentes que atendessem às necessidades especificadas, caso não fosse encontrada, seria então feito um trabalho de elicitação de requisitos.

Na busca por ferramentas existentes, foi realizada uma pesquisa documental o qual resultou em uma lista de 24 ferramentas, que foram analisadas a existência ou não de cada uma das 45 categorias previamente definidas. Cada categoria representava uma funcionalidade geral, como por exemplo, se possui pesquisa de satisfação, se emite alertas, etc. Os 10 softwares que apresentaram mais funcionalidades foram selecionados para uma avaliação à luz das 33 boas práticas extraídas e seus respectivos pesos atribuídos.

Cada ferramenta foi analisada para se identificar se possuía ou não requisitos relacionados à prática. Se a plataforma apresentasse o requisito, seria pontuada de acordo com o peso da prática, e caso negativo, mantinha zerada a pontuação da prática. De um total de 609,5 pontos das práticas somadas, ou seja a pontuação máxima possível, a ferramenta com melhor desempenho teve uma soma total de 472 pontos, ou seja, mais de 20% de defasagem. Portanto a adesão das boas práticas mostrou-se uma situação muito específica, que não foi observada em sua completude nos softwares já existentes no mercado, resultando na necessidade da proposta de um software próprio para as especificações definidas.

Para realizar a elicitação dos requisitos de uma ferramenta de avaliação de riscos do processo de terceirização de TI do IDP alinhado às boas práticas de terceirização de TI e gestão de riscos, foi feito um trabalho da pesquisadora em conjunto com os alunos da disciplina Projeto de Sistemas de Produção 2 (PSP2) da graduação de Engenharia de Produção da UnB. Para se obter um entendimento das funcionalidades deste software ora proposto, foi utilizada a técnica do *Lean Inception* que indica como sugestão uma lista de técnicas/atividades visando a compreensão de um produto mínimo viável, *Minimum viable product* (MVP).

Utilizando-se das técnicas e atividades de visão do produto, É - NÃO É - FAZ - NÃO FAZ, objetivo do produto, *personas* e *brainstorming* de funcionalidades, foi possível obter uma lista de 21 funcionalidades que foram identificadas e descritas.

Na busca por uma validação do resultado final e obtenção do entendimento sobre o software proposto, foi utilizada a prototipação de baixa fidelidade das principais telas do sistema. Foram desenhadas 12 telas no total, que foram associadas com as funcionalidades

desejadas e às boas práticas estudadas. Este resultado final mostra que a utilização da metodologia de estudo de caso foi satisfatória para atingir o objetivo geral desta pesquisa, propor uma ferramenta computacional para avaliação dos riscos na terceirização de TI do IDP, alinhada às boas práticas.

A validação do processo de terceirização de TI vigente do IDP, bem como a proposta do novo processo, a lista de funcionalidades e a proposta de ferramentas, consolidada de forma prática por meio dos protótipos, foram validados por colaboradores da empresa, de diferentes áreas diretamente envolvidos no processo atual. Assim, pela primeira vez foi possível fazer uso de boas práticas para realizar a caracterização de um sistema focado no gerenciamento de riscos da terceirização de TI.

A partir do mapeamento de um novo processo o IDP tem uma proposta clara e detalhada e viável de ser implementada na instituição. O novo processo está alinhado às boas práticas e poderá levar o IDP a uma melhora na terceirização. Isso se torna útil e oportuno pois até o presente momento não se tinha na empresa uma definição documentada dos papéis e atividades envolvidas na terceirização, dificultando o acompanhamento e a gestão contínua de melhoria dos projetos de terceirização.

O comprometimento dos participantes desde o início do trabalho até sua validação final foi de extrema importância para realização desta pesquisa, tornando-a possível. Ressalta-se a participação dos colaboradores do IDP, os quais estiveram dispostos e engajados em todos os pontos de contato ao longo da pesquisa, e a participação dos alunos do "Grupo 1" da disciplina de Projeto de Sistemas de Produção 2 (PSP2) que foram de suma importância para a finalização da coleta de dados da pesquisa, participando ativamente das atividades de comparação de ferramentas existentes, definição do produto e suas funcionalidades e finalmente de sua prototipação.

É importante destacar também que houve, por parte dos colaboradores envolvidos na validação dos produtos desta pesquisa, o interesse do IDP na implementação tanto do novo processo proposto, como do desenvolvimento e utilização do software ora proposto e especificado.

8.1 Proposta de trabalhos futuros

Como trabalhos futuros, visando avaliar a efetividade do novo processo de terceirização de TI aqui mapeado, sugerimos a definição e adoção de indicadores para aplicação no processo de terceirização realizado atualmente na instituição. Com isto será possível ter conhecimento mensurável da situação atual para depois, com a implantação do novo processo proposto nesta pesquisa, sejam aplicados novamente os indicadores e assim poderá ser realizado um comparativo de antes e depois e averiguar se houve de fato efetiva melho-

ria do processo como um todo. Sendo comprovada a efetividade de melhoria da aplicação do novo processo, fazendo uso de todas as especificações da proposta do software, para que ele seja implementado e implantado na instituição. Feito isto, os indicadores poderão ser usados novamente para mais uma vez ser medida a efetividade da utilização do software de avaliação de riscos da terceirização ora proposto.

Referências

- [1] Per Runeson and Martin Höst. Guidelines for conducting and reporting case study research in software engineering. 14(2):131. xi, 4, 5, 34
- [2] Tribunal de Contas da União Brasil. *Referencial básico de gestão de riscos*. xi, 3, 7, 8, 9, 12
- [3] ABNT NBR ISO 31000 NBRISO31000 gestão de riscos - diretrizes. xi, xii, xiv, 3, 8, 9, 10, 13, 16, 18, 22, 23, 42, 50, 51, 52, 53, 54, 129
- [4] Her Majesty Treasury. *The orange book: Management of risk-principles and concepts*. HM Treasury. xi, 10, 11
- [5] ABNT - Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27005 tecnologia da informação - técnicas de segurança - gestão de riscos de segurança da informação. Rio de Janeiro - RJ. xi, 17, 18
- [6] Association of Business Process Management Professionals (ABPMP). *Guia para o Gerenciamento de Processos de Negócio - Corpo Comum de Conhecimento V3.0*. 1 edição edition. xi, 23, 24, 25, 66
- [7] Orlando Oliveira dos Santos. Metodologia de diagnóstico e análise de desempenho de processos (MDADP) : estudo de caso sobre o processo de atendimento de serviços de TI. Accepted: 2017-03-21T13:16:05Z. xi, 24, 25, 26
- [8] Project Management Institute (PMI). *Um Guia do Conhecimento em Gerenciamento de Projetos (Guia PMBOK)*. Guia PMBOK. Project Management Institute, Inc, sexta edição edition. xi, 18, 26, 27, 28, 29
- [9] COBIT | Control Objectives for Information Technologies. *COBIT® 2019 Framework: Introduction and Methodology*. ISACA - Information Systems Audit and Control Association. xi, 42, 45, 129
- [10] International Organization for Standardization (ISO). ISO 37500:2014 guidance on outsourcing. (1):72. xi, xiv, 1, 19, 22, 42, 43, 46, 47, 48, 79, 129, 171, 172, 173, 174, 175, 176, 177
- [11] Paulo Caroli. *Lean Inception: como alinhar pessoas e construir o produto certo*. Caroli, 1ª edição atualizada edition. xii, xiv, 103, 104, 109
- [12] Descubra, compare e escolha os melhores apps empresariais. <https://www.getapp.pt/>. Acessado em 29/09/2021. xiii, 12, 98, 101, 189

- [13] Compare, download & develop open source & business software - SourceForge. <https://sourceforge.net/>. Acessado em 29/09/2021. xiii, 12, 98, 101, 189
- [14] Encontrar software. <https://www.capterra.com.br/>. Acessado em 29/09/2021. xiii, 12, 98, 101, 189
- [15] COBIT | Control Objectives for Information Technologies. *COBIT® 2019 Framework: Governance and Management Objectives*. ISACA - Information Systems Audit and Control Association. xiv, 17, 18, 19, 45, 46, 57, 58, 59, 167, 168, 169, 170, 171
- [16] Jing Mu and Yilei Pei. IT outsourcing business process model innovation based on the theory of change. In Min Zhu, editor, *Business, Economics, Financial Sciences, and Management*, Advances in Intelligent and Soft Computing, pages 395–402. Springer. 1, 2, 3
- [17] Ronan McIvor. A practical framework for understanding the outsourcing process. 5(1):22–36. Publisher: MCB UP Ltd. 1
- [18] Michel Laroche, Gordon H. G. McDougall, Jasmin Bergeron, and Zhiyong Yang. Exploring how intangibility affects perceived risk. 6(4):373–389. Publisher: SAGE Publications Inc. 1
- [19] Henrique Freitas and Rua Washington. A gestão do risco e o impacto da intangibilidade nas decisões de compra de tecnologias da informação. 2
- [20] Leonardo Santana Nobre. Proposta de metodologia de gestão de riscos para as contratações de TI da funasa. Accepted: 2017-11-29T18:55:42Z. 2
- [21] Jane C. Linder. *Outsourcing for Radical Change: A Bold Approach to Enterprise Transformation*. AMACOM, 1st edition edition. 2, 21
- [22] Marta Ávila. Gestão de riscos no setor público. 12:179–198. 2
- [23] Presidência da República Brasil. Lei nº 13.303, de 30 de junho de 2016. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/113303.htm. Acessado em 20/02/2021. 2
- [24] Presidência da República Brasil. Normativa conjunta cgu/mp nº 01, de 10 de maio de 2016. <http://www.ufu.br/legislacoes/instrucao-normativa-conjunta-mpcgu-no-012016.htm>. Acessado em 20/02/2021. 2
- [25] Distrito Federal. Decreto nº 37.302, de 29 de abril de 2016. http://www.sinj.df.gov.br/sinj/Norma/62b125e556c2408ba49802520e9f96e4/Decreto_37302_29_04_2016.html. Acessado em 20/02/2021. 2
- [26] Ulli Arnold. New dimensions of outsourcing: a combination of transaction cost economics and the core competencies concept. 6(1):23–29. 2, 19

- [27] Virginia M. Gibson. Outsourcing can save money and increase efficiency. page 19. 2, 19
- [28] Peter R. Embleton and Phillip C. Wright. A practical guide to successful outsourcing. 6(3):94–106. Publisher: MCB UP Ltd. 2, 19
- [29] J. J. Laabs. Why HR is turning to outsourcing. 2, 19
- [30] W.D. Engelke. The virtual times, outsourcing perspectives. 1-6. 2, 19
- [31] Ali Pirannejad, Hadi Salami, and Abdolazim Mollae. Outsourcing priorities of government functions: Analytic network process approach. 4(9):1723–1735. Publisher: Academic Journals. 2, 19
- [32] Lawrence Loh and N. Venkatraman. Determinants of information technology outsourcing: A cross-sectional analysis. 9(1):7–24. Publisher: Routledge _eprint: <https://doi.org/10.1080/07421222.1992.11517945>. 2, 20
- [33] Prashaya Fusiripong, Fauziah Baharom, and Yuhanis Yusof. Determining multi-criteria supplier selection towards sustainable development of IT project outsourcing. 6:13. 3
- [34] Mary C. Lacity, Shaji A. Khan, and Leslie P. Willcocks. A review of the IT outsourcing literature: Insights for practice. 18(3):130–146. 3, 20, 22
- [35] Eduardo et al Moresi. *Metodologia da Pesquisa*. Universidade Católica de Brasília. 4
- [36] Antônio Carlos Gil. *Como elaborar projetos de pesquisa*, volume 5. Saraiva. 4, 33, 34
- [37] Ginete Cavalcante Nunes, Maria Cristina Delmondes Nascimento, and Maria Aparecida Carvalho de Alencar. Pesquisa científica: conceitos básicos. 10(29):144–151. Number: 29. 4
- [38] Ari Mariano and Maíra Santos. *Revisão da Literatura: Apresentação de uma Abordagem Integradora*. 7
- [39] Committee of Sponsoring Organizations of the Treadway Commission. *COSO : Gerenciamento de Riscos Corporativos - Estrutura Integrada*, volume 2. PricewaterhouseCoopers LLP. 7
- [40] Instituto Brasileiro de Governança Corporativa. *Gerenciamento de riscos corporativos: evolução em governança e estratégia*. Cadernos de Governança Corporativa, 19. Instituto Brasileiro de Governança Corporativa. 8
- [41] Frank Hyneman Knight. Risk, uncertainty and profit. 31. 8
- [42] Aswath Damodaran. *Gestão estratégica do risco*. Bookman, 1 edition. 9
- [43] Adinilson Martins Da Silva. Gestão de riscos legais nas contratações de serviços de desenvolvimento de software baseados em métodos Ágeis. page 143. 9

- [44] ABNT - Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 31004 gestão de riscos: Guia para implementação. Rio de Janeiro - RJ. 9, 12
- [45] Committee of Sponsoring Organizations of the Treadway Commission. *COSO II: Enterprise risk management-integrated framework*. PricewaterhouseCoopers LLP. 10
- [46] Federation of European Risk Management Associations (FERMA). *A Risk Management Standard*. AIRMIC, ALARM, IRM. 11
- [47] SP Global Ratings. *Enterprise risk management evaluation framework*. Standard and Poor's Ratings Services. 11
- [48] Open e Ethics Group Compliance. *A governance, risk and compliance capability model (red book) 3.0*. OCEG. 11
- [49] Joint Task Force. Risk management framework for information systems and organizations: A system life cycle approach for security and privacy. 11
- [50] Risk management society (RIMS). *RIMS Risk Maturity Model (RMM) for Enterprise Risk Management*. Risk and Insurance Management Society, Inc. 11
- [51] Rodrigo Goyannes Gusmão Caiado, Gilson Brito Alves Lima, Daniel Luiz de Matos Nascimento, Julio Vieira Neto, and Rodolpho Augusto Maultasch De Oliveira. Guidelines to risk management maturity in construction project. 13(3):372. 12
- [52] Massimo F. Piepoli. 2016 european guidelines on cardiovascular disease prevention in clinical practice. 24(3):321–419. 12
- [53] The people's safety software. <https://donesafe.com/>. Acessado em 28/09/2021. 12
- [54] Business process management software | onspring. <https://onspring.com/>. Acessado em 28/09/2021. 13
- [55] Securewatch - RiskWatch. <https://riskwatch.com/securewatch/>. Acessado em 28/09/2021. 13
- [56] IBM OpenPages with watson | IBM. <https://www.ibm.com/products/openpages-with-watson>. Acessado em 28/09/2021. 13
- [57] Fusion framework system - fusion risk management. <https://www.fusionrm.com/platform/fusion-framework-system/>. Acessado em 28/09/2021. 13
- [58] SoftExpert software - conformidade, inovação e transformação digital. <https://www.softexpert.com/pt-br/>. Acessado em 28/09/2021. 13
- [59] Software para gestão de riscos - ERM | SoftExpert. <https://www.softexpert.com/pt-br/solucao/gestao-riscos-corporativos-erm/>. Acessado em 28/09/2021. 13, 14

