Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Gestão de Riscos aplicado ao Processo de Desenvolvimento de Software em uma Organização Militar

Jônatas Medeiros de Mendonça

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

Orientadora
Prof.a Dra. Simone Borges Simão Monteiro

Brasília
2019

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

Mg

Mendonça, Jônatas Medeiros de
Gestão de Riscos aplicado ao Processo de Desenvolvimento de Software em uma Organização Militar / Jônatas Medeiros de Mendonça; orientador Simone Borges Simão Monteiro. -- Brasília, 2019.
117 p.

Dissertação (Mestrado - Mestrado Profissional em Computação Aplicada) -- Universidade de Brasília, 2019.

1. Engenharia de Software. 2. Gestão de Riscos. 3. Processo de Desenvolvimento de Software. 4. Melhoria de Processo de Software. I. Monteiro, Simone Borges Simão, orient. II. Título.

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Gestão de Riscos aplicado ao Processo de Desenvolvimento de Software em uma Organização Militar

Jônatas Medeiros de Mendonça

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

Prof.a Dra. Simone Borges Simão Monteiro (Orientadora)
Dep. de Engenharia de Produção - Universidade de Brasília (UnB)

Prof. Dr. Edgard Costa Oliveira
EPR - Universidade de Brasília (UnB)

Prof. Dr. Altino José Mentzingen de Moraes
Min. da Mulher, da Família e dos Direitos Humanos

Prof.a Dra. Aletéia Patrícia Favacho de Araújo Von Paumgartten
Coordenadora do Programa de Pós-graduação em Computação Aplicada

Brasília, 07 de novembro de 2019

Dedicatória

Dedico este trabalho primeiramente a Deus, por ser essencial em minha vida. Aos meus pais, irmãos e familiares que me apoiaram durante toda a caminhada.

Agradecimentos

À professora Simone Borges Simão Monteiro, que foi minha orientadora, tendo toda paciência e me ajudando a concluir este trabalho e agradeço ainda aos meus demais professores que por anos me ensinaram a buscar a realização dos meus sonhos.

Ao Exército Brasileiro e seus militares que contribuíram para a execução da pesquisa, em especial à APG (Assessoria de Planejamento e Gestão do Departamento-Geral de Pessoal), onde a pesquisa foi realizada.

Aos membros do Projeto MAP (professores, assistentes, equipe de processos, requisitos e competências) que auxiliaram na coleta dos dados referente aos processos e sistemas de informação da organização.

Aos meus amigos (Patrícia, David, Eduardo, Camila, Ana Cristina) e a minha prima Daniele que me apoiaram durante o desenvolvimento desta pesquisa.

Aos alunos da turma de 2017 do PPCA, que estiveram presentes nos 2 anos do curso e que participaram direta ou indiretamente na conclusão da pesquisa.

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

O objetivo deste trabalho é aplicar o processo de gestão de risco ao processo de desenvolvimento de software de uma organização militar apoiado por ferramenta computacional de monitoramento. A metodologia de pesquisa adotada foi um estudo de caso, de caráter exploratório, com abordagem qualitativa para a análise e avaliação dos riscos, por meio da adoção da análise do PSR (Probabilidade, Severidade e Relevância) de cada fator de risco para organização. Os dados foram coletados através de entrevistas, análise documental e questionários, no qual, verificou-se o índice de risco das áreas relacionadas com o processo de desenvolvimento de software. Como resultado, foram priorizados os riscos de maior pontuação e propostos planos de ações para o tratamento dos riscos de maneira a subsidiar a melhoria do processo de software da organização. Para o monitoramento dos riscos foi proposto uma ferramenta de monitoração dos riscos e do nível de conformidade do processo de desenvolvimento de software com base nos controles recomendados pelo modelo de referência MPS.BR.

Palavras-chave: Gestão de riscos, Processo de Desenvolvimento de Software, Melhoria de Processo

Abstract

The purpose of this paper is to apply the risk management process to the software development process of a military organization supported by a computational monitoring tool. The research methodology adopted was an exploratory case study, with a qualitative approach to risk analysis and assessment, by adopting PSR (Probability, Severity and Relevance) analyzes of each risk factor for the organization. Data were collected through interviews, documentary analysis and questionnaires, without qualification, verified or analyzed the risk index of areas related to the software development process. As a result, the highest scoring risks and action plans for risk management in a subsidiary manner and improvement of the organization's software process were prioritized. For risk monitoring, a risk monitoring tool and the level of compliance of the software development process were adopted based on the controls recommended by the MPS.BR reference model.

Keywords: *Risk management, Software Development Process, Process Improvement*

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

CETI Concepção Estratégica de Tecnologia da Informação.

DGP Departamento-Geral de Pessoal.

DTI Divisão de Tecnologia da Informação.

ODS Órgão de Direção Setorial.

OETI Objetivos Estratégicos de Tecnologia da Informação.

OM Organização Militar.

PDTI Plano Diretor de Tecnologia da Informação.

PETI Plano Estratégico de Tecnologia da Informação.

TIC Tecnologia da Informação e Comunicação.

Capítulo 1

Introdução

As organizações estão cada vez mais preocupadas em melhorar o desempenho, prazos e redução de custos em seus projetos e procuram se adaptar e melhorar continuamente seus processos e metodologias para o desenvolvimento de software, podendo assim acompanhar e garantir a qualidade de seus processos e dos softwares desenvolvidos [1].

O desenvolvimento de software com qualidade, dentro do prazo, com custos aceitáveis e que satisfaçam às exigências dos usuários, exige dos desenvolvedores e fornecedores de software a melhoria contínua dos processos de tecnologia da informação [2].

Verifica-se, que os ambientes de desenvolvimento de software são considerados complexos e estão suscetíveis a diversas falhas e elevado grau de exposição aos riscos de mercado, financeiro e técnico [3].

Um dos principais problemas relatados na literatura está associado com a falta ou mau gerenciamento dos riscos nos projetos e processo de desenvolvimento de software nas organizações [4]. Diante disso, percebe-se a importância de gerenciar os riscos do processo de desenvolvimento de software de forma a conhecê-los e propor maneiras para reduzi-los.

A aplicação das técnicas e práticas de Gerenciamento de Riscos propicia um grande ganho para a indústria de software, pois contribui para a redução e mitigação de problemas no processo de desenvolvimento de maneira a melhorar a qualidade do software [5, 6].

A Engenharia de Software especifica um modelo padronizado de como projetar e produzir sistemas de informação de forma mais eficiente possível, evitando assim falhas, prejuízos e atrasos nos projetos [1].

Nota-se, que a TI da área de Gestão de Pessoas do órgão objeto de estudo, tem assumido um papel fundamental na organização, uma vez que vem investindo nas melhorias de suas infraestruturas e sistemas de informação[7].

A Organização foco do estudo, possui em sua Estrutura Organizacional uma distribuição por Órgãos Setoriais, no qual o Departamento-Geral de Pessoal (DGP) é um deles, sendo responsável por, dentre outras funções, planejar, organizar, dirigir e controlar, as

atividades de administração de pessoal, assistência social, assistência à saúde, assistência religiosa, promoções, cadastro e avaliação, direitos, deveres, incentivos, inativos, pensionistas, movimentação, pessoal civil e serviço militar que lhe são atribuídas pela legislação específica.

O DGP possui sob sua responsabilidade diversas Organizações Militares (OM) subordinadas. Para gerenciar as diversas informações, o DGP conta com vários sistemas de informação que são utilizados tanto pelas diretorias subordinadas como por toda a organização.

Além disso, a busca por um software de qualidade tem conduzido as organizações a sistematizar seus processos de forma a diminuir os problemas e os riscos encontrados durante todas as fases do desenvolvimento de um software.

Para certos domínios de aplicação, existe uma crescente necessidade de se alinhar os processos de negócios com os sistemas de informação corporativos. Para isso, antes do desenvolvimento, manutenção ou evolução de um software, são necessárias atividades de mapeamento, modelagem e melhoria dos processos. A modelagem dos processos de negócio é o subsídio para verificar a necessidade de desenvolvimento ou modernização do software [8, 9, 10, 11].

Esta pesquisa está inserida dentro do contexto de um projeto de modelagem de processos de negócio e irá analisar o Processo de Desenvolvimento de Software de maneira a avaliar os seus riscos e como resultados serão propostos planos de ações e recomendações para a Melhoria de Processo de Software da Organização estudada.

1.1 Problema de Pesquisa

As organizações frequentemente utilizam inúmeros sistemas legados desenvolvidos há um certo tempo, alguns com tecnologias ultrapassadas, e que não atendem mais as necessidades dos usuários e aos objetivos da instituição.

Ao longo dos anos, foram desenvolvidos e mantidos pelo Departamento de Gestão de Pessoas da organização vários sistemas de informação para o atendimento de suas necessidades, mas não houve um método sistemático para o desenvolvimento de novos softwares ou para a modernização de seus sistemas legados.

Segundo Silva (2011) [12], a maioria dos sistemas corporativos e específicos dos órgãos de direção setorial foram desenvolvidos para atender apenas às necessidades e objetivos dos níveis estratégico e gerencial. Devido a isso, houve a necessidade de criação de sistemas paralelos para atender a realidade das diretorias, o que ocasionou a duplicação dos sistemas e gerou inconsistência nos dados da organização.

De acordo com o Plano Diretor de Tecnologia da Informação (PDTI) [13], o Departamento Geral de Pessoal (DGP) possui 99 sistemas informatizados, desenvolvidos ao longo de vários anos para suprir as necessidades da organização. Muitos desses sistemas são manutenidos e mantidos por militares que não o desenvolveram, apresentando pouca ou nenhuma documentação [13].

Desta forma, verifica-se, na organização, alguns problemas em decorrência da ausência de um processo de desenvolvimento de software definido e do controle pouco efetivo dos recursos de TI, relacionados aos ativos de software, além dos problemas relacionados com a falta de modernização dos sistemas legados [14].

A quantidade de sistemas de informação espalhadas pelas diretorias do DGP, geram altos custos para a sua manutenção. Uma vez que, os sistemas legados existentes necessitam de manutenção continuada, os dados devem ser tratados devido as diversas inconsistências nas informações e as bases de dados dispersas e não integradas que possibilitam falhas nas aplicações [14].

Observa-se também que há uma grande demanda de tempo para a correção de erros na interpretação dos requisitos, na sua implementação, gerando defeitos e falhas nos softwares existentes [14]. Tendo em vista esta conjuntura, essa pesquisa deverá investigar:

Quais são os riscos relacionados com o processo de desenvolvimento de software e como esses riscos podem ser mitigados, de maneira a propor melhorias por meio da execução de planos de ações?

1.2 Justificativa da pesquisa

A organização desenvolve atualmente várias iniciativas de racionalização em todas as áreas, sejam elas administrativas ou tecnológica, no qual visa elevar o nível de eficiência da organização na execução de seus processos, proporcionando maiores níveis de qualidade e economia quanto ao desenvolvimento de software.

A pesquisa teve como ponto de partida a proposta de racionalização da TI da organização publicada na Portaria 180/2014-EME, que regulou a migração de sistemas corporativos do DGP para o DCT e definiu que a infraestrutura dos sistemas corporativos e a manutenção dos códigos dos sistemas sejam assumidos pelo Departamento de Tecnologia do órgão.

O DGP apresenta a maior complexidade técnica entre os Órgão de Direção Setorial (ODS) para a migração e racionalização de TIC e por isso foi lhe concedido um tempo maior para a operacionalização da racionalização [15, 16].

Outra portaria que fornece subsídio para a racionalização é a Portaria 455-EME de 06 de novembro de 2017 [16], que instituiu a Diretriz para a racionalização de Tecnologia da

Informação e Comunicação (TIC) na organização como um todo e a Portaria 169/2018 que aprova o Plano de Racionalização de Tecnologia da Informação [15].

Com o intuito de obter a racionalização dos sistemas de TI da organização, o DGP aprovou em 8 de fevereiro de 2018, a Diretriz de Implantação do Projeto Sistema Corporativo de Gestão de Pessoal [17], que tem como objetivos:

> - "Modernizar a infraestrutura de Tecnologia da Informação (TI) do DGP, a fim de permitir o enlace tecnológico dos sistemas computadorizados com as Bases de Dados Corporativas;
> - Reduzir as vulnerabilidades dos sistemas informacionais computadorizados de gestão do pessoal;
> - Unificar as arquiteturas de desenvolvimento dos sistemas informacionais computadorizados de gestão do pessoal;
> - Mapear e documentar os sistemas informacionais computadorizados de gestão do pessoal;
> - Reduzir o número de sistemas informacionais computadorizados de gestão de pessoal que manipulam as informações do pessoal de forma descentralizadas"[17, p.11–20].

Além disso, verifica-se que o processo de desenvolvimento de software apresenta diversos riscos que ocorrem durante todas as suas fases. Percebe-se que a maioria dos fatores de riscos no desenvolvimento de software estão relacionados com a ausência de um processo definido [18].

Diante do cenário descrito e das portarias estabelecidas para racionalização, é relevante realizar uma análise do processo de desenvolvimento de software da organização, a fim de identificar, analisar e avaliar os riscos existentes e propor formas para o seu tratamento (mitigar, prevenir, eliminar).

1.3 Objetivos

1.3.1 Objetivo Geral

O objetivo geral da pesquisa é aplicar o processo de gestão de risco ao PDS, com vistas a melhoria, via ferramenta computacional de monitoramento.

1.3.2 Objetivos Específicos

Para que seja possível atingir o objetivo geral, será necessário que alguns objetivos específicos sejam alcançados, a saber:

OE1. Entender o Processo de Desenvolvimento de Software, inserido no contexto da TI do DGP.

OE2. Avaliar os riscos associados ao Processo de Desenvolvimento de Software;

OE3. Propor melhorias, a fim de mitigar os riscos do Processo de Desenvolvimento de Software.

OE4. Propor formas de monitoramento dos riscos do PDS.

Com a finalidade de explorar com maior rigor a temática do Processo de Desenvolvimento de Software do Departamento Geral de Pessoas (DGP), a estrutura desse trabalho é composta por 8 capítulos, subdivididos em suas respectivas seções e subseções.

O **capítulo 1** expõe uma introdução ao tema abordado pelo trabalho, explanando o contexto concernente ao processo de desenvolvimento de software, identificando os problemas e suas lacunas e as contribuições para o Departamento-Geral de Pessoal (DGP), objeto de estudo desta pesquisa.

O **capítulo 2** apresenta o referencial teórico do trabalho, onde são definidos os principais conceitos envolvidos com o processo de desenvolvimento de software e gestão de riscos.

O **capítulo 3** mostra a metodologia de pesquisa selecionada para o desenvolvimento deste trabalho, elencando a natureza, abordagem, estratégia e estruturação da pesquisa adotada para que se alcancem os objetivos da pesquisa.

O **capítulo 4** estabelece o contexto da gestão de riscos (interno e externo) e apresenta a área de TI analisada.

O **capítulo 5** apresenta a análise do Processo de Desenvolvimento de Software (PDS) do DGP por meio da modelagem do processo e da identificação de problemas.

O **capítulo 6** apresenta a aplicação da gestão de riscos associados ao Processo de Desenvolvimento de Software do DGP.

O **capítulo 7** apresenta a sugestão de melhoria para o PDS da TI do DGP e a proposta de uma ferramenta computacional para o monitoramento dos riscos do PDS.

Por fim, **o capítulo 8** apresenta as considerações finais.

Capítulo 2

Referencial Teórico

Este capítulo apresenta conceitos concernentes aos modelos de processo de desenvolvimento de software e gestão de riscos que darão subsídios para o desenvolvimento da pesquisa.

Para conhecer as principais contribuições da literatura sobre os riscos relacionados com o Processo de Desenvolvimento de Software foram realizadas buscas nas principais bases de pesquisa (Web of Science, Scopus, Google Scholar) com as palavras chaves: (("software development process"OR "software process") AND ("risk"OR "risk management")) no período de 1945 à 2019 para abranger o maior número possível de artigos. A tabela 2.1 mostra a quantidade de artigos com os termos pesquisados em cada base de dados.

Tabela 2.1: Quantidade de artigos por base de dados

Base de Dados	**Total de Artigos**
Web of Science	299 artigos
Scopus	7763 artigos
Google Acadêmico	17500 artigos

O risco presente na condução do desenvolvimento de software, é um assunto que sempre preocupou a Engenharia de Software. Nos últimos anos, muitos atores vêm pesquisado sobre o tema, analisando maneiras de mitigar os riscos envolvidos no processo de desenvolvimento de software. Verifica-se que o Brasil, ocupa a 3ª colocação com a maior quantidade de publicações sobre o tema, sendo, 20 artigos publicados durante os últimos anos.

Houve um crescimento tanto da quantidade de artigos publicados, como também do número de citações desde os anos de 2004, tendo seu ápice no ano de 2016, onde foram publicados 26 artigos relacionados com as palavras chaves pesquisada e citados 259 artigos, conforme mostra na figura 2.1.

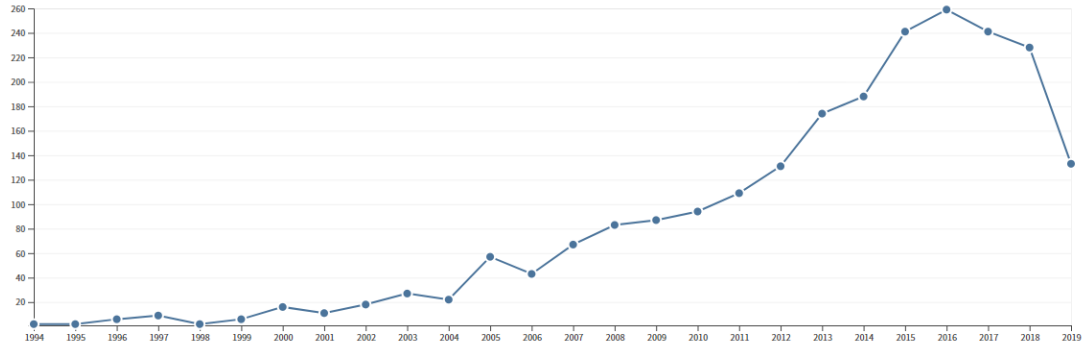


Figura 2.1: Número de Citações por ano - WebOfScience
Fonte: Elaborado pelo autor.

O artigo mais antigo sobre o tema, presente no Web Of Science, foi publicado em 1992 na revista “IEEE Transactions Software Engineering”, possui 103 citações. Os autores descrevem uma abordagem de reconhecimento de padrões para a análise de dados da engenharia de software, denominada de OSR (Redução Otimizada de Conjunto), onde abordam os problemas associados às abordagens usuais para planejar, controlar e avaliar o processo de desenvolvimento de software e discutem técnicas de previsão, gerenciamento de riscos e avaliação da qualidade.

Já o artigo com mais citações, foi publicado em 2011, também na "IEEE Transactions Software Engineering"e aborda uma métrica para o desenvolvimento seguro de software, de maneira a complementar a abordagem tradicional de melhoria da qualidade de código da indústria de software para a mitigação de riscos, relacionados com a segurança, em várias fases do ciclo de vida de desenvolvimento de software e sendo a métrica utilizada no processo de desenvolvimento de software

O artigo mais relevante, foi publicado em 2012, na revista "Information and Software technology", com 121 citações e trata dos fatores situacionais que afetam o processo de desenvolvimento de software, nesse sentido os autores, identificaram 8 classificações e 44 fatores. Para os autores, o processo de desenvolvimento de software ideal é considerado dependente das características situacionais das suas configurações individuais. A estrutura criada pelos autores fornece uma base sólida para a definição e otimização do processo de desenvolvimento de software.

2.1 Processos de Software

A Engenharia de Software, é uma área de conhecimento da Computação, cujos conhecimentos se relacionam basicamente com a especificação, o desenvolvimento e a manutenção de sistemas de software, com o objetivo de organizar o projeto e aumentar a sua produtivi-

dade. Além de fornecer uma estrutura para a construção de software com alta qualidade, obtido por meio da aplicação de práticas de engenharia para o desenvolvimento de software [19].

Segundo Sbroco e Macedo (2012) [19], a engenharia de software deve se apoiar no compromisso com a qualidade e por isso, o foco da qualidade é a camada base de sustentação, seguida pelo uso de processos, uso de métodos e de ferramentas adequadas.

Segundo Pressman (2011) [20], um software é composto por um conjunto de instruções que, quando executadas, produzem a função e o desempenho desejados; são estruturas de dados que possibilitam que os programas manipulem corretamente as informações; e são documentos que descrevem a operação e o uso dos programas.

Para Sommerville (2010) [4], um software não é apenas o programa, mas também toda a documentação associada e os dados de configuração para fazer com que eles operem corretamente. Assim, podemos pensar em software como algo mais abstrato, intangível, não palpável que envolve não só as instruções para o computador propriamente ditas, mas todas as informações para fazê-lo funcionar.

Segundo Sommerville (2010)[4], um sistema é um conjunto de componentes inter-relacionados que funcionam juntos para atingir um objetivo em comum. O sistema é formado por um determinado número de programas separados e arquivos de configurações para eles, podendo incluir documentação específica para descrever a estrutura do sistema, documentação de usuário, entre outros. Portanto, quando se menciona "sistema", refere-se a uma solução abrangente que envolve várias partes interligadas, oferecendo um composto de funcionalidades para atender as necessidades do usuário.

Um processo é definido como "um conjunto inter-relacionado de recursos e atividades que transformam entradas e saídas". O processo, define quem irá fazer e como será atingido o objetivo. Na engenharia de software, um dos objetivos de um processo será de construir um software ou melhorar um existente.

Figura 2.2: Objetivo da Engenharia de Software
Fonte: Adaptado de [19].

Um processo de software, normalmente possui uma estrutura comum, definida com um pequeno número de atividades que são aplicáveis a todos os projetos de software, independentemente do tamanho ou da complexidade[19].

As atividades previstas na estrutura comum podem ser aplicadas e adaptadas às características do projeto de software, além das necessidades da equipe do projeto envolvida. Além dessas atividades, existem aqueles que cobrem todo o modelo de processo, denominados de processos "guarda-chuva", que determinam, em como garantir a qualidade de software, a gestão da configuração. As atividades desses processos são independentes de qualquer atividade e ocorre ao longo de todo o processo de desenvolvimento de software [19].

Na Engenharia de Software, os processos podem ser definidos pelo conjunto de atividades como desenvolvimento, manutenção, aquisição e contratação de software. O processo de desenvolvimento pode ser dividido em subprocessos: levantamento de requisitos, análise, desenho, implementação e testes [4, 20].

A existência de processos definidos é necessária para a maturidade das organizações produtoras de software, o que permitem que a organização produza de forma padronizada e reprodutível. O contrário, também é ruim, uma vez que processos rigorosamente definidos e não alinhados com os objetivos da organização são impedimentos burocráticos, que limitam a produção [19].

É importante deixar claro, que os projetos são diferentes de processos. Os projetos estão relacionados com algo novo e tem início e fim bem definidos. Já os processos ocorrem de maneira contínua, com a finalidade de produzir produtos ou serviços idênticos [19].

Os processos de software são processos de negócio das organizações desenvolvedoras e mantenedoras de software. Em um processo de desenvolvimento de software, o ponto de partida para a arquitetura de um processo é a escolha de um modelo de ciclo de vida [19].

2.2 Modelos e Normas de Processo de Software

Existem vários modelos de processo de software, que descrevem o processo de desenvolvimento do software. Um modelo de processo pode ser descritivo ou prescritivo. O primeiro, é utilizado para descrever o que acontece em um processo de desenvolvimento e é útil na identificação de problemas no processo de desenvolvimento de software. E o segundo, é utilizado para descrever o que poderá acontecer, ou seja, descrever o processo padrão de desenvolvimento de software [19].

Para o SISP (2016) [21], o processo de software aborda não só as atividades relacionadas ao desenvolvimento como também as atividades ligadas ao planejamento dos recursos necessários para que o software tenha o ambiente adequado para o seu funcionamento. A Figura 2.3 apresenta o processo de software do SISP.

Figura 2.3: Processo de Software do SISP.
Fonte: [21].

A norma ISO/IEC 12207 [22] estabelece uma estrutura comum para os processos de ciclo de vida de software como forma de ajudar as organizações a compreenderem todos os componentes presentes na aquisição e fornecimento de software e assim, firmarem contratos e executarem projetos de forma mais eficaz.

A ISO/IEC 12207 [22] é utilizada amplamente em muitos países como referência para a contratação de serviços de desenvolvimento e manutenção de software. Muitas organizações no Brasil a utiliza para definir o seu processo de desenvolvimento de software.

A ISO/IEC 15504 [23], é um modelo que possui como foco a melhoria dos processos de desenvolvimento de software e a determinação da capacidade dos processos da organização.

A ISO/IEC 15504 (SPICE) [23] presta-se à realização de avaliações de processos de software com dois objetivos: a melhoria de processos e a determinação da capacidade de processos de uma organização. Se o objetivo for a melhoria de processos, a organização pode realizar a avaliação gerando um perfil dos processos que será usado para a elaboração de um plano de melhorias. A análise dos resultados identifica os pontos fortes, os pontos fracos e os riscos inerentes aos processos.

A norma 15504 [23] se estrutura em duas dimensões: dimensão de processos, dimensão de capacidade. A dimensão de processos é baseada na ISO/IEC 12207 e estabelece o que a organização deveria executar para ter qualidade na produção, fornecimento, aquisição e operação de software. A dimensão da capacidade é um conjunto de atributos de um processo que estabelece o grau de refinamento e institucionalização com que o processo é executado na organização.

2.3 Processo de Desenvolvimento de Software

O processo de desenvolvimento de software é definido como "um conjunto de atividades, métodos, ferramentas e práticas que são utilizadas para construir um produto de software" [4].

O desenvolvimento de um software é um processo que deve seguir uma sequência de etapas que caracterizam seu ciclo de vida a partir da aplicação de uma metodologia de desenvolvimento, podendo ser aplicado tanto os métodos ágeis como os tradicionais[4, 20].

Existem diversos processos de desenvolvimento de software, no entanto há algumas atividades básicas comuns à grande parte dos processos existentes como: Levantamento de requisitos; Análise de Requisitos; Projeto; Implementação; Testes; Implantação; Suporte e Manutenção [20, 4, 22].

A Norma ISO/IEC 12207 estabelece uma arquitetura comum para o ciclo de vida de processos de software com uma terminologia bem definida. O modelo de ciclo de vida proposto pela ISO/IEC 12207 compreende a "estrutura contendo processos, atividades e tarefas envolvidas no desenvolvimento, operação e manutenção de um produto de software, abrangendo a vida do sistema desde a definição de seus requisitos até o término de seu uso" [22, 20, 24].

A norma estabelece uma ligação muito forte entre sistema e software, sendo o padrão baseado nos princípios gerais da Engenharia de Sistemas (análise, projeto, implementação, testes) e software é tratado como parte integral de um sistema e desempenha certas funções deste sistema [22].

De acordo com Sommerville [4], os processos de software são complexos e dependem das pessoas para a tomada de decisão. Existem dois tipos de processos de software, os modelos prescritivos e os modelos ágeis. Verifica-se que não existe processo ideal, mas sim é necessário que a organização adapte o processo para cada realidade.

Diante disso, a adoção de um processo de desenvolvimento de software bem definido é importante para que a organização entregue os softwares com qualidade de forma a reduzir os riscos inerentes ao processo.

2.3.1 Melhoria da Qualidade no Processo de Desenvolvimento de Software

As mudanças que estão ocorrendo nos ambientes de negócios têm motivado as empresas a modificarem as estruturas organizacionais e os processos produtivos, saindo da visão tradicional baseada em áreas funcionais, e indo em direção a redes de processos centrados no cliente [24]. Diante disso, verifica-se que a qualidade é um fator crítico de sucesso para a indústria de software.

Os modelos de maturidade de software buscam direcionar as organizações em seus processos de desenvolvimento de software como o CMMI (Capability Maturity Model Integration) ou MPS.br (Melhoria de Processo de Software Brasileiro) para melhorar e reduzir custos do desenvolvimento de software [25].

O modelo MPS baseia-se nos conceitos de maturidade e capacidade de processo para a avaliação e melhoria da qualidade e produtividade de software e serviços correlatos e também para a melhoria da qualidade e produtividade dos serviços prestados [24].

A ISO/IEC 15504 presta-se à realização de avaliações de processos de software com dois objetivos: a melhoria de processos e a determinação da capacidade de processos de uma unidade organizacional. Se o objetivo for a melhoria de processos, a unidade organizacional pode realizar uma avaliação para gerar um perfil dos processos que será usado para a elaboração de um plano de melhorias [24].

A análise dos resultados identifica os pontos fortes, os pontos fracos e os riscos inerentes aos processos. No segundo caso, a organização tem o objetivo de avaliar um fornecedor em potencial, obtendo o seu perfil de capacidade. O perfil de capacidade permite ao contratante estimar o risco associado à contratação daquele fornecedor em potencial para auxiliar na tomada de decisão de contratá-lo ou não [24].

2.4 Gestão de Riscos

O risco pode ser definido como o "efeito da incerteza sobre o alcance de objetivos" [26]. O termo "risco" é geralmente usado para descrever eventos adversos com uma probabilidade conhecida, onde verifica-se que a incerteza é um elemento relacionado a confiança na gestão de riscos e decorre da falta de conhecimento e, portanto, tem uma probabilidade desconhecida [27, 28].

Existem diversas abordagens, modelos e frameworks para a gestão de riscos, levando em consideração que todos convergem para um mesmo objetivo, apesar de muitas vezes diferirem em suas nomenclaturas, podemos destacar o ERM/COSO [29], Orange Book, ISO 27005 [30], ISO 31000 [26] e o COBIT 5 for Risk [31] que podem ser aplicados tanto para a área de TI como para toda a organização.

2.4.1 Modelo de Gestão de Riscos baseado na ISO 31000

A International Organization for Standardization (ISO) definiu um padrão para o processo sistemático e lógico de gestão de riscos, nomeado como Risk Management Process (processo de gestão de riscos), o qual conceitua que a gestão de riscos deve fazer parte do processo de gestão, da cultura e prática, adaptada aos processos de negócio da organiza-

ção. Algumas etapas foram definidas pela norma ISO 31000 [26] e estão demonstradas na Figura 2.4.

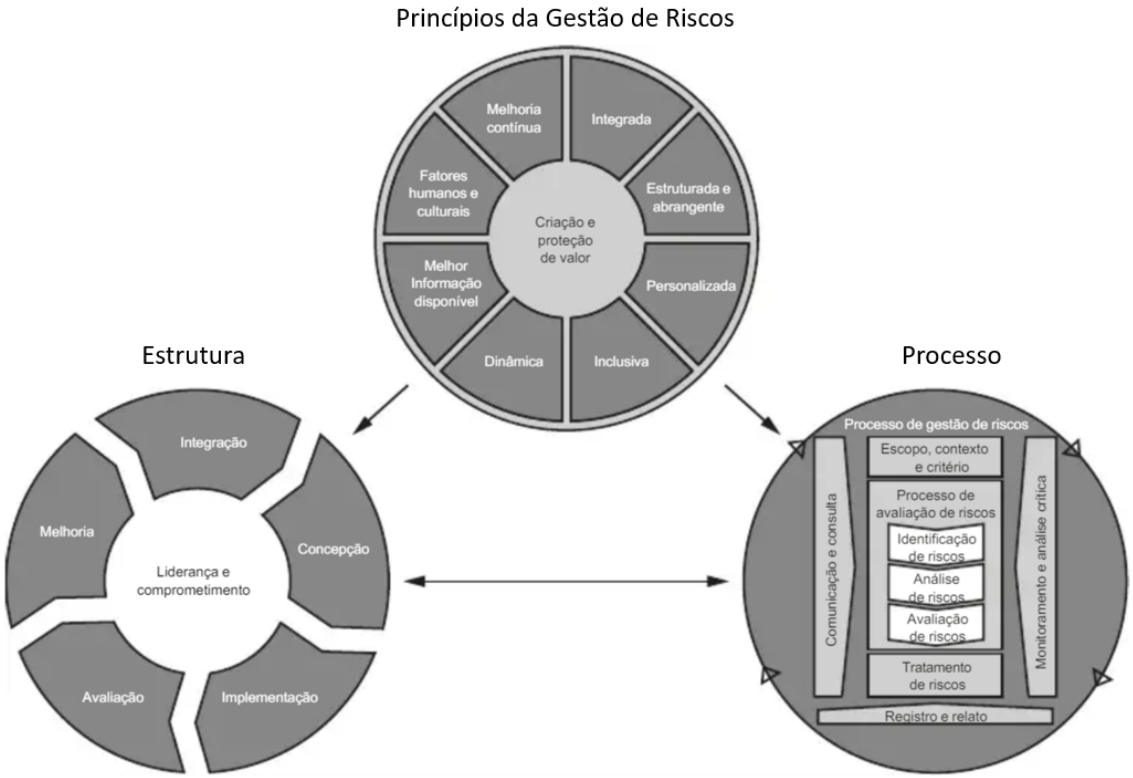


Figura 2.4: Os princípios, a estrutura e o processo de Gestão de Riscos segundo a NBR ISO 31000:2018 (Fonte: [26]).