- [60] Brasileiro INTERISK | software INTERISK. <https://www.brasiliano.com.br/>. Acessado em 28/09/2021. 13
- [61] Services. <https://www.leadmark.nl/services/>. Acessado em 28/09/2021. 14
- [62] GRC software | GRC tools & solutions | reciprocity. <https://reciprocity.com/>. Acessado em 28/09/2021. 14
- [63] FORM I the digital assistant for the frontline. <https://www.form.com/>. Acessado em 28/09/2021. 14
- [64] Resolver | risk & security management software. <https://www.resolver.com/>. Acessado em 28/09/2021. 14, 16
- [65] Módulo risk manager – módulo. <https://www.modulo.com.br/moduloriskmanager/>. Acessado em 28/09/2021. 14
- [66] flowti. Flowti - tecnologia para negócios. <https://flowti.com.br/>. Acessado em 28/09/2021. 15
- [67] SimpleRisk GRC software. <https://www.simplerisk.com/>. Acessado em 28/09/2021. 15
- [68] Open source risk engine – open source risk analytics – open source risk modelling. <https://www.opensourcerisk.org/>. Acessado em 28/09/2021. 15
- [69] PTA - practical threat analysis methodology and risk assessment tools for security experts. <http://www.ptatechnologies.com/>. Acessado em 28/09/2021. 15
- [70] Eramba - open IT GRC. <http://www.eramba.org/>. Acessado em 28/09/2021. 15
- [71] Free open source RA risk coverage software. <https://riskandassurancegroup.org/ra-risk-coverage-software/>. Acessado em 28/09/2021. 15
- [72] OpenVAS - open vulnerability assessment scanner. <https://www.openvas.org/>. Acessado em 28/09/2021. 15, 16
- [73] Project risk management software, consulting and training services. <https://www.project-risk-manager.com/>. Acessado em 28/09/2021. 16
- [74] Linda Wallace, Mark Keil, and Arun Rai. Understanding software project risk: a cluster analysis. 42(1):115–125. 16
- [75] Val Hooper anMarian Carcaryd Tarika Kalidas. IT risk management: A capability maturity model perspective. 16(1):pp3-13–pp3-13. Number: 1. 17, 18, 19
- [76] Deloitte. Os cinco pilares dos riscos empresariais: Como gerenciá-los em um cenário econômico e de negócios desafiador. 17
- [77] International Standards Organization (ISO). ABNT NBR ISO/IEC 13335 information technology - guidelines for the management of it security - part 3: Techniques for the management of it security. Rio de Janeiro - RJ. 17

- [78] Ian McCarthy and Angela Anagnostou. The impact of outsourcing on the transaction costs and boundaries of manufacturing. 88(1):61–71. 19
- [79] Norris F. Krueger, Michael D. Reilly, and Alan L. Carsrud. Competing models of entrepreneurial intentions. 15(5):411–432. 20
- [80] Uday Apte and MaryAnne Winniford. Global outsourcing of information systems functions: opportunities and challenges. In *Proceedings of the 1991 Information Resources Management Association international conference on Managing information technology in a global society*, pages 58–67. IGI Global. 20
- [81] Heather A. Smith and James D. McKeen. Developments in practice XIV: IT sourcing - how far can you go? 13(1). 20
- [82] Huigang Liang, Jian-Jun Wang, Yajiong Xue, and Xiaocong Cui. IT outsourcing research from 1992 to 2013: A literature review based on main path analysis. 53(2):227–251. 20
- [83] Syaripah Ruzaini Syed Aris, Noor Habibah Arshad, and Azlinah Mohamed. Risk management practices in IT outsourcing projects. In *2008 International Symposium on Information Technology*, volume 4, pages 1–8. ISSN: 2155-899X. 20, 21, 22, 129
- [84] Fan Jing Meng, Xiao Yang He, Shun Xiang Yang, and Peng Ji. A unified framework for outsourcing governance. In *The 9th IEEE International Conference on E-Commerce Technology and The 4th IEEE International Conference on Enterprise Computing, E-Commerce and E-Services (CEC-EEE 2007)*, pages 367–374. ISSN: 2378-1971. 21, 23
- [85] Fulvio Cristofoli, Edmir Prado, and Hiroo Takaoka. Resultados obtidos com a terceirização da TI em empresas brasileiras. 21
- [86] Felix Pomeranz. Fraud: The root causes. 15(1):15–18. Publisher: Routledge
_eprint: <https://doi.org/10.1080/09540969509387850>. 22, 23
- [87] Michael J. Earl. The risks of outsourcing IT. 23
- [88] Mohamed Zairi. Business process management: a boundaryless approach to modern competitiveness. 3(1):64–80. Publisher: MCB UP Ltd. 23
- [89] Thomas H. Davenport. *Process Innovation: Reengineering Work Through Information Technology*. Harvard Business Press. Google-Books-ID: kLIOMGaKnsC. 23
- [90] Jan vom Brocke and Michael Rosemann. *Handbook on business process management 1: Introduction, methods, and information systems*. Springer Publishing Company, 2 edição edition. 23
- [91] F. Leymann, D. Roller, and M.-T. Schmidt. Web services and business process management. 41(2):198–211. Conference Name: IBM Systems Journal. 23

- [92] Paul Harmon and Business Process Trends. *Business Process Change: A Guide for Business Managers and BPM and Six Sigma Professionals*. Elsevier. Google-Books-ID: wSLnCTBjbn8C. 23
- [93] Omar AlShathry. Business process management: a maturity assessment of saudi arabian organizations. 22(3):507–521. Publisher: Emerald Group Publishing Limited. 23
- [94] Archie Lockamy and Kevin McCormack. The development of a supply chain management process maturity model using the concepts of business process orientation. 9(4):272–278. Publisher: Emerald Group Publishing Limited. 23
- [95] Roger Tregear. Practical process: What if “top down” isn’t possible? | BPTrends. <https://www.bptrends.com/practical-process-what-if-top-down-isnt-possible/>. Acessado em 03/03/2022. 23
- [96] Carlos Magno da S. Xavier. *Gerenciamento de Projetos*. Saraiva Educação S.A. 28
- [97] Márcio Lemos. Entrevista em profundidade. 1:15. 33
- [98] Robert K Yin. *Estudo de Caso: Planejamento e métodos*. Bookman editora. 34
- [99] Y Rogers, H Sharp, and J Preece. *Interaction design: Beyond human-computer interaction*, jon wiley & sons. 37
- [100] Ian Sommerville and Pete Sawyer. RE: a good practice guide. 113:114. 37
- [101] Adrien Coyette, Stéphane Faulkner, Manuel Kolp, Quentin Limbourg, and Jean Vanderdonckt. SketchiXML: towards a multi-agent design tool for sketching user interfaces based on USIXML. In *Proceedings of the 3rd annual conference on Task models and diagrams*, TAMODIA ’04, pages 75–82. Association for Computing Machinery. 37
- [102] Carlos Rosemberg, Albert Schilling, Cristianne Bastos, and Rodrigo Araripe. Prototipação de software e design participativo: uma experiência do atlântico. In *Proceedings of the VIII Brazilian Symposium on Human Factors in Computing Systems*, IHC ’08, pages 312–315. Sociedade Brasileira de Computação. 37
- [103] R. Budde and H. Zullighoven. Prototyping revisited. In *COMPEURO’90: Proceedings of the 1990 IEEE International Conference on Computer Systems and Software Engineering - Systems Engineering Aspects of Complex Computerized Systems*, pages 418–427. 37
- [104] H. Lichter, M. Schneider-Hufschmidt, and H. Zullighoven. Prototyping in industrial software projects-bridging the gap between theory and practice. 20(11):825–832. Conference Name: IEEE Transactions on Software Engineering. 37
- [105] Ely Severiano Junior and Diego de Oliveira da Cunha. A importância do uso modelo COBIT nos processos de TI diante de um contexto organizacional / the importance of using COBIT model in IT processes in an organizational context. 4(6):2844–2854. Number: 6. 43

- [106] Cristiano Pereira and Carlos Ferreira. Identification of IT value management practices and resources in COBIT 5/identificacao de praticas e recursos de gestao do valor das TI no COBIT 5. (15):17–34. Publisher: AISTI (Iberian Association for Information Systems and Technologies). 43
- [107] COBIT | Control Objectives for Information Technologies. *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*. ISACA - Information Systems Audit and Control Association. 46, 56
- [108] COBIT | Control Objectives for Information Technologies. *COBIT® 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution*. ISACA - Information Systems Audit and Control Association. 46
- [109] Teams login | acessar plataforma colaborativa microsoft teams. <https://www.microsoft.com/pt-br/microsoft-teams/log-in>. Acessado em 30/11/2021. 97, 104
- [110] Miro | online whiteboard for visual collaboration. <https://miro.com/app/dashboard/>. Acessado em 30/11/2021. 104, 113

Apêndice A

Documento de visão elaborado em PSP2

INFORMAÇÕES SOBRE O PROJETO

Gestão de Riscos em projetos de terceirização de TI	
Gestores do Projeto	Stakeholders
João Gonçalves Borsato de Moraes	Thabata Helen Macedo Granja
Isaac Lisboa Cardoso	
Claudio Eduardo Araujo Pereira	
Willian Kesley Oliveira Cardoso	

OBJETIVO DESTE DOCUMENTO

Objetivo deste Documento

Este documento tem como objetivo estabelecer uma visão de alto nível para os requisitos técnicos mais detalhados. Nele serão feitas adaptações necessárias ao longo do projeto para que as necessárias para que as necessidades sejam atendidas.

1. ESCOPO DO PRODUTO

- A. Ranking de ferramentas de gestão de risco;
- B. Matriz comparativa das ferramentas de gestão de risco existentes no mercado;
- C. Documentos de requisitos elicitados de acordo com técnica de Lean Inception;
- D. Proposta de protótipo de telas para a ferramenta.

1. Cronograma

agosto 2021						
S	T	Q	Q	S	S	D
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

setembro 2021						
S	T	Q	Q	S	S	D
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

outubro 2021						
S	T	Q	Q	S	S	D
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

■	Contato inicial com stakeholders
■	Planejamento
■	Comparativo de Ferramentas parte 1
■	Elicitação de requisitos
■	Comparativo de Ferramentas parte 2
■	Prototipação

2. NÃO ESCOPO DO PRODUTO

- Desenvolvimento de Sistema;
- Desenvolvimento de Banco de Dados;
- Obter feedback dos usuários;
- Arquitetura do sistema;
- Ambiente.

3. DESCRIÇÃO DOS ENVOLVIDOS

Ao utilizar o método Lean-inception as personas envolvidas na ferramenta foram o gerente de riscos, o diretor, gerente de TI e o Responsável pela área solicitante de terceirização.

3.1 Resumo dos Usuários/Atores

Nome	Responsabilidade	Necessidades
Gerente de riscos	Identificar, monitorar, avaliar e gerir os riscos	-Controlar projetos de terceirização

	<p>dos processos de terceirização;</p> <p>Conduzir e acompanhar os processos de terceirização de TI</p>	<p>-Gerenciar os riscos dos projetos de terceirização</p> <p>-Avaliar os riscos</p> <p>-Acompanhar as atividades dos projetos</p> <p>-Manter registros e históricos</p>
Diretor	<p>Acompanhar o processo da terceirização de TI;</p> <p>Verificar se os processos de terceirização de TI estão no caminho correto, com os riscos identificados e tratados.</p>	<p>-Ter uma visão simplificada das informações</p> <p>-Informações centralizadas (e financeiras)</p> <p>-Acompanhamento geral dos projetos</p> <p>-Sistema sem linguagens técnicas</p> <p>-Possibilidade de gerar relatórios</p> <p>-Possibilidade de comparativo entre projetos</p>
Gerente de TI	<p>Gerir a ferramenta utilizada para a gestão dos riscos dos processos de terceirização de TI;</p> <p>Buscar uma solução para os pedidos de terceirização da área solicitante, ao verificar a necessidade desse pedido e se existe ou existiu terceirizações equivalentes do pedido;</p> <p>Padronizar o processo de terceirização de TI.</p>	<p>Controlar projetos de terceirização</p> <p>-Acompanhar as terceirizações</p> <p>-Acompanhar os riscos das terceirizações</p> <p>-Relatórios sobre os projetos de terceirização</p> <p>-Catalogar as terceirizações existentes com filtros</p> <p>-Manter registros e históricos</p>

Responsável da área solicitante	Solicitar a demanda da terceirização; Conduzir o projeto de terceirização.	-Acompanhar o projeto de terceirização -Registrar as necessidades de terceirização -Ter fácil navegação no sistema -Ter registros e históricos das terceirizações da área
---------------------------------	---	--

4. VISÃO GERAL DO PRODUTO

Determina-se como cliente principal o IDP (Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa); cujo a falta de padrão, monitoramento e comunicação no processo de terceirização de TI gerou um histórico de aquisições problemáticas para a instituição.

Assim, temos como produto a proposta de uma ferramenta que irá auxiliar o processo de terceirização de TI, sendo seu nome Kyndinos, que é uma ferramenta computacional para a avaliação de riscos na terceirização de TI alinhado com as boas práticas e as necessidades do IDP.

Logo, a ferramenta proposta irá realizar o planejamento, monitoramento, controle unificado e eficaz nos devidos processos citados, denota-se que diferente da falta de controle atual o nosso produto permite a avaliação de riscos nos processos de terceirização de TI.

4.1 Requisitos Funcionais

Nº	Nome	Descrição
RF001	Atualizar informações cadastradas em tempo real	A ferramenta deve permitir o acompanhamento em tempo real do desenvolvimento das atividades.
RF002	Associar os riscos com as áreas envolvidas	Permitir a associação dos riscos com as áreas envolvidas
RF003	Registrar as necessidades de terceirização	Permitir a área do solicitante registrar as necessidades da terceirização, a fim do gestor de TI buscar a solução.
RF004	Receber alertas sobre riscos	Permite alertar periodicamente sobre os eventos de riscos que estão sendo analisados e monitorados.
RF005	Fazer login na ferramenta	Permite ao usuário acesso e interação com a plataforma por meio de input em forma de preenchimento de informações que a plataforma necessita.
RF006	Cadastrar usuários na ferramenta	Permite cadastrar e excluir usuários e modificar informações dos mesmos.
RF007	Gerenciar níveis de acesso	Permite aos usuários acessarem as telas do sistema de acordo com suas necessidades e grau hierárquico.
RF008	Cadastrar projetos de terceirização	Permite o usuário cadastrar os projetos de terceirização.

RF009	Cadastrar riscos	Permite ao usuário cadastrar todos os riscos envolvidos no processo de terceirização.
RF010	Classificar risco	Permite ao usuário classificar todos os riscos envolvidos no processo de terceirização, avaliando o risco em relação ao impacto do risco do desprezível ao extremo e a probabilidade dele do raro ao muito provável.
RF011	Monitorar os riscos	Permite que o usuário tenha uma visão sobre os riscos que já foram identificados no processo, de forma que ele venha ter acesso ao seu monitoramento e assim tomar decisões melhores.
RF012	Ter uma visualização geral dos riscos dos projetos	Permite que o usuário tenha uma visualização geral dos riscos do projeto, com as informações do impacto e probabilidade de cada um.
RF013	Ter uma visualização geral dos projetos	Permite ao usuário ter uma noção consolidada dos projetos que estão em execução pela instituição.
RF014	Associar riscos com as atividades do processo	Permite ao usuário informações detalhadas sobre os riscos atrelados no processo de forma específica de acordo com a atividade.
RF015	Tratar os riscos (Matriz Eisenhower)	Fornecer ao usuário a matriz de Eisenhower com os eixos Importante e Urgente, para identificar os riscos que devem ser tratados primeiro e fornecer o melhor método para tratar o risco.
RF016	Acompanhar os projetos de terceirização	Permite o usuário acompanhar as fases de terceirização

RF017	Consultar terceirizações já finalizadas	Permite que após a finalização do processo das terceirizações, quando já finalizadas, permite que em forma de histórico fique registrado facilitando a consulta ao usuário para consultar um projeto específico.
RF018	Comparar projetos de terceirização quanto aos riscos	Permite ao usuário comparar os riscos de terceirização entre projetos em andamentos, em fase inicial e encerrados .
RF019	Configurar API	Permite a comunicação de serviços ou produtos sem a necessidade de saber como foram implementados, de forma que o trâmite de informação seja simplificado.
RF020	Buscar informações dos projetos de terceirização	Permite o usuário ter acesso a informações, riscos, histórico e demais informações relevantes de outros processos de terceirização finalizados ou em andamento
RF021	Priorizar os riscos	Permite ao usuário classificar o risco e indicar a prioridade para o projeto.
RF022	Personalização da ferramenta (relatórios, painéis)	Permite gerar relatório e painéis personalizados, segundo a necessidade do usuário.
RF023	Gestão de Fornecedores	Permite fazer a avaliação, acompanhamento, manter histórico dos fornecedores.
RF024	Manter listas de soluções alternativas em projetos	Permite salvar uma lista alternativas de soluções para as demandas de terceirização.