Ao longo do processo de gestão de riscos proposto pela ISO 31000, as organizações comunicam e consultam as partes interessadas, monitoram e analisam criticamente os riscos e os controles que o modificam, afim de assegurar que nenhum tratamento de risco adicional seja requerido. As etapas propostas pela ISO 31000 são apresentadas a seguir:

- **Comunicar e consulta as partes interessadas:** podem ser tanto internas ou externas, conforme o mais apropriado, em cada etapa do processo de gerenciamento de riscos e em relação ao processo como um todo.
- **Estabelecer os contextos:** critérios em relação aos quais os riscos serão avaliados devem ser estabelecidos e deve ser definida a estrutura da análise. Podem ser tanto externos, internos e de gerenciamento de riscos onde o processo será realizado.
- **Identificar os riscos:** identificar onde, quando, por quê e como os eventos poderiam impedir, atrapalhar, atrasar ou aprimorar a realização dos objetivos.

- **Analisar os riscos:** identificar e avaliar os controles existentes e determinar as consequências, a probabilidade e, por conseguinte, o nível de risco. Tal análise deve considerar a série de consequências potenciais e como elas podem ocorrer.
- **Avaliar os riscos:** Comparar os níveis de risco estimados aos critérios estabelecidos previamente e considerar o equilíbrio entre os benefícios potenciais e os resultados adversos. Isso permite que sejam tomadas decisões quanto à extensão e à natureza dos tratamentos necessários e em relação às prioridades.
- **Tratar os riscos:** Desenvolver e implantar estratégias efetivas em relação aos custos específicos e planos de ação para aumentar os potenciais benefícios e reduzir os custos potenciais.
- **Monitorar e realizar análise crítica:** Necessidade de monitorar a eficácia de todas as etapas do processo de gerenciamento de riscos, importante para o processo de melhoria contínua. Os riscos e a eficácia das medidas de tratamento precisam ser monitorados como forma de garantir que mudanças nas circunstâncias não alterem as prioridades.

O gerenciamento de riscos envolve um conjunto de etapas estruturadas de forma metodológica com o objetivo de enfrentar os riscos de forma planejada e sistêmica [32].

De acordo com a ISO 31010 [33] existem 31 tipos de técnicas utilizadas para identificação, análise, avaliação e tratamento dos riscos conforme demonstrada na Figura 2.5.

O plano de comunicação pode ser realizado tanto interno (áreas da organização, funcionários, gerentes, parceiros) como externos (clientes, fornecedores, órgãos reguladores), levando em conta as definições da existência de riscos e dos objetivos da gestão [34].

Em relação ao contexto interno, deve-se verificar qual é a missão, visão, políticas, objetivos, estratégias, metas, papéis e responsabilidades, estrutura organizacional, regulamentos entre outros. E em relação ao contexto externo deve-se verificar os aspectos relacionados as leis aplicáveis, economia, política, tecnologia e outros aspectos necessários [34].

De acordo com Aven (2011) [35], a avaliação do risco propõe a sistematizar o conhecimento e incertezas sobre fenômenos, processos e sistemas em análise para estimar potenciais perigos e ameaças, verificando quais são as causas e as consequências.

Na avaliação dos riscos, identifica-se quais são os ativos que devem ser protegidos e quais são as oportunidades e fraquezas da organização, bem como as ameaças a que estão expostas.

De acordo com Ramirez (2011) [34], devem considerar os ativos como sendo os processos, informações, dados e recursos de suporte. As ameaças podem ser do tipo físicos, lógicos ou estratégicos, podendo ser de origem natural, técnica ou humana.

Ferramentas e técnicas	Processo de avaliação de riscos				
	Identificação de riscos	Análise de riscos			Avaliação de riscos
		Consequência	Probabilidade	Nível de risco	
Brainstorming	FA[1]	NA[2]	NA	NA	NA
Entrevistas estruturadas ou semiestruturadas	FA	NA	NA	NA	NA
Delphi	FA	NA	NA	NA	NA
Listas de verificação	FA	NA	NA	NA	NA
Análise preliminar de perigos (APP)	FA	NA	NA	NA	NA
Estudo de perigos e operabilidade (*HAZOP*)	FA	FA	A[3]	A	A
Análise de perigos e pontos críticos de controle (APPCC)	FA	FA	NA	NA	FA
Avaliação de risco ambiental	FA	FA	FA	FA	FA
Ténica etruturada "E se"(SWIFT)	FA	FA	FA	FA	FA
Análise de cenários	FA	FA	A	A	A
Análise de impactos no negócio	A	FA	A	A	A
Análise de causa–raiz	NA	FA	FA	FA	FA
Análise de modos de falha e efeito	FA	FA	FA	FA	FA
Análise de árvore de falhas	A	NA	FA	A	A
Análise de árvore de eventos	A	FA	A	A	NA
Análise de causa e consequência	A	FA	FA	A	A
Análise de causa e efeito	FA	FA	NA	NA	NA
Análise de camadas de proteção (*LOPA)* c	A	FA	A	A	NA
Árvore de decisões	NA	FA	FA	A	A
Análise da confiabilidade humana	FA	FA	FA	FA	A
Análise *Bow tie*	NA	A	FA	FA	A
Manutenção centrada em confiabilidade	FA	FA	FA	FA	FA
Análise de circuitos ocultos	A	NA	NA	NA	NA
Análise de Markov	A	FA	NA	NA	NA
Simulação de Monte Carlo	NA	NA	NA	NA	FA
Estatística Bayesiana e Redes de Bayes	NA	FA	NA	NA	FA
Curvas FN	A	FA	FA	A	FA
Índices de risco	A	FA	FA	A	FA
Matriz de probabilidade/ consequência	FA	FA	FA	FA	A
Análise de custo/benefício	A	FA	A	A	A
Análise de decisão por multicritérios (*MCDA*)	A	FA	A	FA	A

[1] FA - Fortemente aplicável, [2] NA - Não aplicável, [3] A - Aplicável.

Figura 2.5: Ferramentas e Técnicas de avaliação de riscos (Fonte: [33]).

No tratamento são definidas as possíveis ações a serem tomadas para evitar novos riscos. Deve-se gerar um plano de tratamento dos riscos, onde contêm os recursos, responsabilidades e as atividades que serão realizadas. De acordo com Ramirez (2011) [34], as ações também incluem uma análise de custo-benefício, tanto para a implementação como para a manutenção.

A gestão de riscos está associada com a Governança de TI, uma vez que esta, se preocupa em entregar valor ao negócio por parte da TI e a mitigação de riscos associados a TI [36]. Com isso, foi criado um modelo de gestão de riscos baseado no COBIT 5 e são relacionados a TI de uma organização.

2.4.2 COBIT 5 para Risco

O COBIT 5 para Risco, bem como o próprio COBIT 5 é um modelo guarda-chuva para governança e gestão de risco e está alinhado com os principais padrões relacionados com a gestão de riscos (ISO 31000, ISO/IEC 27005 e COSO ERM) [31].

Lançado em 2013 pela ISACA, o COBIT 5 para risco levou uma análise mais profunda dos riscos de TI a gestores e partes interessadas que almejam minimizar perdas e otimizar o desempenho dos negócios de TI.

O risco de TI é definido pela ISACA [31] como sendo o "risco de negócio, associado ao uso, propriedade, operação, envolvimento, influência e adoção da TI dentro da organização." No documento, os riscos de TI são categorizados como:

- **Risco para entrega de valor / benefício de TI:** identificado como risco estratégico, está associado às oportunidades perdidas da utilização da tecnologia com o intuito de melhorar a eficiência e efetividade dos processos de negócio ou como um habilitador para novas iniciativas de negócio.
- **Risco para a entrega de programas e projetos de TI:** associado à contribuição da TI para novas soluções de negócio ou seu aperfeiçoamento, geralmente sob a forma de programas e projetos que fazem parte das carteiras de investimento.
- **Risco para a entrega de operações e serviços de TI:** associado à estabilidade, disponibilidade, proteção e recuperação de operações dos serviços de TI, que podem destruir ou reduzir o valor para a organização.

Existem diversas vantagens para a organização na sua adoção:

- Identificação mais precisa do risco e mensuração do sucesso no tratamento do mesmo;
- Disponibilização de um guia de ponta a ponta sobre como administrar o risco, incluindo um amplo conjunto de medidas;
- Compreensão de como a gestão de riscos eficiente otimiza o valor, junto com a eficácia e eficiência, dos processos de negócio na melhoria da qualidade e na redução dos custos e desperdícios;
- Oportunidades para integrar a gestão de riscos de TI com as estruturas para o risco e a conformidade na empresa;
- Criação de um perfil de risco completo, identificando a exposição total ao risco da empresa e facilitando uma melhor utilização dos seus recursos;
- Melhoria na consciência do risco em toda a empresa.

2.4.2.1 Cenários de Riscos

Um dos desafios da gestão de riscos de TI é reconhecer os riscos indispensáveis, que tem representatividade, entre tudo que pode dar errado. Para solucionar esse desafio, aplica-se a técnica de desenvolvimento e uso de cenários de riscos. Após a elaboração desses cenários, eles são utilizados durante a análise de riscos, quando se pode aferir a frequência com que os cenários ocorrem e o impacto que causam nos negócios [37].

De acordo com o COBIT 5 par Risco (ISACA, 2013)[38], um cenário de risco é uma descrição possível que, caso ocorra, terá um impacto no alcance dos objetivos corporativos. Esse impacto pode ser positivo ou negativo.

Os cenários de riscos são um elemento chave do processo de gestão de riscos do COBIT 5 e possuem duas abordagens: *top-down*, quando são usados os objetivos corporativos globais para definir os cenários de riscos de TI mais relevantes e prováveis de impactarem e a abordagem *bottom-up*, no qual são usados uma lista de cenários genéricos para definir um conjunto de cenários personalizados mais relevantes e que são aplicáveis à organização.

A abordagem *top-down* e *bottom-up* são complementares e devem ser usados simultaneamente e os cenários de riscos devem ser relevantes e relacionados aos riscos de negócios reais.

Quando um cenário de risco se materializa, um evento de perda ocorre. Esse evento de perda é disparado por um evento ameaça e a frequência do evento ameaça é influenciado por uma vulnerabilidade.

A vulnerabilidade é usualmente um estado, podendo ser incrementada ou reduzida por eventos de vulnerabilidade, ou seja, pela força de controles de ameaças.

2.4.2.2 Perspectivas de Risco

O COBIT 5 provê orientação e descreve como cada habilitador contribui para a Governança e a Gestão da função de risco, sendo necessário verificar quais processos são importantes para definir e sustentar a função de risco e quais fluxos de informação são imprescindíveis para governar e gerenciar os riscos e quais estruturas organizacionais são fundamentais para governar e gerenciar riscos de forma efetiva, bem como as pessoas e habilidades devem ser postas em prática para estabelecer e operar uma função de risco efetiva.

São definidos sete princípios de risco pelo COBIT que são necessários para prover uma abordagem sistemática, estruturada e tempestiva da gestão de riscos e contribuir para a obtenção de resultados consistentes, comparáveis e confiáveis. Na figura 2.6 são apresentados os 7 princípios.

Figura 2.6: Princípios da Gestão de Riscos
Fonte: Adaptado de [38]

Os princípios de risco formalizam e padronizam a implementação de políticas, tanto as políticas de risco de TI como também as auxiliares, como a política de segurança da informação e a política de continuidade de negócios.

No COBIT 5 para risco são identificados todos os processos necessários à função de risco, sendo os processos EDM03 - Garantir a otimização de risco e APO12 - Gerenciar risco os principais processos de riscos presente no COBIT 5 e estão destacados em azul claro. Além desses processos, existem os processos chaves de suporte ao risco como os destacados de rosa escuro e os processos de suporte destacados de rosa claro na Figura 2.7.

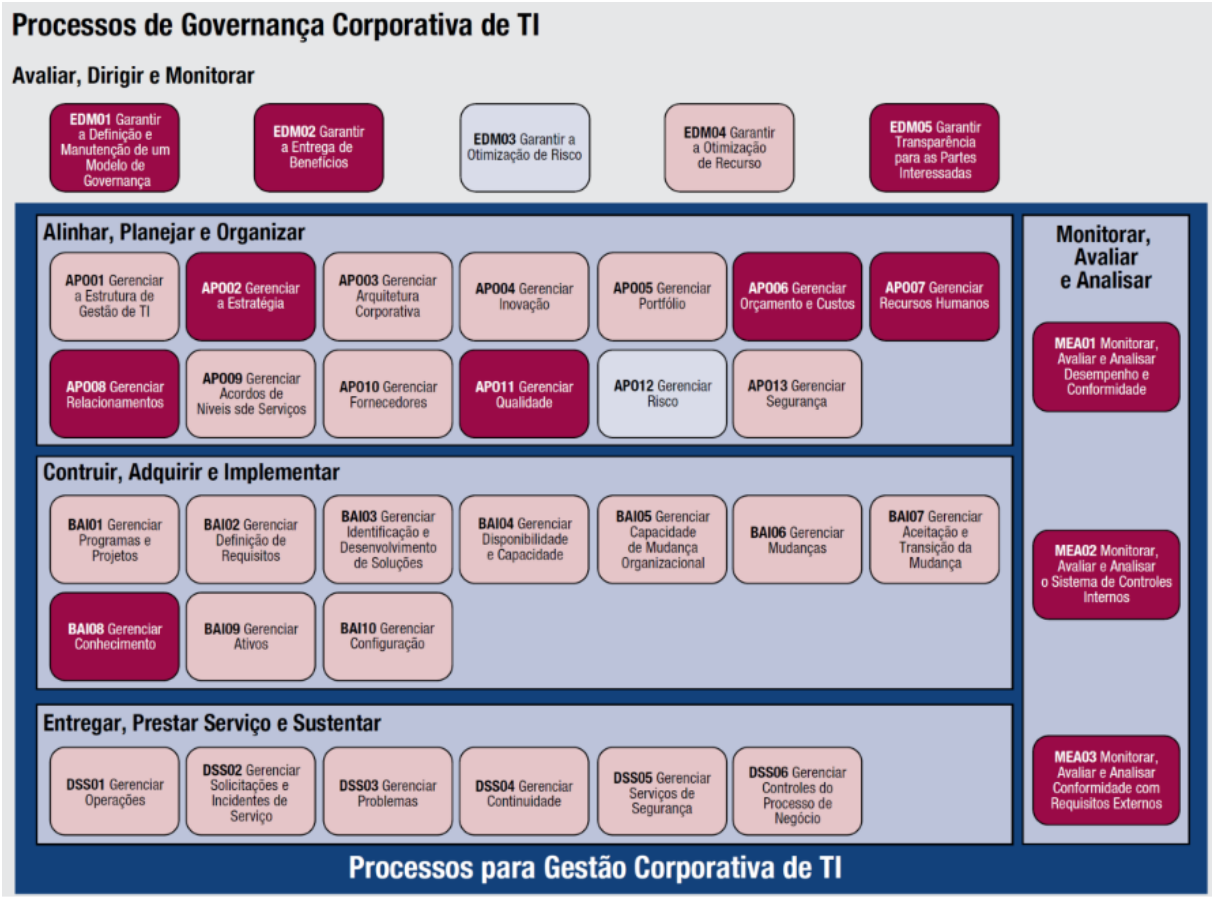


Figura 2.7: Processos de Governança Corporativa de TI
Fonte: [38]

Sabe-se que os sistemas de informação representam uma vantagem competitiva nas organizações. De acordo com Nolan e MCFarlan (2005) [39], as atividades de TI representam para muitas organizações grande importância estratégica e para outras representa um alto custo.

Diante disso, é importante analisar como as incertezas da área de tecnologia da informação podem afetar na obtenção dos objetivos da organização.

2.5 Gestão de Riscos aplicado ao Processo de Desenvolvimento de Software

A tecnologia da informação possui um papel fundamental nas organizações, sendo utilizada como ferramenta estratégica, o que garante maior dinamismo aos negócios, mas também propicia riscos à estrutura quando não há aderência às melhores práticas existentes [40].

O risco de TI compreende o risco de negócio associado ao uso, gerenciamento, operação, suporte, inovação, influência ou adoção da tecnologia da informação para efetuar os negócios da organização [41].

Com isso, o riscos de TI podem ser definidos como a possibilidade de que algum evento imprevisto, que envolva falha ou mau uso da TI, ameace um objetivo organizacional [42].

A gestão de riscos de TI pode ser entendida como fator crítico de sucesso para que uma organização atinja aos seus objetivos [43]. O objetivo principal da gestão de riscos de TI é maximizar as oportunidades e minimizar as perdas, buscando um equilíbrio entre o risco e a oportunidade, de acordo com a tolerância ao risco que foi definida pela organização e envolve os processos, políticas, estruturas que propicia no conhecimento do risco de TI na organização [40].

A maioria dos riscos de TI, não decorre de problemas técnicos ou gerados por funcionários de baixo escalão, mas sim de falhas provenientes da supervisão e da governança de TI, ou seja, a maior parte destes riscos não resulta da tecnologia em si, mas de processos decisórios que, de modo consciente ou não, ignoram as possíveis consequências destes riscos para os negócios [42].

Chaves (2011) [44] cita que as causas que levam os riscos da TI estão relacionadas com a governança de TI ineficaz, a complexidade descontrolada e a falta de atenção ao risco.

A governança de TI ineficaz decorre da ausência de estruturas e processos apropriados para um amplo envolvimento de todas as áreas da organização nos investimentos e nas decisões relativas à TI, além disso, acaba levando a decisões otimizadas localmente, mas que geram riscos para a organização [44].

Westerman e Hunter (2007) [42] citam 4 fatores de riscos associados aos objetivos de negócios da TI, são eles:

- **Disponibilidade:** manter os sistemas e os processos de negócio por eles suportados em operação e recuperá-los em caso de interrupções;
- **Acesso:** assegurar um acesso adequado a dados e sistemas, de modo que as pessoas certas o tenham quando necessário e as pessoas erradas não;
- **Precisão:** prover informações corretas, oportunas e completas, que satisfaçam aos requisitos da administração, dos colaboradores, clientes, fornecedores e órgãos reguladores;
- **Agilidade:** Possuir a capacidade de mudar com custos controlados e rapidez.

Na Engenharia de Sistemas, os projetos são desenvolvidos em ambientes de incerteza, onde a gestão de riscos apresenta como sendo primordial. Os riscos podem ser classificados como sendo riscos técnicos de custo, cronogramas e programáticos [45].

Em relação aos riscos associados com a racionalização de sistemas legados, Arnold (1992) [46] elenca alguns riscos referentes com a reengenharia de sistemas de TI, uma vez que representa uma maneira de racionalizar os sistemas de TI nas organizações:

- **Riscos de integração:** estão associados com aplicações que não pode satisfatoriamente ser integrado ou possuir interfaces com os demais sistemas existentes;
- **Riscos em relação a manutenção:** devido a eventuais dificuldades de manutenção, muitas vezes um sistema que sofreu uma reengenharia pode piorar, em vez de melhorar;
- **Riscos de processo:** os riscos podem estar associados aos processos da organização;
- **Riscos de cronograma:** associados aos atrasos ocorridos no projeto;
- **Riscos de aceitação:** relacionado a obtenção de um produto que não é adequado a interação das pessoas, ou que é inaceitável para a organização;
- **Riscos de aplicação:** ter um produto que não satisfaz a aplicação ou o propósito pretendido;
- **Riscos associados a ferramentas e disponibilidades de métodos:** Os trabalhos de reengenharia dependem de métodos e técnicas que ainda não foram dominados pelos seus executantes.
- **Riscos associados à estratégia, liderança e cultura organizacionais:** Quando a solução não puder ser aceita pelo ambiente de sua organização proprietária.

De acordo com Rovai (2005) [32], os riscos associados ao desenvolvimento e integração de softwares apresenta como um grande problema para as organizações devido a falta de entendimento das implicações ou mudanças nos processos. Além disso, os riscos organizacionais estão relacionados com os problemas provenientes da cultura da organização, uma vez que é de difícil mudança [32].

Os riscos de origem tecnológica podem afetar as metas e objetivos organizacionais, além de poder ser a causa de outros tipos de riscos, relacionados com o uso da tecnologia [34]. Os riscos causados pela interrupção, alteração ou falha derivada do uso dos sistemas de TI podem implicar em perdas significativas para a organização como as perdas financeiras, além de afetar a imagem da organização causando inconvenientes tanto a nível operacional quanto a nível estratégico [34].

Segundo Rovai (2005) [32], anteriormente a maioria dos softwares eram desenvolvidos de forma isolada e individualmente, onde os desenvolvedores tinham controle total dos

requisitos, do projeto e do processos utilizados para a elaboração do software, diferente dos dias de hoje que a maioria dos softwares são desenvolvidos de forma integrada, o que requer o conhecimento maior dos requisitos de cada componente de software e não tendo o controle de todas as variáveis, surgindo diversos riscos com a integração dos softwares da organização.

Os riscos associados ao processo de desenvolvimento de software devem ser analisados, avaliados e tratados. Portanto, compreender, avaliar e tratar o risco é importante para garantir que se atinja os objetivos da organização [47].

2.5.1 Fatores de Risco no processo de Desenvolvimento de Software

O risco que envolve o desenvolvimento de um software está relacionado com os aspectos operacionais, contratuais e organizacionais. O gerenciamento de risco de software consiste em avaliar e controlar os riscos que podem afetar o projeto, o processo, ou o produto de software e são gerenciados pelas seguintes atividades: identificação, análise, planejamento, acompanhamento e resolução dos riscos.

O'Connor e Clarke (2012) [48] realizou uma pesquisa para identificar os fatores situacionais que afetam o processo de desenvolvimento de software, onde identificaram 44 fatores divididos em 8 classificações. Para os autores, o processo de desenvolvimento de software ideal é considerado dependente das características situacionais das configurações individuais do desenvolvimento de software. A estrutura criada pelos autores fornece uma base sólida para a definição e otimização do processo de desenvolvimento de software.

Verifica-se que o risco do desenvolvimento de software é um domínio de pesquisa grande e bastante distinto que cresceu durante as últimas décadas. Casher (1984) [49] em sua pesquisa, identificou 21 riscos associados a projetos de sistemas de informação, incluindo os fatores de riscos do desenvolvimento de software.

Barry Bohem (1991) [50] publicou os 10 principais itens de risco de software. No processo de desenvolvimento de software, Bohem (1991) divide o gerenciamento de riscos em dois blocos: avaliação e controle. Na avaliação, os riscos são identificados, analisados em função de sua ocorrência, gravidade e relacionamento e por fim priorizados pela ordem de tratamento. O bloco de controle representa o planejamento das atividades de gerenciamento de riscos, implementação de ações e o constante monitoramento das variáveis identificadas.

Para Lyytinen et. al (1998) [51], os riscos de software são situações inconsistentes que fazem parte de um modelo sociotécnico de mudança organizacional que inclui atividade, estrutura, tecnologia e pessoas. Essa incongruência pode levar a falhas no desenvolvi-

mento ou implementação do software/sistema e, portanto, a grandes perdas. Os autores sintetizaram um conjunto de 17 fatores de risco de software classificadas em 5 tipos, além de identificar técnicas de resolução de riscos, que abrangem os componentes sociotécnicos e suas interações.

Na pesquisa realizada por Ropponen e Lyytinen (2000) [52] foram identificados 6 componentes de risco de desenvolvimento de software, divididos em 26 itens de riscos associados e 4 fatores ambientais que estão atuando no componente de risco, sendo observado que os riscos de software podem ser melhor gerenciados combinando considerações específicas de gerenciamento de riscos com uma compreensão detalhada do contexto ambiental com boas práticas gerenciais.

No trabalho de Barki et al (201) [53] foi desenvolvido uma estrutura de riscos de desenvolvimento de software que engloba um espectro mais amplo de riscos do que as estruturas de risco anteriores - incluindo novos itens de risco, como conflitos interpessoais e atitudes do usuário. A estrutura inclui 35 fatores de risco que são classificados sob 18 conceitos subjacentes. Além disso, alguns dos fatores de risco são ainda mais decompostos em uma série de componentes.

Leopoldino (2004) [54] classifica os fatores de riscos em 7 variáveis que definem os fatores de risco do desenvolvimento de software: Gerência de Projetos, Equipe de Desenvolvimento; Escopo e Requisitos; Conhecimento e Incerteza Tecnológica; Relacionamento com o Ambiente Externo; Relacionamento com o Cliente/usuário e Valor/Importância atribuídos ao projeto.

2.6 Terminologias

Para o alinhamento entre os principais termos utilizados na pesquisa, foram definidos os significados para as terminologias adotadas.

Ativo: Um ativo é qualquer item de valor da organização que possa ser afetado e leve a um impacto no negócio, ou seja, é qualquer coisa com valor tangível ou intangível que vale a pena proteger, incluindo pessoas, sistemas, infraestrutura, finanças e reputação [31, 55].

Evento: É uma divulgação (de informação confidencial), interrupção (de um sistema ou projeto), roubo ou destruição. A ação também inclui o projeto ineficaz (de sistemas, processos etc.), uso inapropriado, mudanças nas regras e nos regulamentos que impactam o sistema de modo relevante, ou a execução ineficaz dos processos, por exemplo, procedimentos de gestão de mudança, procedimentos de aquisição, processos de priorização de projetos [31].

Ameaças: São eventos não esperados (deliberados ou acidentais), externos ao sistema de software, que podem ocorrer, resultando em prejuízos aos ativos e recursos de informação [55].

Vulnerabilidades: Uma fraqueza no desenho, implementação ou controle interno de um processo que possa expor o sistema a ameaças adversas de eventos de ameaça [31].

Risco: A ISO/IEC 27005 [30] define risco como o potencial de uma determinada ameaça explorar vulnerabilidades, proporcionando perdas ou danos a um ativo ou grupo, de forma direta ou indireta para organização.

Fatores de Risco: Um fator de risco "representa um atributo incerto de um projeto ou de um ambiente contextual [56] que pode "afetar adversamente um projeto, a menos que os gerentes de projeto tomem contramedidas apropriadas"[57]. Essas contramedidas podem incluir alterações no processo de desenvolvimento de software.

O Cobit 5 define risco como "a condição que pode influenciar a frequência e/ou a magnitude e, em última análise, o impacto no negócio dos eventos/cenários relacionados à TI" [31].

Análise do Risco: É um processo segundo o qual a frequência e a magnitude dos cenários do risco da TI são estimados [31]. As etapas iniciais da gestão de risco são: análise do valor dos ativos para o negócio, identificação das ameaças, para esses ativos e avaliar a vulnerabilidade de cada recurso a essas ameaças [31].

Avaliação do Risco: Um processo usado para identificar e avaliar o risco e seus efeitos potenciais [31].

Capítulo 3

Metodologia de Pesquisa

O presente capítulo apresenta a metodologia aplicada no trabalho, também serão apresentados os métodos utilizados e os procedimentos para o alcance do objetivo geral e de cada um dos objetivos específicos propostos nesta pesquisa.

3.1 Método de Pesquisa

O método pode ser entendido como um conjunto de processos empregados na investigação e na demonstração da verdade, por tanto não é inventado e depende do objeto da pesquisa. Já a técnica é a aplicação do plano metodológico e a forma em que deve ser executado [58].

A pesquisa é uma atividade voltada para a solução de problemas teóricos ou práticos com o uso de processos científicos [58]. Os diferentes tipos de pesquisa podem ser classificados segundo a abordagem, natureza, objetivos e estratégia [59, 60]. A figura 3.1 apresenta a classificação da pesquisa os métodos e as técnicas que são utilizadas.

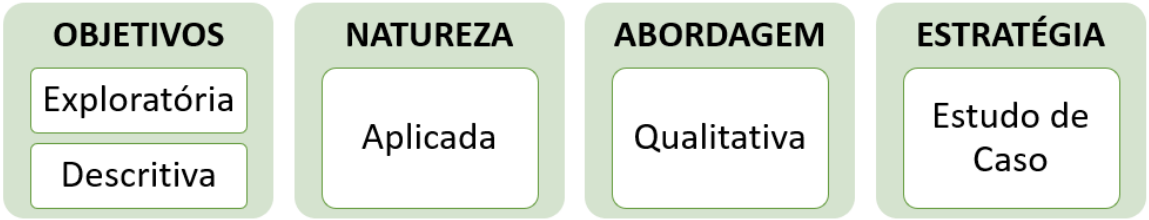


Figura 3.1: Classificação da Pesquisa

- **Quanto aos objetivos:**

  - A pesquisa tem **caráter exploratório**, que conforme Gil (2008) [61] é desenvolvida mediante os conhecimentos disponíveis e a utilização cuidadosa de métodos e técnicas. A pesquisa visa proporcionar maior familiaridade com o problema com vistas a torná-lo explícito.
  - A **pesquisa descritiva** foi utilizada para registrar o conhecimento obtido com os processos de negócio modelados e descrever os fenômenos estudados, no qual foi possível entender como as atividades da organização são realizadas e quais são os sistemas utilizados, bem como no entendimento do processo de desenvolvimento de software da organização.

- **Quanto à natureza:** esta pesquisa pode ser considerada aplicada, pois busca gerar conhecimentos acerca da problemática com aplicação prática na análise dos riscos do processo de desenvolvimento de software e propondo melhorias para o processo [62].

  O objeto de estudo é de grande importância para a organização, uma vez que a quantidade de sistemas utilizado nos processos de negócio impactam em suas atividades.

- **Quanto à abordagem:** A pesquisa é classificada como qualitativa quanto ao entendimento do comportamento da organização e de seus profissionais, seus valores e objetivos que auxiliam na identificação dos fatores de riscos do processo de desenvolvimento de software.

  Além disso, percebe-se que o ambiente é uma grande fonte de dados para o pesquisador, sendo uma característica importante em pesquisa qualitativas onde ocorre as relações entre o pesquisador e as pessoas envolvidas no ambiente [32].

- **Quanto à estratégia:** A pesquisa constitui-se como um estudo de caso, que foi aplicado dentro das atividades realizadas no Projeto MAP/UnB, onde são modelados, os processos do Departamento-Geral de Pessoal de uma organização pública militar.

  O estudo de caso foi utilizado, pois visa conhecer o como e o porquê acontece uma determinada situação e por ser caracterizado como um estudo de uma entidade bem definida como um programa, uma instituição, um sistema educativo, uma pessoa, ou uma unidade social [60].

3.2 Estruturação da Pesquisa

A estrutura da pesquisa está dividida em quatro etapas, aplicadas no estudo de caso desenvolvido neste trabalho, conforme mostrado na Figura 3.2.

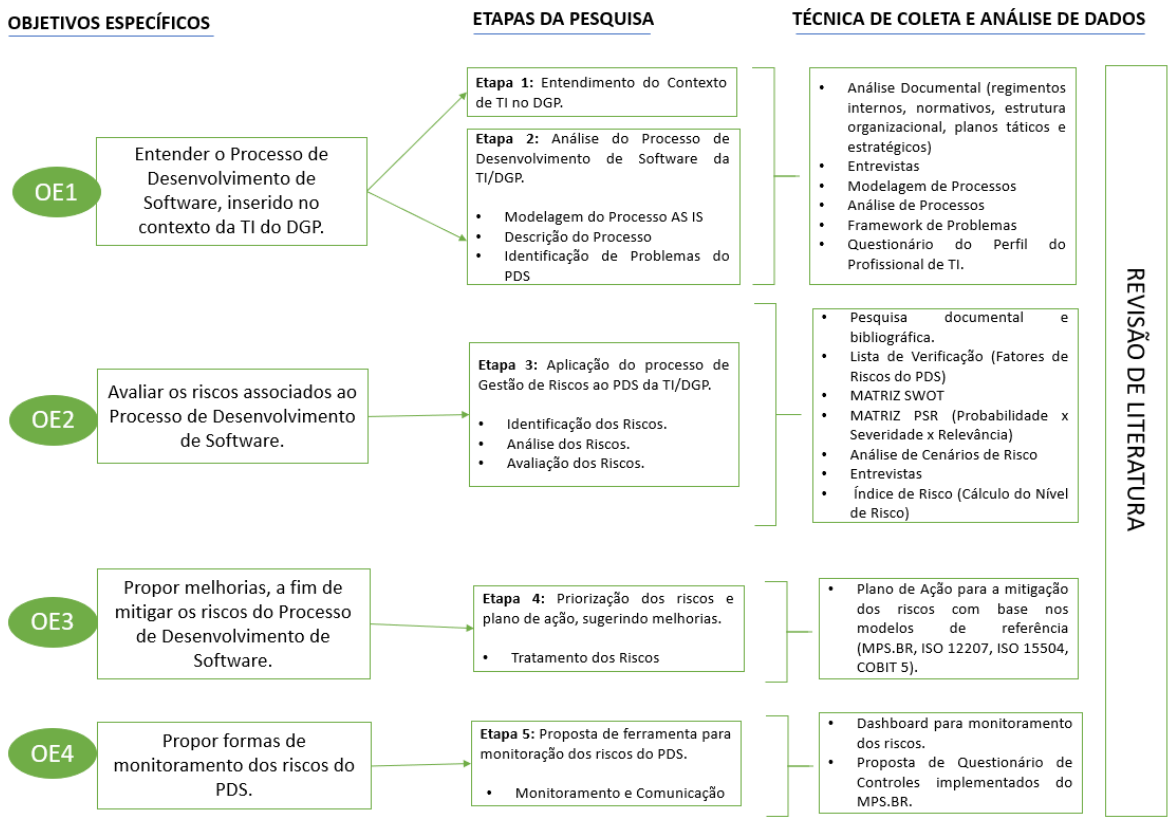


Figura 3.2: Estrutura da Pesquisa

A revisão da literatura foi a base de toda a pesquisa, sendo importante em todas as etapas, no qual foi necessário realizar a pesquisa bibliográfica com os temas referente ao estudo (técnicas, modelos de processos de software; melhoria de processos de software; gestão de riscos no processo de desenvolvimento de software).

Foram realizadas leituras de livros, artigos científicos, dissertações e teses que auxiliaram no referencial teórico ao longo de toda a pesquisa. Tendo em vista a figura 3.2, pode-se detalhar cada etapa da seguinte forma:

3.2.1 Etapa 1 - Entendimento do Contexto da TI do DGP

Para atingir o primeiro objetivo, foi necessário pesquisar a documentação interna do órgão de maneira a analisar os regimentos internos, estrutura organizacional, os planos táticos

e estratégicos e os normativos.

A primeira etapa consiste em entender o contexto de onde está inserido a avaliação de riscos, identificando o contexto interno e externo por meio de um diagnóstico organizacional.

Para aplicar o processo de gestão de riscos, é necessário conhecer a organização que está sendo estudada, analisar o contexto interno e externo, ou seja, os processos de negócio, as pessoas envolvidas, a tecnologia utilizada e os objetivos estratégicos [26].

Nessa etapa é realizado o entendimento do contexto de TI do DGP, que são identificados, por meio da análise da cadeia de valor, quais são os processos de negócio relacionados com a TI do DGP e como o processo de desenvolvimento de software está inserido no departamento.

Além disso, é importante identificar quem são as pessoas responsáveis pela TI do departamento. Com isso, foi elaborado um questionário para identificar o perfil do profissional de TI do DGP.

A coleta de informação para o levantamento dos problemas gerados pelos softwares da organização ocorreu por meio de entrevistas semi-estruturadas para a modelagem dos processos de negócio e a aplicação de questionários com os usuários dos sistemas de informação e com os envolvidos no desenvolvimento dos softwares da organização.

Foi aplicado um questionário para analisar o perfil do profissional de TI do DGP, onde possibilitou identificar o nível de formação dos militares de TI do DGP, além de analisar o conhecimento técnico, as experiências profissionais, e a área de atuação, de forma a mapear o perfil da TI do DGP. O apêndice B apresenta o questionário aplicado aos profissionais de TI do DGP. A Tabela 3.1 apresenta o quantitativo de questões analisadas no QPTI.

Tabela 3.1: Quantitativo de questões por dimensões analisadas - QPTI

Dimensão	**Questões**
Área de Atuação (PPA)	3
Experiência (PE)	9
Conhecimento Técnico	6
Formação (FM)	7
Questões Gerais (QG)	2

De aproximadamente 106 profissionais de TI do DGP, 35 responderam ao questionário do perfil de profissional de TI (QPTI). A Tabela 3.2 apresenta o total de profissionais de TI do DGP e o total de respondentes em cada questionário.

Tabela 3.2: Total de profissionais de TI por área do DGP (Julho de 2019)

Área	**Quantidade de militares**	**Militares que responderam ao QPTI**
DCEM	22	2
DCIPAS	3	0
D Sau	13	13
DSM	11	3
D A Prom	16	11
DTI	42	6
Total	**106**	**35**

O questionário foi enviado aos militares da área de TI do DGP, com auxílio da ferramenta Google Forms.

3.2.2 Etapa 2 - Análise do Processo de Desenvolvimento de Software da TI do DGP

Na segunda etapa, após entender o contexto da TI do DGP, foram elencados os processos pertencentes ao Ciclo de Vida de Software no DGP, por meio da análise da Cadeia de Valor do departamento e selecionado o Processo de Desenvolvimento de Software para ser modelado e com isso, analisar e identificar quais são os principais problemas que ocorrem atualmente no processo.

Para o entendimento do macroprocesso, foi utilizado a técnica SIPOC (supplier (fornecedores), input (entradas), process (processo), output (saídas) e customer (clientes)), onde foi possível identificar o objetivo, as entradas e saídas, bem como os clientes e fornecedores do processo.

Foi realizada uma pesquisa de campo, com entrevistas para a modelagem dos processos com os profissionais de TI do departamento que são responsáveis pelos processos modelados. Além de realizar a análise de documentos dos processos e da legislação existente na organização.

As entrevistas foram realizadas em conjunto com as atividades do Projeto MAP/UnB no DGP, onde estão sendo modelados os processos de negócio e realizando uma análise dos sistemas de informação do departamento de maneira a proporem uma racionalização tanto em seus processos como também nos sistemas de informação.

Os processos pertencentes ao macroprocesso, foram modelados utilizando a notação BPMN com os atores e gestores envolvidos nos processos, utilizando a ferramenta ARIS Express.

A modelagem dos processos (AS IS) foram realizadas em três reuniões para cada processo conforme ilustra na Figura 3.3, onde a primeira (R1) consistiu em entender o fluxo do processo, a segunda (R2) em complementar o entendimento do processo e a terceira (R3) em validar o processo modelado.

Figura 3.3: Processo utilizado para a modelagem dos processo

A primeira entrevista foi realizada com o gestor e os executores do processo coletando as informações necessárias para diagramá-lo. Possui o objetivo de entender como o processo é executado, identificando as atividades, os artefatos e os sistemas que são utilizados pelo processo, gerando um Relato de Reunião e levantando informações para o primeiro esboço do diagrama do processo.

A segunda entrevista teve o objetivo de verificar junto aos atores do processo se as atividades que estão representadas no diagrama estão em consonância com o fluxo real do processo. Em caso de incongruência, os atores podem solicitar a adição de atividades essenciais para o entendimento do processo, bem como indicar atividades que foram erroneamente atribuídas ao fluxo.

Na terceira entrevista foi realizada a validação final do processo com o cliente e serão coletadas informações para o diagnóstico dos sistemas de informação utilizados no processo, além de validar o que já foi levantado de possíveis requisitos para a sistematização de atividades do processo, para o alinhamento das suas necessidades.

Com as reuniões de modelagem de processo, foi possível identificar os principais problemas existentes e com isso foi necessário analisar, documentar os dados coletados e solidificar o diagnóstico dos principais problemas e dificuldades existentes nos processos de negócio e recomendar as possíveis soluções. A Figura 3.4 apresenta a estrutura do *framework* de problemas utilizado.

O levantamento dos principais problemas existente no processo de desenvolvimento de software foi realizado com base no *framework* de análise de problemas proposto no BABOK 3 [63] e consiste em uma declaração do problema ou da visão que declara a necessidade do negócio, identifica as principais partes interessadas e descreve brevemente

ID: [PN001]	[Nome do problema]
O problema:	[descreva o problema].
Envolvidos afetados:	[quais os envolvidos pelo problema].
Impacto gerado pelo Problema:	[qual é o impacto do problema para o cliente?].
Solução para o Problema:	[apresentar a solução do problema e identificar os benefícios para o cliente através da informatização das etapas do processo].

Figura 3.4: Framework de Problemas
Fonte: Adaptado de [63].

o impacto na organização e nos seus processos, além de propor soluções para a resolução dos problemas encontrados[63].

3.2.3 Etapa 3: Aplicação do Processo de Gestão de Riscos ao PDS da TI/DGP

O estudo de caso foi realizado a partir da necessidade de verificar como os riscos comuns do processo de desenvolvimento de software identificado na literatura ocorrem na unidade organizacional que está sendo estudada.

A aplicação da gerência de riscos é conduzida pelo estabelecimento e manutenção de uma estratégica para identificar, analisar e avaliar os riscos existentes no processo.

A pesquisa partiu do modelo de análise de riscos utilizado por [64] com base na customização de ferramentas de riscos para a análise do processo de software, onde a metodologia utiliza o conceito que a exposição ao nível do risco é calculada por meio da probabilidade e do impacto da sua ocorrência.

Para a delimitação da pesquisa, o ativo da organização selecionado foi o Processo de Desenvolvimento de Software, sendo agrupado em 19 áreas definidas pelo modelo MPS-BR [25]. A pesquisa não pretende avaliar o nível de maturidade do processo de software da organização e sim levantar indícios de onde o processo pode ser melhorado com base nas áreas de processos do MPS-BR.

Foram selecionadas as etapas do processo de desenvolvimento de software presentes na organização por meio da modelagem do processo de negócio. Para cada área do processo de negócio, foi verificado quais eram os controles e os resultados esperados (REP) previstos no MPS-BR.

3.2.3.1 Identificação de Riscos

O primeiro momento foi identificar por meio de pesquisa documental, quais eram os principais riscos na TI do DGP, e a partir dessa análise, verificar quais estavam relacionados com o processo de desenvolvimento de software.

Depois, buscou-se identificar os riscos inerentes ao Processo de Desenvolvimento de Software do DGP e quais situações poderiam afetar o alcance dos resultados esperados para o processo.

O instrumento para a definição da lista de fatores de riscos (itens de verificação), foi construído com base em pesquisa bibliográfica, onde foram identificados os fatores de riscos que impactam o processo de desenvolvimento de software.

A lista de verificação é uma técnica considerada como "Fortemente aplicável"na fase de identificação de riscos pela ABNT NBR ISO 31010 [33]. A lista de riscos utilizada na pesquisa encontra-se no Apêndice C e foi dividida em três fontes de identificação (processo AS IS modelado, PDTI e os fatores identificados na literatura).

Com a lista de riscos desenvolvida, o instrumento foi submetido à avaliação dos especialistas de TI do DGP, para verificar quais desses riscos ocorrem no processo de desenvolvimento de software atual do DGP, além de identificar outros riscos que ocorrem no processo.

A técnica utilizada foi a entrevista que é considerada como "Fortemente aplicável - FA"na fase de identificação de riscos pela ABNT NBR ISO 31010 [33].

A escolha dos especialistas teve como critério de seleção os gestores e profissionais dos processos estudados, tendo como as principais funções: gestores, analistas e desenvolvedores que atuam no desenvolvimento de software da organização.

A unidade analisada possui 42 profissionais de TI de diversas áreas. Para a realização da entrevista, foram selecionados 6 profissionais de TI, sendo os chefes das seções de análise e de desenvolvimento, mais 4 especialistas de TI das suas respectivas equipes com conhecimento nos processos analisados.

Na entrevista, os especialistas entraram em consenso na identificação e análise dos riscos, pontuando cada fator de risco.

3.2.3.2 Análise de Riscos

A análise de riscos busca compreender a natureza do risco e determinar o seu nível e fornece uma base para a avaliação destes [26]. São coletados dados para identificar o nível de exposição a riscos da organização, onde são avaliados segundo seus ativos organizacionais, representados pelos seus processos, pessoas, papéis, tecnologia ou ambiente [64].

A exposição ou nível de risco é calculado por meio do índice PSR (Probabilidade da ocorrência do risco, da Severidade desta ocorrência e da Relevância do ativo para a organização. Na avaliação, são atribuídos os valores de 1 a 5 e o valor final representa a multiplicação das três variáveis [64, 65]. A tabela 3.3 apresenta os valores atribuídos ao PSR e o valores possíveis para cada nível de risco.

Tabela 3.3: Valores atribuídos do PSR

Nível de Risco	**Prob.**	**Sev.**	**Rel.**	**Valores Possíveis do PSR**
Muito Baixo	1	1	1	1, 2, 3, 4, 5, 6
Baixo	2	2	2	8, 9, 10, 12, 15,16
Médio	3	3	3	18, 20, 24, 25, 27, 30
Alto	4	4	4	32, 36, 40, 45, 48, 50
Muito Alto	5	5	5	60, 64, 75, 80, 100, 125

A Probabilidade e a Severidade atribuídas a cada controle podem variar de muito baixo, baixo, médio, alto e muito alto, sendo as notas de 1 a 5 atribuídas respectivamente a esses conceitos. A Relevância de cada ativo empregada no cálculo de risco também utiliza a escala semelhante de ponderação (valores variando de 1 a 5).

A partir da multiplicação dos valores da Probabilidade e da Severidade do controle, pela Relevância do ativo tem-se o risco atribuído a cada controle, sendo os valores limites para o PSR (Probabilidade x Severidade x Relevância) para cada controle de 125. O PSR é calculado pela equação:

$$Risco = PxSxR \tag{3.1}$$

A figura 3.5 apresenta o modelo de análise riscos adotado pela pesquisa.

Com isso, foi aplicado o *checklist* com os fatores de riscos do processo de desenvolvimento de software na organização para verificar quais vulnerabilidades podem impactar o negócio, o processo a continuidade do projeto e a probabilidade da ocorrência do risco. A avaliação leva em conta a relevância dada a cada área do processo de desenvolvimento de software. A Figura 3.6 demonstra o instrumento utilizado para a análise e avaliação dos riscos.

A avaliação foi realizada pelos gestores e desenvolvedores que participam do processo de desenvolvimento de software da organização.

3.2.3.3 Avaliação de Riscos

Na avaliação dos riscos são comparados os resultados da análise de riscos com os critérios de risco para determinar se o risco e sua magnitude é aceitável ou tolerável [26].

	Probabilidade (A ocorrência da vulnerabilidade ser explorada por uma ameaça)	Severidade (A consequência da vulnerabilidade ser explorada pelas ameaças)	Relevância (Importância estratégica cujo um ativo está inserido)	
5	É quase certo que o risco irá ocorrer. (> 90%)	Impactará extremamente o negócio, processo e a continuidade do projeto.	Afeta todo o negócio da organização e os prejuízos são extremamente altos.	Muito alta
4	É altamente provável que o risco ocorra. (65% < p < 95%)	Impactará gravemente o negócio, processo e a continuidade do projeto.	Afeta um ou mais negócios da organização e os prejuízos são muito altos	Alto
3	É provável que o risco ocorra. (35% < p < 65%)	Prejuízo moderado ao negócio, processo e projeto.	Afeta uma parte do negócio da organização e os prejuízos são razoáveis	Médio
2	É improvável que o risco ocorra. (5% < p < 35%)	Impactará pouco o negócio, processo e a continuidade do projeto.	Afeta uma parte pequena e localizada do negócio da organização e os prejuízos são baixos	Baixo
1	É altamente improvável que o risco ocorra. (< 5%).	Quase não impactará o negócio, processo e a continuidade do projeto.	Afeta uma parte muito pequena e localizada do negócio da organização e os prejuízos são desprezíveis.	Muito Baixo

Figura 3.5: Modelo de Gestão de Riscos
Fonte: Adaptado de [64]

FATORES DE RISCO								
Área do Processo	ID	DESCRIÇÃO DO FATOR DE RISCO	P	S	R	PSR	% PSR	Nível de Risco
GP- Gestão de Projetos	FR01	Distribuição incorreta de recursos alocados para o projeto, prejudicando o andamento das atividades da organização e dos projetos.						
REQ - Requisitos	FR19	Existência de requisitos incompletos, inconsistentes, inválidos, incorretos ou não verificáveis que impedem a correta implementação.						
PI - Projeto e Implementação	FR24	Implementação do produto não atende aos projetos do produto. Inconsistência entre o que foi projetado e o que foi desenvolvido pelo projeto.						

Figura 3.6: Modelo de instrumento para a análise e avaliação dos riscos
Fonte: Adaptado de [64].

A técnica utilizada foi o "Índice de Risco", considerada como "Fortemente Aplicada - FA" na fase de "Avaliação de Risco" pela ISO 31010[33]. A Tabela 3.4 apresenta os critérios de riscos utilizados para comparar as vulnerabilidades identificadas no Processo de Desenvolvimento de Software do DGP.

Tabela 3.4: Interpretação do nível de risco

Valor PSR	**Índice do Risco**	**Descrição**
De 60 a 125	Muito Alto	são riscos inaceitáveis, e os gestores dos ativos devem ser orientados para que minimizem imediatamente.
De 32 a 50	Alto	são riscos inaceitáveis e os gestores dos ativos devem ser orientados para pelo menos controlá-los;
De 18 a 30	Médio	são riscos que podem ser aceitáveis após revisão e confirmação dos gestores dos ativos, contudo a aceitação do risco deve ser feita por meios formais;
De 08 a 16	Baixo	são riscos que podem ser aceitáveis após revisão e confirmação dos gestores dos ativos;
De 01 a 06	Muito Baixo	são riscos aceitáveis e devem ser informados para os gestores dos ativos.

O valor atribuído ao índice do risco para cada vulnerabilidade define o nível de risco que servirá como critério de comparação. Com isso, será possível analisar quais fatores de riscos (vulnerabilidades e ameaças) são significantes para a organização, sendo que os riscos com alto nível devem ser tratados pela organização.

Com os dados levantados, será possível identificar quais áreas dos processos apresentam o maior índice de risco, ou seja, verificar quais áreas apresenta a maior participação dos riscos, sendo uma área prioritária para a melhoria do processo de desenvolvimento de software.

3.2.4 Etapa 4: Sugestão de Melhorias para o PDS da TI/DGP

Com base nas melhores práticas proposta pela literatura e nas oportunidades identificadas, deve-se elaborar e executar um plano de ação para a melhoria do processo de desenvolvimento de software do DGP e a mitigação dos riscos.

No tratamento de riscos são definidas as possíveis ações a serem tomadas nos riscos, no qual, deve-se gerar um plano de tratamento dos riscos, onde deve conter os recursos, responsabilidades e as atividades que serão realizadas. De acordo com Ramirez (2011) [34], as ações também deve incluir uma análise de custo-benefício, tanto para a implementação como para a manutenção.

Os riscos podem ser tratados, segundo a ABNT/ISO 27005 como sendo:

- Evitar o Risco: Eliminar as causas ou as consequências;

- Reduzir o Risco: Limitar o risco através de controles que reduzam ou eliminam o impacto gerado pela exploração de uma vulnerabilidade;
- Reter o risco: Aplicar controles de correções como base o conhecimento de vulnerabilidades, falha ou defeito.
- Transferir o Risco: Adotar outras opções que compensam a perda e transferir a responsabilidade pelo gerenciamento do risco, mas não a responsabilidade pelas consequências.

As recomendações serão realizadas de acordo com os controles e áreas do processo de desenvolvimento de software que apresentaram o maior risco identificados.

O plano de ação deve ser elaborado de maneira a responder às seguintes questões:

- O que deve ser feito? (a ação, em si);
- Por que esta ação deve ser realizada? (o objetivo);
- Quem deve realizar a ação? (os responsáveis);
- Onde a ação deve ser executada? (a localização);
- Quando a ação deve ser realizada? (tempo ou condição);
- Como deve ser realizada a ação? (modo, meios, método, etc);
- Quanto será o custo da ação a realizar? (custo, duração, intensidade, profundidade, nível de detalhamento, etc).

Na próxima seção são mostrados os resultados do diagnóstico da organização contendo informações sobre o contexto interno e externo, obedecendo o processo indicado na norma ISO/IEC 31000 [26]. O entendimento do contexto no qual o objeto do estudo de caso está inserido, é fundamental para a identificação dos riscos.

Capítulo 4

Estabelecimento do Contexto da TI do DGP

Este capítulo relata o diagnóstico organizacional contemplando, os processos, pessoas e a tecnologia utilizada pela área de Gestão de Pessoas da organização, bem como o entendimento dos problemas oriundos dos sistemas de TI do DGP.

4.1 Entendimento do Contexto de TI do DGP

O diagnóstico organizacional é o primeiro passo para o entendimento do contexto externo e interno de onde se pretende realizar o gerenciamento dos riscos. Pode ser considerado um facilitador para a definição de alternativas que possam subsidiar o processo de tomada de decisão na organização.

O objetivo do diagnóstico é analisar a TI do DGP de maneira a verificar como as unidades de TI do DGP estão inseridas neste contexto, considerando a estrutura organizacional, as responsabilidades e autoridades que possuem em suas unidades constituintes, além de analisar a percepção dos profissionais integrantes quanto a governança de TI e os serviços prestados. Representa o estado atual (AS IS) da área de TI da organização, dos processos e sistemas de informação.

O diagnóstico de tecnologia da informação poderá ser utilizado na elaboração de diretrizes de desenvolvimento de software existentes no DGP e consistiu em uma análise dos processos operacionais e gerenciais que envolve os sistemas de informação utilizados, a fim de identificar os eventuais *gaps* (necessidade de melhorias) que podem ser implementados pela organização.

As melhorias propostas servirão para otimizar os processos e na identificação dos riscos que podem provocar perdas para o negócio. Além disso, muitos destes sistemas automa-

tizam apenas os processos operacionais, e não disponibilizam as informações gerenciais necessárias (KPI – *Key Performance Indicators*) para a administração do negócio.

O primeiro passo para a elaboração do diagnóstico de TI, é o entendimento da organização, identificando seus processos de negócio, as pessoas envolvidas, a tecnologia utilizada, bem como a análise do contexto interno e externo.

4.1.1 Contexto Externo

O estabelecimento do contexto externo é fundamental para assegurar que os processos e objetivos identificados estejam alinhados com os interesses da organização. Para verificar esse alinhamento será necessário analisar o ambiente cultural, social, político, legal, regulatório, financeiro, tecnológico, econômico, natural e competitivo no qual a organização se insere, bem como fatores-chave e tendências que tenham impacto sobre os objetivos da organização e relações com as partes interessadas e suas percepções e valores.

Diante disso, verificou-se que no dia 17 de dezembro de 2014, a Portaria nº 295-EME aprova a Diretriz de Racionalização Administrativa do órgão (EB20D-01.016) [66] com o objetivo de:

> - Implantar a cultura de inovação em todos os sistemas da organização, a partir da Alta Administração, contribuindo para melhorar a gestão do bem público em toda a Instituição.
> - Estabelecer a Sistemática de Racionalização Administrativa na organização, para atender às demandas de cargos do Processo de Transformação.
> - Aumentar o emprego de militares temporários especialistas e de prestadores de tarefa por tempo certo, minimizando a utilização de militares combatentes em atividades administrativas, contribuindo para que se tenha uma Força Terrestre mais eficiente, eficaz e efetiva [66, p.14].

De acordo com a diretriz publicada, a racionalização administrativa é o estudo das causas e soluções dos processos administrativos, abrangendo a responsabilidade básica de planejar e aperfeiçoar a gestão, as estruturas organizacionais e o pessoal empregado.

A racionalização deve ser entendida como a busca incansável da efetividade para o desenvolvimento de um processo, bem como de realizar a gestão do bem público com eficiência e assim proporcionar a eficácia e a efetividade organizacional [66].

Para isso, deve-se eliminar controles desnecessários e passos intermediários, sejam eles de forma manual ou automatizada, que não agregam valor, além de evitar a duplicidade na

organização. Ainda, deve-se trazer uma melhora em seus processos finalísticos utilizando-se da inovação em todos os seus processos, métodos e relações interpessoais e na realização de suas atividades por meios de tecnologias disponíveis [66].

A racionalização de seus recursos, sejam eles materiais, tecnológicos e financeiros devem ser direcionados para o atendimento e concretização da governança corporativa além de ser embasado no alinhamento estratégico da organização.

A racionalização administrativa prevê a modelagem, análise e melhoria de processos de forma a aperfeiçoar os processos e reduzir as atividades desnecessárias, seja pela integração de processos ou pela utilização de ferramentas de Tecnologia da Informação para a sua execução.

Diante disso, verifica-se que a TI, também deve estar alinhada com o negócio, uma vez que serão utilizados sistemas de informação como forma de melhoria e redução das atividades executadas nos processos de negócio e para isso é importante conhecer os sistemas de TI utilizados e verificar se também não há a duplicação e inconformidade de informações entre eles.

Com isso, foi aprovada no dia 06 de novembro de 2017 a Diretriz para a Racionalização de Tecnologia da Informação e Comunicações (TIC) na organização (EB20-D-02.006) [16], de forma que também esteja alinhado com a diretriz de racionalização administrativa [66].

As principais ameaças que podem ser identificadas relacionadas ao contexto externo da organização são:

- Dificuldade de comunicação entre as áreas de negócio e tecnologia da informação;
- Não entendimento dos processos de negócio pela alta gerência;
- Dificuldade em aceitar mudanças;
- Cultura organizacional.

4.1.1.1 A Governança de TI na Organização

No contexto da organização, a Governança de TI significa avaliar e direcionar o emprego atual e futuro da TI, para assegurar que a sua utilização atenda aos objetivos organizacionais, bem como monitorar o seu desempenho na busca dos resultados pretendidos [67].

A Governança de TI assume importante papel no direcionamento das ações e investimentos para alcançar os resultados desejados pela instituição [68]. Na figura 4.1 apresenta o funcionamento da governança e gestão de TI da organização e a relação com a TI do DGP.

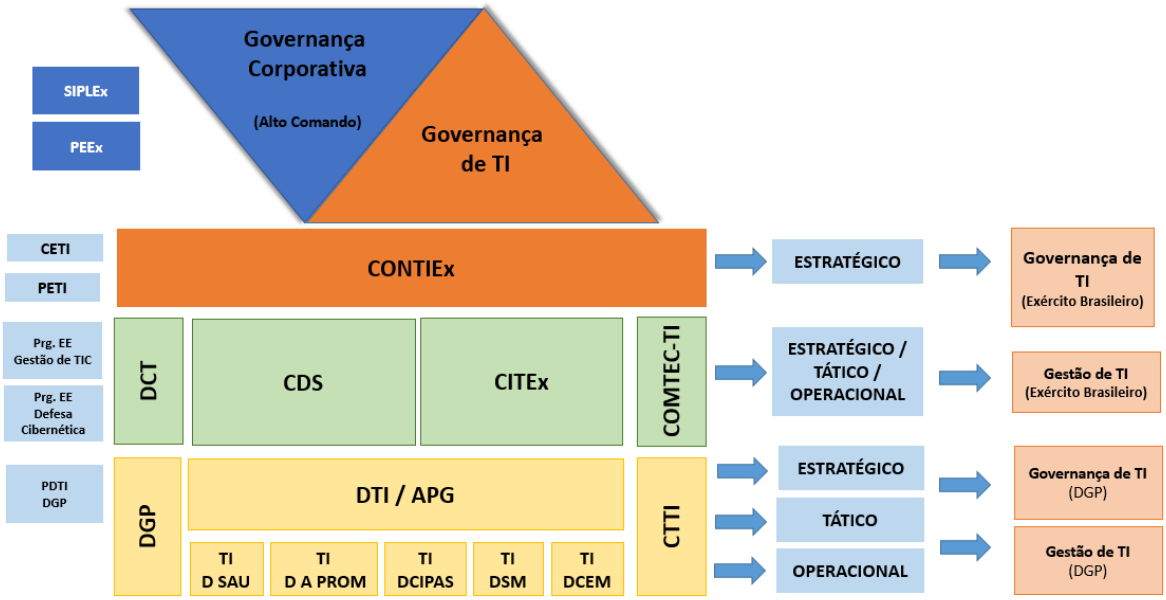


Figura 4.1: Modelo de Governança e Gestão de TI da organização
Fonte: Adaptado de [69, 13].

Sendo de responsabilidade da alta administração e exercida por meio do Conselho de Tecnologia da Informação da Organização, tem a finalidade de controlar o estado atual da gestão, como do futuro da TI na organização como um todo[67].

A visão de futuro da TI da organização com base no Mapa Estratégico de Tecnologia da Informação [68] deve:

> até 2022, garantir soluções tecnológicas de qualidade, particularmente em apoio ao processo de transformação da organização, e ser reconhecida, interna e externamente, como modelo de excelência na governança e gestão, projetando como uma organização moderna e capaz de enfrentar os desafios do século XXI [68, p. 20].

Um dos instrumentos de governança de TI na instituição é a Concepção Estratégica de Tecnologia da Informação (CETI), aprovada pela portaria nº 233 de 20 de março de 2014 e tem a finalidade de orientar na elaboração do Plano Estratégico de Tecnologia da Informação (PETI), que define como a Tecnologia da Informação deve ser estruturada para o atendimento das necessidades da organização [68].

O CETI foi elaborado por meio da realização de diagnóstico estratégico, no qual considerou os ambientes internos e externos e com a participação dos principais operadores de TI na organização e pelo PEEx.

A tecnologia da Informação, segundo a NBR ISO/IEC 38500:2009 [70, 71] é definida como os recursos necessários para adquirir, armazenar e disseminar informações. Verifica-se que os recursos de TI têm sido utilizados em uma escala cada vez maior e permeia todas as atividades desenvolvidas no âmbito da organização.

Pode-se observar que a proposta do trabalho está em consonância com os Objetivos Estratégicos de Tecnologia da Informação (OETI), sendo os principais objetivos atendidos:

Figura 4.2: Objetivos Estratégicos de Tecnologia da Informação
Fonte: Adaptado de [69, 67].

Outro instrumento relacionado a Governança de TI é o Plano Diretor de Tecnologia da Informação (PDTI), que é um instrumento de diagnóstico, planejamento e gestão dos recursos e processos de Tecnologia da Informação e Comunicação de um órgão ou entidade para um determinado período [72].

Em 2010 o documento se tornou obrigatório a partir da Instrução Normativa SLTI 04/2010 [72], pela Secretaria de Logística e Tecnologia da Informação (SLTI), do Ministério do Planejamento, Orçamento e Gestão (MPOG), órgão central do Sistema de Administração dos Recursos de Informação e Informática (SISP).

O desenvolvimento do PETI e do PDTI deve ser alinhado ao PEEx (Planejamento Estratégico da organização) [69].

A Governança e a Gestão de TI devem ser aprimoradas, em conformidade com as orientações emanadas pelo TCU e devem ser apoiadas pela adoção de melhores práticas metodológicas e por ferramentas de TI [72, 13].

Ainda deve considerar a implementação de um sistema informatizado que reúna informações sobre os recursos de TI existentes no âmbito da organização, de forma a melhor orientar e normatizar sua gestão.

Em relação ao desenvolvimento de software, o DCT elaborou diversas diretrizes para serem utilizadas pela unidades de TI do órgão[68]:

- Instruções Gerais para a interoperabilidade e padronização do software na Organização.
- Metodologia de Desenvolvimento de Software da Organização.

O DCT espera com a racionalização de TIC no órgão a melhoria dos processos de TI, a eliminação de redundâncias, a centralização das aquisições e contratações de serviços de TI, bem como na padronização dos processos de desenvolvimento e a consolidação/-simplificação dos sistemas específicos e corporativos do órgão de maneira a aumentar a eficiência do uso da TI pelas organizações militares.

4.1.1.2 Estrutura Organizacional do DGP

O Departamento-Geral do Pessoal é um Órgão de Direção Setorial responsável por, dentre outras funções, planejar, organizar, dirigir e controlar, em nível setorial as atividades de administração de pessoal, assistência social, assistência à saúde, assistência religiosa, promoções, cadastro e avaliação, direitos, deveres e incentivos, inativos e pensionistas, movimentação, pessoal civil e serviço militar que lhe são atribuídas pela legislação específica.

Atualmente a estrutura organizacional do DGP possui 5 diretorias, além de diversas assessorias e unidades. O organograma do DGP está estruturado de acordo com a Figura 4.3.