4.2 Requisitos Não Funcionais

Nº	Nome	Descrição
RNF001	Personalizado	O sistema deve ser adequado aos processos e usuários do IDP.
RNF002	Interativo	O sistema deve permitir ao usuário a interação de forma intuitiva e simples, facilitando sua compreensão.
RNF003	Plataforma única	O sistema possui apenas uma única plataforma onde todas as informações vão ser centralizadas.
RNF004	Intuitivo	O sistema deve ser intuitivo a fim de fornecer acessibilidade de forma clara e sucinta.
RNF005	Eficiente	O sistema deve possuir eficiência a fim de fornecer tudo que é proposto pela ferramenta.
RNF006	Disponibilizado em Português (BR)	O sistema deve estar disponível em Português (BR).
RNF007	Seguro	As informações do sistema devem ser de acesso exclusivo para usuários do IDP.
RNF008	Baseado em boas práticas de terceirização e gestão de riscos	O sistema deve seguir a ISO 91000 de terceirização, ISO 31000 de gestão de risco e COBIT - Controle de Objetivos para a Informação e Tecnologia Relacionadas.
RNF009	Boa suportabilidade	O sistema deve possuir uma suportabilidade eficiente de forma que não prejudique o uso.
RNF010	Boa performance	O sistema deve possuir uma performance significativa que atenda às expectativas do usuário.

RNF011	Confiável	O sistema deve possuir uma estrutura confiável de forma que o usuário se sinta seguro ao compartilhar seus dados com a plataforma.
RNF012	Ferramenta colaborativa	O sistema deve permitir aos usuários colaborarem entre si para realizar determinadas etapas no sistema.

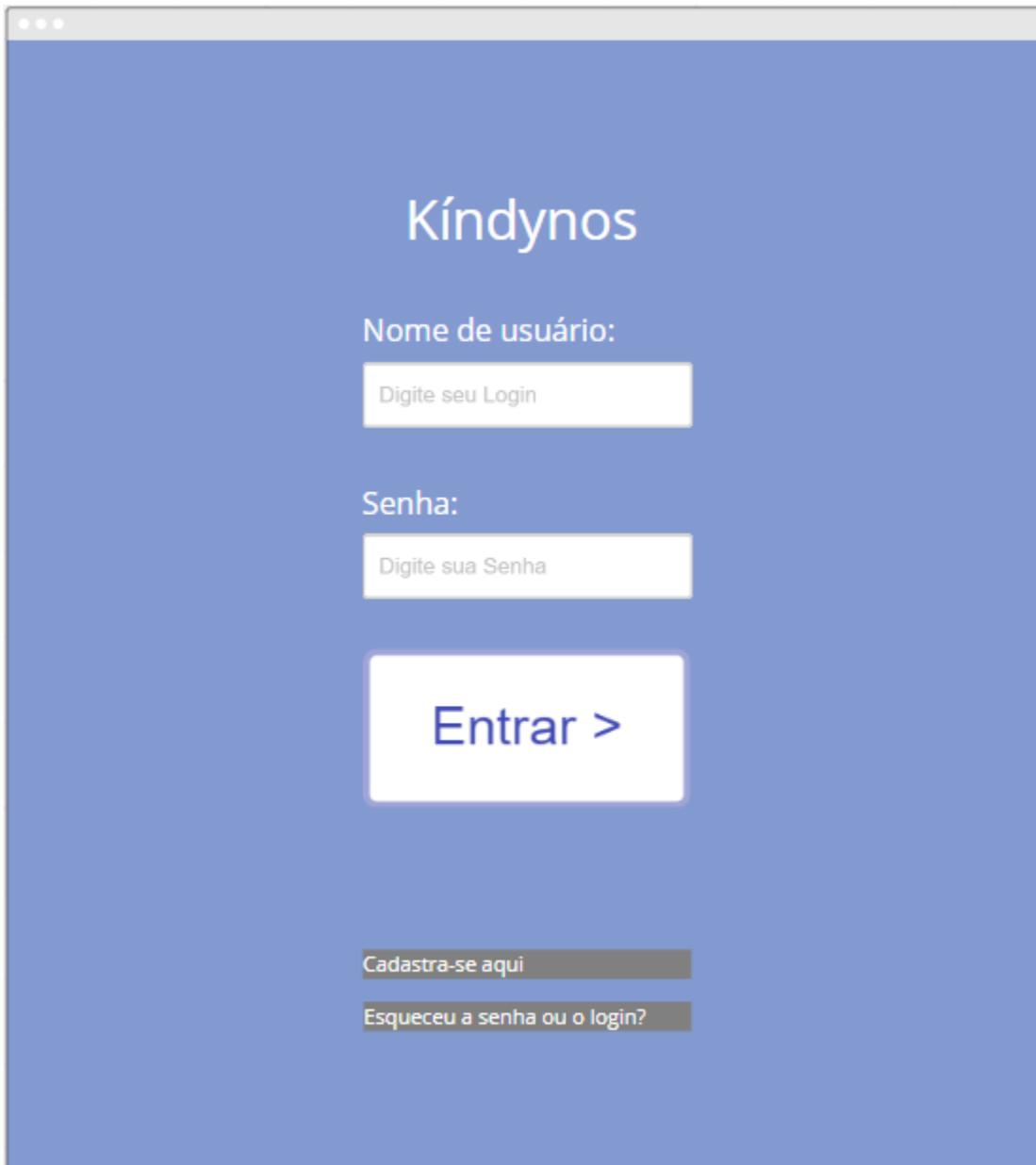
5. RESTRIÇÕES

- Projeto não envolve custos financeiros;
- Não pode haver encontros presenciais por conta da pandemia;
- Necessidade de reuniões semanais entre os stakeholders;
- O projeto por estar sendo desenvolvido no contexto da disciplina de PSP2, deve ser finalizado antes do término do semestre 01/2021 da Universidade de Brasília.

6. INTERFACE

Interface 1 - Login

Requisitos: RF005



The image shows a login interface for 'Kíndynos' within a browser window. The background is a solid blue color. At the top center, the word 'Kíndynos' is written in a white, sans-serif font. Below this, the text 'Nome de usuário:' is displayed in white. Underneath is a white rectangular input field with the placeholder text 'Digite seu Login'. Below the first field, the text 'Senha:' is displayed in white. Underneath is another white rectangular input field with the placeholder text 'Digite sua Senha'. Below the second field is a large white rectangular button with the text 'Entrar >' in blue. At the bottom of the interface, there are two smaller white rectangular buttons: 'Cadastra-se aqui' and 'Esqueceu a senha ou o login?'. The browser window has a standard title bar with three dots on the left.

Descrição : O usuário deverá acessar o sistema Kíndynos usando seu usuário e senha previamente cadastrados e clicar em entrar.

Passos: Preencher campo " Nome do usuário" -> Preencher campo "Senha" -> Clicar em Entrar>.

Interface 3 - Informações do projeto

Requisitos: RF024,RF012 e RF010.

The screenshot shows a user interface for viewing project details. At the top, there is a navigation bar with a user profile icon, a home icon, and a search bar. The main title is 'Projeto 1'. Below this, the section 'Informações do projeto 1:' contains several data fields: 'Fornecedor' (Microsoft), 'Área' (Financeiro), 'Responsável' (João Cândido), 'Status' (Aprovado), 'Solução' (a dropdown menu with a placeholder), 'Valor do projeto' (R\$100.000), and 'Tratamento dos riscos' (85% tratados). A 'Ver mais' button is located to the right of the 'Tratamento dos riscos' field. Below these fields is a 'Descrição' section with a large text area containing a placeholder. At the bottom, there are two date fields: 'Data de inicio' (24/10/11) and 'Data de final' (24/10/23). A navigation bar at the very bottom includes a back arrow and a button labeled 'Lista de projetos de terceirização'.

Descrição : O usuário poderá se informar com inúmeras informações do projeto, como fornecedor, área solicitante, responsável, Data inicial e final do contrato, tratamento dos riscos, estado do projeto (status).

Passos: Menu-> selecionar "Lista de projetos de terceirização"-> Buscar projeto -> Clicar no projeto desejado-> Informações do projeto-> Navegar no menu do lado direito para obter informações

Interface 4 - Cadastro e avaliação de risco

Requisitos: RF014, RF021, RF002, RF015, RF009 e RF010.

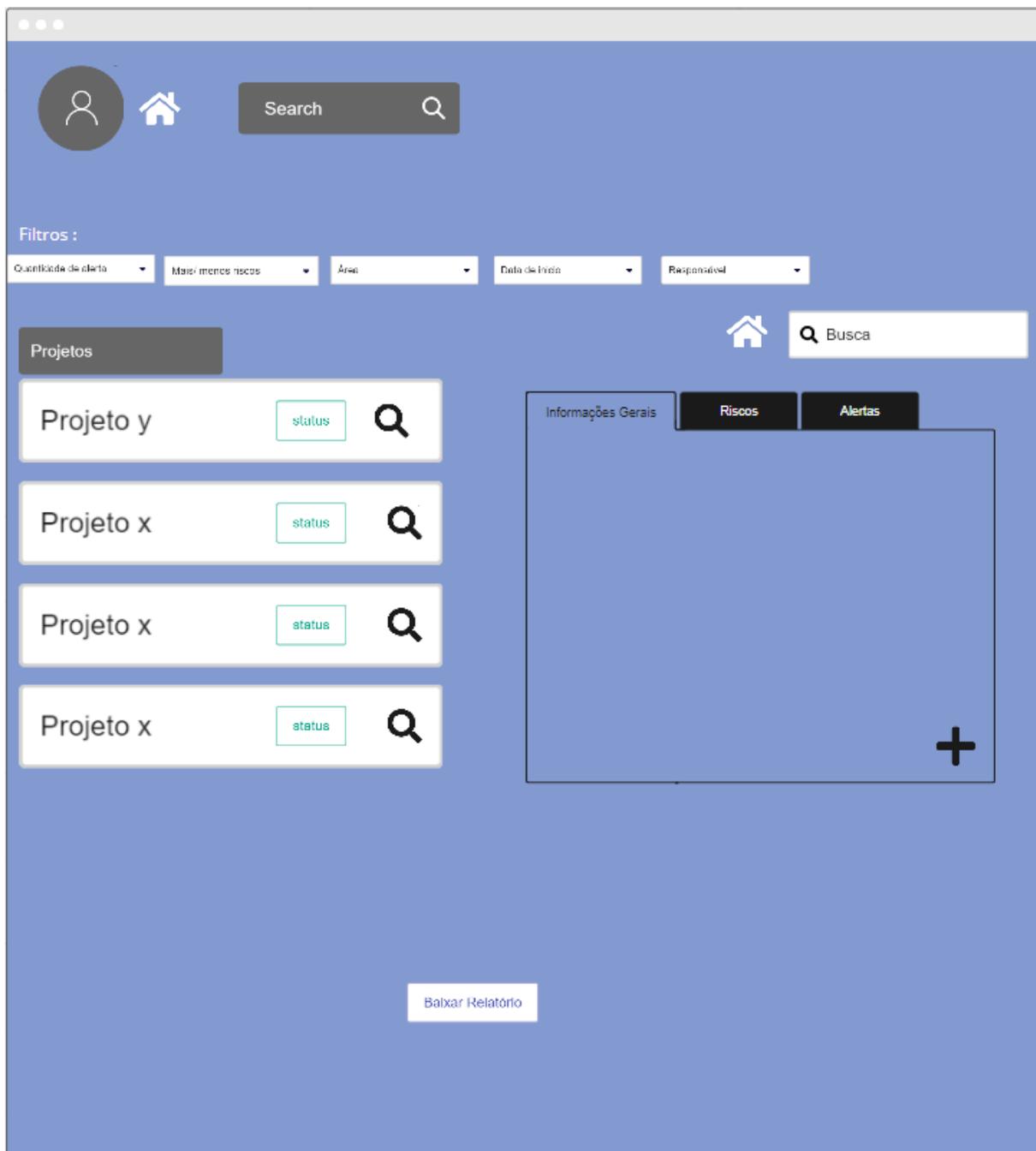
The screenshot displays a web interface with a blue background. At the top left, there are icons for a user profile and a home page. A search bar is located at the top right. The interface is divided into two main sections: 'Cadastro de Riscos' (Risk Registration) on the left and 'Avaliação de Riscos' (Risk Evaluation) on the right. The 'Cadastro de Riscos' section contains a vertical list of input fields: 'Evento de Risco' (with the letter 'E'), 'Processo Inserido', 'Projeto Inserido', 'Classificação do Risco' (with the letter 'E'), 'Prioridade do Risco' (with a sub-label 'Prioridade do Risco'), 'Área do Risco' (with the letter 'A'), 'Nível Crítico', 'Causas', 'Efeitos', 'Responsável', 'Descrição do Risco', and 'Status do Risco'. At the bottom of this section are 'Cadastrar' and 'Cancelar' buttons. The 'Avaliação de Riscos' section has 'Evento de Risco' and 'Projeto Inserido' dropdown menus, both labeled 'Add text'. Below these is a 'Dados do Risco' section with three tabs: 'Causas', 'Efeitos', and 'Prob.&Impac'. The 'Efeitos' tab is currently selected, showing a large empty text area.

Descrição : O usuário poderá cadastrar os riscos de forma intuitiva e simples, assim quando o mesmo for cadastrado nos seus devidos campos de preenchimento, o usuário terá visão e acesso às informações sobre os dados do riscos inseridos, ademais o risco associado ao processo e o projeto inserido.

Passos: “Cadastro de Risco” -> Evento de Risco -> Projeto Inserido -> Classificação dos Riscos -> Prioridade dos Riscos -> Área do Risco -> Nível Crítico -> Causas-> Efeitos -> Responsáveis -> Descrição do Risco -> Status do Risco -> “Cadastrar ou Cancelar”-> -> Avaliação de riscos -> Evento de Risco -> Projeto Inserido -> “Dados dos Projetos”

Interface 5 - Acompanhamento do projeto

Requisitos:RF001, RF022, RF020, RF012, RF011, RF017 e RF016



Descrição : O usuário poderá obter informações de riscos, alertas de cada projeto bastando selecionar a lupa, sendo possível verificar os status e realizar filtros ou busca para localizar o projeto.

Passos: Menu-> selecionar "Acompanhar projetos"-> Filtrar ou Buscar projeto -> Clicar na lupa do projeto desejado-> Navegar pela página para obter informações

Interface 6 - Histórico de projetos de terceirização

Requisitos: RF017



Descrição : O usuário poderá ver os projetos de terceirização já finalizados, usando as buscas de filtro e área, para identificar as áreas que já contrataram o software e filtrar o tipo de contrato, como contrato de software para texto.