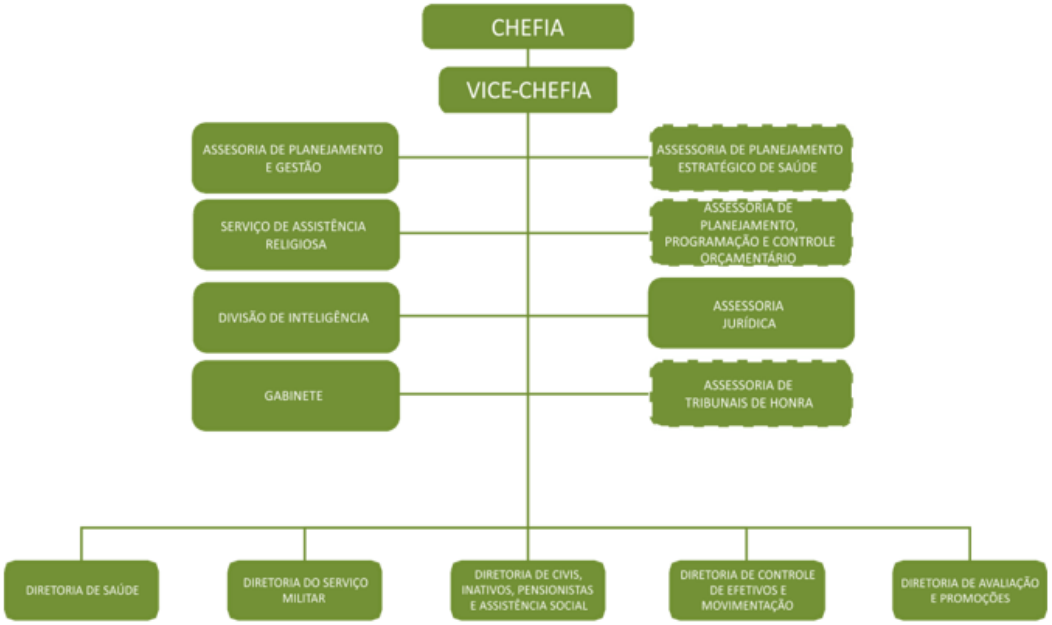


Figura 4.3: Estrutura Organizacional do DGP
Adaptado de [73].

Cada uma das diretorias e assessorias, possuem diversos processos de negócio, tanto finalísticos, gerenciais e de gestão interna.

4.1.1.3 Processos de Negócio

Para o entendimento dos sistemas de informação da organização é necessário compreender o ambiente de relacionamento entre as áreas de negócio envolvidas com a área de TI da organização e com isso, identificar os usuários chaves e suas principais atividades dentro do processos funcionais que impactam diretamente em soluções sistêmicas.

Por isso, foram realizadas pelo projeto MAP/UnB, entrevistas com os gestores de cada seção para a identificação dos processos de negócio. Foram identificados 368 processos contidos no DGP e agrupados em 14 macroprocessos na cadeia de valor. A figura 4.4 representa a cadeia de valor desenvolvido pelo projeto MAP/UnB para o DGP.

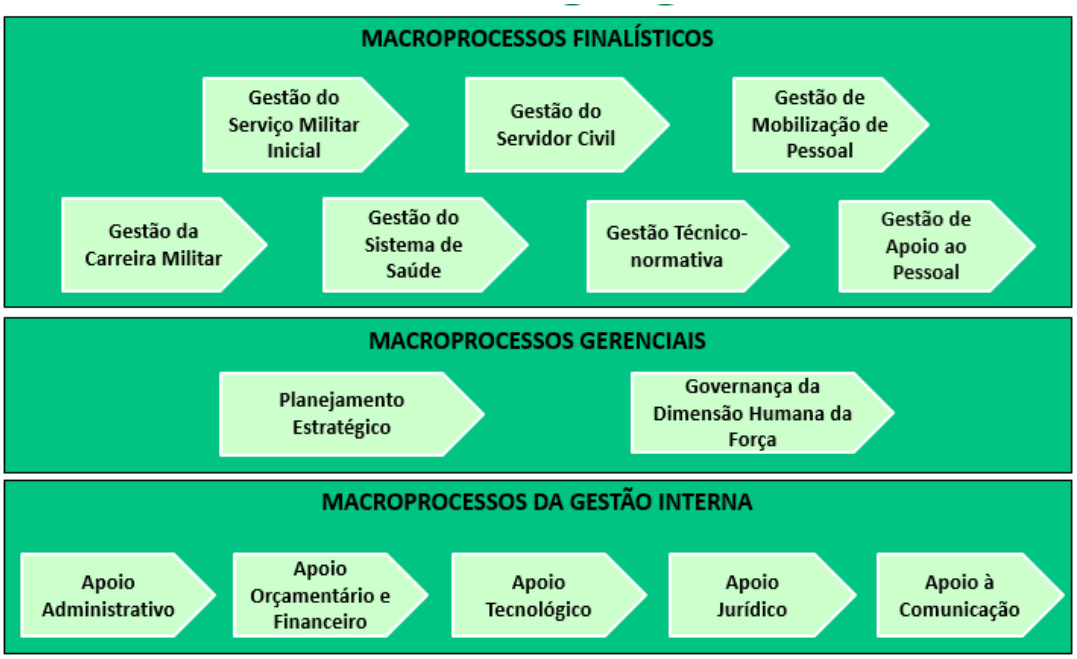


Figura 4.4: Cadeia de valor do DGP
Fonte: Projeto MAP (2018).

Em cada processo de negócio, foi proposto a identificação das atividades que estão informatizadas, e as que necessitam de informatização. Com isso, foi possível compreender o nível de informatização de cada processo modelado.

Após a análise do contexto externo, deve-se analisar o contexto interno do ambiente onde a pesquisa está inserida.

4.2 Contexto Interno

A análise do ambiente interno é primordial para realizar o diagnóstico da organização, pois influencia o modo com que os objetivos são estabelecidos, os negócios são estruturados, e os riscos identificados, avaliados e geridos de maneira a influenciar o desempenho e o funcionamento das atividades dos processos e dos sistemas de informação e comunicação utilizados [74].

Na organização, o ambiente interno compreende os valores éticos da instituição, a competência e desenvolvimento pessoal dos militares e civis, a estrutura organizacional e as responsabilidades, bem como a história e cultura da organização [74].

As principais ameaças que podem ser identificadas relacionadas ao contexto interno são:

- Seções de TI descentralizadas e que não se comunicam em seus processos de desenvolvimento e manutenção;

- Falta de entendimento sobre a governança de TI na organização;
- Falta de integração entre os sistemas existentes no DGP;
- Duplicação de informações nos diferentes sistemas da unidade, gerando retrabalhos;
- Não conhecimento dos processos de negócio que impactam a organização no andamento e na continuidade do negócio.

Para que a TI possa suportar e apoiar a organização, faz-se necessário o conhecimento do negócio para o desenvolvimento de soluções que estejam alinhadas com os objetivos estratégicos da organização.

4.2.1 Governança e Gestão de TI no DGP

No DGP verifica-se a presença de Comitês Técnicos relacionados às áreas de (Gestão Estratégica; Tecnologia da Informação; Gestão de Riscos; e Planejamento e Acompanhamento da Execução Orçamentária), sendo partes integrantes da Governança Corporativa da unidade.

É uma das responsabilidades do Comitê de Gestão Estratégica, a proposição do desenvolvimento de projetos do DGP/OM, particularmente os relacionados à infraestrutura física ou de TI.

O Comitê Técnico de Tecnologia da Informação (CTTI) é responsável por:

- Elaborar, manter e revisar o Plano Diretor de Tecnologia da Informação (PDTI);
- Elaborar propostas de objetivos, indicadores, metas e prioridades na área de sistemas e infra-estrutura de TI no âmbito do DGP.
- Analisar e propor a aprovação de portfólio, programas e projetos de TI, na área de pessoal; e
- Acompanhar e avaliar os resultados alcançados pelas ações planejadas.

O PDTI é o instrumento de Governança utilizado pelo DGP, no qual é desenvolvido pelo CTTI com membros das áreas de TI das diretorias do DGP e da DTI/APG e foi elaborado com base nas ações que o DGP deve tomar para atingir aos objetivos estratégicos de pessoal relacionado com a eficiência do uso da TI. A figura 4.5 mostra o relacionamento da missão do DGP com os objetivos estratégicos de pessoal relacionados com a Governança e Gestão de TI.

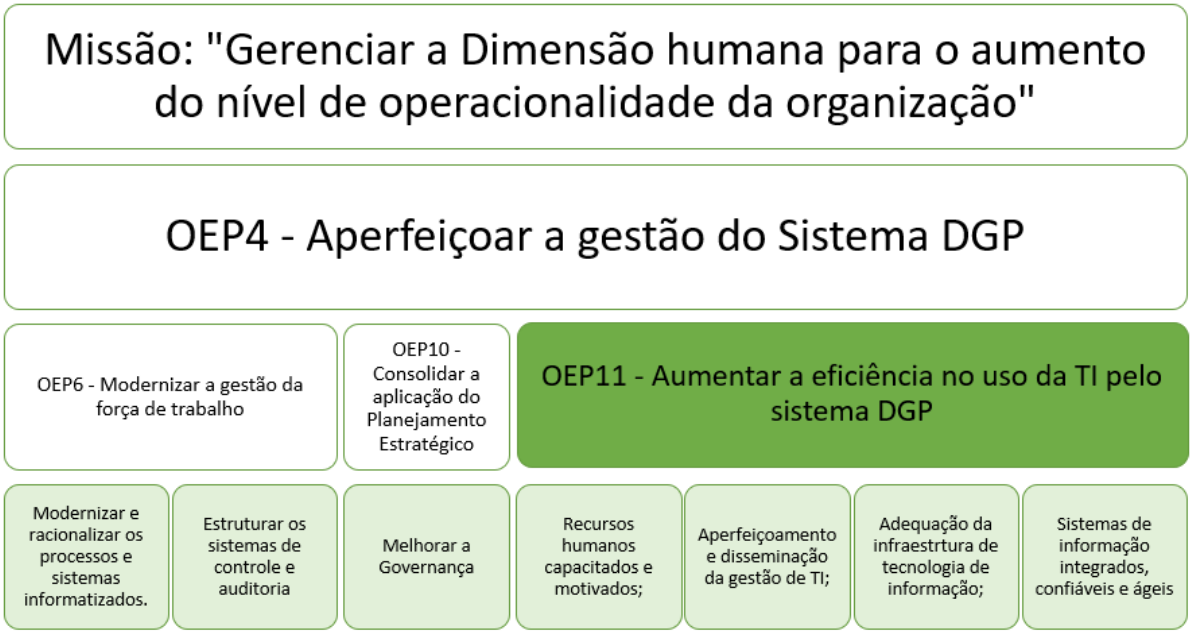


Figura 4.5: Objetivos Estratégicos de Pessoal x Fatores Críticos de Sucesso
Fonte: Adaptado de [69, 13].

Os fatores críticos de sucesso para a implantação das ações no DGP são:

- Modernizar e racionalizar os sistemas informatizados.
- Estruturas os sistemas de controle e auditoria.
- Recursos humanos capacitados e motivados.
- Aperfeiçoamento e gestão de TI.
- Adequação da infraestrutura de TI.
- Sistemas de informação integrados, confiáveis e ágeis.

Esses fatores devem ser levados em consideração para a melhoria dos seus processos de governança e gestão da organização.

Segundo Haes & Grembergen (2008) [75], a estrutura de governança envolvem o posicionamento da área de TI na estrutura hierárquica da organização, bem como a clara definição de papéis e responsabilidades dos cargos que compõem essa estrutura. O modelo da tabela 4.1 representa a estrutura de governança e a classificação dos atores envolvidos com o desenvolvimento de sistemas de informação no DGP.

Tabela 4.1: Estrutura de Governança e Gestão de TI - Áreas envolvidas no Ciclo de Desenvolvimento de Sistemas de Informação do DGP.

RESPONSÁVEL		**ATRIBUIÇÕES**
Patrocinador (Governança de TI) (Nível Organização)	CONTIEx	O CONTIEx tem a função de direcionar, monitorar e avaliar o resultado das execuções do desenvolvimento dos sistemas de informação à nível estratégico.
Patrocinador (Governança de TI) (Nível DGP)	CTTI / DGP	O CTTI do DGP tem a função de direcionar, monitorar e avaliar o resultado das execuções do desenvolvimento dos sistemas de informação à nível setorial. Responsável por consolidar e elaborar o PDTI do DGP.
Gestor Técnico	DCT	O DCT é responsável por prover a infraestrutura dos serviços de Tecnologia da Informação no EB por meio do CITEx e do CTA, e no desenvolvimento e manutenção dos sistemas corporativos da organização por meio do CDS.
Gestor Técnico Negocial	DTI/DGP	A DTI do DGP deverá coordenar a execução das iniciativas de desenvolvimento de sistemas de informação do DGP de maneira a integrar todas às áreas de TI das diretorias finalísticas. Também é responsável por consolidar e elaborar o PDTI do DGP.
Gestor Negocial	TI das diretorias finalísticas	Manter os dados e sistemas de informação específicos de cada diretoria.
Gestor Negocial	Diretorias finalísticas	Demandar para a área de TI, o desenvolvimento de novas funcionalidades ou sistemas de TI para atender ao negócio.
Patrocinador (Governança de TI) Área de Saúde da organização	APESS	Assessorar as soluções de TI propostas para a área de saúde da organização.

Após analisar o panorama da governança de TI no DGP, propõem-se ações necessárias ao aperfeiçoamento e ao exercício de uma eficiente governança e gestão de TI no DGP que necessitam de um planejamento criterioso para que o objetivo estratégico de pessoal seja cumprido, o que pode ser garantido pela aderência às boas práticas de governança e gestão de TI na organização.

4.2.2 Processos de TI do DGP

Na construção da cadeia de valor do DGP pelo Projeto MAP/UnB, foram levantados quais eram os processos de TI existentes no departamento. Este macroprocesso é composto de 4 macroprocessos de nível 2, 8 macroprocessos de nível 3 e 20 processos (nível 4) como mostra na figura 4.6.

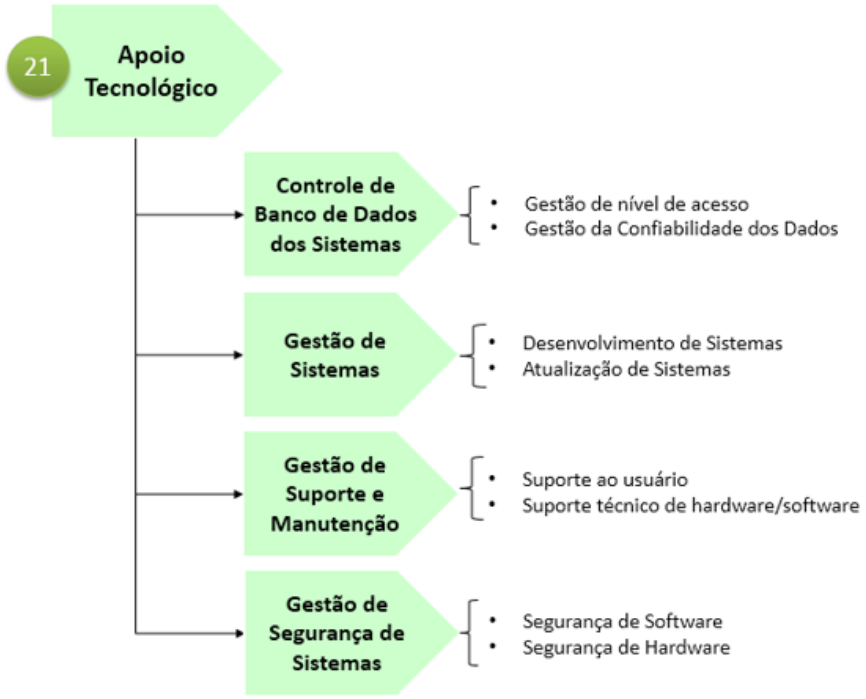


Figura 4.6: Processos identificados na TI do DGP.
Fonte: Projeto MAP/UnB - 2018/2019.

Os processos identificados, estão presentes nas diversas diretorias e assessorias do DGP. Sendo o foco da pesquisa, os processos relacionados com o ciclo de vida do desenvolvimento de software na organização, desde a sua concepção, passando pelo desenvolvimento, pelas manutenções, evoluções e o seu desfazimento quando obsoleto. A figura 4.7 apresenta os processos modelados tanto na DTI como nas áreas de TI de cada diretoria.

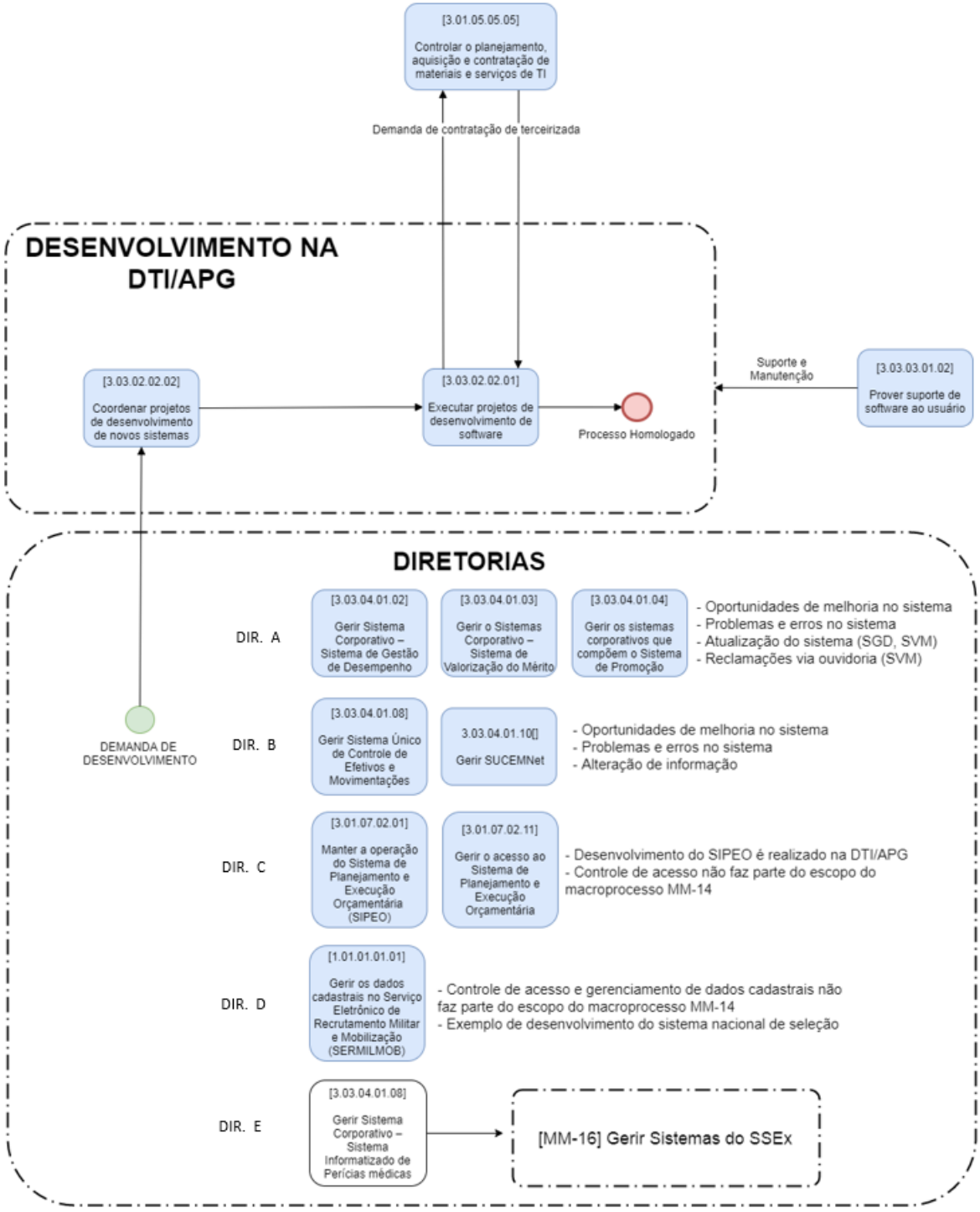


Figura 4.7: Relacionamento entre os processos de desenvolvimento de software modelados na DTI e nas diretorias

Fonte: Projeto MAP/UnB - 2018/2019.

O escopo do processo tem como objetivo gerenciar o ciclo de vida dos sistemas de informação desde a oficialização da demanda, passando pelos estágios do processo de

desenvolvimento de software, às manutenções evolutiva e corretiva.

4.2.3 Estrutura organizacional de TI do DGP

Com relação à estrutura de TI do DGP, verifica-se que cada Diretoria possui uma área de TI responsável por manutenir os sistemas específicos e dar suporte técnico aos usuários da área de negócio.

No Apêndice A são mostradas as unidades de TI existentes em cada Diretoria. A identificação da estrutura organizacional de TI foi realizada por meio de análise dos regimentos internos disponíveis em cada uma das diretorias e assessorias do DGP.

A principal unidade de TI do DGP é uma divisão que faz parte da Assessoria de Planejamento e Gestão (APG). É responsável por assessorar o Chefe e o Vice Chefe do DGP nas áreas de planejamento, orientação, coordenação, controle, supervisão, execução e avaliação de atividades relacionadas a assuntos que envolvem mais de uma diretoria [73].

Possui como atribuições, o desenvolvimento e promoção de estudos prospectivos, análises e pesquisas, alteração de legislação, coordenação de processos e projetos, bem como na fiscalização e gerenciamento da elaboração, do desenvolvimento e da manutenção de sistemas informatizados no DGP e nas suas diretorias, da segurança da tecnologia da informação e da administração de dados [73].

A **Divisão de Tecnologia da Informação (DTI)** é a maior divisão de TI do DGP, com militares distribuídos em 5 seções: seção de informação organizacional e segurança de tecnologia da informação, seção de redes, seção de sistemas, seção de administração de dados e seção de administração de material de informação. Além da DTI, em cada diretoria foram identificadas outras seções de TI que atendem as necessidades de cada área.

Cada diretoria e assessoria possui área de TI própria que desenvolvem softwares, na maioria das vezes de forma descentralizada para o atendimento das demandas específicas de cada unidade. Diante disso, verifica-se uma grande quantidade de sistemas de TI que ainda não possuem suas devidas integrações com os sistemas corporativos da organização e aos demais sistemas de gestão de pessoas.

4.2.3.1 Análise do Perfil do Profissional de TI do DGP

Dos aproximadamente 106 militares envolvidos na TI do DGP, 35 pessoas responderam o questionário de Perfil do Profissional. O apêndice B apresenta o questionário aplicado aos profissionais de TI do DGP.

Da amostra analisada podemos perceber que 31,43% dos militares entrevistados são da área de desenvolvimento de software, o que colabora para a proposta da pesquisa em

identificar como é desenvolvido os sistemas de informação do DGP. A figura 4.8 apresenta o percentual de militares por área no DGP.

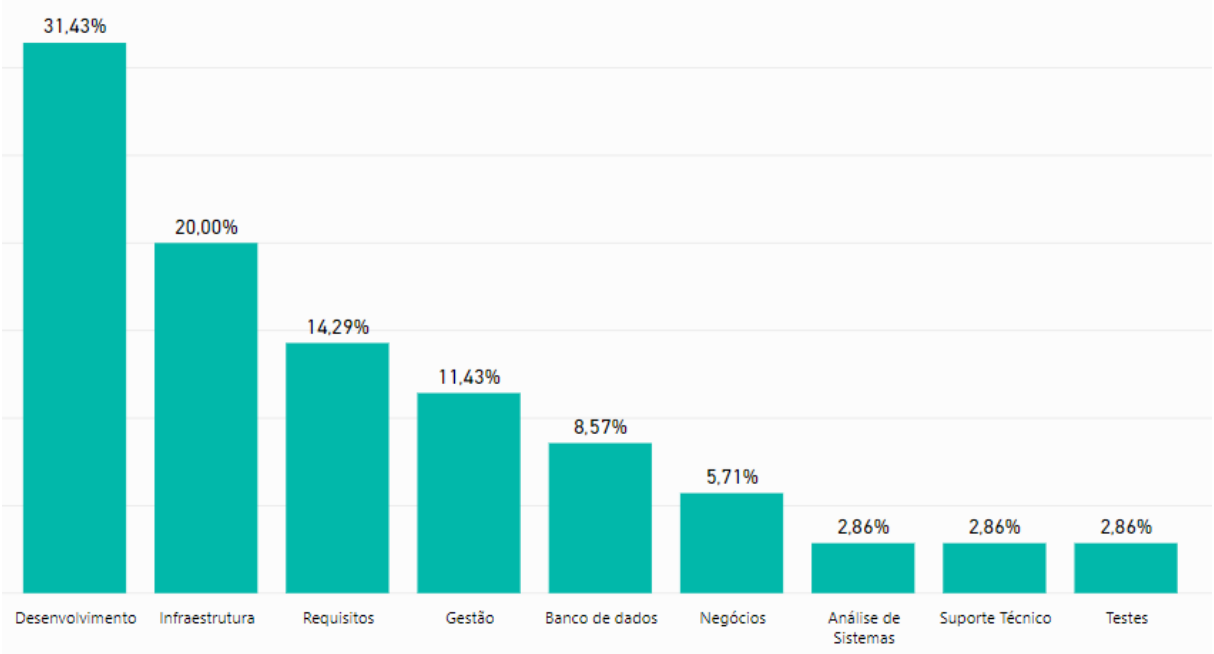


Figura 4.8: Principais áreas de TI dos entrevistados
Fonte: Elaboração própria.

Dos 35 profissionais de TI que preencheram o questionário, 44,8% são da D Sau, 37,9% da DA Prom e 10,3% da DSM e 6,9% da DCEM.

Em relação ao tempo de serviço, podemos verificar que a grande maioria estão entre 1 a 3 anos ou menos de 1 ano no DGP, o que explica a grande rotatividade dos militares que desenvolvem os sistemas de informação da organização. A maior parte do quadro temporário de militares nas patentes de tenente e sargento.

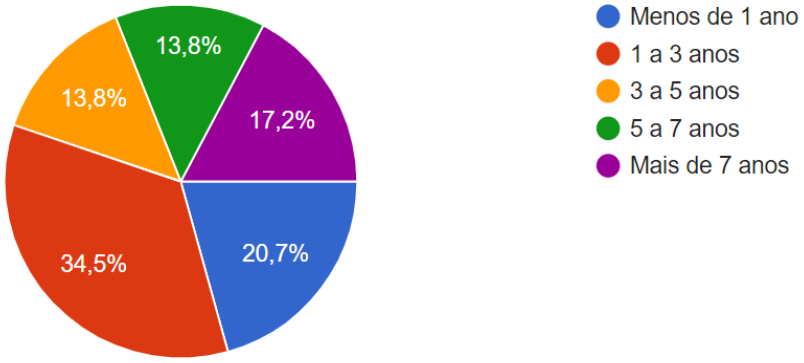


Figura 4.9: Tempo de Serviço no DGP
Fonte: Elaboração própria.

Nota-se, que dos profissionais de TI do DGP, 58,62% apenas trabalharam na seção atual, conforme mostra na Figura 4.10.

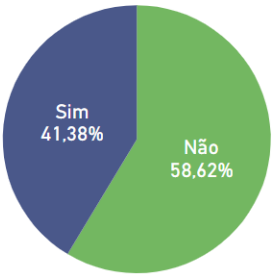


Figura 4.10: PE02 - Você já trabalhou em outras unidades de TI da organização?
Fonte: Elaboração própria.

Verifica-se que a maioria dos profissionais de TI que responderam ao questionário, são militares que estão no início da vida militar, sendo a maioria oficiais temporários.

Além disso, a pesquisa analisou o conhecimento do militares quanto a gestão de riscos, onde apenas 4 militares apresentaram conhecimento em algum modelo e em relação a governança de TI, verifica-se a grande utilização do ITIL e COBIT pelos militares tanto com conhecimento a nível básico, intermediário, avançado ou certificação.

Dos profissionais de TI que responderam ao questionário, verifica-se que a maioria possui graduação nas áreas de TI, sendo 34,48% fizeram o curso de Sistemas de Informação conforme mostra na Figura 4.11.

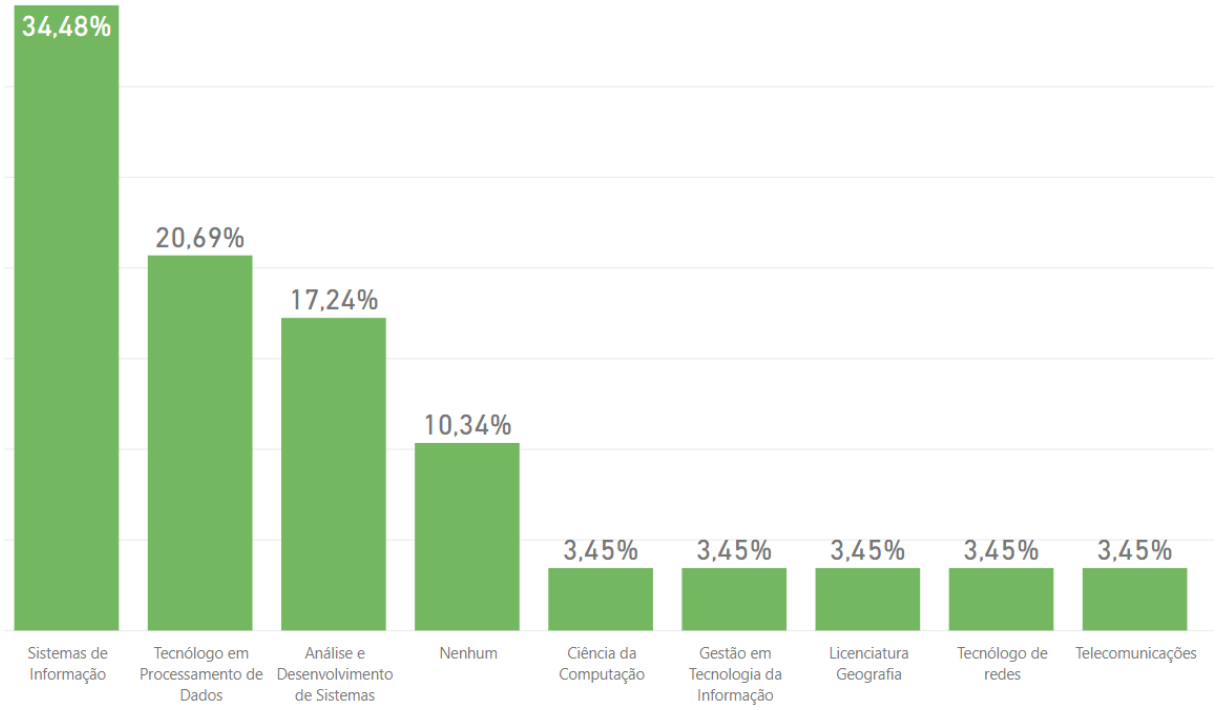


Figura 4.11: Nível de formação superior dos militares do DGP.
Fonte: Elaboração própria.

Nota-se que 10,34% dos profissionais de TI do DGP não possuem graduação. Quanto aos cursos de pós-graduação lato senso (especialização, MBA), verifica-se que 51,7% dos militares possuem algum curso e apenas 10,3% cursaram mestrado ou doutorado, sendo esses na área de Ciências Militares.

Após analisar o contexto interno e externo da organização e o contexto da TI, é importante verificar de que forma o processo de desenvolvimento de software é realizado no DGP.

Capítulo 5

Análise do Processo de Desenvolvimento de Software da TI do DGP

5.1 Ciclo de Vida de Software no DGP

O Ciclo de Vida de Software da organização, de acordo com as as Instruções Gerais (IG), compreende os processos de aquisição, fornecimento, desenvolvimento, produção e manutenção [76]. O diagrama da Figura 5.1 demonstra a dinâmica do ciclo de vida de software na organização.

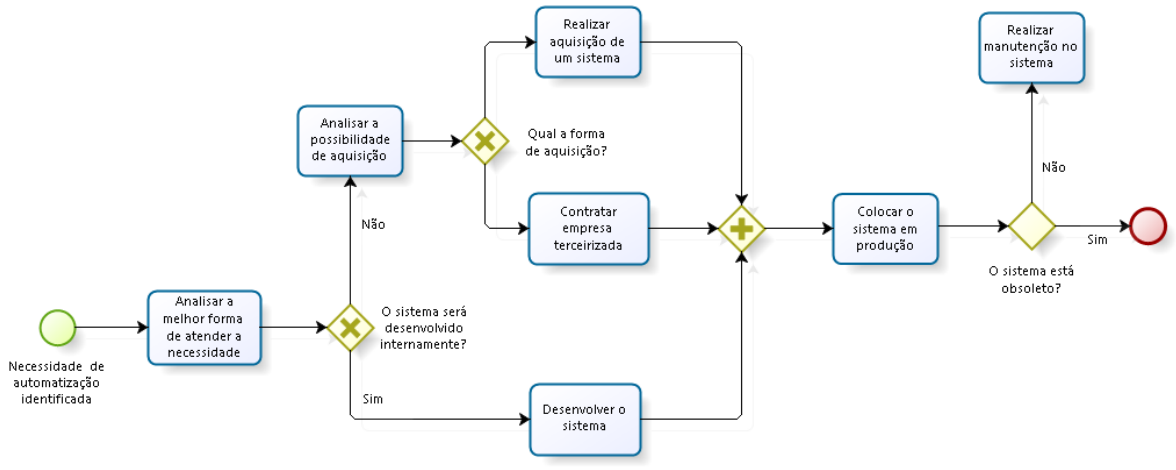


Figura 5.1: Dinâmica do Ciclo de vida de Software na organização.
Fonte: Adaptado de [77].