Passos: Menu-> selecionar "Histórico de projetos de terceirização"-> Filtrar ou Buscar projeto -> Clicar na lupa do projeto desejado-> Navegar pela página para obter informações

Interface 7 - Cadastro dos projetos

Requisitos: RF008 e RF003

Cadastro dos projetos

Search

Filtro Add text

Área Add text

Dados de projetos semelhantes

Tab 1 Tab 2 Tab 3

Quantidade de projetos encontrados: xxx

Nome Add text

Responsável Add text

Departamento Add text

Contrato Add text

Solução Add text

Valor do projeto Add text

Data de inicio Add text Data de prevista de termino Add text Data de final Add text

Descrição Add text

Cadastro de riscos do projeto Cadastrar Cancelar

Descrição : Nesta tela, o usuário poderá cadastrar novos projetos do “zero”, com suas informações de nome, responsável, departamento, contrato, solução, valor do projeto, datas (de início, prevista de término, final) e descrição. Ou ainda, visando

manter a uniformidade e padronização das informações na plataforma, e agilidade na inserção desses dados, consultar cadastros de projetos anteriores.

Pode ainda ter acesso a tela de Interface 4 - “Cadastro de riscos do projeto”.

Passos: Menu -> Organização -> Cadastro dos projetos -> Filtro

- 1) Área -> Dados dos fornecedores (opções 1, 2, 3 ...) e Projetos associados (opções 1, 2, 3 ...)*
- 2) Inserção de dados (Nome, Responsável, Departamento, Contrato, Solução, Valor do projeto, Datas (de início, prevista de término, final) e descrição) -> Cadastrar*

Interface 8 - Riscos no processo

Requisitos:RF009, RF010 e RF015

Riscos no projeto X

Matriz de Eisenhower

	URGENTE	NÃO URGENTE
IMPORTANTE	"FAÇA AGORA!" Risco1	"AGENDE" Risco2
NÃO IMPORTANTE	"DELEGUE" Risco3	"ELIMINE" Risco4

Matriz de Probabilidade vs. Impacto

Impacto	1	2	3
3	Amarelo	Amarelo	Vermelho
2	Verde	Verde	Amarelo
1	Verde	Verde	Amarelo

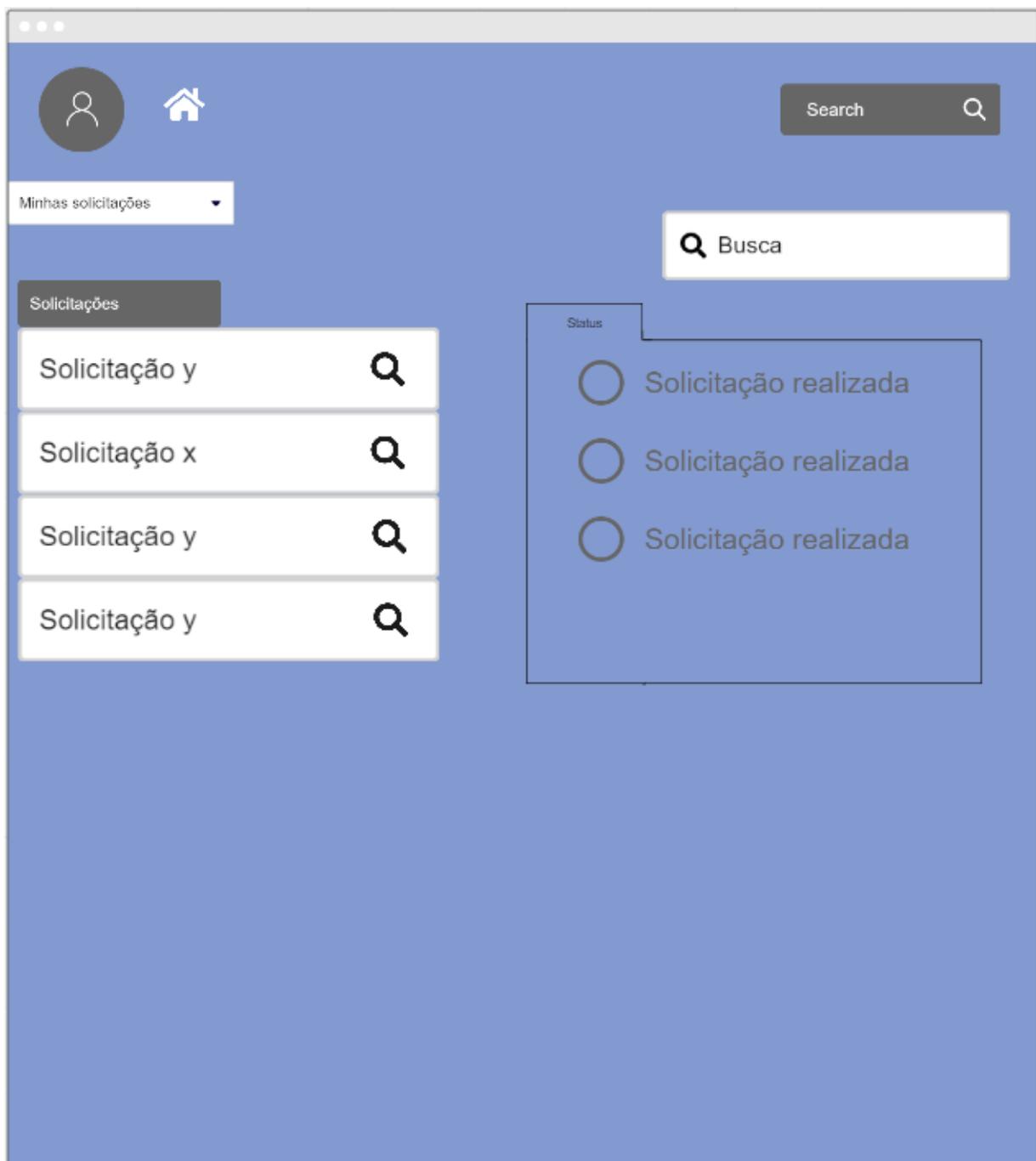
←

Descrição: Nessa tela tem-se a interface gráfica das informações cadastradas na "Interface 4 - Cadastro e avaliação de risco", na qual o usuário terá visão geral dos riscos inseridos, podendo compará-los através da Matriz de Eisenhower e da Matriz de Probabilidade vs. Impacto.

Passos: Menu -> Riscos -> Cadastro de Riscos -> Cadastrar -> Riscos no projeto X

Interface 9 - Acompanhamento do solicitante

Requisitos:RF020 e RF001



Descrição: O responsável por cadastrar o projeto poderá nesta tela acompanhar o andamento de análise do mesmo.

Passos:Menu-> Meu espaço -> Minhas solicitações -> Pesquisa projeto -> selecionar lupa do projeto desejado -> observar informações ao lado direito.

Interface 10 - Cadastro de usuário

Requisitos:RF007 e RF006

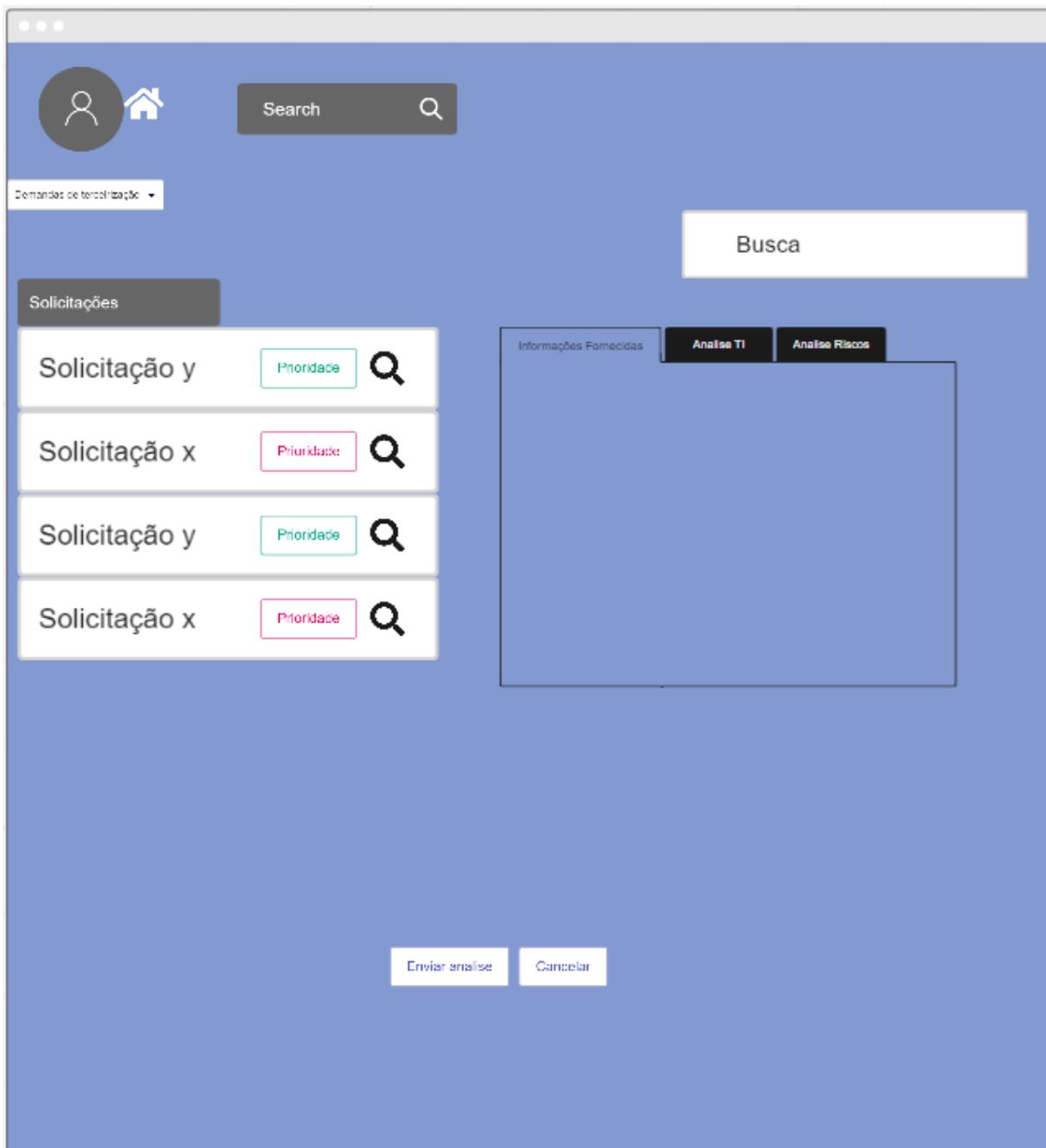
The screenshot shows a web application interface for user management. At the top, there is a navigation bar with a user profile icon, a home icon, and a search bar. Below the navigation bar, there is a dropdown menu labeled 'Organização'. The main content area is divided into two panels by a vertical line. The left panel is titled 'Novo usuário' and contains the following fields: 'Nome:' with a text input field containing 'Add text'; 'E-mail:' with a text input field containing 'Add text'; 'Senha:' with a text input field containing 'Add text' and a checkbox labeled 'Redefinir no primeiro acesso'; 'Perfil:' with a dropdown menu containing 'Add text'; and 'Válido até:' with a text input field containing 'xx/xx/xxxx'. The right panel is titled 'Excluir usuário' and contains the following elements: 'Nome:' with a search input field containing 'Search'; a user profile icon; a square box with a large 'X' over it; and a checkbox labeled 'Excluir usuário que não pode ser reutilizado'. At the bottom of the interface, there are two buttons: 'Confirmar' and 'Cancelar'.

Descrição : Na tela é possível o cadastro de novos usuário, configurar o nível de acesso dentro da plataforma ou a exclusão de algum usuário.

Passos: Menu-> Organização-> Preencha ou os campos referente a parte de novo usuário ou pesquisa o usuário que deseja excluir -> confirmar .

Interface 11 - Acompanhamento de atividades

Requisitos:RF010,RF009, RF018,RF017, RF022 e RF004.

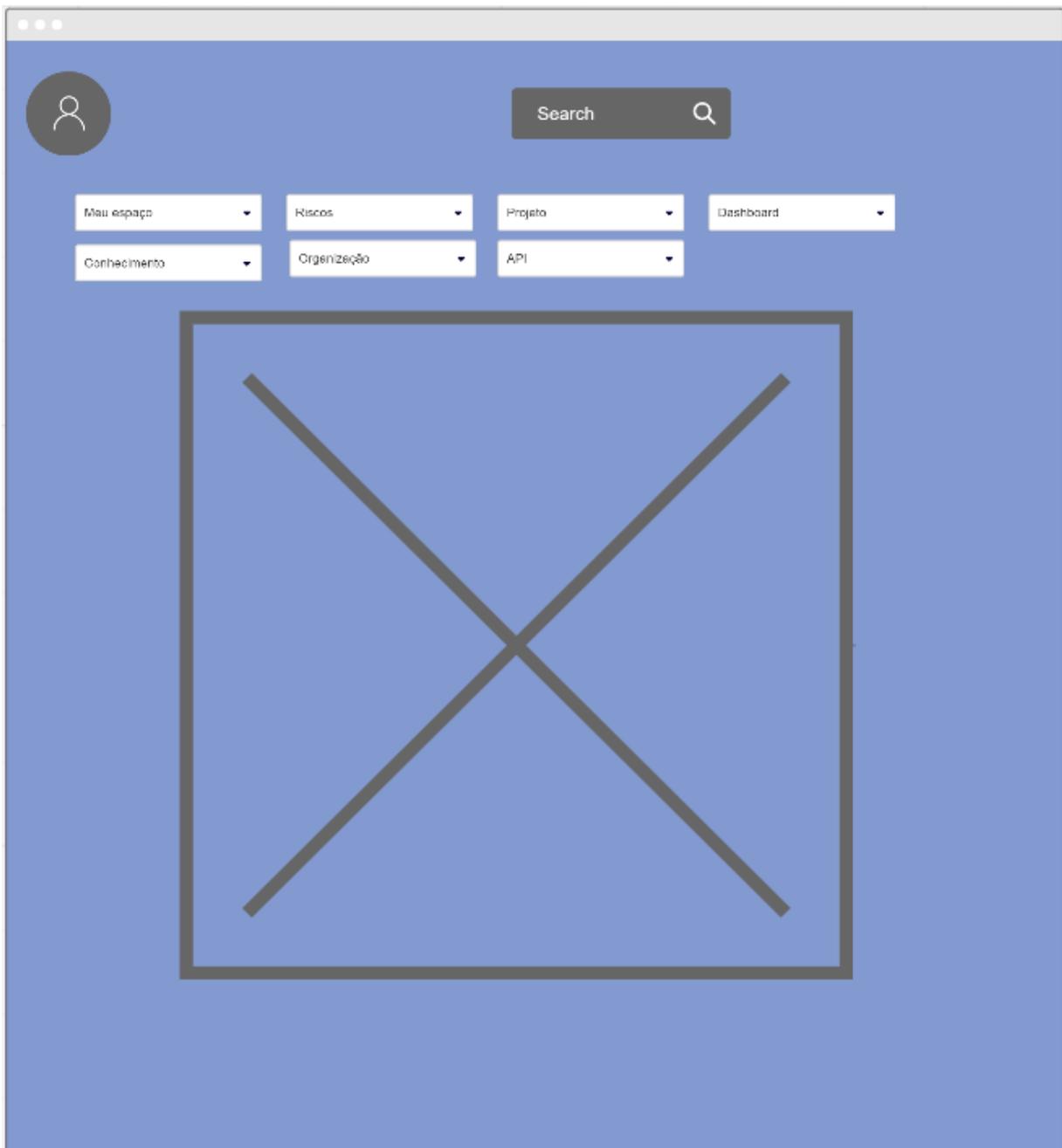


Descrição : A tela mostra ao usuário quais ferramentas então para serem analisadas, permitindo adicionar a analisar no menu à direita.

Passos:Menu-> Meu espaço -> minhas atividades-> Buscar projeto-> Clicar na lupa-> Navegar no menu ao lado direito -> adicionar análise de sua responsabilidade-> Enviar análise.

Interface 12 - Menu

Requisitos: RF007



Descrição :Ao acessar a ferramenta o usuário encontra todas as opções de navegação dentro do sistema.

Passos:Login-> Selecionar qual área deseja acessar clicando sobre.

Interface 13 - Cadastro de fornecedor

Requisitos:RF023

Área

Dados de fornecedores semelhantes

Tab 1 Tab 2 Tab 3

Quantidade de fornecedores encontrados: xx

Nome

Responsável

Contato

Soluções

Descrição

Projetos associados

Tab 1 Tab 2 Tab 3

Quantidade de projetos encontrados: xx

←

Descrição : Nesta tela, o usuário poderá cadastrar novos fornecedores do “zero”, com suas informações de nome, responsável, contato, soluções e descrição. Ou ainda, visando manter a uniformidade e padronização das informações na

plataforma, e agilidade na inserção desses dados, consultar cadastros de fornecedores anteriores e projetos associados.

Passos: Menu -> Organização -> Cadastro dos fornecedores ->

- 1) Área -> Dados dos fornecedores (opções 1, 2, 3 ...) e Projetos associados (opções 1, 2, 3 ...)*
- 2) Inserção de dados (Nome, Responsável, Contato, Soluções, Descrição) -> Cadastrar*

Interface 14 - Configurar API

Requisitos:RF019

Configuração de API

API Details
Authenticationr

GET

NOTES

Baixar documentação da API

Descrição : Ao acessar esta página o usuário consegue configurar uma API e adicionar uma descrição (notes).

Passos:Menu-> Configuração da API

Anexo I

Atividades extraídas das boas práticas

Conjunto de atividades descritas listadas e associadas com as práticas do COBIT 5 [15], apresentada na Tabela I:

Tabela I.1: Atividades extraídas do COBIT 5 [15]

Prática	Atividade descrita	Referência
Avalie as capacidades atuais, desempenho e digital/maturidade da empresa	Manter uma linha de base de negócios atuais e capacidades de serviços de TI identificando suas amplas categorias para definir as aquelas que apoiam a estratégia da empresa, bem como as restrições que devem ser abordadas, incluindo tanto em toda a empresa quanto restrições específicas do projeto (por exemplo, tempo, cronograma, recursos, etc.) para entender os negócios atuais, problemas, gargalos de processo ou outras restrições onde tecnologias agregariam	APO02.02 APO03.01 APO04.02 EDM02.01
Crie um ambiente propício à inovação	Incentive ideias de inovação de clientes, fornecedores e parceiros de negócios. Manter uma compreensão da estratégia empresarial e TI e operações empresariais e atuais desafios para aplicar o conhecimento para identificar a tecnologia potencial de valor agregado e inovar a TI	APO04.01 APO04.02 APO04.03 APO09.01

Tabela I.1 – Atividades extraídas do COBIT 5 [15]

Prática	Atividade descrita	Referência
Gerenciar finanças e contabilidade	Gerenciar e classificar os custos relacionados	APO06.01
Identifique os serviços de TI	Avaliar os serviços e níveis de serviço atuais de TI para identificar lacunas entre os serviços existentes e as atividades de negócios que eles suportam. Identificar áreas para melhoria dos serviços existentes e opções de nível de serviço	APO09.01
Monitore e relate os níveis de serviço	Monitorar e coletar dados de nível de serviço para avaliar o desempenho dos contratos de serviço de acordo com os termos acordados para garantir que estejam em vigor e atualizados e fornecer relatórios regulares e formais do desempenho do contrato de serviço. Se necessário chegue a um acordo sobre planos de ação, remediações e revisão do contrato de serviço existente para quaisquer problemas de desempenho ou tendências negativas	APO09.04 APO09.05
Identifique e avalie relacionamentos e contratos com fornecedores	Identificar, registrar e categorizar fornecedores e contratos de acordo com critérios (tipo, importância e criticidade)	APO10.01
Selecione fornecedores	Reunir as soluções e revisar propostas para garantir que reflitam claramente os requisitos da área solicitante	APO10.02
Selecione fornecedores	Selecione o mais adequado com base em critérios de viabilidade, incluindo risco e custo resultando no fornecedor que melhor atende aos requisitos. Certifique-se de que o patrocinador do negócio ou proprietário do produto faça a escolha final da solução	APO10.02 BAI02.02 BAI02.04
Selecione fornecedores	Obter aconselhamento jurídico	APO10.02
Selecione fornecedores	Preparar o contrato e incluir os direitos e obrigações de todas as partes e os potenciais riscos e seus tratamentos	APO10.02 APO10.04

Tabela I.1 – Atividades extraídas do COBIT 5 [15]

Prática	Atividade descrita	Referência
Selecione fornecedores	Assinar o contrato	APO10.02
Gerenciar relacionamentos e contratos com fornecedores	Atribuir responsáveis internos pelo projeto de terceirização	APO10.03
Gerenciar relacionamentos e contratos com fornecedores	Acordar, gerenciar, manter e renovar contratos formais com o fornecedor. Confirme se os prestadores de serviços cumprem as normas legais e requisitos regulamentares e obrigações contratuais	APO10.03 MEA02.01
Gerenciar relacionamentos e contratos com fornecedores	Confirmar que os requisitos acordados estão sendo atendidos de forma adequada	APO10.03
Gerenciar relacionamentos e contratos com fornecedores	Definir e formalizar funções e responsabilidades para cada fornecedor	APO10.03
Gerenciar o risco do fornecedor	Identificar, monitorar e, quando apropriado, gerenciar os riscos relacionados à capacidade do fornecedor de entregar o serviço contratado	APO10.04
Monitore o desempenho e a conformidade do fornecedor	Definir pontos de verificação e documentar os critérios para monitorar o desempenho do fornecedor alinhado com os acordos de nível de serviço. No final de cada marco, facilite a discussão dos critérios aprovados com as partes interessadas	APO10.05 BAI01.05
Monitore o desempenho e a conformidade do fornecedor	Monitorar e analisar a entrega do serviço para garantir que o fornecedor está oferecendo uma qualidade de serviço aceitável, atendendo os requisitos e aderência às condições do contrato	APO10.05

Tabela I.1 – Atividades extraídas do COBIT 5 [15]

Prática	Atividade descrita	Referência
Gerenciar o engajamento das partes interessadas	Identificar, envolver e gerenciar as partes interessadas dentro e fora da empresa suas preocupações e objetivos	BAI01.03 EDM05.01 APO03.01
Desenvolver e manter o plano do programa	Especifique o custo, o cronograma e as interdependências com outros projetos	BAI01.04
Inicie e execute o programa	Gerenciar cada projeto para garantir que as atividades de tomada de decisão e entrega sejam focadas no valor, abordando os riscos e atendendo aos requisitos das partes interessadas	BAI01.05
Fechar um programa	Trazer o programa a um encerramento ordenado, incluindo aprovação formal. Revise e documente as lições aprendidas	BAI01.09
Definir e manter o negócio funcional e técnico requisitos	Garantir que todos os requisitos das partes interessadas, incluindo critérios de aceitação relevantes, sejam considerados, capturados, priorizados e registrados em termos de como deve ser a lacuna entre os recursos de negócios atuais e desejados abordado	BAI02.01
Definir e manter o negócio funcional e técnico requisitos	Especificar e priorizar informações, requisitos funcionais e técnicos	BAI02.01
Definir e manter o negócio funcional e técnico requisitos	Rastreie e controle o escopo, os requisitos e as mudanças ao longo do ciclo de vida da solução conforme a compreensão da solução evolui	BAI02.01
Realizar um estudo de viabilidade e formular soluções alternativas	Definir e executar um estudo de viabilidade, piloto ou solução básica de trabalho que descreva de forma clara e concisa a alternativa soluções e mede como eles satisfariam os requisitos de negócios e funcionais	BAI02.02
Adquira componentes da solução	Siga as aprovações necessárias nos principais pontos de decisão durante os processos de aquisição	BAI03.04

Tabela I.1 – Atividades extraídas do COBIT 5 [15]

Prática	Atividade descrita	Referência
Adquira componentes da solução	Monitore e controle os serviços, ativos e recursos de TI criados ou alterados como resultado do projeto. Observe a implementação e datas em serviço. Registre o recebimento de todas as aquisições de infraestrutura e software em um inventário de ativos	BAI03.04 BAI01.06
Soluções de construção	Configure o software aplicativo adquirido para atender aos requisitos de processamento de negócios	BAI03.05
Gerenciar mudanças nos requisitos	Avalie o impacto de todas as solicitações de mudança da solução no desenvolvimento da solução. Categorize e priorize-os de acordo	BAI03.09
Gerenciar mudanças nos requisitos	Rastreie as mudanças nos requisitos, permitindo que todas as partes interessadas monitorem, revisem e aprove as mudanças	BAI03.09
Gerenciar serviços terceirizados de TI	Garantir que os requisitos da empresa para a segurança dos processos de informação, prioridades de processamento de TI e negócios operacionais cumpram os contratos	DSS01.02
Definir a política de continuidade de negócios, objetivos e escopo	Identificar atividades de serviço que são essenciais para as operações da empresa. Obtenha um entendimento comum entre a TI e as outras funções de negócios sobre as oportunidades potenciais para a TI permitire contribuir para a estratégia empresarial	DSS04.01 EDM02.01
Desenvolva e implemente uma resposta de continuidade de negócios	Certifique-se de que os principais fornecedores e parceiros terceirizados tenham planos de continuidade eficazes em vigor. Obtenha evidências auditadas conforme necessário	DSS04.03

Conjunto de atividades descritas listadas e associadas com as fases propostas pela ISO 37500 [10], apresentada na Tabela I:

Tabela I.2: Fases e atividades extraídas da ISO 37500 [10]

Fase	Referencia Atividade	Atividade	Descrição
Análise de estratégia de terceirização	AET01	verificar os pré-requisitos da terceirização	Garantir a identificação do negócio e suas funções juntamente como alinhamento deles com as estratégias e objetivos de sourcing, e garantir que estas sejam específicas o suficiente para ser capaz de julgar e direcionar se as iniciativas de terceirização contribuirão para os objetivos estratégicos e considerar os serviços, desafios e mercados atuais e futuros
	AET02	compreender os serviços elegíveis para terceirização	identificar os serviços, seu papel na cadeia de valor da organização, sua importância estratégica, seus elementos, recursos e ativos, custos, riscos e restrições destacando metas de melhoria e restrições estratégicas
	AET03	avaliar o impacto organizacional da terceirização de serviços	Determinar os benefícios da terceirização em comparação com a situação atual, seus custos, riscos e restrições envolvidos entendendo todos os fatores impactados após a terceirização
	AET04	definir estratégia de terceirização	Determinar abordagem do risco, seleção de fornecedores, transferência os envolvidos (internos e externos) e transformação da terceirização na organização
	AET05	avaliar e decidir	Decidir pela terceirização ou não baseada no consolidado das informações
	AET06	montar projeto de terceirização	criar um termo de abertura do projeto, determinar os limites do projeto em termos de custos, escopo, tempo, etc
Iniciação e Seleção	IS01	detalhar os serviços necessários	Descrever todas as informações possíveis sobre os serviços necessários como: qualidade, quantidade, preço, indicadores de medição de desempenho, limites do serviço, avaliação dos riscos

Tabela I.2 – *Fases e atividades extraídas da ISO 37500 [10]*

Fase	Referencia Atividade	Atividade	Descrição
	IS02	definir os requisitos e estrutura do contrato	Fazendo uso de acordos existentes como referência, definir (ou analisar) requisitos e estrutura do contrato
	IS03	identificar provedores potenciais	elaborar e preparar uma lista de provedores potenciais (sejam eles novos, ou com contratos vigentes na instituição) ponderados e classificados de acordo com os requisitos definidos
	IS04	fornecedores da lista restrita	Solicitar propostas
			analisar e ordenar as propostas recebidas de acordo com os requisitos e limitantes definidos
	IS05	contratos básicos	revisar e avaliar legalmente os contratos de terceirização
			identificar questões abertas para negociações
	IS06	negociar e estabelecer acordos	negociar acordos
			finalmente selecione o provedor apropriado
			assinar os contratos
Transição	T1	estabelecer a equipe do projeto de transição	definir, atribuir funções e responsabilidades aos membros individuais da equipe do cliente e do provedor
	T2	estabelecer governança de terceirização	fornecer ambiente de trabalho e infraestrutura, se aplicável
			validar se as funções e responsabilidades são compreendidas e podem ser desempenhadas

Tabela I.2 – *Fases e atividades extraídas da ISO 37500 [10]*

Fase	Referencia Atividade	Atividade	Descrição
			definir o processo de avaliação do progresso do projeto e revisão dos principais documentos e entregas do projeto
	T3	refinar a estrutura de entrega e o plano de transição	refinar a estrutura de entrega realizando uma análise de lacunas, definindo métricas e medições e gerenciamento de desempenho
			iniciar a aquisição e/ou configuração de maquinários, softwares e licenças regulatórias, outras atividades que tenham prazo de entrega
	T4	refinar a aquisição de conhecimento	fornecer recursos operacionais, incluindo ambiente de trabalho e infraestrutura, tanto pelo cliente quanto pelo fornecedor, para apoiar a aquisição de conhecimento e elaboração de documentos conforme apropriado
	T5	realizar a transição de conhecimentos, pessoas, processos e tecnologia	implementar todos os procedimentos, currículos e manuais de treinamento, planos de treinamento, apostilas, padrões e SOPs
			fornecer direitos de usuário, níveis de acesso, restrições, etc. em ambientes de trabalho do cliente e do provedor
			garantir que a transferência de conhecimento seja concluída por meios apropriados, incluindo programas de treinamento / autoestudo, políticas operacionais, procedimentos e práticas aplicáveis no novo ambiente
			assegurar que todas as alterações / revisões pendentes nos sistemas e processos sejam implementadas

Tabela I.2 – *Fases e atividades extraídas da ISO 37500 [10]*

Fase	Referencia Atividade	Atividade	Descrição
	T6	implantar as estruturas de qualidade, risco, auditoria e conformidade	implementar mecanismo de obtenção de informações das equipes de gestão de qualidade, riscos, conformidade e desempenho de um fornecedor
	T7	implantar a estrutura de gerenciamento de ativos e conhecimento	implementar a política de gestão de registros para a manutenção da atualidade dos registros
	T8	implantar estruturas de tipo de entrega	atribuir recursos de acordo com o plano de capacidade e introduzir tarefas e responsabilidades
	T9	testar a capacidade de entrega do serviço	invocar planos de continuidade de negócios e capacidade da equipe de resposta
	T10	piloto e transferência	realizar o piloto executado pelo provedor de acordo com o plano e consolidar os resultados de desempenho
			transferir o processo formalmente de acordo com o plano de ativação mutuamente acordado
Entrega de valor	EV1	prestar serviço	planejamento e acompanhamento das atividades de prestação de serviços ou utilização de ferramentas. Deve abranger a gestão dos ativos físicos, da infraestrutura tecnológica, de software e das pessoas. Os planos de entrega de serviço devem ser atualizados como uma atividade de gerenciamento contínua