O ciclo de vida consiste na história completa do produto através de suas fases de concepção, definição, operação e obsolescência e seu modelo contém os processos, atividades e tarefas envolvidos no desenvolvimento, produção, operação e manutenção de um produto de software, abrangendo a vida do sistema desde a definição de seus requisitos até a sua desativação ou descarte [77, 76].

O processo empregado no ciclo de vida de software de acordo com o normativo deve envolver a capacitação científico-tecnológica dos recursos humanos envolvidos, bem como da conscientização do público interno.

Na Divisão de Tecnologia da Informação (DTI) da APG do DGP, o processo COBIT 5 BAI03 é coberto, em grande medida, pelo macroprocesso "Gerir Desenvolvimento de Sistemas de Informação" que por sua vez, é composto pelos processos "Coordenar desenvolvimento de novos softwares", "Executar projetos de desenvolvimento de software", "Contratar soluções de tecnologia da informação" conforme mostrado na figura 5.2.

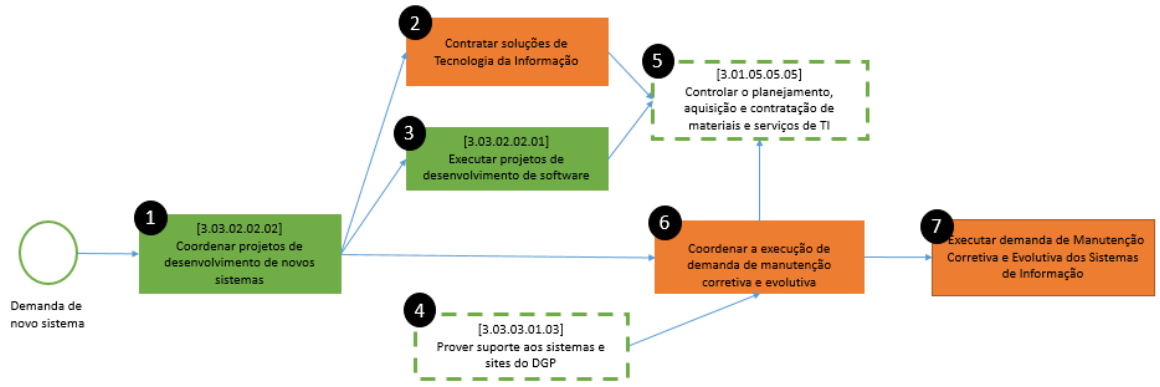


Figura 5.2: Macroprocesso: "Gerir Desenvolvimento de Sistemas de Informação".
Fonte: Elaboração própria.

O macroprocesso é baseado no ciclo de vida de software da organização e aborda não apenas as atividades do desenvolvimento de software, mas também as demais referente ao gerenciamento e suporte, sendo importante gerir não só os ativos reutilizáveis (produtos) produzidos durante o ciclo de desenvolvimento, mas também os ativos (ferramentas e plataformas) necessárias para produzi-los.

Verifica-se que na TI do DGP possui 3 etapas relacionadas ao ciclo de desenvolvimento de software: a) Oficialização da demanda, b) o Ciclo de Vida do desenvolvimento de software e c) a Sustentação.

5.1.1 Oficialização da Demanda

As demandas de novos softwares são realizadas por meio de um documento, aberto no sistema SPED, pelo qual os demandantes informam a DTI as demandas relacionadas a Tecnologia da Informação. A Tabela 5.1 apresenta o SIPOC do processo relacionado com a oficialização da demanda de um novo software.

Tabela 5.1: SIPOC de Oficialização de Demanda: Processo "Coordenar projetos de desenvolvimento de novos softwares".

Fornecedores	**Entrada**	**Escopo**	**Saída**	**Cliente**
Assessorias e Diretorias do DGP	DIEx de Pedido de Demanda	Coordenar os projetos de desenvolvimento de novos sistemas das diretorias demandantes do DGP.	DIEx de Pedido de Demanda	Contratar soluções de Tecnologia da Informação; Coordenar a execução de demanda de manutenção corretiva e evolutiva; Executar projetos de desenvolvimento de software.

O processo “Coordenar projetos de desenvolvimento de novos softwares” é executado na DTI/APG do DGP, e tem como insumo uma demanda que pode ser tanto de novo desenvolvimento ou de manutenção e como saída o encaminhamento dessa demanda para o desenvolvimento, neste processo será verificado se a demanda é consistente, se é viável e se não há outro software que já atenda a demanda.

As demandas encaminhadas à DTI/DGP são classificadas em duas categorias conforme mostra na tabela 5.2.

Tabela 5.2: Critérios para Classificação de Demandas

Categoria	**Descrição**
Novo Desenvolvimento	Novo projeto de software requisitado via DIEx de Pedido de Demanda.
Manutenção	Manutenção em sistemas informatizados disponíveis em ambiente de produção

Após a classificação, a demanda será remetida para o desenvolvimento de um novo software ou para a manutenção do software em produção.

5.1.2 Processo de Desenvolvimento de Software no DGP

O processo de desenvolvimento de software no DGP é executado pelas diretorias e pela Divisão de Tecnologia da Informação presente APG/DGP. Cada área possui uma forma de desenvolver software na organização, uma vez que possuem autonomia para a execução do seu processo de desenvolvimento.

O processo "Executar processo de desenvolvimento de software", modelado na DTI, tem como objetivo realizar o desenvolvimento de novos softwares quando é elaborado pela própria DTI ou acompanhar o desenvolvimento quando é feita a contratação de uma empresa terceirizada. A figura 5.3 apresenta as fases do processo de desenvolvimento de software modelado no DGP.

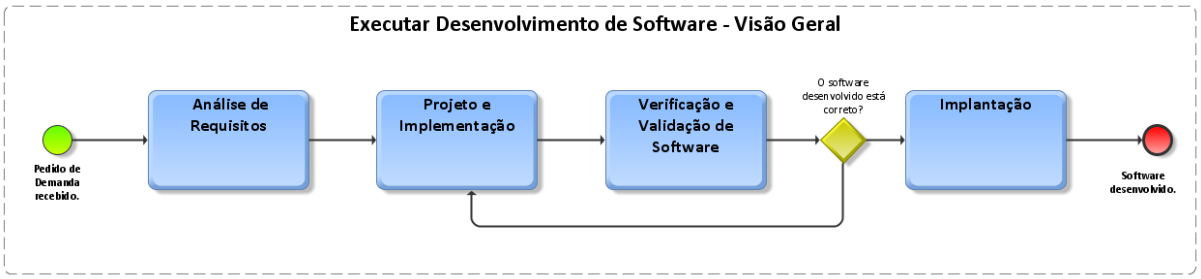


Figura 5.3: Processo: "Executar Desenvolvimento de Software - Visão Geral".
Fonte: Elaboração própria.

O processo tem como entrada a demanda de um novo software a ser desenvolvido e como saída, o software em produção e disponibilizado para a área demandante. Este novo software entrará no portfólio de sistemas e serviços do DGP e será uma entrada para o macro "Monitorar Banco de Dados de Sistemas". Na Tabela 5.3 apresenta o SIPOC do processo relacionado com a oficialização da demanda de um novo software.

Tabela 5.3: SIPOC - Executar processo de desenvolvimento de software no DGP.

Fornecedores	Entrada	Escopo	Saída	Cliente
Coordenar projetos de TI; Seção de redes; Empresa contratada	DIEx Solicitação de Novo Sistema; Ambiente (de desenvolvimento e de produção); Código do sistema	A partir da solicitação de um novo sistema, desenvolver o sistema internamente ou em parceira com alguma empresa contratada, contemplando as atividades de documento de visão, arquitetura do sistema, levantamento de requisitos, desenvolvimento e teste do código até o sistema ser colocado em produção e entregue ao demandante	DIEx Resposta; Ordem de Serviço; Solicitação Correção; Solicitação Ambiente; Solicitação Adaptação; Solicitação Colocar em Produção	Coordenar projetos de TI; Seção de redes; Empresa contratada; Controlar o planejamento, aquisição e contratação de materiais e serviços de TI

Os subprocessos presentes no processo de executar desenvolvimento de software serão detalhados em cada subseção.

5.1.2.1 Análise de Requisitos

A Subseção de Análise de Requisitos, da DTI, receberá por meio de um DIEx, a solicitação para o desenvolvimento de um novo software e irá marcar uma reunião inicial com o cliente para o entendimento das necessidades. Com isso, elabora-se o Documento de Visão com o que foi levantado na reunião inicial.

Tabela 5.4: SIPOC - Análise e Especificação de Requisitos

Fornecedor	Entrada	Subprocesso	Saída	Cliente
- Demandantes; - Chefe da DTI;	- DIEx Solicitação de Novo Software	Análise de Requisitos	- Atas; - Documento Visão; - Especificação e Diagramas de Casos de Uso; - Abertura de OS.	- Subseção de Desenvolv. de Sistemas; - Empresa Terceirizada.

O analista de requisitos irá estudar a arquitetura que será utilizada no desenvolvimento, com base no Documento de Visão, nas Atas e no DIEx de solicitação de novo software.

Os casos de usos são listados de acordo com os estudos e reuniões realizadas até o momento. Novas reuniões com o cliente são necessárias para levantar os requisitos do sistema, onde os casos de uso listados são apresentados e especificados, podendo surgir novos.

Ao fim das reuniões de levantamento de requisitos, são especificados os casos de uso, que serão entregues fisicamente para validação pelo cliente. Caso não esteja em conformidade, deverá ser corrigido e remetido novamente para validação. Algumas vezes, são necessárias, novas reuniões para o entendimento das funcionalidades. Caso o cliente concorde, deverá assinar a aprovação da especificação dos casos de uso.

O desenvolvimento poderá ser realizado, tanto pela equipe interna da Subseção de Desenvolvimento de Sistemas, como por empresa terceirizada. Nos ambos casos, será aberto uma Ordem de Serviço para desenvolvimento.

5.1.2.2 Projeto e Implementação de Software

O projeto e implementação de software no DGP pode ser realizado tanto via desenvolvimento interno, como externo. Nos softwares desenvolvidos pelas empresas terceirizadas, o projeto e implementação é de responsabilidade do contratado, que entregará o código desenvolvido ao final para validação.

Quando o desenvolvimento é realizado internamente, a OS será aberta para Subseção de Desenvolvimento, e passará primeiramente no Chefe da Subseção, que definirá quem será o chefe da equipe do projeto, este por sua vez, terá a responsabilidade de acompanhar o desenvolvimento do projeto, definir desenvolvedores, solicitar os ambientes necessários (homologação e produção) e colocar o software/sistema em produção quando finalizado. A tabela 5.5 apresenta o SIPOC do subprocesso.

Tabela 5.5: SIPOC - Projeto e Implementação de Software

Fornecedor	**Entrada**	**Subprocesso**	**Saída**	**Cliente**
Analista de Requisitos	- Ordem de Serviço - Casos de Uso - Redmine	Projeto e Implementação de Software	Código finalizado.	Analista de Requisitos / Testes

O desenvolvedor será responsável por codificar o novo software/sistema com base nos casos de uso aprovados.

5.1.2.3 Verificação e Validação de Software

Após a finalização, o desenvolvedor, envia o código para a validação pelo analista de requisitos, que irá verificar se a implementação do código está conforme aos requisitos especificados, realizando o teste do tipo caixa preta, ou seja, o teste funcional. Se o

que foi desenvolvido não estiver correto, deverá retornar ao desenvolvedor para correções. Sendo que esse teste só é realizado para o principal sistema de gestão de pessoas da organização. Para os demais sistemas, não são realizados testes.

Caso esteja conforme, será validado as funcionalidades desenvolvidas com o cliente por meio de reuniões que irá verificar se o que foi desenvolvido atendeu ao que foi demandado. Se não for válido, o analista irá gerar um relatório de erros e informar ao desenvolvedor as necessidades de melhoria no código por meio de uma nova tarefa no Redmine.

5.1.2.4 Implantação de Software

Quando o desenvolvimento for finalizado, o chefe da equipe de desenvolvimento do projeto irá analisar se o ambiente de produção está em conformidade com o ambiente de homologação e caso esteja tudo correto, irá subir o software/sistema para produção, ou seja, será disponibilizado para o uso do cliente e usuários.

A informação pela finalização do desenvolvimento é de responsabilidade do analista de requisitos que irá elaborar um DIEx Resposta informando que todas as funcionalidades e casos de uso foram codificados e validados.

5.1.3 Sustentação

Após a implantação do software na organização, são necessárias atividades de sustentação, ou seja, o suporte e as manutenções corretivas, preditivas e evolutivas.

O SISP define que a sustentação e a evolução, consiste na manutenção da saúde do sistema ou serviço (incluindo, mas não limitado à processos de backup de dados, segurança de acesso e outros), o suporte continuado aos usuários e o atendimento de novos requisitos que surgem do próprio uso e mudanças de processos no negócio [21]. As demandas de manutenção de software no DGP são classificadas em 3 tipos conforme mostra a tabela 5.6.

Foram modelados os processos referente ao suporte e manutenção dos principais sistemas de gestão de pessoas do DGP a fim de entender o seu funcionamento. Esses processos servirão de análise de melhoria tanto nos processos finalísticos das áreas negociais como também da área de TI do Órgão.

Tabela 5.6: Categorias de Manutenção de Software

Categoria	Descrição
Corretiva	É aberto uma solicitação via Pedido de Suporte para a correção de defeitos de um produto de software, realizada depois de entregue, para corrigir falhas ocorridas.
Perfectiva (Melhoria)	É aberto uma solicitação via Pedido de Suporte correspondente às adequações do software à necessidades de melhorias, sem alteração de funcionalidades, sob o ponto de vista do usuário.
Nova Funcionalidade (Evolutiva)	É aberto uma solicitação via Pedido de Suporte para a extensão do software além de seus requisitos funcionais originais para atender a alterações de regras de negócio ou necessidades que irão prover mais benefícios, ou seja, para a modificação do produto de software em produção. Com isso, é elaborado um novo de caso de uso para a funcionalidade.

Após a análise do processo de desenvolvimento de software do DGP, foram identificados os problemas inerentes ao processo analisado.

5.2 Identificação de Problemas no Processo de Desenvolvimento de Software

Na modelagem desses processos, verificou-se a existência de alguns problemas que foram relatados pelos gestores e executores do processo. Os problemas foram identificados nos processos de negócio modelados. Esses problemas referem-se a situações que podem gerar eventos de riscos.

- **Processo de Desenvolvimento**

Tabela 5.7: Problema 1 - Ausência de um processo de desenvolvimento de software

Nome	Justificativas
O problema de:	Ausência de um processo definido para o desenvolvimento de software.
Afeta (Envolvidos):	DTI, diretorias do DGP.
Cujo impacto é:	Possível retrabalho.
Benefícios de uma solução seriam:	Melhoria no processo de desenvolvimento, evitando retrabalhos.

- **Gestão da Configuração**

Tabela 5.8: Problema 2 - Ausência de padronização de ferramentas de desenvolvimento de software

Nome	**Justificativas**
O problema de:	Ausência de padronização das ferramentas para o desenvolvimento de um novo software.
Afeta (Envolvidos):	Subseção de Análise e Subseção de desenvolvimento.
Cujo impacto é:	Afeta o controle e qualidade do desenvolvimento do software.
Benefícios de uma solução seriam:	Padronizar as ferramentas utilizadas para o desenvolvimento de um novo software.

- **Documentação - Gestão do Conhecimento**

Tabela 5.9: Problema 3 - Ausência de padronização na documentação para o desenvolvimento de um novo software

Nome	**Justificativas**
O problema de:	Ausência de padronização da documentação para o desenvolvimento de um novo software.
Afeta (Envolvidos):	Subseção de Análise e Subseção de desenvolvimento.
Cujo impacto é:	Afeta a rastreabilidade dos documentos e o controle de versões.
Benefícios de uma solução seriam:	Padronizar as documentações para o desenvolvimento de software.

- **Gestão da Demanda**

Tabela 5.10: Problema 4 - Ausência de padronização na solicitação de demandas de novos softwares/sistemas.

Nome	**Justificativas**
O problema de:	Não existe um processo bem definido para a solicitação de demandas de novos softwares/sistemas.
Afeta (Envolvidos):	DTI e Diretorias do DGP.
Cujo impacto é:	Os pedidos de demandas que chegam até a DTI não chegam padronizados, dificultando assim, a análise prévia por parte da DTI da coerência do pedido e o levantamento de funcionalidades pela Subseção de Análise.
Benefícios de uma solução seriam:	Padronizar o processo de levantamento de necessidades e funcionalidades dos sistemas do DGP, em que é realizado nas diretorias do DGP.

- **Verificação, Validação e Teste**

Tabela 5.11: Problema 5 - Ausência de realização de testes nos softwares durante o desenvolvimento.

Nome	**Justificativas**
O problema de:	Ausência de realização de testes nos softwares desenvolvidos.
Afeta (Envolvidos):	Usuários, desenvolvedores, suporte.
Cujo impacto é:	Diminuição da qualidade do software, aumentando as manutenções corretivas e a insatisfação dos usuários.
Benefícios de uma solução seriam:	Aplicar o processo de verificação, validação e testes nos softwares que são desenvolvidos na organização.

- **Gestão de Portfólio**

Tabela 5.12: Problema 6 - Desconhecimento dos software/sistemas elaborados pelas diretorias

Nome	**Justificativas**
O problema de:	Desconhecimento dos softwares/sistemas elaborados pelas diretorias por parte da DTI.
Afeta (Envolvidos):	DTI, diretorias do DGP.
Cujo impacto é:	Como a DTI não tem conhecimento de todas as funcionalidades empregadas nos sistemas desenvolvidos pelas diretorias do DGP, podem existir sistemas com funcionalidades redundantes e informações repetidas em diferentes bases de dados. Além disso, caso ocorra algum problema com esses sistemas, a DTI é acionada para resolvê-lo, mesmo ela não tendo conhecimento de como o sistema opera.
Benefícios de uma solução seriam:	Manter o portfólio dos softwares e sistemas desenvolvidos no DGP e possuir uma área integradora dos projetos de TI do DGP.

Com base no diagnóstico levantado, a próxima seção irá tratar do processo de gestão de riscos aplicado no estudo de caso com a utilização de técnicas previstas na ISO 31010 e no Cobit 5 para Risco.

Capítulo 6

Aplicação do Processo de Gestão de Riscos do PDS da TI/DGP

De acordo com a ISO 31000 [26], o processo de gestão de riscos envolve a aplicação sistemática de políticas, procedimentos e práticas para as atividades de comunicação e consulta, estabelecimento do contexto e avaliação, tratamento, análise crítica, registro e relato de riscos.

Na organização, verifica-se que a estrutura do modelo de gestão de riscos é baseado no modelo do COSO ERM [78] e possui oito componentes inter-relacionados e integrados com o processo de gestão das Organizações Militares: análise do ambiente interno, fixação de objetivos, identificação de eventos, avaliação de riscos, resposta a riscos, atividades de controles internos, informação e comunicação [74].

Segundo o Manual de Gestão de Riscos da organização (2017), a implementação da gestão de riscos na organização deve ocorrer de maneira gradual e devem ser realizadas nos programas, projetos e processos que impactam no alcance dos objetivos estratégicos e devem estar integradas aos macroprocessos existentes[74].

O modelo de gestão de riscos utilizado na pesquisa será o proposto no Cobit 5 for Risk (COBIT 5 para Risco) [31] por se tratar de um modelo utilizado para a gestão e governança de tecnologia da informação e que aborda todos os componentes definidos pela ISO 31000, ISO 27005 e pelo COSO ERM de maneira a estender a sua cobertura para as especificidades do uso da TI na organização.

Além disso, o processo definido no ISO 31000 está totalmente coberto pelos diferentes processos e práticas do modelo do COBIT 5 para Risco por meio dos princípios e dos modelos de habilitadores.

6.1 Identificação dos Riscos do Processo de Desenvolvimento de Software do DGP

De acordo com a ISO 31000 [26], a identificação de riscos tem como propósito encontrar, reconhecer, e descrever os riscos que possam ajudar ou impedir que uma organização alcancem os objetivos.

Para apontar os eventos de risco e cenários de risco é necessário conhecer os objetivos que a organização deseja atingir e com isso, identificar, analisar e avaliar os riscos quanto a sua realização e administração. A identificação dos riscos para o processo de desenvolvimento de software contemplou 5 etapas, que são explicitadas a seguir.

6.1.1 Etapa 1. Avaliação da relevância dos objetivos do Negócio, a partir da visão dos especialistas de TI.

Seguindo a abordagem *top-down*, do ponto de vista estratégico, o primeiro passo foi identificar os objetivos de negócio e os cenários com maior impacto no atingimento desses objetivos. Os objetivos foram identificados por meio da análise do Planejamento Estratégico e do Plano Diretor de Tecnologia da Informação da Organização.

O Departamento-Geral de Pessoal tem como um dos objetivos estratégicos de pessoal: "Aumentar a eficiência do uso da TI pelo Sistema DGP" no qual deverá "Modernizar e ampliar a utilização de estruturas de TI para apoio aos processos de todo o sistema DGP [79].

A estratégia definida pelo departamento foi a de otimização dos sistemas informatizados (Dtz Ch DGP 2011-2018) e elencaram 3 ações a serem realizadas [79]:

1. Fiscalizar a implantação e a gerência de todos os sistemas informatizados do DGP, otimizando a utilização dos mesmos e reduzindo as vulnerabilidades oriundas de acessos indevidos.

2. Coordenar as atividades de Tecnologia da Informação (TI) do Departamento e das Diretorias, priorizando o aperfeiçoamento e a manutenção do banco de dados corporativo do Sistema de Pessoal da organização, controlando, coordenando e fiscalizando o desenvolvimento de novos sistemas de TI na área de pessoal, visando à unificação de plataformas e linguagens, bem como à otimização dos meios.

3. Modernizar os sistemas existentes, aperfeiçoando e integrando os sistemas de Tecnologia da Informação (TI) envolvidos nos processos pertencente à Diretoria, consonante as Diretrizes da APG [79].

Com isso, foi solicitado para que os especialistas de TI avaliassem qual a relevância de cada um dos objetivos de negócio da organização. A figura 6.1 apresenta a relevância de cada objetivo de acordo com a percepção dos especialistas de TI.

OBJETIVOS DO NEGÓCIO			
ID	**DESCRIÇÃO DO OBJETIVO**		**Relevância**
OBJ01	Aumentar a eficiência do uso da TI pelo DGP.	4	Alta (> 65% e <= 95%)
OBJ02	Modernizar e ampliar a utilização de estruturas de TI para apoio aos processos do DGP.	5	Muito Alta (> 95%)
OBJ03	Reduzir os riscos para a administração pública na aquisição ou desenvolvimento de ferramentas de TI.	3	Média (> 35% e < = 65%)
OBJ04	Otimizar os sistemas informatizados do DGP.	5	Muito Alta (> 95%)
OBJ05	Fiscalizar a implantação e a gerência de todos os sistemas informatizados do DGP, otimizando a utilização dos mesmos e reduzindo as vulnerabilidades de acessos indevidos.	4	Alta (> 65% e <= 95%)
OBJ06	Coordenar as atividades de TI do DGP e das Diretorias, priorizando o aperfeiçoamento e a manutenção do banco de dados corporativo de pessoal.	5	Muito Alta (> 95%)
OBJ07	Controlar, coordenar e fiscalizar o desenvolvimento de novos sistemas de TI na área de pessoal, visando à unificação de plataformas e linguagens.	4	Alta (> 65% e <= 95%)
OBJ08	Modernizar os sistemas existentes.	3	Média (> 35% e < = 65%)

Figura 6.1: Relevância dos Objetivos de Negócio
Fonte: Elaboração própria.

Verifica-se que os objetivos OBJ02, OBJ04 e OBJ06 são os mais relevantes para os especialistas entrevistados.

- OBJ02 - Modernizar e ampliar a utilização de estruturas de TI para apoio dos processos de negócio.
- OBJ04 - Otimizar os sistemas informatizados.
- OBJ06 - Controlar, coordenar e fiscalizar as atividades de TI do DGP e das diretorias, priorizando o aperfeiçoamento e a manutenção dos banco de dados de pessoal.

A informatização dos processos de negócio é de suma importância para a organização gerir de forma eficaz as informações geradas e assim integrar os diversos setores. Com isso, a TI torna-se primordial, pois suporta todos os dados dos mais variados setores e

assegura que eles sejam corretamente armazenados, compilados e disponibilizados sempre que necessário.

Para uma boa informatização da organização, os profissionais de TI deverão entender como funciona o processo e os serviços oferecidos pela organização e como os setores estão interligados.

A qualidade do processo de desenvolvimento de software e os próprios sistemas de informação da organização contribuem para análise dos objetivos estratégicos elencados. Além disso, o processo de desenvolvimento de software da organização deve ser definido para que os profissionais de TI consigam informatizar e integrar os processos de negócio.

6.1.2 Etapa 2. Escolha do processo que impacta o objetivo do negócio.

Com base nesses objetivos, o processo de desenvolvimento de software do departamento foi selecionado para a identificação e análise dos riscos que impactam em atingir os objetivos estratégicos propostos pela organização.

O processo de desenvolvimento de software possui os seguintes objetivos específicos:

- Analisar as demandas recebidas para o desenvolvimento de novos software ou de funcionalidades para os sistemas existentes;
- Verificar a possibilidade de contratação de serviços de empresas terceirizadas para o desenvolvimento do um novo software ou funcionalidade;
- Executar o desenvolvimento do novo software ou funcionalidade por conta dos profissionais militares da organização;
- Realizar a manutenção preventiva, preditiva e corretiva nos sistemas de informação da organização;
- Prestar suporte aos usuários dos sistemas de informação da organização;

Com base nesses objetivos específicos, foi necessário avaliar a relevâncias dos ativos de TI, que nesse caso, são as áreas do processo de desenvolvimento de software.

6.1.3 Etapa 3. Avaliação da relevância dos ativos do Negócio, a partir da visão dos especialistas de TI.

De acordo com Ramirez (2011) [34], os ativos podem ser processo, pessoa, ambiente ou tecnologia. Para a pesquisa, utilizou-se o ativo do tipo “Processo”, sendo o principal

fator para o alcance dos objetivos da organização e consequentemente, a principal fonte de evidências da implementação do modelo ou norma de referência.

As ameaças podem ser do tipo físicos, lógicos ou estratégicos, podendo ser de origem natural, técnica ou humana. A figura 6.2 apresenta a avaliação da relevância de cada ativo (áreas do processo) pelos profissionais de TI do DGP.

Relevância das Áreas de Processo de Software

ID	ÁREA DO PROCESSO	R	RELEVÂNCIA
GP	Gestão de Projetos	5	Muito Alta (> 95%)
GOV	Governança	5	Muito Alta (> 95%)
PDS	Processo de Desenvolvimento de Software	5	Muito Alta (> 95%)
PI	Projeto e Implementação de Software (Desenvolvimento e Codificação)	5	Muito Alta (> 95%)
VV	Verificação, Validação e Teste	5	Muito Alta (> 95%)
REQ	Análise e Especificação de Requisitos	4	Alta (> 65% e <= 95%)
GCS	Gestão da Configuração	4	Alta (> 65% e <= 95%)
GD	Gestão de Demandas	4	Alta (> 65% e <= 95%)
MNT	Manutenção de Software (Preventiva, Corretiva e Evolutiva)	4	Alta (> 65% e <= 95%)
QS	Qualidade de Software	4	Alta (> 65% e <= 95%)
RH	Recursos Humanos	4	Alta (> 65% e <= 95%)
GCS	Gestão do Conhecimento	3	Média (> 35% e < = 65%)
IP	Integração de Produtos de Software	3	Média (> 35% e < = 65%)
SUP	Suporte ao Usuário	3	Média (> 35% e < = 65%)
Total			

Fonte: Dados coletados na entrevista com os profissionais de TI do departamento.

Figura 6.2: Relevância dos Ativos
Elaborado pelo autor.

Os ativos selecionados estão relacionados com as áreas do processo de desenvolvimento de software e representam os principais recursos que participam do processo de desenvolvimento de software na organização e que consequentemente são os pontos de verificação de riscos e conformidade do processo.

Para os entrevistados, o processo de desenvolvimento de software como todo é relevante para a organização, sendo as áreas de maior relevância: requisitos, gestão de projetos, governança, projeto e implementação de software, bem como a área de verificação, validação e testes que possuem uma importância estratégica e a suas ausências afetam todo o negócio da organização e os prejuízos são extremamente altos.

6.1.4 Etapa 4. Identificação das fraquezas e ameaças da organização, por meio da matriz SWOT.

Na quarta etapa, identificou-se por meio de pesquisa documental, quais eram os principais riscos na TI do DGP, e a partir dessa análise, foi verificado quais estão relacionados com o processo de desenvolvimento de software da organização. Com isso, foi identificada as forças, oportunidades, fraquezas da organização, bem como as ameaças a que estão expostas. A figura 6.3 apresenta a Matriz SWOT da TI do DGP.

Figura 6.3: Matriz SWOT da TI do DGP
Adaptado de [13].

Na matriz SWOT da TI do DGP é possível identificar quais são as principais fraquezas e ameaças, bem como na identificação de forças e oportunidades.

6.1.5 Etapa 5. Identificação do cenário de risco para o processo de desenvolvimento de software.

Com base na análise das fraquezas e ameaças da organização, foi possível identificar os cenários de riscos envolvidos no processo de desenvolvimento de software. A análise de cenários de riscos é uma técnica para tornar o risco de TI mais concreto e tangível, possibilitando uma análise e avaliação de riscos aprimorada [31].

Para realizar uma tomada de decisão mais efetiva, o COBIT propõem um modelo para analisar os riscos de TI com base na análise de cenários de riscos. A figura 6.4 mostra o cenário de risco que será analisado.

Categoria do Cenário de Risco 9: Software
Título do Cenário de Risco: Cenário de risco no processo de desenvolvimento de software do Departamento-Geral de Pessoal.
Categoria de Cenário de Risco: 09 - Software
Cenário de Risco: Foram identificadas por meio da modelagem de processos e análise documental alguns problemas e vulnerabilidades que ameaçam a organização a obter o objetivo planejado: 1. Desconhecimento por parte da Divisão de Tecnologia da Informação da Assessoria de Planejamento e Gestão do DGP dos sistemas de informação elaborados pelas diretorias de seu departamento. 2. Ausência de padronização no processo de pedidos de demandas de sistemas de informação pelas diretorias. 3. Ausência de padronização de documentos e *templates* relacionado ao processo de desenvolvimento de software. 4. Ausência de documentação dos softwares que foram desenvolvidos no DGP. 5. O usuário não possui facilidade no uso de alguns sistemas do DGP.

Figura 6.4: Cenário de Risco
Fonte: Elaboração própria.

Os componentes do cenário de risco conforme proposto no COBIT 5 possuem: um tipo de ameaça para cada vulnerabilidade identificada, um ator que desencadeia a ameaça e que explora uma vulnerabilidade, eventos que sempre tem causas e consequências, um ativo, ou seja, algo que possua valor tangível ou intangível que deverá ser protegido e os recursos e prazos que podem ajudar a alcançar os objetivos.

6.2 Análise dos Riscos

O objetivo em realizar uma análise de risco é fornecer à organização uma visão clara da situação atual, para prestar apoio na tomada de decisão [80]. Sendo de suma importância, que a organização realize a análise dos riscos antes de iniciar um projeto ou um novo processo de negócio, ou o desenvolvimento de um novo software/sistema [80].

Para a ISO 31000 [26], a análise dos riscos envolve a consideração detalhada de incertezas, fontes de riscos, consequências, probabilidade, eventos no qual podem ter múltiplas causas. Nessa etapa, é necessário compreender a natureza do risco e suas características e o nível do risco identificado.

Buscou-se então entender os riscos identificados no processo de desenvolvimento de software e determinar a probabilidade de ocorrência e a severidade de cada fator de risco se ocorrer. A análise foi dividida em 3 partes: a primeira, relacionado com o processo de desenvolvimento modelado, a segunda com as fraquezas identificados na Matriz SWOT e a terceira, com os fatores de riscos levantados na literatura.

Foi realizada a entrevista com os especialistas de TI do departamento, onde em conjunto, pontuaram de 1 a 5, qual a probabilidade de ocorrência e a severidade de cada um dos fatores de riscos identificados no processo de desenvolvimento de software modelado, sendo os resultados apresentados na figura 6.5.