Tabela I.2 – *Fases e atividades extraídas da ISO 37500 [10]*

Fase	Referencia Atividade	Atividade	Descrição
			fornecer treinamento para ajudar os usuários finais a obter o melhor do serviço prestado
			obter e analisar o feedback das partes interessadas
	EV2	monitorar e revisar o desempenho do serviço	relatórios de desempenho de serviço e relacionamento devem ser produzidos de acordo com um cronograma acordado, o que permite uma avaliação periódica de desempenho acordada
	EV3	gerenciar e resolver problemas	um processo documentado para registrar, classificar, escalar e comunicar questões e problemas com base em sua gravidade
	EV4	entregar e gerenciar mudanças	procedimentos documentados para registrar, classificar, avaliar e aprovar solicitações de mudança que devem levar em consideração os riscos, os impactos potenciais aos serviços, o cliente, os requisitos do serviço, os benefícios do negócio, a viabilidade técnica e o impacto financeiro
	EV5	entregar inovação (opcional)	capturar ideias de inovação que devem explorar os benefícios potenciais para o negócio e caso de investimento que devem resultar em projetos de iniciativas para aplica-los
	EV6	administrar as finanças	documentar e implementar os procedimentos necessários para gerenciar e controlar os aspectos financeiros do acordo
			executar a administração financeira para o contrato, criação, validação e processamento de notas fiscais. gerenciamento de problemas de pagamento e gerenciamento de preços
	EV7	gerenciar relacionamentos	garantir que cliente e fornecedor sejam claros sobre os comportamentos esperados um do outro, em particular garantindo abertura, transparência e comunicação honesta em todos os momentos. Os processos também devem abranger a integração de novos membros da equipe

Tabela I.2 – *Fases e atividades extraídas da ISO 37500 [10]*

Fase	Referencia Atividade	Atividade	Descrição
			garantir que as expectativas de desempenho estejam alinhadas com os requisitos acordados por meio de interações regulares com as partes interessadas e definição de expectativas
	EV8	gerir o contrato	garantir que o acordo permaneça atual e atualizado. Quaisquer mudanças no acordo devem ser tratadas e assinadas pelo comitê de governança apropriado
			fornecer alterações e / ou renovação do acordo com consentimento mútuo
	EV9	garantia de valor e business case	documentar os resultados da análise de valor e compartilhá-los com o fornecedor para ajudar a facilitar as melhorias de desempenho
	EV10	continuação ou término da preparação do contrato	identificar os critérios para tomar a decisão de continuação
			manutenção de um plano de saída atualizado, que seja bem compreendido, compreensível e tenha sido testado e revisado quanto à integridade e adequação contínua; o plano de saída deve incluir direitos de propriedade intelectual (DPI) e conhecimento do processo, que são essenciais para a continuidade do negócio

Atividades resultantes da extração de boas práticas, suas descrições e referências são compiladas e apresentadas da Tabela I:

Tabela I.3: Atividades, descrições e referências das boas práticas

Atividade (31000 + 37500 + COBIT)	Descrição	Referências COBIT	Referências 37500	Referências 31000
verificar os pré-requisitos da terceirização	Garantir a identificação do negócio, identificando suas amplas categorias e suas funções juntamente como alinhamento deles com as estratégias e objetivos de sourcing, e garantir que estas sejam específicas o suficiente para ser capaz de julgar e direcionar se as iniciativas de terceirização contribuirão para os objetivos estratégicos e considerar os serviços, desafios e mercados atuais e futuros	APO02.02 APO03.01 APO04.02 EDM02.01	AET01	
Identificar serviços impactados	identificar os serviços, seu papel na cadeia de valor da organização, sua importância estratégica, seus elementos, recursos e ativos, custos, riscos e restrições destacando metas de melhoria e restrições estratégicas	DSS04.01 EDM02.01	AET02	Contexto risco
Avaliar o impacto organizacional da terceirização	Determinar os benefícios da terceirização em comparação com a situação atual, seus custos, riscos e restrições envolvidos entendendo todos os fatores impactados após a terceirização		AET03	Contexto risco

Tabela I.3 – Atividades, descrições e referências das boas práticas

Atividade (31000 + 37500 + COBIT)	Descrição	Referências COBIT	Referências 37500	Referências 31000
Definir estratégia de terceirização	Determinar abordagem do risco, seleção de fornecedores, transferência os envolvidos (internos e externos) e transformação da terceirização na organização		AET04	
Consultar catálogo base de TI	Avaliar os serviços e níveis de serviço atuais de TI para identificar lacunas entre os serviços existentes e as atividades de negócios que eles suportam. Identificar áreas para melhoria dos serviços existentes e opções de nível de serviço	APO09.01		
Gerenciar partes interessadas	Identificar, envolver e gerenciar as partes interessadas dentro e fora da empresa suas preocupações e objetivos	BAI01.03 EDM05.01 APO03.01		
Descrever contexto de riscos, prazos e custos da solicitação	Especifique o custo, o cronograma e as interdependências com outros projetos	BAI01.04		Contexto risco
Deliberar sobre a realização da terceirização	Decidir pela terceirização ou não baseada no consolidado das informações		AET05	
Montar projeto base de terceirização	criar um termo de abertura do projeto, determinar os limites do projeto em termos de custos, escopo, tempo, etc		AET06	

Tabela I.3 – Atividades, descrições e referências das boas práticas

Atividade (31000 + 37500 + COBIT)	Descrição	Referências COBIT	Referências 37500	Referências 31000
Detalhar os serviços necessários	Descrever todas as informações possíveis sobre os serviços necessários como: qualidade, quantidade, preço, indicadores de medição de desempenho, limites do serviço, avaliação dos riscos	BAI02.01	IS01	Contexto risco
Definir os requisitos e estrutura do contrato	Fazendo uso de acordos existentes como referência, definir (ou analisar) requisitos e estrutura do contrato incluindo os direitos e obrigações de todas as partes		IS02	
Identificar provedores potenciais	Identificar, registrar e categorizar fornecedores e contratos de acordo com critérios (tipo, importância e criticidade)	APO10.01	IS03	
Solicitar propostas	Solicitar proposta dos fornecedores		IS04	
Analisar e ordenar as propostas recebidas	Reunir as soluções e revisar propostas para garantir que reflitam claramente os requisitos da área solicitante	APO10.02	IS04	
Obter aconselhamento jurídico		APO10.02	IS05	
Estabelecer acordos	Siga as aprovações necessárias nos principais pontos de decisão durante os processos de aquisição	BAI03.04	IS06	

Tabela I.3 – Atividades, descrições e referências das boas práticas

Atividade (31000 + 37500 + COBIT)	Descrição	Referências COBIT	Referências 37500	Referências 31000
Selecionar provedor	Selecione o mais adequado com base em critérios de viabilidade, incluindo risco e custo resultando no fornecedor que melhor atende aos requisitos. Certifique-se de que o patrocinador do negócio ou proprietário do produto faça a escolha final da solução	APO10.02 BAI02.02 BAI02.04	IS06	
Realizar avaliação dos riscos	Identificação riscos e seus tratamentos	APO10.02 APO10.04		Avaliação risco
Assinar o contrato		APO10.02	IS06	
Estabelecer a equipe do projeto de transição	definir, atribuir funções e responsabilidades aos membros individuais da equipe do cliente e do provedor	APO10.03	T1	
Monitorar riscos durante a implantação	Identificar, monitorar e, quando apropriado, gerenciar os riscos relacionados à capacidade do fornecedor de entregar o serviço contratado	APO10.04		Avaliação e tratamento risco
Avaliar plano de continuidade dos fornecedores	Certifique-se de que os principais fornecedores e parceiros terceirizados tenham planos de continuidade eficazes em vigor. Obtenha evidências auditadas conforme necessário	DSS04.03	T9	

Tabela I.3 – Atividades, descrições e referências das boas práticas

Atividade (31000 + 37500 + COBIT)	Descrição	Referências COBIT	Referências 37500	Referências 31000
Estabelecer governança de terceirização	definir o processo de avaliação do progresso do projeto e revisão dos principais documentos e entregas do projeto	BAI02.02	T2	
Refinar a estrutura de entrega e o plano de transição	iniciar a aquisição e/ou configuração de maquinários, softwares e licenças regulatórias, outras atividades que tenham prazo de entrega		T3	
Refinar a aquisição de conhecimento	fornecer recursos operacionais, incluindo ambiente de trabalho e infraestrutura, tanto pelo cliente quanto pelo fornecedor, para apoiar a aquisição de conhecimento e elaboração de documentos conforme apropriado		T4	
Realizar a transição de conhecimentos, pessoas, processos e tecnologia	implementar todos os procedimentos, currículos e manuais de treinamento, planos de treinamento, apostilas, padrões e SOPs. Fornecer direitos e acessos. Garantindo que a transferência de conhecimento seja concluída por meios apropriados, assegurando que todas as alterações / revisões pendentes nos sistemas e processos sejam implementadas		T5	

Tabela I.3 – Atividades, descrições e referências das boas práticas

Atividade (31000 + 37500 + COBIT)	Descrição	Referências COBIT	Referências 37500	Referências 31000
Implantar as estruturas de qualidade, risco, auditoria e conformidade	implementar mecanismo de obtenção de informações das equipes de gestão de qualidade, riscos, conformidade e desempenho de um fornecedor		T6	Avaliação risco
Implantar a estrutura de gerenciamento de ativos e conhecimento	implementar a política de gestão de registros para a manutenção da atualidade dos registros		T7	
Implantar estruturas de tipo de entrega	atribuir recursos de acordo com o plano de capacidade e introduzir tarefas e responsabilidades		T8	
Finalizar transferência	transferir o processo formalmente de acordo com o plano de ativação mutuamente acordado		T10	
Iniciar terceirização	Gerenciar cada projeto para garantir que as atividades de tomada de decisão e entrega sejam focadas no valor, abordando os riscos e atendendo aos requisitos das partes interessadas	BAI01.05		Monitoramento risco
Configurar ferramenta/serviço	Configure ferramenta/serviço adquirido para atender aos requisitos de processamento de negócios	BAI03.05		
Realizar treinamentos necessários	fornecer treinamento para ajudar os usuários finais a obter o melhor da terceirização		EV1	

Tabela I.3 – Atividades, descrições e referências das boas práticas

Atividade (31000 + 37500 + COBIT)	Descrição	Referências COBIT	Referências 37500	Referências 31000
Gerenciar escopo da terceirização	Rastreie e controle o escopo, os requisitos e as mudanças ao longo do ciclo de vida da solução conforme a compreensão da solução evolui	BAI02.01		
Monitorar a terceirização	Monitorar e coletar dados de nível de serviço para avaliar o desempenho dos contratos de serviço de acordo com os termos acordados para garantir que estejam em vigor e atualizados e fornecer relatórios regulares e formais do desempenho do contrato de serviço. Se necessário chegue a um acordo sobre planos de ação, remediações e revisão do contrato de serviço existente para quaisquer problemas de desempenho ou tendências negativas	APO09.04 APO09.05		
Gerenciar e resolver problemas	registrar, classificar, escalar e comunicar questões e problemas com base em sua gravidade		EV3	
Monitorar e revisar o desempenho da terceirização	Definir pontos de verificação e documentar os critérios para monitorar o desempenho do fornecedor alinhado com os acordos de nível de serviço. No final de cada marco, facilite a discussão dos critérios aprovados com as partes interessadas	APO10.05 BAI01.05		

Tabela I.3 – Atividades, descrições e referências das boas práticas

Atividade (31000 + 37500 + COBIT)	Descrição	Referências COBIT	Referências 37500	Referências 31000
Gerir o contrato	Garantir que os requisitos da empresa para a segurança dos processos de informação, prioridades de processamento de TI e negócios operacionais cumpram os contratos	DSS01.02	EV8	
Analisar terceirização	Monitorar e analisar a entrega do serviço para garantir que o fornecedor está oferecendo uma qualidade de serviço aceitável, atendendo os requisitos e aderência às condições do contrato	APO10.05		
Documentar informações sobre a terceirização	relatórios de desempenho de serviço e relacionamento devem ser produzidos de acordo com um cronograma acordado, o que permite uma avaliação periódica de desempenho acordada		EV2	
Gerenciar recursos de TI durante a terceirização	Monitore e controle os serviços, ativos e recursos de TI criados ou alterados como resultado do projeto. Observe a implementação e datas em serviço. Registre o recebimento de todas as aquisições de infraestrutura e software em um inventário de ativos	BAI03.04 BAI01.06		

Tabela I.3 – Atividades, descrições e referências das boas práticas

Atividade (31000 + 37500 + COBIT)	Descrição	Referências COBIT	Referências 37500	Referências 31000
Gerenciar mu- danças	procedimentos documentados para registrar, classificar, avaliar e aprovar solicitações de mudança que devem levar em consideração os riscos, os impactos potenciais aos serviços, o cliente, os requisitos do serviço, os benefícios do negócio, a viabilidade técnica e o impacto financeiro	BAI03.09	EV4	
Definir funções e responsabilidades	garantir que cliente e fornecedor sejam claros sobre os comportamentos esperados um do outro, em particular garantindo abertura, transparência e comunicação honesta em todos os momentos. Os processos também devem abranger a integração de novos membros da equipe	APO10.03	EV7	
Alinhar expecta- tivas	garantir que as expectativas de desempenho estejam alinhadas com os requisitos acordados por meio de interações regulares com as partes interessadas e definição de expectativas		EV7	
Administrar cus- tos da terceiriza- ção	executar a administração financeira para o contrato, criação, validação e processamento de notas fiscais. gerenciamento de problemas de pagamento e gerenciamento de preços	APO06.01	EV6	

Tabela I.3 – Atividades, descrições e referências das boas práticas

Atividade (31000 + 37500 + COBIT)	Descrição	Referências COBIT	Referências 37500	Referências 31000
Incentivar inovações	Incentive ideias de inovação de clientes, fornecedores e parceiros de negócios. Manter uma compreensão da estratégia empresarial e TI e operações empresariais e atuais desafios para aplicar o conhecimento para identificar a tecnologia potencial de valor agregado e inovar a TI	APO04.01 APO04.02 APO04.03 APO09.01	EV5	
Analisar renovação da terceirização	identificar os critérios para tomar a decisão de continuação		EV10	
Finalizar terceirização	Trazer o programa a um encerramento ordenado, incluindo aprovação formal. Revise e documente as lições aprendidas	BAI01.09		

Peso de cada fase baseado na média por prática, apresentado na Tabela I:

Tabela I.4: Peso de cada fase baseado no peso médio das práticas

Fase	Peso
Análise de estratégia de terceirização	152
Iniciação e Seleção	106,67
Transição	63
Entrega de valor	231,83

Anexo II

Comparativo das ferramentas de gestão de riscos existentes

A Figura II.1 apresenta a tabela comparativa entre ferramentas de gestão de riscos baseadas nas categorias elaboradas a das informações retiradas dos sites GetApp[12], SourceForge[13] e Capterra[14]. O 1 é indicativo que a ferramenta apresenta e a célula vazia indica que a ferramenta não apresenta dada categoria:

Sistema / Funcionalidade	Donesafe	Onspring	Risk/Secure Watch	IBM OpenPages	Fusion Framework System	Soft'epert	INTERISK	Riskid	TRAC governance cloud	A1 Tracker	ZenGRC	FORM Op1	Resolver	SoNE pert ERM	Modulo Risk Manager	FLOWTI	Portal ISO	Open Source Risk Engine	SimpleRisk	Eramba	RA Risk Coverage Software	PTA Professional	OpenVAS	Project Risk Manager
Gestão de risco de TI	1	1	1		1		1		1		1				1	1	1	1				1	1	1
Gerenciamento de serviços e objetivos de negócios				1			1		1			1			1	1		1					1	1
Obrigações de contrato / gerenciamento de métricas	1	1	1						1															
Pesquisas de satisfação				1		1			1				1											
Gerenciamento de reuniões	1		1		1		1	1	1						1	1								
Gerenciamento de riscos e problemas	1	1	1	1	1	1	1	1	1	1	1	1	1		1		1	1	1	1	1	1	1	1
Relatórios e painéis	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1								
Relatórios de trabalho e os relatórios são automatizados	1	1	1	1	1	1	1	1	1						1	1								
Única plataforma			1	1	1		1	1	1					1	1		1							
Versão Mobile	1		1						1															
Versão Gratuita																								
Assistência Consultoria (?)	1	1	1		1				1	1	1	1	1	1	1									
Interface simples, sem precisar de treinamento				1		1		1							1									
Treinamento									1															
Venda Web	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1							
Buy Side (fornecedores)/Gestão de fornecedores	1	1	1	1	1	1			1	1	1	1	1	1	1									
Restreamento de Conclusão									1			1					1							
Gestão do ciclo de vida do contrato				1					1	1	1					1								
Assinatura Eletrônica	1								1	1					1									
Pesquisa de Terço Completo									1	1	1		1	1	1									
Contratos Governamentais			1						1								1							
ESG/ Compliance	1	1	1				1																	
Modelos pré-construídos			1			1			1	1		1	1			1	1							
Lado de vendas (clientes)			1		1				1		1		1			1								
Contratos Especiais									1		1		1			1								
Controle de venda	1	1	1				1		1	1	1	1	1											
Gestão de furto de trabalho	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1			1	1	1	1	1	1	1
Alertas/notificações	1	1	1	1	1			1	1	1	1	1	1	1	1		1	1	1	1	1	1	1	1
Controle do andamento			1		1	1	1	1	1	1	1	1	1			1	1							1
Restreamento de conformidade	1	1	1						1		1	1	1	1	1	1								
Resumos e análise de dados			1	1	1	1	1	1	1	1	1	1	1	1	1	1	1							
Análise de painel de detalhamento em tempo real	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1							
Monitoramento do progresso da avaliação e remediação	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1							
Altamente/totamente personalizável	1	1	1	1	1						1	1	1	1	1									
Third party	1	1	1	1	1					1	1	1	1	1	1									
Auditoria	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1					1	1	1	1	1
Acompanhamento de despesas	1									1	1	1	1	1	1									
armazenamento de documentos	1	1			1	1	1	1	1	1	1	1	1	1	1									
Controles de acesso ou permissões	1	1	1		1	1	1	1	1	1	1	1	1	1	1									
Relatórios personalizáveis	1	1	1	1	1	1			1		1	1					1			1	1	1	1	1
Colaboração em equipe	1	1	1				1				1	1												
Controle de processos de aprovação	1	1			1					1														
Gestão de avaliação	1	1			1			1					1			1	1							
Conformidade com os padrões ISO	1	1	1			1	1	1						1	1	1	1				1	1	1	1
Código Aberto																								
Total de categorias presentes	29	25	29	17	24	14	22	8	29	26	19	22	21	13	29	17	9	6	7	7	7	7	5	5

Figura II.1: Tabela comparativa entre ferramentas de gestão de riscos baseadas em categorias genéricas. Fonte: [12] [13] [14]

A Figura II.2 apresenta a tabela comparativa das 10 ferramentas de gestão de riscos que apresentaram maior quantidade de funcionalidades em relação a sua aderência às boas práticas descritas na Tabela 4.3.

Referência da prática	Prática	Peso da prática	Módulo Risk Manager	Donesafe	Risk Watch	TRAC governance cloud	A1 Tracker	Onspring	Fusion Framework System	INTERISK	FORM OpX	Resolver
APO02.02	Avalie as capacidades atuais, desempenho e digital maturidade da empresa	20,5	20,5	20,5	20,5	20,5	20,5	20,5	20,5?	20,5	20,5	20,5
APO03.01	Desenvolva a visão da arquitetura corporativa	24	24	24	24	24	24	24	24	24	24	24
APO04.01	Crie um ambiente propício à inovação	7	0	0	0	0	0	0	7	0	0	0
APO04.02	Mantenha uma compreensão do ambiente corporativo	7	7	7	7	7	7	7	0	7	7	7
APO04.03	Monitore e analise o ambiente de tecnologia	7	0	0	0	0	0	0	0	0	0	0
APO06.01	Gerenciar finanças e contabilidade	19,5	0	0	19,5	0	19,5	19,5	0	0	19,5	19,5
APO09.01	Identifique os serviços de TI	18	18	0	18	18	18	18	0	0	0	18
APO09.04	Monitore e relate os níveis de serviço	18	18	18	18	18	18	18	18	18	18	18
APO09.05	Revise os acordos e contratos de serviço	18	18	18	18	18	18	18	0	18	18	18
APO10.01	Identifique e avalie relacionamentos e contratos com fornecedores	29	29	29	29	29	29	29	29	0	29	29
APO10.02	Selecione fornecedores	29	29	29	0	0	0	0	0	0	29	29
APO10.03	Gerenciar relacionamentos e contratos com fornecedores	29	29	29	29	29	29	29	29	29	29	29
APO10.04	Gerenciar o risco do fornecedor	29	29	29	29	29	29	29	29	29	29	29
APO10.05	Monitore o desempenho e a conformidade do fornecedor	29	29	29	29	29	29	29	29	29	29	29
BAI01.02	Iniciar um programa	14	14	14	14	14	14	14	0	14	14	14
BAI01.03	Gerenciar o engajamento das partes interessadas	14	14	0	0	14	0	0	0	14	14	14
BAI01.04	Desenvolver e manter o plano do programa	14	14	14	14	14	14	14	0	0	14	14
BAI01.05	Inicie e execute o programa	14	14	14	14	14	14	14	14	14	14	14
BAI01.06	Monitorar, controlar e relatar os resultados do programa	14	0	14	14	14	14	14	14	0	14	14
BAI01.09	Fechar um programa	14	14	14	14	14	14	14	0	14	14	14
BAI02.01	Definir e manter o negócio funcional e técnico requisitos	15	0	0	0	0	0	15	15	0	0	0
BAI02.02	Realizar um estudo de viabilidade e formular soluções alternativas	15	0	0	15	0	0	0	0	0	15	15
BAI02.04	Obtenha a aprovação de requisitos e soluções	15	0	15	15	15	15	15	0	0	15	15
BAI03.04	Adquirir componentes da solução	15	15	15	0	0	0	0	0	15	0	0
BAI03.05	Soluções de construção	15	15	15	15	15	15	15	15	0	15	15
BAI03.09	Gerenciar mudanças nos requisitos	15	15	15	15	15	15	15	15	15	15	15
DSS01.02	Gerenciar serviços terceirizados de TI	17	17	17	17	0	17	17	0	0	0	0
DSS01.05	Gerenciar instalações	17	17	17	17	0	17	17	0	0	0	0
DSS04.01	Definir a política de continuidade de negócios, objetivos e escopo	26	26	26	26	26	26	26	0	26	0	26
DSS04.03	Desenvolva e implemente uma resposta de continuidade de negócios	26	0	0	0	0	0	0	0	26	0	26
EDM02.01	Estabeleça o mix de investimento alvo	17,5	0	17,5	0	0	17,5	17,5	0	0	0	0
EDM04.01	Priorizar a alocação de recursos	24,5	0	0	0	0	0	0	0	0	0	0
EDM05.01	Avalie o envolvimento das partes interessadas e os requisitos de relatórios	23,5	23,5	23,5	23,5	23,5	23,5	23,5	0	23,5	23,5	0
	Total de pontos	609,5	449	463,5	454,5	400	457	472	238	336	419,5	466

Figura II.2: Tabela comparativa das ferramentas em relação às práticas. Fonte: autora

Anexo III

Primeira versão das funcionalidades e protótipos

É apresentado a seguir o resultado do trabalho realizado em conjunto com os alunos e a pesquisadora na especificação das funcionalidades que foram ordenadas e descritas, conforme apresentado a Tabela III.

Tabela III.1: Funcionalidades identificadas e descritas

ID	Nome	Descrição
RF001	Atualizar informações cadastradas em tempo real	A ferramenta deve permitir o acompanhamento em tempo real do desenvolvimento das atividades.
RF002	Associar os riscos com as áreas envolvidas	Permitir a associação dos riscos com as áreas envolvidas
RF003	Registrar as necessidades de terceirização	Permitir a área do solicitante registrar as necessidades da terceirização, a fim do gestor de TI buscar a solução.
RF004	Receber alertas sobre riscos	Permite alertar periodicamente sobre os eventos de riscos que estão sendo analisados e monitorados.
RF005	Fazer login na ferramenta	Permite ao usuário acesso e interação com a plataforma por meio de input em forma de preenchimento de informações que a plataforma necessita.
RF006	Cadastrar usuários na ferramenta	Permite cadastrar e excluir usuários e modificar informações dos mesmos.

Tabela III.1 – *Funcionalidades identificadas e descritas*

ID	Nome	Descrição
RF007	Gerenciar níveis de acesso	Permite aos usuários acessarem as telas do sistema de acordo com suas necessidades e grau hierárquico.
RF008	Cadastrar projetos de terceirização	Permite o usuário cadastrar os projetos de terceirização.
RF009	Cadastrar riscos	Permite ao usuário cadastrar todos os riscos envolvidos no processo de terceirização.
RF010	Classificar risco	Permite ao usuário classificar todos os riscos envolvidos no processo de terceirização, avaliando o risco em relação ao impacto do risco do desprezível ao extremo e a probabilidade dele do raro ao muito provável.
RF011	Monitorar os riscos	Permite que o usuário tenha uma visão sobre os riscos que já foram identificados no processo, de forma que ele venha ter acesso ao seu monitoramento e assim tomar decisões melhores.
RF012	Ter uma visualização geral dos riscos dos projetos	Permite que o usuário tenha uma visualização geral dos riscos do projeto, com as informações do impacto e probabilidade de cada um.
RF013	Ter uma visualização geral dos projetos	Permite ao usuário ter uma noção consolidada dos projetos que estão em execução pela instituição.
RF014	Associar riscos com as atividades do processo	Permite ao usuário informações detalhadas sobre os riscos atrelados no processo de forma específica de acordo com a atividade.
RF015	Tratar os riscos (Matriz Eisenhower)	Fornece ao usuário a matriz de Eisenhower com os eixos Importante e Urgente, para identificar os riscos que devem ser tratados primeiro e fornecer o melhor método para tratar o risco.
RF016	Acompanhar os projetos de terceirização	Permite o usuário acompanhar as fases de terceirização

Tabela III.1 – *Funcionalidades identificadas e descritas*

ID	Nome	Descrição
RF017	Consultar terceirizações já finalizadas	Permite que após a finalização do processo das terceirizações, quando já finalizadas, permite que em forma de histórico fique registrado facilitando a consulta ao usuário para consultar um projeto específico.
RF018	Comparar projetos de terceirização quanto aos riscos	Permite ao usuário comparar os riscos de terceirização entre projetos em andamentos, em fase inicial e encerrados .
RF019	Configurar API	Permite a comunicação de serviços ou produtos sem a necessidade de saber como foram implementados, de forma que o trâmite de informação seja simplificado.
RF020	Buscar informações dos projetos de terceirização	Permite o usuário ter acesso a informações, riscos, histórico e demais informações relevantes de outros processos de terceirização finalizados ou em andamento
RF021	Priorizar os riscos	Permite ao usuário classificar o risco e indicar a prioridade para o projeto.
RF022	Personalização da ferramenta (relatórios, painéis)	Permite gerar relatório e painéis personalizados, segundo a necessidade do usuário.
RF023	Gestão de Fornecedores	Permite fazer a avaliação, acompanhamento, manter histórico dos fornecedores.
RF024	Manter listas de soluções alternativas em projetos	Permite salvar uma lista alternativas de soluções para as demandas de terceirização.

Conjunto de telas prototipadas associadas a funcionalidades e boas práticas, resultado de um trabalho em conjunto entre a pesquisadora e os alunos, são apresentadas nas imagens a seguir.

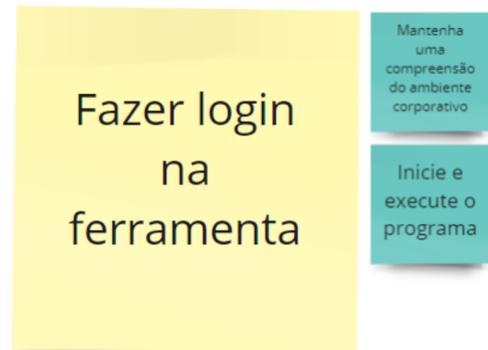
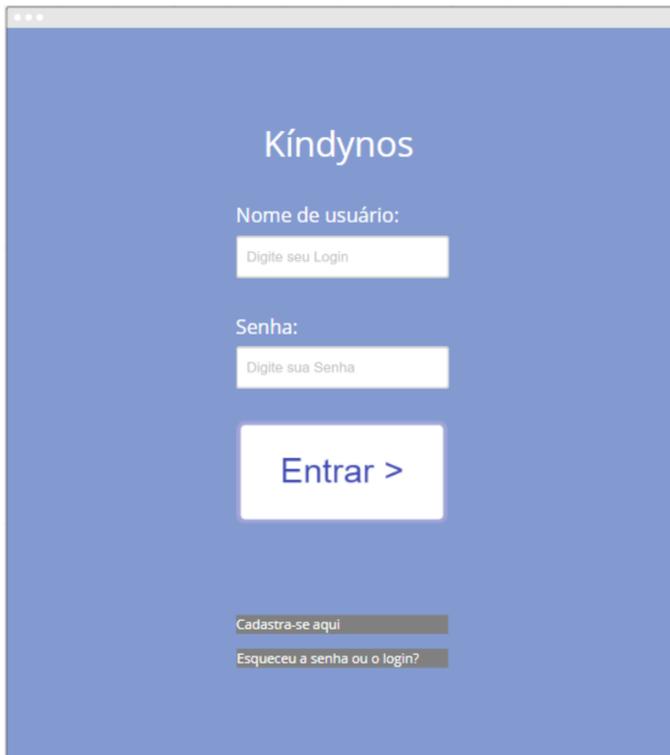