FATORES DE RISCO (PROBLEMAS DO PROCESSO)						
ÁREA	ID	DESCRIÇÃO DO FATOR DE RISCO	P	S	R	PSR
GCS	FRP01	Ausência de padronização das ferramentas para o desenvolvimento de um novo software.	4	1	4	16
REQ	FRP02	Ausência de padronização da documentação para o desenvolvimento de um novo software.	4	3	4	48
VV	FRP03	Realização apenas de um tipo de teste para o principal sistema da organização.	2	4	5	40
GC	FRP04	Desconhecimento dos softwares/sistemas elaborados pelas diretorias por parte da DTI.	5	3	5	75
GD	FRP05	O pedido de demanda é feito por meio de um DIEx, pois não existe um modelo pronto (*template*) que distingue os tipos de demanda.	5	3	4	60
GD	FRP06	Falta de padronização no processo de pedidos de demandas das diretorias.	5	5	4	100
SUP	FRP07	Falta comunicação entre níveis de suporte.	5	5	3	75
VV	FRP08	Ausência de realização de testes nos softwares desenvolvidos	5	5	5	125

Figura 6.5: Análise dos Fatores de Risco do Processo de Desenvolvimento de Software Modelado

Fonte: Elaboração própria.

Já a Figura 6.6 apresenta os fatores de riscos relacionados com as fraquezas identificadas na TI do departamento.

FATORES DE RISCO (FRAQUEZAS DTI - SWOT)						
ÁREA	ID	DESCRIÇÃO DO FATOR DE RISCO	P	S	R	PSR
REQ	FRS01	Insuficiência da documentação de sistema;	5	5	4	100
MNT	FRS02	Desempenho insatisfatório de sistemas;	3	4	4	48
RH	FRS03	Rotatividade de pessoal;	5	5	4	100
GOV	FRS04	Falta de adoção de mecanismos de governança de TI automatizados, baseados em melhores práticas.	5	5	5	125
RH	FRS05	Falta de pessoal.	3	2	4	24
VV	FRS06	Rotina de teste deficiente.	5	5	5	125
RH	FRS07	Capacitação deficiente de parte do efetivo.	3	4	4	48

Figura 6.6: Análise do Fatores de Risco do Processo de Desenvolvimento de Software - SWOT

Fonte: Elaboração própria.

Nas figuras 6.5 e 6.6 verifica-se que as ameaças para cada vulnerabilidade/problema estão relacionadas com falhas no processo, uma vez que, existe uma ausência de padronização das demandas de software e dos documentos gerados no processo de desenvolvimento de software, bem como a ausência de um processo definido. Para cada fator de risco, foi calculado o índice PSR (Probabilidade Severidade e Relevância).

Foi solicitado aos profissionais de TI do DGP, analisar a probabilidade de ocorrer uma ameaça presente na literatura e se ocorrer, qual seria o impacto/severidade para a organização. A figura 6.7 apresenta essa análise realizada.

FATORES DE RISCO						
Área	ID	DESCRIÇÃO DO FATOR DE RISCO	P	S	R	PSR
GP	FR01	Distribuição incorreta de recursos alocados para o projeto, prejudicando o andamento das atividades da organização e dos projetos.	5	5	5	125
GP	FR03	Definição indevida de prioridades, ou seja, identificação incorreta de necessidades, fazendo com que componentes prioritários sejam desenvolvidos tardiamente e que tarefas sejam acompanhadas de forma	4	3	5	60
GP	FR05	Descumprimento de prazo. O tempo previsto para a conclusão do projeto ou entrega do produto tende a ser desobedecido.	5	5	5	125
GP	FR06	Desestabilização do projeto. Atividades e tarefas do projeto não são executadas conforme o planejado.	3	3	5	45
GP	FR07	Problemas no acompanhamento do Projeto. Dificuldades no acompanhamento da execução das atividades e tarefas do projeto.	3	2	5	30
GP	FR08	Definição imprópria de papéis e responsabilidades.	5	3	5	75
RH	FR11	Problemas de comunicação entre os interessados. Comunicação ineficiente entre os interessados no projeto, gerando inconsistências, consumindo recursos dos projetos e dificultando o trabalho	4	4	4	64
PDS	FR13	Falta de alinhamento da organização à implantação de processos de software.	4	4	5	80
PDS	FR16	Processo com baixa eficiência. Problemas técnicos na execução do processo consomem mais recursos para a realização das tarefas e o desenvolvimento do produto.	5	5	5	125
PDS	FR17	Retrabalho inútil. Despender tempo em atividades que serão refeitas ou executar ou executar o mesmo trabalho mais de uma vez, indicando um ponto de desperdício de recursos.	5	5	5	125
PDS	FR18	Falta de metodologia/processo de desenvolvimento.	5	5	4	100
REQ	FR19	Existência de requisitos incompletos, inconsistentes, inválidos, incorretos ou não verificáveis que impedem a correta implementação.	5	5	4	100
REQ	FR20	Requisitos mudam com frequência.	4	4	4	64
REQ	FR21	Escopo e os objetivos do projeto mudam constantemente.	4	4	4	64
REQ	FR22	Os requisitos são mal entendidos.	4	4	4	64
REQ	FR23	Falha em obter comprometimento do cliente / fornecedores de requisitos.	5	5	4	100
PI	FR24	Implementação do produto não atende aos projetos do produto. Inconsistência entre o que foi projetado e o que foi desenvolvido pelo projeto.	3	4	5	60
PI	FR25	Limitações técnicas. Barreiras técnicas no desenvolvimento do sistema que limitam algumas das funcionalidades ou até mesmo tornando impossível a realização de sua definição primária.	4	4	5	80
GC	FR26	Utilização de Ferramentas inadequadas	1	1	4	4
GC	FR27	Perda de controle sobre os itens de configuração modificados. Alterações nos itens de configuração (ambiente de desenvolvimento, versões de artefatos, baselines) acontecem de forma desestruturada.	3	5	4	60
VV	FR28	Falha de Software. Código ineficaz, fora de especificação, incompatível com outros módulos de software ou hardware, ou falhas provocadas por parâmetros configurados indevidamente.	3	4	5	60
VV	FR29-A	Baixa qualidade dos novo produtos desenvolvidos.	2	2	5	20
VV	FR29-B	Baixa qualidade dos produtos legados desenvolvidos.	5	5	5	125
IP	FR30	Dificuldade de integração dos componentes do software.	2	3	3	18
MNT	FR31	Ineficiência na implementação ou controle de solicitações de mudança.	5	5	4	100
MNT	FR32	Baixa manutenabilidade dos produtos gerados no desenvolvimento do software.	5	5	4	100
MNT	FR33	A aplicação do software é obsoleta. Por exemplo: tecnologia antiga, com má documentação, de manutenção custosa, difícil de entender, não integrada na atual arquitetura.	4	5	4	80

Figura 6.7: Análise dos Fatores de Riscos do Processo de Desenvolvimento de Software listado na literatura.

Fonte: Elaboração própria.

As vulnerabilidades / problemas são desencadeados por atores humanos, podendo ser tanto internos como externos. Na Tabela 6.1 apresenta a descrição do risco que para esse caso foi considerado como primário.

Tabela 6.1: Descrição do risco identificado para os problemas e vulnerabilidades do macroprocesso de desenvolvimento de software.

Fonte: Elaboração própria.

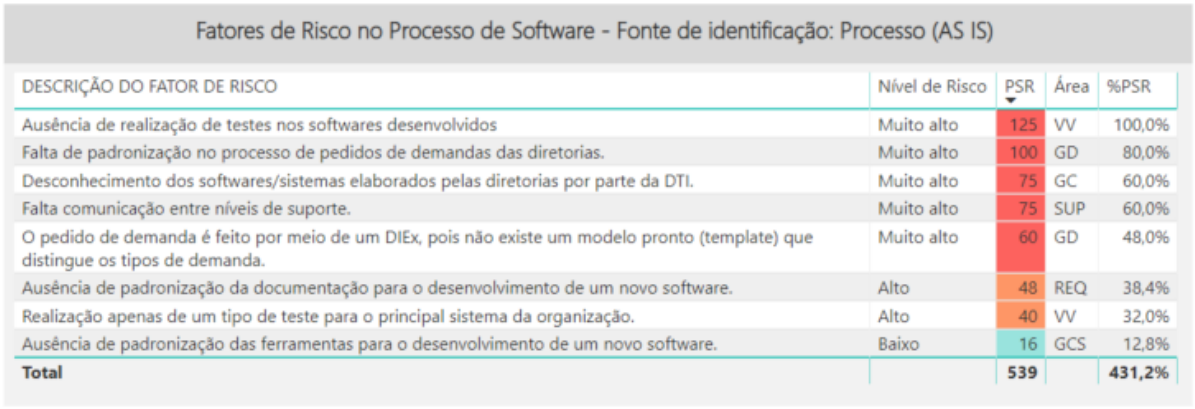
Tipo de Risco: (P) Primário, (S) Secundário ou (NA) Não se aplica	
Tipo de Risco	**Descrição do Risco**
Primário	A ausência da documentação dos sistemas de informação da organização auxilia para o desconhecimento por parte da DTI dos sistemas de informação e por sua vez irá dificultar o atendimento do objetivo de otimizar os recursos de TI da organização. Além disso, nota-se que o processo de desenvolvimento de software não é padronizado na organização, afetando também o atingimento dos objetivos.

A análise do cenário de risco é uma técnica para tornar o risco mais compreensível de forma a permitir a análise a avaliação apropriada do risco. Os resultados da análise de risco consiste em um cenário estimado de frequência e impacto, além das opções para reduzir o cenário de frequência e impacto.

6.3 Avaliação dos Riscos

Nessa etapa, busca-se avaliar os riscos identificados por meio da atribuição de níveis (muito alto, alto, médio, baixo, muito baixo), comparando-os com os critérios de avaliação e priorização dos riscos.

De acordo com o índice PSR atribuído a cada vulnerabilidade, foi definido o nível de risco seguindo os critérios adotados na seção 3.2.3.3. A figura 6.8 apresenta o nível de significância dos riscos identificados no processo de desenvolvimento de software modelado na organização por ordem de maior risco.



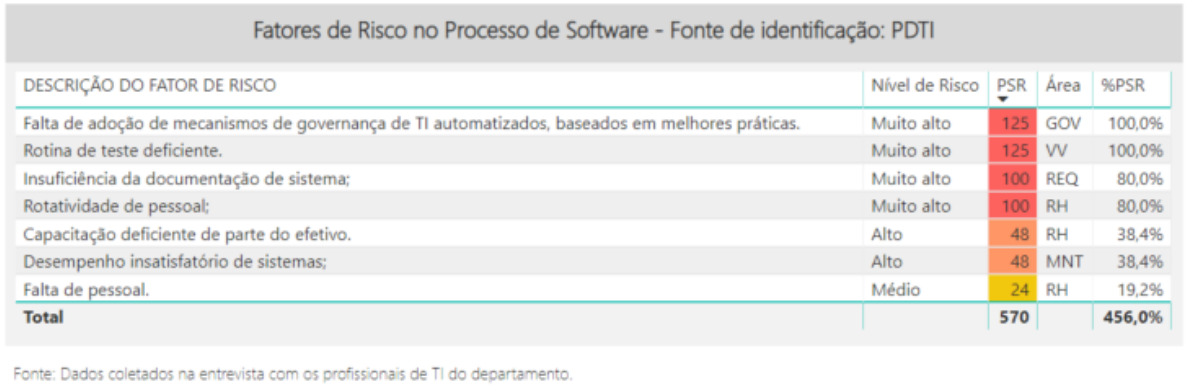
Fatores de Risco no Processo de Software - Fonte de identificação: Processo (AS IS)

DESCRIÇÃO DO FATOR DE RISCO	Nível de Risco	PSR	Área	%PSR
Ausência de realização de testes nos softwares desenvolvidos	Muito alto	125	VV	100,0%
Falta de padronização no processo de pedidos de demandas das diretorias.	Muito alto	100	GD	80,0%
Desconhecimento dos softwares/sistemas elaborados pelas diretorias por parte da DTI.	Muito alto	75	GC	60,0%
Falta comunicação entre níveis de suporte.	Muito alto	75	SUP	60,0%
O pedido de demanda é feito por meio de um DIEx, pois não existe um modelo pronto (template) que distingue os tipos de demanda.	Muito alto	60	GD	48,0%
Ausência de padronização da documentação para o desenvolvimento de um novo software.	Alto	48	REQ	38,4%
Realização apenas de um tipo de teste para o principal sistema da organização.	Alto	40	VV	32,0%
Ausência de padronização das ferramentas para o desenvolvimento de um novo software.	Baixo	16	GCS	12,8%
Total		**539**		**431,2%**

Fonte: Dados coletados na entrevista com os profissionais de TI do departamento.

Figura 6.8: Nível dos Riscos do Processo de Desenvolvimento de Software - Processo Modelado "AS IS".
Fonte: Elaboração própria.

A avaliação também foi realizada para as vulnerabilidades relatadas no PDTI da organização por meio da Matriz SWOT elaborado na seção de identificação de riscos, sendo apresentado o nível de significância dos riscos na Figura 6.9.



Fatores de Risco no Processo de Software - Fonte de identificação: PDTI

DESCRIÇÃO DO FATOR DE RISCO	Nível de Risco	PSR	Área	%PSR
Falta de adoção de mecanismos de governança de TI automatizados, baseados em melhores práticas.	Muito alto	125	GOV	100,0%
Rotina de teste deficiente.	Muito alto	125	VV	100,0%
Insuficiência da documentação de sistema;	Muito alto	100	REQ	80,0%
Rotatividade de pessoal;	Muito alto	100	RH	80,0%
Capacitação deficiente de parte do efetivo.	Alto	48	RH	38,4%
Desempenho insatisfatório de sistemas;	Alto	48	MNT	38,4%
Falta de pessoal.	Médio	24	RH	19,2%
Total		**570**		**456,0%**

Fonte: Dados coletados na entrevista com os profissionais de TI do departamento.

Figura 6.9: Nível dos Riscos do Processo de Desenvolvimento de Software - Análise SWOT.
Fonte: Elaboração própria.

Em relação aos fatores de riscos listados na literatura, são apresentados na Figura 6.10, o nível de risco para cada vulnerabilidade identificada. Os riscos foram avaliados de acordo com a pontuação atribuída pelos profissionais de TI do departamento.

Fatores de Risco no Processo de Software listados na literatura e que podem ocorrer na organização

DESCRIÇÃO DO FATOR DE RISCO	Nível de Risco	PSR	Área	%PSR
Baixa qualidade dos produtos legados desenvolvidos.	Muito alto	125	VV	100,0%
Descumprimento de prazo. O tempo previsto para a conclusão do projeto ou entrega do produto tende a ser desobedecido.	Muito alto	125	GP	100,0%
Distribuição incorreta de recursos alocados para o projeto, prejudicando o andamento das atividades da organização e dos projetos.	Muito alto	125	GP	100,0%
Falta de metodologia/processo de desenvolvimento.	Muito alto	125	PDS	100,0%
Processo com baixa eficiência. Problemas técnicos na execução do processo consomem mais recursos para a realização das tarefas e o desenvolvimento do produto.	Muito alto	125	PDS	100,0%
Retrabalho inútil. Despender tempo em atividades que serão refeitas ou executar ou executar o mesmo trabalho mais de uma vez, indicando um ponto de desperdício de recursos.	Muito alto	125	PDS	100,0%
Baixa manutenabilidade dos produtos gerados no desenvolvimento do software.	Muito alto	100	MNT	80,0%
Existência de requisitos incompletos, inconsistentes, inválidos, incorretos ou não verificáveis que impedem a correta implementação.	Muito alto	100	REQ	80,0%
Falha em obter comprometimento do cliente / fornecedores de requisitos.	Muito alto	100	REQ	80,0%
Ineficiência na implementação ou controle de solicitações de mudança.	Muito alto	100	MNT	80,0%
A aplicação do software é obsoleta. Por exemplo: tecnologia antiga, com má documentação, de manutenção custosa, difícil de entender, não integrada na atual arquitetura.	Muito alto	80	MNT	64,0%
Falta de alinhamento da organização à implantação de processos de software.	Muito alto	80	PDS	64,0%
Limitações técnicas. Barreiras técnicas no desenvolvimento do sistema que limitam algumas das funcionalidades ou até mesmo tornando impossível a realização de sua definição primária.	Muito alto	80	PI	64,0%
Definição imprópria de papéis e responsabilidades.	Muito alto	75	GP	60,0%
Escopo e os objetivos do projeto mudam constantemente.	Muito alto	64	REQ	51,2%
Os requisitos são mal entendidos.	Muito alto	64	REQ	51,2%
Problemas de comunicação entre os interessados. Comunicação ineficiente entre os interessados no projeto, gerando inconsistências, consumindo recursos dos projetos e dificultando o trabalho colaborativo.	Muito alto	64	RH	51,2%
Requisitos mudam com frequência.	Muito alto	64	REQ	51,2%
Definição indevida de prioridades, ou seja, identificação incorreta de necessidades, fazendo com que componentes prioritários sejam desenvolvidos tardiamente e que tarefas sejam acompanhadas de forma incorreta.	Muito alto	60	GP	48,0%
Falha de Software. Código ineficaz, fora de especificação, incompatível com outros módulos de software ou hardware, ou falhas provocadas por parâmetros configurados indevidamente.	Muito alto	60	VV	48,0%
Implementação do produto não atende aos projetos do produto. Inconsistência entre o que foi projetado e o que foi desenvolvido pelo projeto.	Muito alto	60	PI	48,0%
Perda de controle sobre os itens de configuração modificados. Alterações nos itens de configuração (ambiente de desenvolvimento, versões de artefatos, baselines) acontecem de forma desestruturada.	Muito alto	60	GC	48,0%
Desestabilização do projeto. Atividades e tarefas do projeto não são executadas conforme o planejado.	Alto	45	GP	36,0%
Problemas no acompanhamento do Projeto. Dificuldades no acompanhamento da execução das atividades e tarefas do projeto.	Médio	30	GP	24,0%
Baixa qualidade dos novo produtos desenvolvidos.	Médio	20	VV	16,0%
Dificuldade de integração dos componentes do software.	Médio	18	IP	14,4%
Utilização de Ferramentas inadequadas	Muito baixo	4	GC	3,2%
Total		**2078**		**1662,4%**

Figura 6.10: Nível dos Riscos do Processo de Desenvolvimento de Software - Fatores listados na Literatura. Fonte: Elaboração própria.

Verifica-se que a maioria dos riscos avaliados, possuem um nível de risco muito alta, ou seja, são riscos inaceitáveis, e os gestores e profissionais de TI relacionados com os processos devem ser orientados para minimizarem os riscos imediatamente. A figura 6.11 apresenta o gráfico com o percentual do nível de risco.

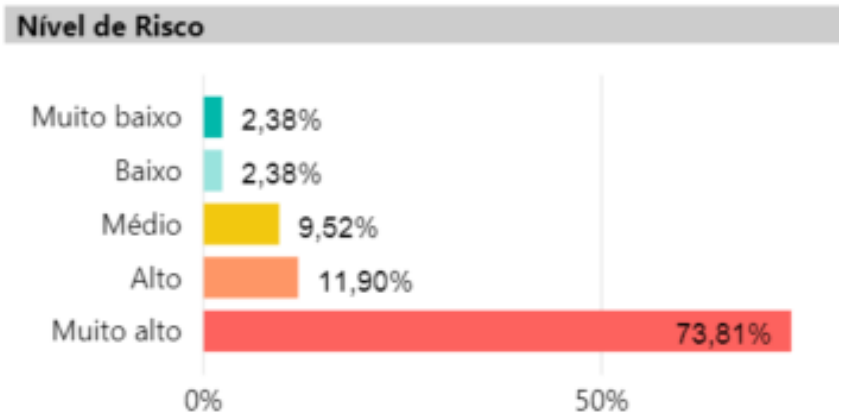


Figura 6.11: Gráfico do nível de risco encontrado para os fatores analisados
Fonte: Elaboração própria.

Com base na avaliação do nível de significância de cada risco, será necessário propor plano de ações para auxiliar no tratamento dos riscos mais críticos para a organização. A tabela 6.2 apresenta a lista com a priorização dos riscos.

Tabela 6.2: Lista de Riscos Priorizados

ID	**Risco Priorizado**	**PSR (Valor do Risco)**	**Área do Processo**	**Fonte**
1.	Ausência de realização de testes nos softwares desenvolvidos	125 - Muito Alto	Verificação, Validação e Testes	Processo "AS IS"modelado
2.	Rotina de teste deficiente.	125 - Muito Alto	Verificação, Validação e Testes	PDTI
3.	Baixa qualidade dos produtos legados desenvolvidos devido a ausência de testes.	125 - Muito Alto	Verificação, Validação e Testes	Literatura / Entrevista
4.	Ausência de metodologia e processo de desenvolvimento de software.	125 - Muito Alto	Processo de Desenvolvimento de Software	Literatura / Entrevista

A priorização levou em consideração os riscos que apresentaram a maior pontuação em cada uma das três fontes levantadas (processo "AS IS"modelado, PDTI do departamento é da literatura). Os riscos relacionados com a área de "Verificação, Validação e Testes"apareceram como o prioritário nas três análises e por isso foi escolhido para a elaboração do plano de tratamento dos riscos.

A figura 6.12 apresenta a análise dos riscos para a área de verificação, validação e testes de software.

Fatores de Risco no Processo de Software - Verificação e Validação de Software

DESCRIÇÃO DO FATOR DE RISCO	Nível de Risco	PSR	%PSR	FONTE
Ausência de realização de testes nos softwares desenvolvidos	Muito alto	125	100,0%	PROCESSO
Baixa qualidade dos produtos legados desenvolvidos.	Muito alto	125	100,0%	LITERATURA
Rotina de teste deficiente.	Muito alto	125	100,0%	SWOT
Falha de Software. Código ineficaz, fora de especificação, incompatível com outros módulos de software ou hardware, ou falhas provocadas por parâmetros configurados indevidamente.	Muito alto	60	48,0%	LITERATURA
Realização apenas de um tipo de teste para o principal sistema da organização.	Alto	40	32,0%	PROCESSO
Baixa qualidade dos novo produtos desenvolvidos.	Médio	20	16,0%	LITERATURA
Total		**495**	**396,0%**	

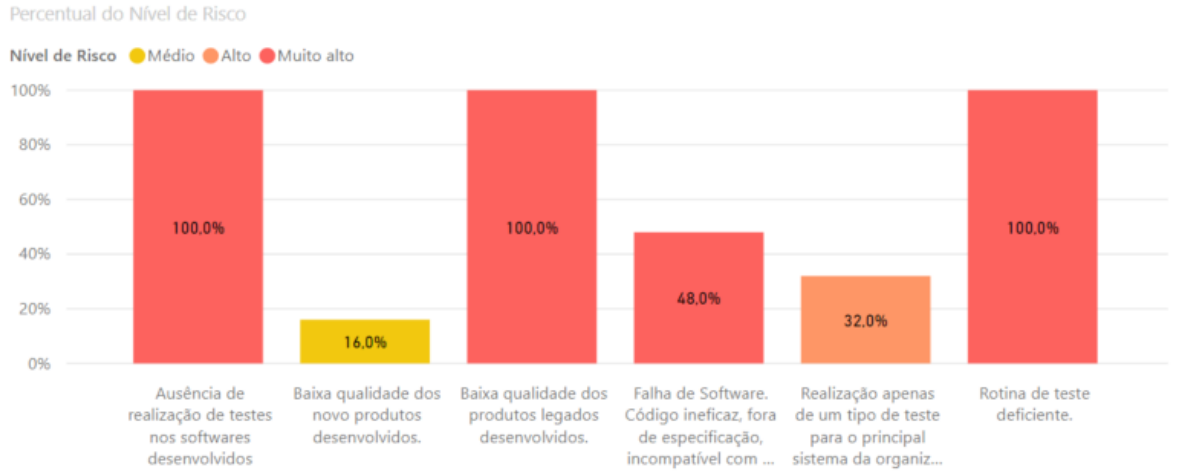


Figura 6.12: Análise dos fatores de risco da área de Verificação, Validação e Teste de Software

Fonte: Elaboração própria.

Dos 6 fatores de riscos identificados, quatro deles apresentaram com o nível de risco muito alto, sendo que três apresentam o valor máximo do PSR (125).

Além da área de Verificação e Validação, verifica-se, que os principais problemas do processo de desenvolvimento de software da organização estão relacionados com a ausência de um processo de desenvolvimento de software definido, que impacta na qualidade dos produtos de software desenvolvidos.

Esse problema foi relatado durante a entrevista pelos profissionais de TI do departamento e por isso será necessário as recomendações de melhoria de processo de software.

6.4 Tratamento dos riscos

No tratamento de riscos são definidas as possíveis ações a serem tomadas nos riscos. Deve-se gerar um plano de tratamento dos riscos, onde deve conter os recursos, responsabilidades e as atividades que serão realizadas. De acordo com Ramirez (2011) [34], as ações também deve incluir uma análise de custo-benefício, tanto para a implementação como para a manutenção.

Os riscos podem ser tratados, segundo a ABNT/ISO 27005 como sendo:

1. Evitar o Risco: Eliminar as causas ou as consequências;
2. Reduzir o Risco: Limitar o risco através de controles que reduzam ou eliminam o impacto gerado pela exploração de uma vulnerabilidade;
3. Reter o risco: Aplicar controles de correções como base o conhecimento de vulnerabilidades, falha ou defeito.
4. Transferir o Risco: Adotar outras opções que compensam a perda e transferir a responsabilidade pelo gerenciamento do risco, mas não a responsabilidade pelas consequências.

Em relação aos riscos identificados na entrevista com os profissionais de TI, foi selecionado o risco "ausência de realização de testes de software"como sendo um dos riscos que apresentam um maior potencial de probabilidade de ocorrência e de impacto na qualidade do software desenvolvido e por isso, é necessário a proposição de um plano de ação, representado na Tabela 6.3.

Tabela 6.3: Plano de gestão de risco - Processo de desenvolvimento de software - Área de Teste

Processo de Desenvolvimento de Software	
Plano de Gerenciamento de Risco	
Nome do Risco	Ausência de realização de testes de software no desenvolvimento dos sistemas de informação do departamento.
Descrição do Risco	Este risco está relacionado à falta de realização de testes nos produtos de software gerados pelo departamento avaliado.
Probabilidade	Muito alta – É quase certo que o risco irá ocorrer (>90%).
Severidade	Muito alta, pois impactará extremamente o negócio, o processo e a qualidade do produto de software que está sendo desenvolvido.
Índice de Risco (PSR)	125 – Muito Alto.
Descrição do Índice de Risco	Apresenta um risco muito alto, sendo considerado inaceitável, no qual, os gestores deverão tomar medidas para mitigação do risco.
Indicadores	• Quantidade de defeitos encontrados no processo de verificação e validação do software. • Número de defeitos encontrados por tipo. • Nível de severidade do defeito. • Quantidade de casos de teste. • Total de defeitos encontrados VS Total de defeitos corrigidos. • Percentual em que um software foi testado em relação ao número de casos de testes existentes e executados. • Quantidade de defeitos abertos encontrados em relação à severidade.
Medição	• Verificar se a quantidade de defeitos diminuiu em cada ciclo de desenvolvimento de softwares na organização.
Estratégia de diminuição.	1 – Evitar o Risco Implantar uma cultura de realização de testes de software na organização. •Criação de casos de testes; •Criação de plano de testes; •Execução de casos de testes; •Gestão de defeitos;
Plano de Contingência.	Alocar recursos humanos para a realização de testes em todas as etapas do processo de desenvolvimento de software.

Os habilitadores do COBIT foram utilizados para descrever como a organização funcionará para evitar a materialização do risco. Um habilitador é considerado essencial se possuir um alto efeito na redução do impacto ou da frequência do cenário.

Capítulo 7

Recomendações de Melhoria para o PDS do DGP

A implementação da melhoria do processo de software na área de TI do Departamento de Gestão de Pessoas do órgão é de suma importância para a qualidade dos produtos de software gerados pela área. Neste sentido, é necessário o conhecimento das boas práticas referente ao processo de desenvolvimento de software presente na literatura e na indústria de software contemporânea.

As recomendações estão baseadas nos aspectos relacionados com a melhoria de processo de software proposto pelos modelos de referência (MPS.BR-SW, ISO 12207, Cobit 5 e na estrutura do processo de software para o SISP-PSW).

O COBIT 5 propõe várias ações e respostas para mitigar os cenários de riscos. O Cenário de Risco escolhido está relacionado com a ausência de um processo de desenvolvimento de software definido.

Desta forma, as recomendações de melhorias devem ser aplicadas em todas as fases e áreas do desenvolvimento de software da organização (concepção e alinhamento estratégico; especificação e dimensionamento; estratégia de desenvolvimento, desenvolvimento; implantação e estabilização; e sustentação e evolução) e eixos de trabalhos (alinhamento estratégico, gestão de projetos, produção colaborativa, gestão de segurança, engenharia de software, gestão da contratação, gestão de infraestrutura e gestão de sustentação).

7.1 Recomendação 1 - Implantar uma cultura de realização de testes de software na organização

É importante que a organização tenha uma cultura de implantação de testes de software, que podem ser incorporados desde o início do seu processo de desenvolvimento de software de maneira a entregar um produto de qualidade aos usuários da organização por meio da realização de verificação, validação e testes em todas as fases do desenvolvimento e não apenas ao final do processo.

Como uma etapa na busca de melhoria contínua na disponibilização de sistemas de informação com uma maior qualidade é necessário a disseminação da cultura de testes pelos diversos setores envolvidos com o desenvolvimento de software na organização.

7.1.1 Recomendação 1.1. Garantir a Qualidade do Software

Para se obter a garantia da qualidade de software, deve-se adotar práticas de gestão por meio da execução de atividades como a especificação de critérios de qualidade de maneira a criar insumos para monitorar a qualidade do produto desenvolvido. A figura 7.1 apresenta a prática de gestão relacionada a garantia da qualidade proposto pelo COBIT 5 e os relacionamentos com as demais normas e áreas do MPS-BR-SW.

Prática de Gestão: BAI03.06 - Executar a garantia de qualidade.

Descrição da Prática de Gestão	Entradas	Saídas
BAI03.06 - Desenvolver, obter recursos e executar um plano de garantia de qualidade alinhado com o sistema de garantia de qualidade para atingir a qualidade especificada na definição de requisitos e os procedimentos e padrões corporativos de qualidade.	**APO 11.01** – Estabelecer um Sistema de Gerenciamento de Qualidade (QMS). • Resultados das revisões de efetividade do sistema de gestão da qualidade. **BAI01.09** – Gerencie a qualidade dos programas e dos projetos. • Plano de Gestão da qualidade.	**APO11.04** – Realizar o monitoramento da qualidade, controle e revisões. • Plano de Garantia da Qualidade.

Atividades:

1. Definir um plano e práticas de garantia de qualidade, como, por exemplo, a especificação de critérios de qualidade, processos de validação e verificação, definição de como a qualidade será revisada, qualificações necessárias aos revisores de qualidade e papéis e responsabilidades.
2. Monitorar frequentemente a qualidade da solução com base em requisitos de projeto, políticas corporativas, aderência às metodologias de desenvolvimento, procedimentos de gestão da qualidade e critérios de aceite.
3. Empregar a inspeção de código, práticas de desenvolvimento orientadas a testes, testes automatizados, integração contínua, walkthroughs e testes de aplicações quando apropriado. Reportar resultados dos processos de monitoramento e teste para a equipe de desenvolvimento de sistema e para a gestão de TI.
4. Monitorar todas as exceções de qualidade e endereçar todas as ações corretivas. Manter um registro com todas as revisões, resultados, exceções e correções. Repetir as revisões de qualidade, quando apropriado, com base na quantidade de retrabalho e ações corretivas.

Normas relacionadas: Square ISO 25010, ISO 9126, modelos de qualidade de: McCall's, Bohem's, Dromey's, FURPS.

Área do MPS-BR-Software: GQA – Garantia da Qualidade; VER- Verificação, VAL – Validação, GCO - Gerência de Configuração.

Figura 7.1: Práticas de gestão para a área de testes usando os habilitadores de processo do COBIT para a mitigação do risco.
Fonte: Adaptado de [41]

A garantia da qualidade de software consiste em criar um conjunto de atividades que ajudam a garantir que todo o produto gerado (artefatos, códigos) apresente alta qualidade [20], sendo atingida por meio de um Plano de Garantia da Qualidade que estabelece os métodos a serem utilizados no projeto.

O MPS.BR-SW [25] possui um processo de Garantia da Qualidade, quem tem o objetivo de assegurar que os produtos de trabalho e a execução dos processos estejam em conformidade com os planos, procedimentos e padrões estabelecidos e recomenda que

para a organização atender a esse processo de garantia, e deverá implementar as seguintes práticas:

- Avaliar objetivamente os produtos de trabalho selecionados com relação à descrição do processo, padrões e procedimentos aplicáveis.
- Avaliar objetivamente os processos selecionados em relação às descrições de processo, padrões e procedimentos aplicáveis.
- Comunicar as questões críticas relativas à qualidade e assegurar a solução de não-conformidades com a equipe e com os gerentes.
- Estabelecer e manter registros das atividades de garantia da qualidade.
- Comunicar as questões críticas relativas à qualidade e assegurar a solução de não-conformidades com a equipe e com os gerentes.

Alguns indicadores são definidos para a garantia da qualidade de software. Um indicador é uma medida de grande importância para a organização, devendo ser analisada e acompanhada periodicamente. conforme demonstrado na Tabela 7.1.

Tabela 7.1: Indicadores de Qualidade de Software

Indicadores	**Descrição dos indicadores**
Total de defeitos encontrados (TDE)	Quantidade de defeitos encontrados nas atividades de teste.
Total de defeitos corrigidos (TDC)	Quantidade de defeitos corrigidos após a execução dos testes.
Tempo Médio de Reparo (MTTR)	Tempo em quanto se leva, em média, para que a equipe de desenvolvedores consiga identificar os erros no sistema e corrigi-los.
Tempo Médio Entre Falhas (MTBF)	Indica os intervalos de tempo entre um defeito e outro. MTBF = (soma do tempo operacional / número total de falhas).
Taxa de sucesso da resolução de defeitos.	Compara a quantidade do total de defeitos solucionados com os reincidentes.
Satisfação do Usuário (SU)	Nível de satisfação do usuário com o software desenvolvido.

Além disso, verifica-se que a qualidade de um produto de software está fortemente relacionada à satisfação do usuário e com isso deve aplicar avaliações para validar se o produto desenvolvido atende as necessidades para uso.

7.1.2 Recomendação 1.2. Planejar os testes de software

Segundo Pressman (2011) [20], os testes são utilizados para se obter a qualidade dos produtos de software e tem o principal objetivo de encontrar defeitos antes do seu uso.

Existem diversas abordagens de testes que podem ser utilizadas no DGP, como: testes caixa branca, testes caixa preta, testes caixa cinza, regressão, unidade, integração, sistema, testes de aceitação.

A realização dos testes, devem ser planejados, para saber quando testar, o que testar e como testar. A norma IEEE 829 recomenda a utilização de alguns documentos para as atividades de testes conforme descritos na Tabela 7.2.

Tabela 7.2: Documentos de atividades de testes segundo a norma IEEE 829

Artefato	**Descrição**
Plano de Teste	Apresenta o planejamento para a execução do teste, ou seja, os recursos que serão utilizados, as atividades e cronogramas, e as abordagens de testes a serem utilizadas.
Especificação de Projeto de Teste	Refina o plano de teste apresentando as funcionalidades e características a serem testadas e os tipos de testes associados. Além de identificar os casos e procedimentos de teste, bem como os critérios de aceitação.
Especificação de Caso de Teste	Define os casos de teste, incluindo os dados de entrada, resultados esperados e as ações para a execução do teste.
Especificação de Procedimento de Teste	Especifica os passos para executar um conjunto de casos de teste.
Diário de Teste	Apresenta registros cronológicos dos detalhes relevantes relacionados com a execução dos testes.
Relatório de Incidente de Teste	Documenta qualquer evento que ocorra durante a atividade de teste.

O plano de teste, contém os casos de teste que guiarão a execução dos testes em um sistema. Os casos de teste podem ser descritos por meio de um *checklist* a ser seguido por um testador para validar um fluxo de uma aplicação, ou um cenário de uso.

A figura 7.2 apresenta as práticas de gestão que devem ser adotadas para planejar os testes na organização e por sua vez mitigar os riscos do processo de desenvolvimento de software.

BAI03.07 - Preparar para teste da solução.		
Descrição da Prática de Gestão	**Entradas**	**Saídas**
BAI03.07 - Estabelecer um plano de teste e ambientes necessários para testes unitários e integrados dos componentes da solução, incluindo os processos de negócio e serviços de suporte, aplicações e infraestrutura.	- Lista de funcionalidades - Escopo da solução.	BAI07.03 – Planejar testes de aceitação • Plano de teste • Procedimentos de teste
Atividades: 1. Criar um plano de teste integrado e práticas de acordo com o ambiente corporativo e planos estratégicos de tecnologia que possibilitarão a criação de ambientes de teste e simulação para auxiliar a verificar que a solução operará com sucesso no ambiente produtivo, entregará os resultados pretendidos e que os controles são adequados. 2. Criar um ambiente de teste que suporte o escopo completo da solução e reflita, o mais próximo possível, de condições reais de uso, incluindo processos e procedimentos de negócio, número de usuários, tipos de transação e condições de desenvolvimento. 3. Criar procedimentos de teste alinhados com o plano e práticas e permitem a avaliação da operação da solução em condições reais de uso. Assegurar que os procedimentos de teste avaliam a adequação dos controles, com base em padrões corporativos que definem papéis, responsabilidades e critérios de teste e que são aprovadas pelas partes interessadas do projeto, pelo patrocinador e pelo proprietário do processo de negócio.		
Normas relacionadas: ISO/IEC/IEEE 29119-1, IEEE 829. **Área do MPS-BR-Software:** GQA – Garantia da Qualidade; VER- Verificação, VAL – Validação; GRE – Gerenciar Requisitos		

Figura 7.2: Práticas de gestão para a área de testes usando os habilitadores de processo do COBIT para a mitigação do risco.
Fonte: Adaptado de [41]

Recomenda-se a utilização de ferramentas para gerenciar e automatizar os testes de software. A figura 7.3 apresenta algumas ferramentas que podem ser utilizadas pela organização durante o desenvolvimento do software.

Figura 7.3: Recomendações de ferramentas de gerenciamento e automação de testes.
Fonte: Elaborado pelo autor.

Essas ferramentas auxiliam a organização a planejar e executar os testes nos produtos de softwares. Sendo importantes a sua utilização no processo de desenvolvimento de software da organização.

Para minimizar os riscos do desenvolvimento de software, recomenda-se a utilização da ferramenta de Gestão de Riscos para a qualidade de software proposto por Lima (2019) [81]. Essa ferramenta auxilia na identificação de quais tipos de testes podem ser utilizados em cada fase do desenvolvimento da solução de maneira a auxiliar na garantia da qualidade do produto de software, por meio do controle de testes específicos para cada tipo de funcionalidade [81].

7.1.3 Recomendação 1.3: Executar Teste de Software

A figura 7.4 apresenta a prática de gestão relacionada com a execução do teste de software que deverá ser adotada pela organização para a minimização dos riscos do processo de desenvolvimento e com isso desenvolver software de qualidade.

BAI03.08 - Executar testes de solução.		
Descrição da Prática de Gestão	**Entradas**	**Saídas**
BAI03.08 - Executar testes continuamente durante o desenvolvimento, incluindo testes de controle, de acordo com o plano de teste definido e práticas de desenvolvimento no ambiente apropriado. Assegurar a participação de proprietários de processos de negócio e usuários finais no time de teste. Identificar e priorizar erros e problemas identificados durante o teste.	APO04.05 – Recomendar ações adicionais futuras • Análise de iniciativas rejeitadas.	BAI07.03 – Planejar testes de aceitação • Registros de resultados de teste e trilhas de auditoria. • Comunicação de resultados de teste.
Atividades: 1. Executar testes de soluções e seus componentes, com representantes dos processos de negócio e usuários finais. Assegurar que os testes sejam conduzidos somente nos ambientes de desenvolvimento e teste. 2. Utilizar instruções de teste claros, como definido no plano de testes, e considerar a proporção adequada de testes automatizados e testes interativos com usuários. 3. Executar todos os testes de acordo com práticas e o plano de teste incluindo a integração de processos de negócio e soluções de TI e requisitos não-funcionais (ex: segurança, interoperabilidade, usabilidade). 4. Identificar, registrar e classificar erros (ex: menor, significativo e missão crítica) durante os testes. Repetir os testes até que todos os erros significativos tenham sido resolvidos. Assegurar que uma trilha de auditoria com os resultados de teste seja mantida. 5. Registrar os resultados de teste e comunicar os resultados para as partes interessadas de acordo com o plano de teste.		
Normas relacionadas: ISO/IEC/IEEE 29119-1, IEEE 829. **Área do MPS-BR-Software:** GQA – Garantia da Qualidade; VER- Verificação, VAL – Validação;		
Métricas associadas: • Quantidade de erros identificados durante os testes. • Tempo e esforço para completar as tarefas.		

Figura 7.4: Práticas de gestão para a área de testes usando os habilitadores de processo do COBIT para a mitigação do risco.
Fonte: Adaptado de [41]

Os testes devem ser realizados durante todo o desenvolvimento do software e deverá envolver os donos dos processos de negócio e os usuários da solução que está sendo desenvolvida. Para isso, são indicados os testes de aceitação e de usabilidade [82].

Os testes de aceitação são testes de correção e validação, idealmente especificados por clientes ou usuários finais do sistema para verificar se um módulo funciona como foi especificado [83].

Para a execução dos testes de aceitação, recomenda-se a utilização da abordagem BDD *Behavior Driven Development* - Desenvolvimento dirigido por comportamento, uma vez que com essa abordagem, o esforço do desenvolvimento irá focar na descoberta e entrega das funcionalidades que agregam valor para a organização e a prática do BDD assume a utilização de ferramentas como suporte para o desenvolvimento de software [84].

7.2 Recomendação 2 - Disseminar na organização a implantação dos modelos de melhoria de processos de software

O desenvolvimento dos sistemas de informação devem ser baseados em melhores práticas do mercado e da literatura como, por exemplo, as normas NBR ISO/IEC 12207, NBR ISO/IEC 15504 e os modelos de referência para melhoria de processos de software como o MPS.BR. A figura 7.5 apresenta as principais normas e modelos de referência que podem ser utilizados no processo de desenvolvimento de software da organização.

Figura 7.5: Modelos de Referência auxiliar na melhoria do processo de software

O macroprocesso "Gerir Desenvolvimento de Software", é um processo que foi selecionado para ser melhorado na organização e as normas e modelos de referência serão importantes para a execução das atividades de melhoria de processo.

Com isso, será importante verificar qual o nível de maturidade de cada um dos processos elencados no ciclo de vida do desenvolvimento de software da organização.

Assim, será necessário identificar quais processos necessitam ser melhorados e os que geram riscos para a organização, sendo proposto a realização de um diagnóstico para analisar se a organização atende aos requisitos esperados pelos processos do MPS.BR.

Foi elaborado um modelo baseado no MPS.BR para aplicação de um *checklist* na organização para verificar quais controles estão implementados ou não. Consiste em avaliar se a organização atende os objetivos do processo.

Na aplicação, são definidas a probabilidade e severidade caso os requisitos esperados do processo não forem implementados. Durante a avaliação, os controles são respondidos associando os valores: implementado, não implementado, não aplicável e não respondido. Para cada controle devem ser registrados comentários e evidências que colaboram o valor associado conforme o exemplo da Figura 7.6 e 7.7.

PROCESSO: GERÊNCIA DE REQUISITOS - GRE

Propósito do processo: Gerenciar os requisitos do produto e dos componentes do produto do projeto e identificar inconsistências entre os requisitos, os planos do projeto e os produtos de trabalho do projeto.

REP	Descrição do REP	Situação	Probabilidade (P)	Severidade (S)	Relevância do Ativo	Evidências
GRE1	O entendimento dos requisitos é obtido junto aos fornecedores de requisitos.	Implementado	Baixa (> 5% e <= 35%)	Baixa	Alta	São realizadas reuniões com os demantes para o entendimento das necessidades do negócio. Artefatos: Ata de Reunião
GRE2	Os requisitos são avaliados com base em critérios objetivos e um comprometimento da equipe técnica com estes requisitos é obtido.	Não Implementado	Alta (> 65% e <= 95%)	Alta	Alta	
GRE3	A rastreabilidade bidirecional entre os requisitos e os produtos de trabalho é estabelecida e mantida;.	Não Implementado	Alta (> 65% e <= 95%)	Alta	Alta	
GRE4	Revisões em planos e produtos de trabalho do projeto são realizadas visando identificar e corrigir inconsistências em relação aos requisitos.	Não Implementado	Muito Alta (> 95%)	Muito Alta	Alta	
GRE5	Mudanças nos requisitos são gerenciadas ao longo do projeto.	Não Implementado	Alta (> 65% e <= 95%)	Muito Alta	Alta	

Figura 7.6: Resultados esperados do processo
Fonte: Adaptado de [25, 64].

PROCESSO: DESENVOLVIMENTO DE REQUISITOS - DRE						
Propósito do processo: definir os requisitos do cliente, do produto e dos componentes do produto.						
REP	**Descrição do REP**	**Situação**	**Probabilidade (P)**	**Severidade (S)**	**Relevância do Ativo**	**Evidências**
DRE1	As necessidades, expectativas e restrições do cliente, tanto do produto quanto de suas interfaces, são identificadas;	Implementado	Média (> 35% e < = 65%)	Média	Média	
DRE2	Um conjunto definido de requisitos do cliente é especificado e priorizado a partir das necessidades, expectativas e restrições identificadas;	Implementado	Baixa (> 5% e <= 35%)	Baixa	Média	
DRE3	Um conjunto de requisitos funcionais e não-funcionais, do produto e dos componentes do produto que descrevem a solução do problema a ser resolvido, é definido e mantido a partir dos requisitos do cliente;	Não Implementado	Muito Alta (> 95%)	Muito Alta	Média	
DRE4	Os requisitos funcionais e não-funcionais de cada componente do produto são refinados, elaborados e alocados. Interfaces internas e externas do produto e de cada componente do produto são definidas;	Não Implementado	Muito Alta (> 95%)	Muito Alta	Média	
DRE5	Conceitos operacionais e cenários são desenvolvidos;	Não Implementado	Muito Alta (> 95%)	Alta	Média	
DRE6	Os requisitos são analisados, usando critérios definidos, para balancear as necessidades dos interessados com as restrições existentes;	Não Implementado	Muito Alta (> 95%)	Muito Alta	Média	
DRE7	Os requisitos são validados.	Não Implementado	Muito Alta (> 95%)	Muito Alta	Média	

Figura 7.7: Resultados esperados do processo
Fonte: Adaptado de [25, 64].

Com base nesses dados será possível identificar o nível de conformidade com o modelo MPS.BR e assim identificar as possíveis ações de melhorias para a organização.

7.2.1 Ferramenta computacional para monitoramento dos riscos do Processo de Desenvolvimento de Software

Segundo a ISO 31000:2009 [26], durante todas as etapas do processo de gerenciamento de riscos, é importante comunicar as partes interessadas e monitorar os riscos identificados. O monitoramento, no âmbito do processo de gerenciamento de riscos, deve ser realizado pelas áreas responsáveis pelo Processo de Desenvolvimento de Software na organização, de maneira que consigam, com base nos dados coletados, criar ações para a melhoria do processo e reduzir os riscos identificados.

A fase de monitoramento dos riscos possuem os seguintes objetivos:

- Garantir que os controles sejam eficazes e eficientes;

- Analisar as ocorrências dos riscos;
- Detectar mudanças que possam requerer revisão dos controles e/ou do Plano de Tratamento;
- Identificar os riscos emergentes.

Como proposta de monitoramento dos riscos do processo de desenvolvimento de software foi proposto uma ferramenta (dashboard) com base em indicadores. Essa ferramenta foi criada com o auxílio do software Microsoft Power BI e Excel.

O Microsoft Power BI é um serviço de análise de negócios e tem o objetivo de fornecer visualizações interativas e recursos de Business Intelligence para a criação de relatórios e dashboards.

7.2.1.1 Definição de Indicadores para a Melhoria de Processo de Desenvolvimento de Software

Foram criados indicadores chaves de performance ou KPI's que irão auxiliar no monitoramento dos riscos identificados e na proposta de ações para a melhoria do processo de desenvolvimento de software da organização.

Os indicadores propostos foram levantados a partir da priorização dos riscos mais relevantes para o PDS.

1. **Nível de Conformidade (NC):** Representa o percentual de conformidade com o modelo de referência MPS.BR. Foi utilizado o seguinte *script* para o seu cálculo:

```
Nível de Conformidade = (CALCULATE(COUNT(REP[Situação]);
FILTER(REP; REP[Situação] = "Implementado")))/COUNT(REP[REP])
```

2. **Controles Implementados (CI):** Representa o total de controles implementados, ou seja, quantos REP's (Requisitos Esperados do Processo) foram implementados na organização.

```
Total de Controles Implementados =
(CALCULATE(COUNT(REP[Situação]);
FILTER(REP; REP[Situação] = "Implementado")))
```

3. **Controles não Implementados (CNI):** Representa o total de controles que ainda não foram implementados na organização.

```
Total de Controles Não Implementados =
(CALCULATE(COUNT(REP[Situação]);
FILTER(REP; REP[Situação] = "Não Implementado")))
```

4. **Riscos evitados (REV):** Os riscos evitados estão relacionados com o total de PSR existente nos controles implementados. Segue a seguinte fórmula:

$$\sum_{k=1}^{CI} PSR(CI); \tag{7.1}$$

   Utiliza-se o seguinte script para a definição da regra dos riscos evitados:

```
Riscos Evitados = (CALCULATE(sum(REP[PSR]);
FILTER(REP; REP[Situação] = "Implementado")))
```

5. **Riscos existentes (REX):** Representa os riscos relacionados aos controles que não foram implementados na organização. É calculado pela seguinte fórmula.

$$\sum_{k=1}^{CNI} PSR(CNI); \tag{7.2}$$

   Utiliza-se o seguinte script para a definição da regra dos riscos existentes:

```
Riscos existentes = (CALCULATE(sum(REP[PSR]);
FILTER(REP; REP[Situação] = "Não implementado")))
```

A ferramenta possui alguns gráficos que foram criados para auxiliar os gestores na tomada de decisão sobre os riscos do PDS.

1. **Quadro de Acompanhamento dos resultados:** Apresenta um quadro com os seguintes dados: área, total de controles implementados, total de controle não implementado, nível de conformidade, valor total do PSR, riscos existentes e riscos evitados.

Área	Total de Controles Implementados	Total de Controles Não Implementados	Nível de Conformidade	Valor Total do PSR	Riscos existentes	Riscos Evitados
Gerência de Configuração	5	2	71%	252	104	148
Verificação	4	2	67%	430	185	245
Desenvolvimento de Requisitos	2	5	29%	532	480	52
Garantia da Qualidade	1	4	20%	348	300	48
Gerência de Requisitos	1	4	20%	324	308	16
Validação	1	6	14%	725	600	125
Total	**14**	**23**	**38%**	**2611**	**1977**	**634**

Figura 7.8: Quadro de Acompanhamento dos Resultados

2. **Total de Controles Implementados X Total de Controles não Implementados por área:** Apresenta um comparativo entre os controles implementados e não implementados por área do PDS.

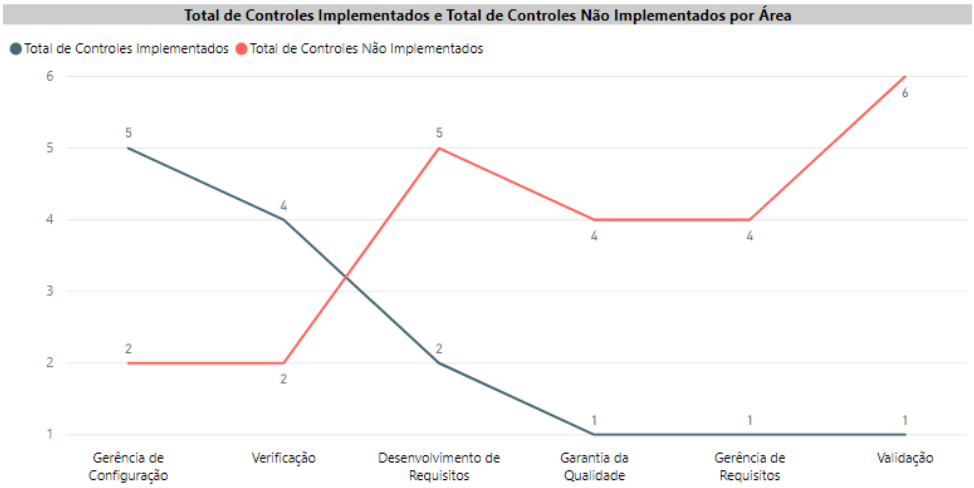


Figura 7.9: Comparação entre o total de controles implementados X controles não implementados

3. **Nível de Risco:** Apresenta um gráfico com o nível de risco que podem ser (muito baixo, baixo, médio, alto, muito alto).

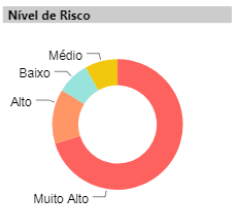


Figura 7.10: Nível de Risco

4. **Nível de conformidade por área:** Apresenta um gráfico com o nível de conformidade com o MPS.BR, onde será possível saber qual área apresenta o maior e o menor nível de conformidade com o processo.

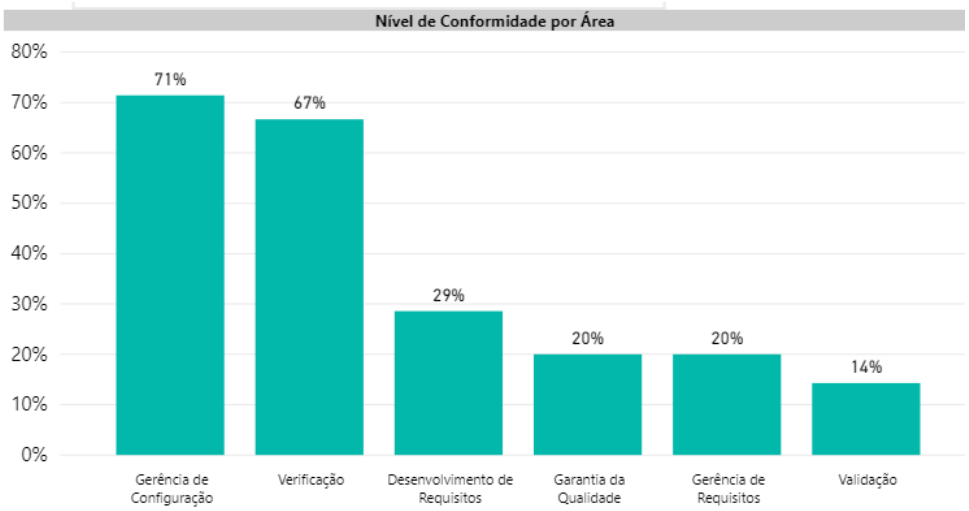


Figura 7.11: Nível de Conformidade por Área

5. **Total de Riscos Evitados X Total de Riscos Existentes:** Apresenta um comparativo entre os riscos existentes e os evitados.

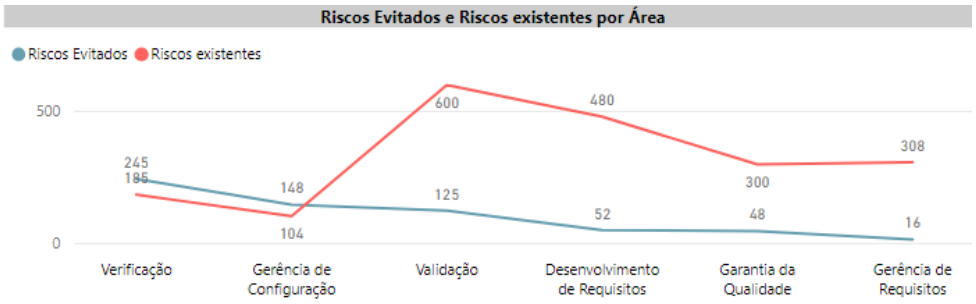


Figura 7.12: Comparação entre os riscos evitados e os riscos existentes por área

A figura 7.13 apresenta um *dashboard* que foi criado com os indicadores levantados para a análise da melhoria do processo de software da organização.

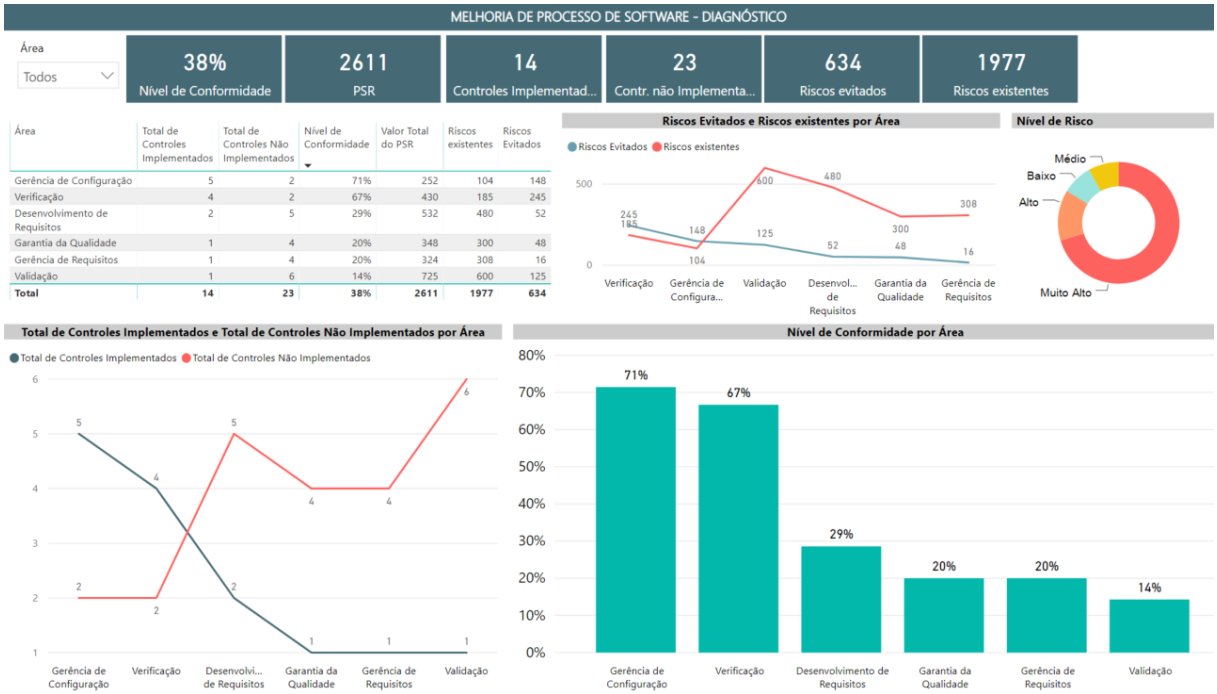


Figura 7.13: Indicadores de melhoria de processo
Fonte: Elaborado pelo autor.

Com a análise da maturidade dos processos de desenvolvimento de software na organização será possível verificar os pontos que necessitam de melhorias. O modelo MPS para software (MPS-SW) tem como base os requisitos de processos definidos nos modelos de melhoria de processo e atende a necessidade de implantar os princípios de Engenharia de Software de forma adequada ao contexto das organizações, estando em conformidade com as principais abordagens internacionais para definição, avaliação e melhoria de processos de software [24].

7.2.2 Fatores essenciais para a melhoria de processo de software

7.2.2.1 Desenvolver software de forma colaborativa entre as diretorias e demais departamentos da organização

Os softwares desenvolvidos no DGP devem ser feitos em conjuntos com as diferentes diretorias, ou seja, processos que promovam o levantamento de requisitos comuns a mais de uma diretoria.

Verifica-se que no processo de desenvolvimento de software no DGP é necessário envolver tanto o DCT, como o departamento responsável pelos sistemas corporativos da organização, como também da DTI/APG e das unidades de TI de cada diretoria, bem como as áreas de negócio demandantes.

Diante disso, a estrutura organizacional é um fator essencial para o sucesso da implementação da melhoria do processo de software, no qual, é importante verificar se os recursos humanos atuais suportam o novo ambiente e quais são as qualificações necessárias [85].

As estruturas organizacionais são entidades de tomada de decisão da organização. A figura 7.14 apresenta as contribuições do habilitador "Estruturas Organizacionais"para mitigar os cenários de riscos.

Estrutura Organizacional	
Referência	**Contribuição para a resposta**
Departamento de Tecnologia da Informação (DCT)	O DCT, como Órgão Central da gestão da TI deverá subsidiar Responsável em definir os procedimentos que devem ser usados no desenvolvimento de software dentro da organização, bem como por manter os sistemas de informação operante.
Divisão de Tecnologia da Informação (DTI/APG) do DGP	A DTI, como principal unidade de TI do DGP necessita ser um elo integrador entre as áreas de TI das diretorias de maneira que os sistemas desenvolvidos sejam aprovados e comunicados efetivamente.
Seções de TI de cada diretoria do DGP	Responsável por desenvolver e manter os sistemas de informação de caráter específico, de responsabilidade de sua diretoria.

Figura 7.14: Habilitador "Estruturas Organizacionais"para mitigar os cenários de riscos
Fonte: Elaborado pelo autor.

O desenvolvimento de sistemas corporativos podem auxiliar a manterem as atividades alinhadas à estratégia da organização, aumentando a padronização entre os sistemas de informação desenvolvidos.

7.2.2.2 Mitigar os riscos do processo de desenvolvimento de software

O habilitador "Cultura, Ética e Comportamento"listado no COBIT 5 evidencia-se o comportamento relativo à assunção de riscos, onde é verificado em que medida a organização está disposta a assumir os riscos.

Deve-se analisar o comportamento relativo à adoção de políticas, no qual, verifica-se em que medidas a organização adota ou cumpre uma determinada política e analisar o comportamento no caso de resultados negativos, ou seja, como a organização lida com os prejuízos ou perdas de oportunidades [41]. A figura 7.15 mostra as contribuições para a resposta ao cenário de risco.

Utilizando os Habilitadores do COBIT para Mitigação dos Riscos	
Cultura, Ética e Comportamento	
Referência	**Contribuição para a resposta**
Ética Individual	Os valores pessoais dos militares e civis são importantes para mitigar os riscos no processo de desenvolvimento de software da organização.
Comunicação entre as áreas de negócio e tecnologia da organização	Adotar a comunicação por toda a organização de forma a deixar claro as políticas e princípios adotados pela organização.
Comportamento em Conformidade.	Os resultados dos processos não serão alcançados caso o comportamento não estiver em conformidade.
Teste realizado em todos os níveis apropriados	Os usuários, desenvolvedores, analistas de requisitos e testes devem realizar os testes de software durante todo o ciclo de desenvolvimento. Além disso, é necessário realizar mais de um tipo de teste no desenvolvimento da solução.

Figura 7.15: Habilitador "Cultura, ética e comportamento"para mitigar os cenários de risco.

Fonte: Elaboração própria.

As boas práticas que devem ser adotadas são: comunicação para toda a organização; orientação por meio de regulamentos e normas deixando claro as políticas e princípios adotados pela organização.

Para o habilitador de Cultura, Ética e Comportamentos verifica-se que está relacionado com problemas de qualidade nos novos softwares da organização, uma vez que mesmo adotando uma sólida metodologia de desenvolvimento de projeto de software, muitas vezes os problemas gerados pelo software causam equívocos operacionais no cotidiano da organização.

Outro ponto está relacionado ao cumprimento da metodologia e dos procedimentos quando não existe por motivos de tempo e orçamento, mesmo gerando uma maior qualidade para os softwares desenvolvido, sendo o caso da aplicação da fase de testes, onde foi verificado no DGP que não são realizados os diversos tipos de testes disponíveis nas práticas de Engenharia de Software.

Além disso, foi verificado nos processos que o envolvimento da área de negócio e de desenvolvimento cessa ao ser transferido para a área operacional, sendo criado apenas processos de controle de incidentes e de problemas.

7.2.2.3 Gerir o conhecimento dos produtos gerados no desenvolvimento de software

No desenvolvimento de um software, é importante gerenciar a informação para gerar conhecimento para a organização e por isso deve ser usada para auxiliar na definição

das especificações do software e dos processos de negócio. A Figura 7.16 apresenta as contribuições do habilitador "Informação"do Cobit 5 para mitigar os cenários de riscos.

Utilizando os Habilitadores do COBIT para Mitigação dos Riscos	
Informação	
Referência	**Contribuição para a resposta ao Cenário**
Modelo de Arquitetura	A arquitetura deverá ser capaz de acoplar e integrar os sistemas de informação da organização de forma que não necessite de duplicação de informações.
Especificações de Projeto	A especificação do projeto do sistema auxilia no esclarecimento das necessidades aos usuários.
Plano de Garantia de Qualidade	Realizar os testes necessários para garantir a qualidade do software desenvolvido. É necessário definir os passos a serem dados.
Plano de Manutenção	Todo software que for desenvolvido na organização deverá possuir um plano de manutenção de forma planejada.