Figura III.1: Tela de Login. Fonte: autora

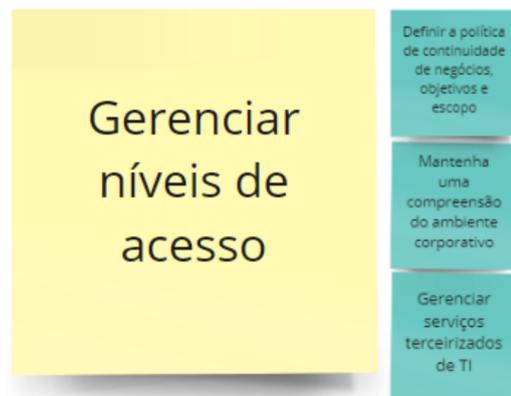
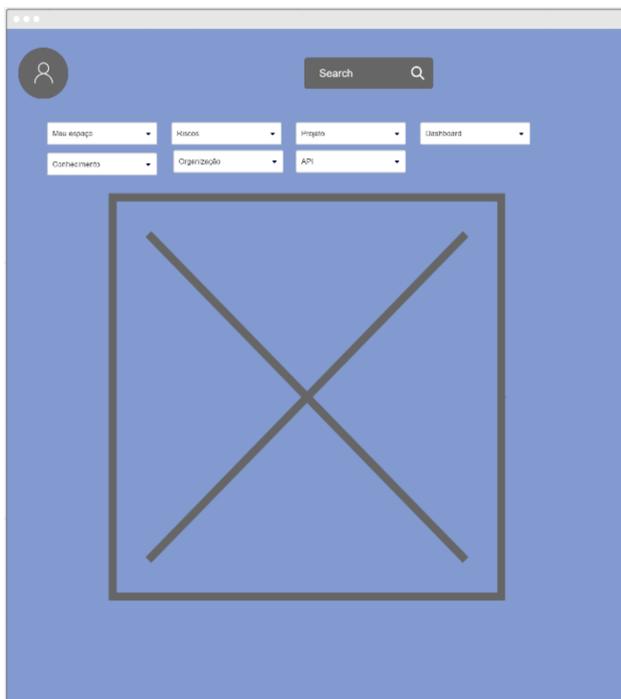


Figura III.2: Tela do Menu. Fonte: autora

Projetos:	Área	Última Atualização:	Responsável	estado
Projeto1	Financeiro	24/10/21	João Cândido	Aprovado
Projeto2	Facilities	23/09/21	Carlos Gomes	Terminado
Projeto3	Dados	05/10/21	Clara Souza	Aprovado

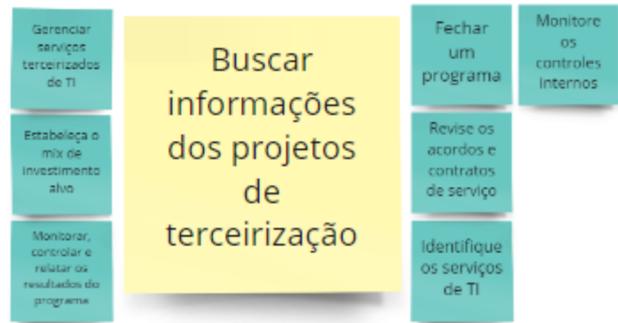


Figura III.3: Tela de lista de projetos. Fonte: autora

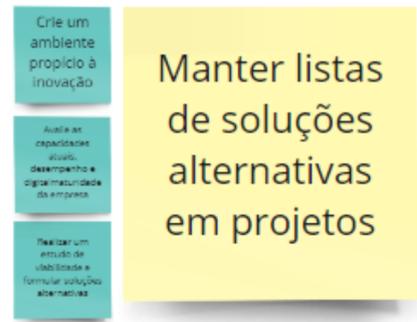


Figura III.4: Tela de informações sobre o projetos. Fonte: autora



Figura III.5: Tela de histórico de projetos. Fonte: autora



Figura III.6: Tela de acompanhamento de projetos. Fonte: autora

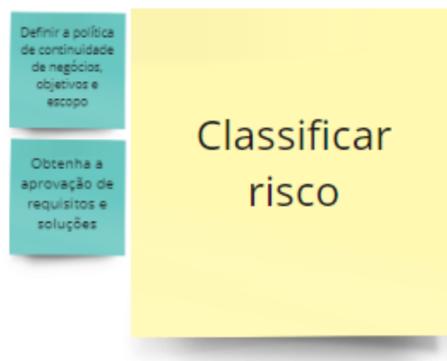


Figura III.7: Tela de cadastro de riscos. Fonte: autora

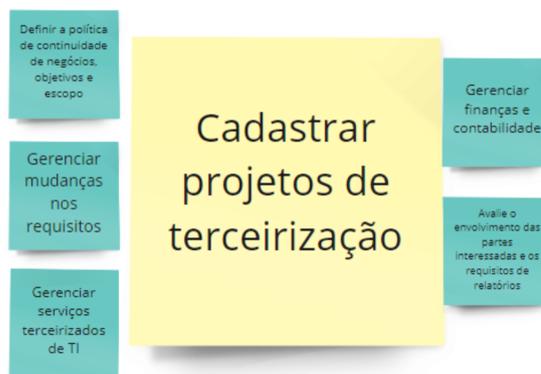


Figura III.8: Tela de cadastro de projetos. Fonte: autora

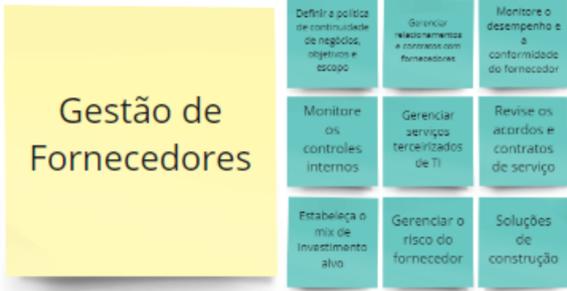
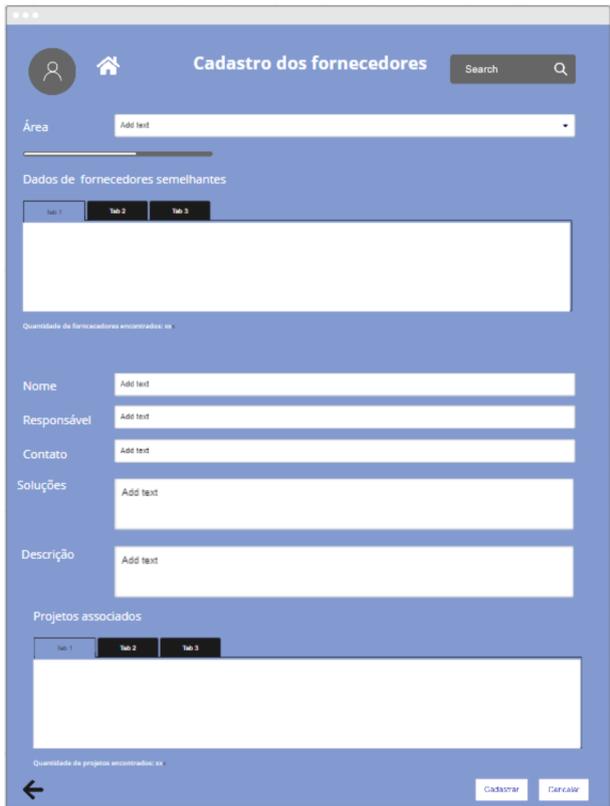


Figura III.9: Tela de cadastro de fornecedores. Fonte: autora

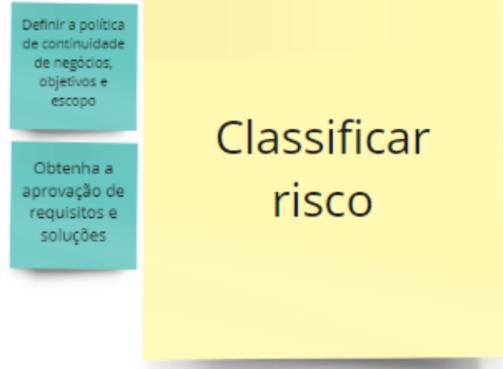
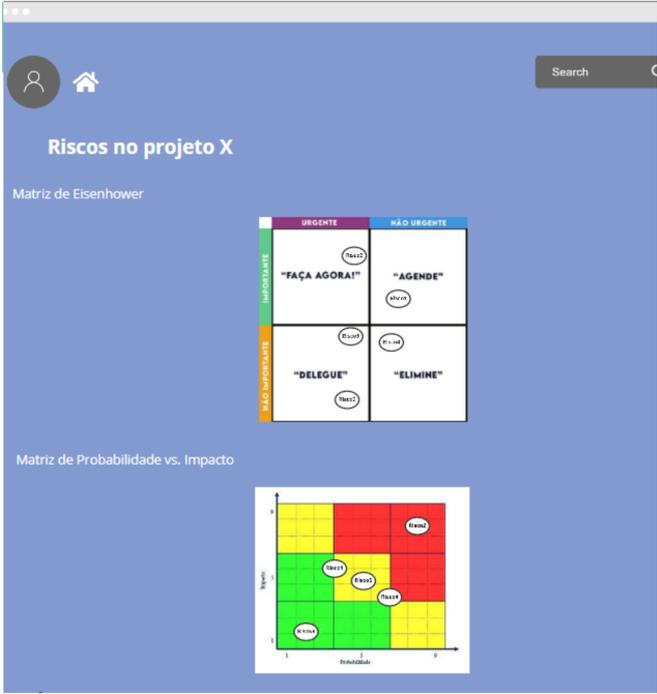


Figura III.10: Tela de monitoramento de riscos. Fonte: autora

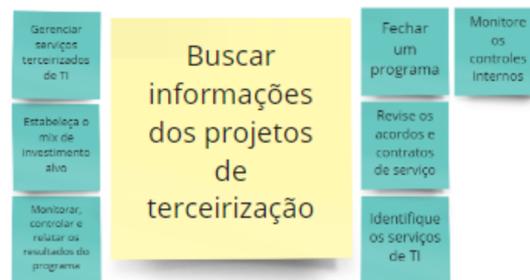
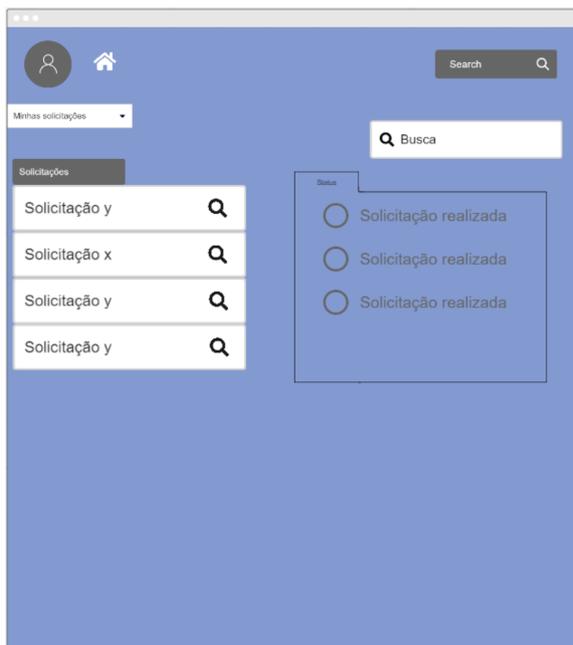


Figura III.11: Tela da visão do solicitante da terceirização. Fonte: autora

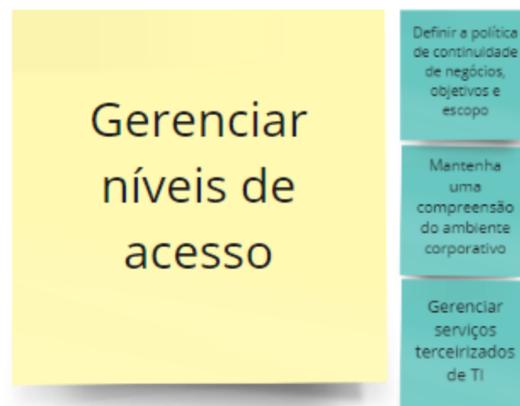
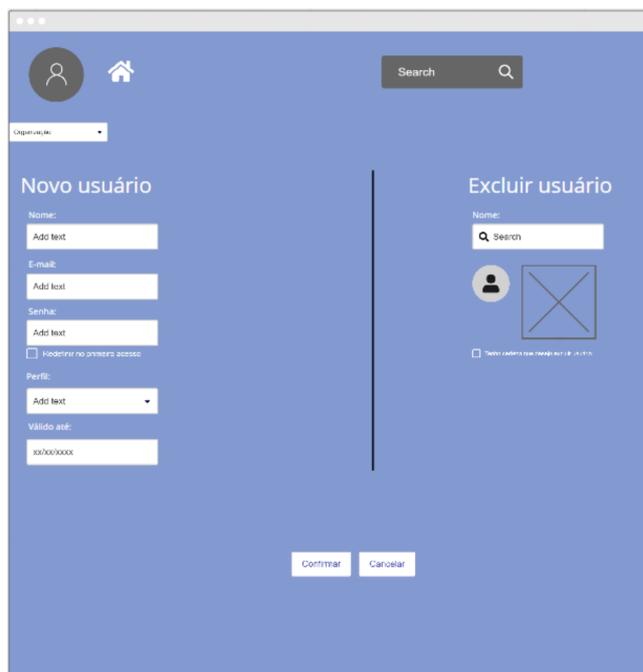


Figura III.12: Tela de cadastro de usuários. Fonte: autora



Figura III.13: Tela de acompanhamento de atividades do projeto. Fonte: autora

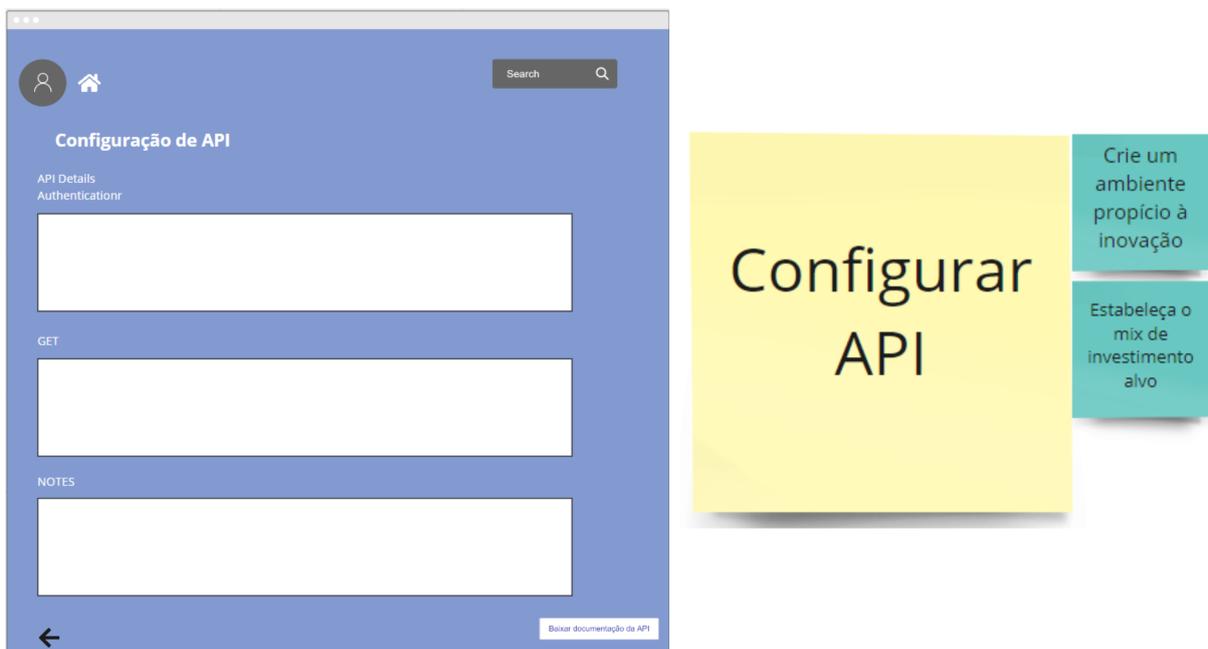


Figura III.14: Tela de integração por API. Fonte: autora