Figura 7.16: Habilitador "Informação"para mitigar os cenários de risco
Fonte: Elaboração própria.

Uma das análises que podem ser realizadas são referentes aos fatores intangíveis como vantagem competitiva, satisfação do cliente e incerteza tecnológica.

A organização gera benefícios a partir das análises somente após o recurso da informação ser aplicado ou utilizado, e desse modo o valor da informação é determinado exclusivamente através do seu uso (internamente ou pela sua venda) e a informação não tem valor intrínseco. O valor só pode ser gerado quando a informação é colocada em ação [41].

7.2.2.4 Capacitar os profissionais de TI da organização

Em relação a gestão de pessoas, verifica-se a importância da capacitação dos profissionais de TI para aumentar o nível de qualificação dos militares e desta forma, as necessidades identificadas em termos de capacitação são:

- Curso de Desenvolvimento ágil de sistemas de informação;
- Curso de ferramentas lowcode, como o Outsystems;
- Cursos de ferramentas de análise de dados como Power BI, Microstratagy, Pentaho, R, entre outras;
- Cursos de modelagem de processos com ferramentas como: Aris, Bizagi, entre outras.

O COBIT 5 define metas para o habilitador "Pessoas, Habilidades e Competências"que estão relacionadas com o nível de educação, qualificação, habilidades técnicas, níveis de

experiência, conhecimento e habilidades comportamentais necessários para realizar e desenvolver as atividades do processo com sucesso.

É importante que a organização saiba qual é a atual base de habilidades de forma que com essa informação consiga auxiliar no planejamento estratégico, definindo os objetivos em que a organização deseja alcançar.

Além disso a organização deverá avaliar as competências necessárias e promover o desenvolvimento das habilidades por meio de treinamentos e transferência de conhecimento [41]. A figura 7.17 apresentam as contribuições relacionada ao habilitador.

Utilizando os Habilitadores do COBIT para Mitigação dos Riscos	
Pessoas, Habilidades e Competências	
Referência	**Contribuição para a resposta**
Habilidades Técnicas	Investimentos em conhecimento técnico aos profissionais de TI do órgão para projetar e desenvolver os componentes de softwares apropriados para a organização.
Habilidades de arquitetura	Desenvolver uma arquitetura eficiente e eficaz alinhada aos requisitos de negócio.

Figura 7.17: Habilitador "Pessoas, habilidades e competências" para mitigar os cenários de risco.

Fonte: Elaboração própria.

Como boa prática, os requisitos de qualificação devem ser claros e objetivos e as definições de habilidades devem ser disponibilizadas. Pode ser utilizado frameworks como o "Skills Framework for Information Age (SFIA)", que descreve o gerenciamento das habilidades e competências dos profissionais que trabalham com tecnologia, engenharia de software e transformação digital.

7.2.2.5 Gerir os projetos de desenvolvimento de software

A gestão de projetos possui importância no processo de desenvolvimento de software de forma a controlar o andamento da execução do projeto. O processo "BAI01 - Gerenciar programas e projetos" poderá ser utilizado como guia na organização, além das boas práticas adotadas no PMBOK, Prince2 e SCRUM[86, 87].

- Adotar um software de gerenciamento de projetos no desenvolvimento de todos os sistemas de informação da organização para a visualização de cada etapa do projeto. Assim você pode acompanhar o desenvolvimento do projeto e interferir no momento certo, caso seja necessário [21].
- Acompanhar o andamento da execução dos projetos de desenvolvimento de software na organização de maneira mais efetiva e próxima dos executores do processo de desenvolvimento.

- Centralizar as informações, evitando redundâncias e falhas, já que as informações podem ser atualizadas em tempo real. Dessa forma, os gestores conseguem tomar decisões mais assertivas e com embasamento em dados [21].

O GPEx é o sistema utilizado para manter os projetos a nível estratégico, mas não é o utilizado no desenvolvimento de softwares nos departamentos e nas diretorias. É importante que a área de TI utilize um sistema com informações de todos os projetos de desenvolvimento e manutenção dos sistemas de informação do DGP, de forma que os responsáveis pela área de TI do DGP conheçam as iniciativas de cada área.

7.2.2.6 Melhorar a segurança e a infraestrutura dos ativos de TI utilizados para o desenvolvimento de software na organização

A segurança do ambiente é primordial para o desenvolvimento de maneira a preservar a confidencialidade, integridade e disponibilidade das informações através do estabelecimento de políticas, práticas e processos.

A infraestrutura de TI adequada também é primordial para o bom desempenho no processo de desenvolvimento de software de forma que o ambiente utilizado tenha a capacidade necessária para prover os serviços utilizados.

As boas práticas aplicada ao habilitador são: reaproveitamento de componentes comuns de arquitetura; compra ou desenvolvimento, ou seja, as soluções devem ser compradas a menos que haja uma justificativa aprovada para seu desenvolvimento interno; simplicidade de forma que arquitetura corporativa seja projetada e mantida de forma simples e que atenda aos requisitos da organização; agilidade em satisfazer as necessidades de mudança dos negócios de forma eficaz e eficiente. A figura 7.18 apresenta as contribuições relacionada ao habilitador.

Utilizando os Habilitadores do COBIT para Mitigação dos Riscos	
Serviços, Infraestrutura e Aplicações	
Referência	**Contribuição para a resposta**
Repositórios de Conhecimento	O DGP deverá possuir os repositórios para a gestão do conhecimento dos sistemas que foram desenvolvidos de forma a compartilhar e coordenar o conhecimento em relação às atividades de desenvolvimento.
Ambiente de desenvolvimento integrado	Facilitar o desenvolvimento, utilizando editor de código-fonte padronizado ou ferramentas de desenvolvimento *low-code* e ferramentas de automação e um depurador de códigos.

Figura 7.18: Habilitador "Serviços, infraestrutura e aplicações"para mitigar os cenários de risco.

Fonte: Elaboração própria.

A utilização de diretrizes, modelos ou padrões podem ser adotados como por exemplo o ITIL e o TOGAF. Outro ponto importante é adoção de uma base de conhecimento dos sistemas de informação da organização [88, 89].

A sustentação de sistemas consiste na gestão corretiva, adaptativa e evolutiva dos sistemas de TI utilizados. O processo de sustentação deve ser planejado de maneira que o software desenvolvido seja mantido, operado e evoluído de forma sustentável e viável.

Este serviço deverá ser utilizado para evitar os prejuízos que podem causar ao DGP se apresentarem erros, panes ou *bugs* nos sistemas de informação utilizados.

Capítulo 8

Considerações Finais

A gestão de riscos é de suma importância para identificar, analisar e avaliar os riscos que são inerentes ao processo de desenvolvimento de software de uma instituição, analisando os seus impactos e formas de mitigá-los.

O desenvolvimento do presente estudo possibilitou uma análise do processo de desenvolvimento de software da organização estudada, identificando lacunas e vulnerabilidades no seu processo, de maneira a analisar e avaliar os riscos do processo de desenvolvimento de software do departamento de gestão de pessoas da organização.

A pesquisa abordou todas as etapas da Gestão de Riscos proposta pela ISO 31000 (Comunicação e Consulta, Estabelecimento do Contexto, Identificação de Riscos, Análise de Riscos, Avaliação de Riscos, Tratamento de Riscos e Monitoramento e Análise Crítica):

- **Comunicação e Consulta:** Foram consultados os profissionais de diferentes áreas envolvidos no processo de desenvolvimento de software da organização de maneira a compartilharem opiniões distintas sobre o conjunto de riscos que afetam a organização em seu processo de desenvolvimento de software.

  Obteve-se o engajamento entre as partes interessadas (analistas de requisitos desenvolvedores e gestores) para uma melhor compreensão dos riscos enfrentados pela organização e formas de tratamento.

- **Estabelecimento de Contexto:** A pesquisa identificou o contexto em que a gestão de riscos está inserida, levando em conta a governança, a estrutura organizacional, os sistemas de informação e os profissionais envolvidos no processo.

- **Avaliação de Riscos:** Foram identificados os riscos que ocorrem no processo de desenvolvimento de software da organização por meio das ferramentas de análise de listas de verificação *(checklists)* para priorizar por meio de um índice de risco (PSR), os riscos que apresentam as maiores probabilidade de ocorrência, severidade e relevância para o departamento.

Verifica-se que os riscos relacionados com a ausência de um processo de desenvolvimento de software na organização e a rotina dos testes deficientes como sendo os principais riscos encontrados no processo, no qual, contribui para que os softwares sejam entregues sem garantir a sua qualidade.

- **Tratamento de Riscos:** Com os riscos priorizados, foram propostas ações para o seu tratamento, bem como sugestões para a melhoria do processo de desenvolvimento de software da organização.

  Foi proposto o planejamento e a execução de teste de software em todas as fases do desenvolvimento de software. Sendo necessário monitorar os defeitos identificados nos softwares desenvolvidos.

- **Monitoramento e Análise Crítica:** Foi proposta uma ferramenta (dashboard) para monitorar os riscos do processo de desenvolvimento de software com base em ações de melhoria do modelo de referência MPS.BR.

Com isso, verifica-se que a pesquisa atingiu seu objetivo de aplicar o gerenciamento de riscos ao processo de desenvolvimento de software da organização com a utilização de ferramentas para auxiliar na monitoração de seus riscos.

Além disso, percebe-se que a pesquisa esteve alinhada com os princípios do GRC (Governança, Riscos e *Complience*). O resultado do trabalho serve de*input* para que a Governança de TI, os riscos e *complience* possam ser repensados.

Cabe destacar que essa pesquisa serve somente para a organização pesquisada e não tem poder de generalização. Além disso, observa-se que esta é válida para o tempo na qual a mesma foi realizada servindo como um diagnóstico da situação dos riscos atuais da organização e que futuramente poderão haver mudanças de percepção e outros desdobramentos organizacionais que podem alterar os resultados obtidos.

Em relação a metodologia utilizada, poderá ser reaplicada em outros contextos e organizações, de maneira a avaliar os riscos do desenvolvimento de software.

Espera-se a aplicação da melhoria nos processos de desenvolvimento de software da organização, de maneira a desenvolverem sistemas de informação alinhados com os objetivos do negócio, e também garantir a qualidade dos softwares desenvolvidos e que satisfaçam as necessidades dos usuários.

Os resultados da pesquisa, servirão de insumos para a melhoria do macroprocesso de "Gerir Desenvolvimento de Software do departamento".

8.1 Trabalhos Futuros

Os conhecimentos obtidos com essa dissertação podem ser aplicados na organização para a melhoria do processo de desenvolvimento de software por meio da avaliação dos riscos.

Na sequência do presente trabalho surgiram alguns aspectos que se revelaram interessantes para uma abordagem mais detalhada, sendo objeto de futura investigação:

- Aplicar a análise dos requisitos esperados no processo de desenvolvimento de software, de maneira a identificar os controles implementados e não implementados na organização.
- Analisar a maturidade da organização no desenvolvimento de software.
- Aplicar a melhoria de processo de software na organização, partindo como base os modelos de referência (MPS.br, CMMI, ISO 12207, ISO 15504).
- Implantar a ferramenta de monitoração dos riscos para as áreas que desenvolvem software na organização.
- Analisar o funcionamento da Governança de TI aplicada ao processo de desenvolvimento de software na organização.

Com base nos resultados da pesquisa, propõe-se o desenvolvimento de artigos sobre a temática abordada como forma de gerar conhecimento tanto na área profissional como na científica.

Referências

[1] Luz, Kerlla Souza, Rayan Felipe Patrício Lopes e Willians Paulo da Silva: *Mapeamento da utilização de modelos mps. br e cmmi para melhorias no processo de desenvolvimento de software no mercado nacional.* TECNOLOGIAS EM PROJEÇÃO, 7(1):62–69, 2016. 1

[2] Moraes, Emerson Augusto Priamo e Sandra Regina Holanda Mariano: *Uma releitura dos principais modelos de governança de tecnologia da informação.* Revista Vianna Sapiens, 1(1):17–17, 2010. 1

[3] Dey, Prasanta Kumar, Jason Kinch e Stephen O Ogunlana: *Managing risk in software development projects: a case study.* Industrial Management & Data Systems, 107(2):284–303, 2007. 1

[4] Sommerville, Ian: *Software engineering.* New York: Addison-Wesley, 2011. 1, 8, 9, 11

[5] Coser, Maria Angela e Hélio Gomes de Carvalho: *Práticas de gestão do conhecimento em empresas de software: grau de contribuição ao processo de especificação de requisitos.* Gepros: Gestão da Produção, Operações e Sistemas, 7(2):109, 2012. 1

[6] Macedo, Mateus Henrique Basso e Eduardo Gomes Salgado: *Gerenciamento de risco aplicado ao desenvolvimento de software.* Sistemas & Gestão, 10(1):158–170, 2015. 1

[7] Morais, Nathaniel Simch de: *Proposta de modelo de migração de sistemas de ambiente tradicional para nuvem privada para o polo de tecnologia da informação do exército brasileiro.* 2015. 1

[8] Bleistein, Steven J, Karl Cox, June Verner e Keith T Phalp: *Requirements engineering for e-business advantage.* Requirements Engineering, 11(1):4–16, 2006. 2

[9] Ramesh, Balasubramaniam, Radhika Jain, Mark Nissen e Peng Xu: *Managing context in business process management systems.* Requirements Engineering, 10(3):223–237, 2005. 2

[10] Dietz, Jan LG e Antonia Albani: *Basic notions regarding business processes and supporting information systems.* Requirements Engineering, 10(3):175–183, 2005. 2

[11] Regev, Gil, Pnina Soffer e Ilia Bider: *Coordinated development of business processes and their support systems.* Requirements Engineering, 10(3):173–174, 2005. 2

[12] Silva, Cel de Comunicações Fortunato Menezes da: *A governança de tecnologia da informação na administração pública federal e seus reflexos para o exército brasileiro.* 2011. 2

[13] Brasil, Exército Brasileiro, Departamento Geral de Pessoal: *Plano diretor de tecnologia da informação (pdti) dgp 2017-2021.* 2016. 3, 40, 41, 46, 69

[14] Assis Neto, Francisco de: *Governança de tecnologia da informação em saúde: proposta de ações baseada em riscos e requisitos de interoperabilidade para o sistema de saúde do exército brasileiro.* 2015. 3

[15] Brasil, Exército Brasileiro, Secretaria Geral do Exército: *Portaria n º 169, de 21 de fevereiro de 2018 - plano de racionalização de tecnologia da informação do quartel-general do exército (eb20-p-02.001).* Boletim do Exército 9/2018, páginas 11–16, 2018. 3, 4

[16] Brasil, Exército Brasileiro, Secretaria Geral do Exército: *Portaria nº 455-eme - diretriz para racionalização de tecnologia da informação e comunicações (tic) no quartel-general do exército (eb20-d-02.006).* Boletim do Exército 46/2017, páginas 40–50, 2017. 3, 39

[17] Brasil, Exército Brasileiro, Secretaria Geral do Exército: *Portaria n º 031-dgp, de 8 de fevereiro de 2018 - diretriz de implantação do projeto sistema corporativo de gestão de pessoal do exército.* Boletim do Exército 9/2018, páginas 24–31, 2018. 4

[18] Charette, Robert N: *Why software fails [software failure].* IEEE spectrum, 42(9):42–49, 2005. 4

[19] Sbrocco, JHTC e P Macedo: *Metodologias ágeis: engenharia de software sob medida.* São Paulo: Érica, 2012. 8, 9

[20] Pressman, R. S.: *Engenharia de Software: uma abordagem profissional.* 2011. 8, 9, 11, 82, 84

[21] Brasil, Ministério do Planejamento, Desenvolvimento e Gestão e Universidade de Brasília UnB: *Kits de governança de ti*, 2018. `http://www.planejamento.gov.br/assuntos/empresas-estatais/publicacoes/kits-governanca-ti`. 9, 10, 60, 99, 100

[22] ISO/IEC: *Iso/iec 12207 systems and software engineering-software life cycle processes.* International Organization for Standardization, Geneva, Switzerland, 2008. 10, 11

[23] Pino, Francisco J, Félix García e Mario Piattini: *Software process improvement in small and medium software enterprises: a systematic review.* Software Quality Journal, 16(2):237–261, 2008. 10

[24] SOFTEX-ASSOCIAÇÃO, PARA PROMOÇÃO DA EXCELÊNCIA: *Do software brasileiro–softex.* MPS. BR–Guia Geral MPS de Software, 2012. 11, 12, 95

[25] BR, MPS: *Mps. br–melhoria de processo do software brasileiro*. 2016. 12, 31, 82, 89, 90

[26] ISO, ABNT Norma NBR: *Iso 31000: Gestão de riscos*. Rio de Janeiro: ABNT, 2009. 12, 13, 28, 32, 33, 36, 64, 65, 70, 90

[27] Amendola, Aniello: *Recent paradigms for risk informed decision making*. Safety Science, 40(1-4):17–30, 2002. 12

[28] Adams, John: *[book review] risk, the policy implications of risk compensation and plural rationalities*. Economist, 334(906):86–86, 1995. 12

[29] Cendrowski, Harry e WILLIAM C MAIR: *Enterprise Risk Management and COSO A Guide for Directors, Executives, and Practitioners*. Wiley Online Library, 2009. 12

[30] ISO, I e I Std: *Iso 27005: 2011*. Information technology–Security techniques–Information security risk management. ISO, 2011. 12, 24

[31] *COBIT 5 for Risk*. Information Systems Audit and Control Association, 2013, ISBN 9781604204575. `https://books.google.com.br/books?id=k_hgAwAAQBAJ`. 12, 16, 23, 24, 64, 69

[32] Rovai, Ricardo Leonaldo: *Modelo estruturado para gestão de riscos em projetos: estudo de múltiplos casos*. Tese de Doutoramento, Universidade de São Paulo, 2005. 14, 21, 26

[33] ISO, ABNT NBR: *Iec 31010-2012: Gestão de riscos-técnicas para o processo de avaliação de riscos*. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2012. 14, 15, 32, 34

[34] Ramírez Castro, Alexandra e Zulima Ortiz Bayona: *Gestión de riesgos tecnológicos basada en iso 31000 e iso 27005 y su aporte a la continuidad de negocios*. Ingeniería, 16(2), 2011. 14, 15, 21, 35, 67, 78

[35] Aven, Terje: *Selective critique of risk assessments with recommendations for improving methodology and practise*. Reliability Engineering & System Safety, 96(5):509–514, 2011. 14

[36] Pereira, Cristiano e Carlos Ferreira: *Identificação de práticas e recursos de gestão do valor das ti no cobit 5*. RISTI-Revista Ibérica de Sistemas e Tecnologias de Informação, (15):17–33, 2015. 15

[37] Fischer, Urs: *Identify, govern and manage it risk (part 1): Risk it based on cobit objectives and principles*. ISACA Journal, 4:29–31, 2009. 17

[38] Babb, S, E Anton, J Bleicher, S Reznik, G Rouissi e A Tuteja: *Cobit 5 for risk*, 2013. 17, 18, 19

[39] Nolan, Richard e F Warren McFarlan: *Information technology and the board of directors*. Harvard business review, 83(10):96, 2005. 19

[40] Ramos, Luciano Helou *et al.*: *Avaliação e resposta ao risco de ti na prevenção de fraudes no sistema de transporte público coletivo do distrito federal*. 2018. 19, 20

[41] ISACA: *Cobit 5*. ISA, 2012, ISBN 1604202378, 9781604202373. 20, 82, 85, 87, 96, 98, 99

[42] Westerman, George e Richard Hunter: *IT risk: turning business threats into competitive advantage*. Harvard Business School Press Boston, 2007. 20

[43] Magalhães, Andréa, Cláudia Cappelli, Fernanda Baião, Flávia Santoro, Hadeliane Iendrike, RM Araujo e VT Nunes: *Uma estratégia para gestão integrada de processos e tecnologia da informação através da modelagem de processos de negócio em organizações*. Revista Cientefico–Faculdade Ruy Barbosa, páginas 45–53, 2007. 20

[44] Chaves, Sidney: *A questão dos riscos em ambientes de computação em nuvem*. Tese de Doutoramento, Universidade de São Paulo, 2011. 20

[45] Barbosa, Guilherme Eduardo da Cunha: *Reengenharia de sistemas na recuperação e modernização de produtos: proposta de um modelo baseado em risco*. Tese de Doutoramento, Universidade de São Paulo, 2015. 20

[46] Arnold, Robert S: *Common risks of reengineering*. IEEE Computer Society Reverse Engineering Newsletter, páginas 1–2, 1992. 21

[47] Rosa, Germano Mendes e José Carlos de TOLEDO: *Gestão de riscos e a norma iso 31000: importância e impasses rumo a um consenso*. Em *Anais do V Congresso Brasileiro de Engenharia de Produção*, páginas 18–41, 2015. 22

[48] Clarke, Paul e Rory V O'Connor: *The situational factors that affect the software development process: Towards a comprehensive reference framework*. Information and Software Technology, 54(5):433–447, 2012. 22

[49] Casher, Jonathan D: *How to control risk and effectively reduce the chance of failure*. Management review, 73(6):50–54, 1984. 22

[50] Boehm, Barry W.: *Software risk management: principles and practices*. IEEE software, 8(1):32–41, 1991. 22

[51] Lyytinen, Kalle, Lars Mathiassen e Janne Ropponen: *Attention shaping and software risk—a categorical analysis of four classical risk management approaches*. Information Systems Research, 9(3):233–255, 1998. 22

[52] Ropponen, Janne e Kalle Lyytinen: *Components of software development risk: How to address them? a project manager survey*. IEEE transactions on software engineering, 26(2):98–112, 2000. 23

[53] Barki, Henri, Suzanne Rivard e Jean Talbot: *An integrative contingency model of software project risk management*. Journal of management information systems, 17(4):37–69, 2001. 23

[54] Leopoldino, Cláudio Bezerra: *Avaliação de riscos em desenvolvimento de software.* 2004. 23

[55] Redwine, Samuel T: *Software assurance: A guide to the common body of knowledge to produce, acquire and sustain secure software, version 1.1.* US Department of Homeland Security, Washington, DC, 2006. 23, 24

[56] Benaroch, Michel e Ajit Appari: *Financial pricing of software development risk factors.* IEEE software, 27(5):65–73, 2010. 24

[57] Wallace, Linda e Mark Keil: *Software project risks and their effect on outcomes.* Communications of the ACM, 47(4):68–73, 2004. 24

[58] Cervo, Amado Luiz: *Metodologia científica/amado luiz cervo, pedro alcino bervian, roberto da silva.-*, 2007. 25

[59] Ruy, Marcelo: *Aprendizagem organizacional no processo de desenvolvimento de produtos: estudo exploratório em três empresas manufatureiras. 2002. 131 p.* Tese de Doutoramento, Dissertação (Mestrado em Engenharia de Produção). Departamento de Engenharia de Produção. Universidade Federal de São Carlos, São Carlos, 2002. 25

[60] Fonseca, João José Saraiva: *Metodologia da pesquisa científica.* 2002. 25, 26

[61] Gil, Antonio Carlos: *Métodos e técnicas de pesquisa social.* 6. ed. Ediitora Atlas SA, 2008. 26

[62] Silva, EL e EM Menezes: *Metodologia da pesquisa e elaboração de dissertação: Ufsc*, 2005. 26

[63] Business Analysis, International Institute of: *A Guide to the Business Analysis Body of Knowledge (BABOK Guide), Version 2.0.* International Institute of Business Analysis, 2009. 30, 31

[64] Espinha, Rafael de Souza Lima: *Uma Abordagem para a Avaliação de Processos de Desenvolvimento de Software Baseada em Risco e Conformidade.* Tese de Doutoramento, PUC-Rio, 2007. 31, 32, 33, 34, 89, 90

[65] Brasil, TRT3: *Avaliação dos riscos dos ativos de infraestrutura do sistema pje - produção*, nov 2017. `https://portal.trt3.jus.br/internet/conheca-o-trt/gestao-estrategica/gestao_de_riscos/downloads/2017.11.24_Relatorio_de_Analise_de_Riscos_Ativos_PJe.pdf`. 33

[66] Brasil, Exército Brasileiro, Secretaria Geral do Exército: *Portaria nº 295-eme - diretriz de racionalização administrativa do exército brasileiro (eb20d-01.016).* Boletim do Exército 1/2015, 2015. 38, 39

[67] BRASIL: *Regulamento do conselho superior de tecnologia da informaÇÃo contiex eb10-r-09.001.* Exército Brasileiro, páginas 16–22, 2013. 39, 40, 41

[68] Brasil, Exército Brasileiro, Secretaria Geral do Exército: *Portaria 233-eme - concepção estratégica de tecnologia da informação*. Boletim do Exército 13/2014, páginas 11–20, 2014. 39, 40, 42

[69] Brasil, Exército Brasileiro, Secretaria Geral do Exército: *Plano estratÉgico do exÉrcito 2016-2019*. Boletim Especial do Exército 6/2017, 2017. 40, 41, 46

[70] FERNANDES, Aguinaldo A e Vladimir F ABREU: *Nbr iso/iec 38500: 2009: Governança corporativa de tecnologia da informação*. Rio de Janeiro, Associação Brasileira de Normas Técnicas, 2009. 41

[71] Calder, Alan: *ISO/IEC 38500: the IT governance standard*. IT Governance Ltd, 2008. 41

[72] Brasil, Ministério do Planejamento, Orçamento e Gestão. Secretaria de Logística e Tecnologia da Informação.: *Instrução normativa slti 04, de 19 de maio de 2008.* 41

[73] Brasil, Exército Brasileiro, Secretaria Geral do Exército: *Portaria nº 169-dgp - regimento interno do departamento-geral do pessoal (eb30-ri-10.001)*. Separata ao Boletim do Exército 33/2017, 2017. 43, 50, 113

[74] Brasil: *Portaria n º 004, de 3 de janeiro de 2019 - aprova política de gestão de riscos do exército brasileiro (eb10-p-01.004)*. Relatório Técnico, Exército Brasileiro, 2019. 44, 64

[75] De Haes, Steven e Wim Van Grembergen: *Analysing the relationship between it governance and business/it alignment maturity*. Em *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)*, páginas 428–428. IEEE, 2008. 46

[76] Exército Brasileiro, Departamento de Ciência e Tecnologia: *Manual Técnico para Metodologia de Desenvolvimento de Software do Exército*, 2012. 54, 55

[77] Brasil, Exército Brasileiro, Secretaria Geral do Exército: *Portaria 508 - instruções gerais do ciclo de vida de software (eb10-ig-01.006)*. Boletim do Exército 26/2013, páginas 13–22, 2013. 54, 55

[78] Neto, Américo Alexandre Ribeiro: *Gerenciamento de riscos e a eficiência nas atividades do conformador de registro de gestão no exército brasileiro*. 2018. 64

[79] Brasil, Exército Brasileiro, Departamento Geral de Pessoal: *Ações, programas e projetos*, dec 2018. `http://www.dgp.eb.mil.br/images/img_institucional/pdf/acoes_e_programas.pdf`. 65

[80] Casquinha, Paula Sofia Ricardo *et al.*: *Gestão de riscos: análise de impacto no negócio*. Tese de Mestrado, 2014. 70

[81] Lima, Ana Cristina Fernandes: *Ferramenta de gestão de riscos aplicada a ambientes de desenvolvimento de software com foco na garantia da qualidade do produto*. Dissertação de mestrado, Universidade de Brasília, 2019. 86

[82] Mendonça, Jônatas Medeiros de e Rodrigo Medeiros Soares da Silva: *Técnicas de usabilidade e testes automatizados em processos de desenvolvimento de software empírico*. Universidade de Brasília, Brasília, Distrito Federal, 2014. 88

[83] Martin, Robert C.: *The test bus imperative: Architectures that support automated acceptance testing*. 2005. `http://www.martinfowler.com/ieeeSoftware/testBus.pdf`. 88

[84] Haring, Ronald: *Behavior driven development-behavior driven development (bdd) is geen nieuw framework of een compleet nieuwe methodiek voor software development. het is een collectie van bestaande technieken die gericht is op het opstellen van duidelijke testcases die zowel door developers als gebruikers wordt begrepen. deze bestaande technieken zijn voornamelijk afkomstig van test driven development (tdd) en domain driven design/development. volgens ronald haring is bdd een betere versie van test driven development.* Java Magazine, (1):14, 2011. 88

[85] Riekstin, Ana Carolina: *Modelo de governança de tecnologia da informação do escritório ao chão de fábrica.* Tese de Doutoramento, Universidade de São Paulo, 2012. 96

[86] Cruz, Fábio: *Scrum e PMBOK unidos no Gerenciamento de Projetos*. Brasport, 2013. 99

[87] Bentley, Colin: *Prince2: a practical handbook*. Routledge, 2012. 99

[88] Steinberg, RA *et al.*: *Itil service operation 2011 edition*. TSO, London, 2011. 101

[89] Haren, Van: *Togaf version 9.1 a pocket guide*. 2011. 101

Apêndice A

Estrutura Organizacional da TI do DGP

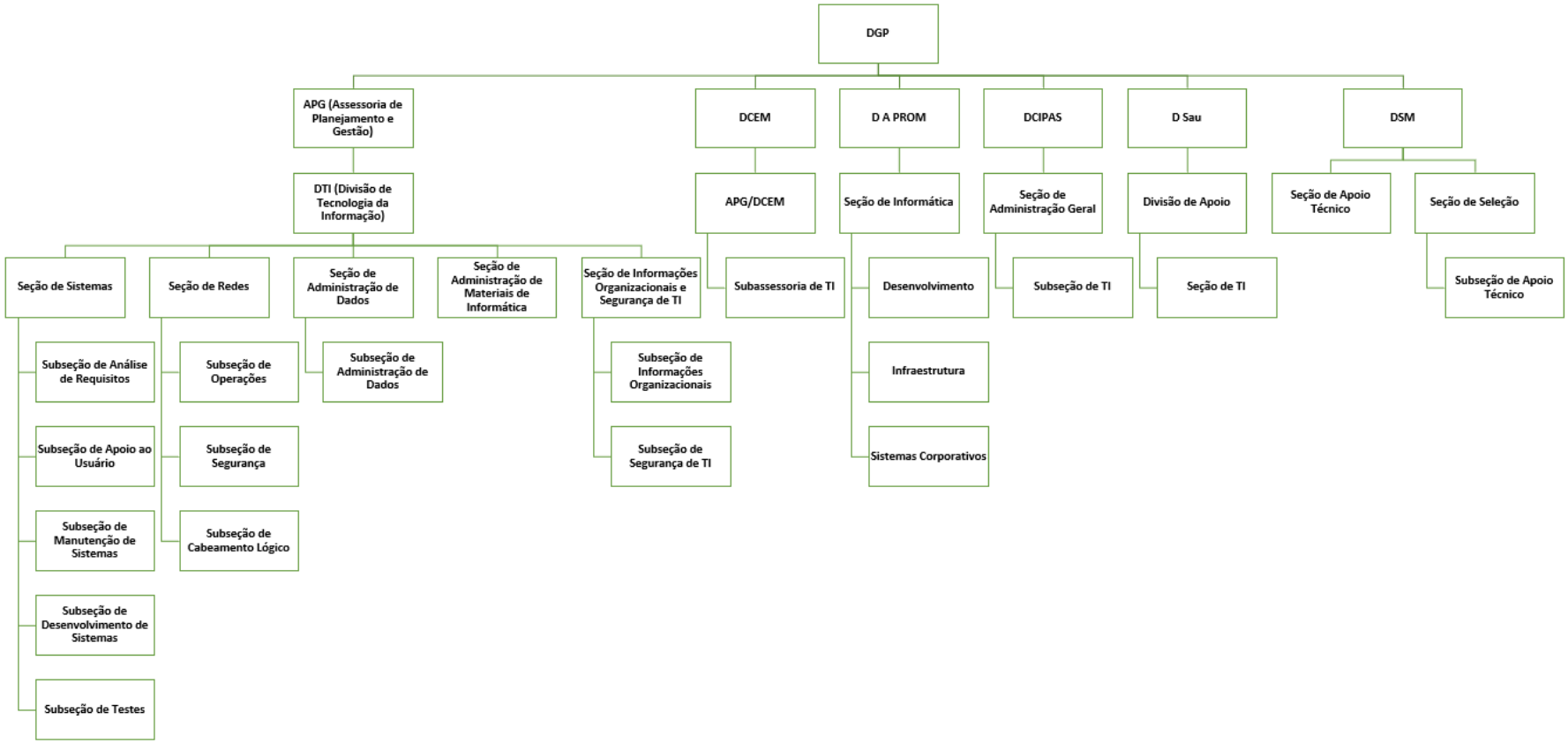


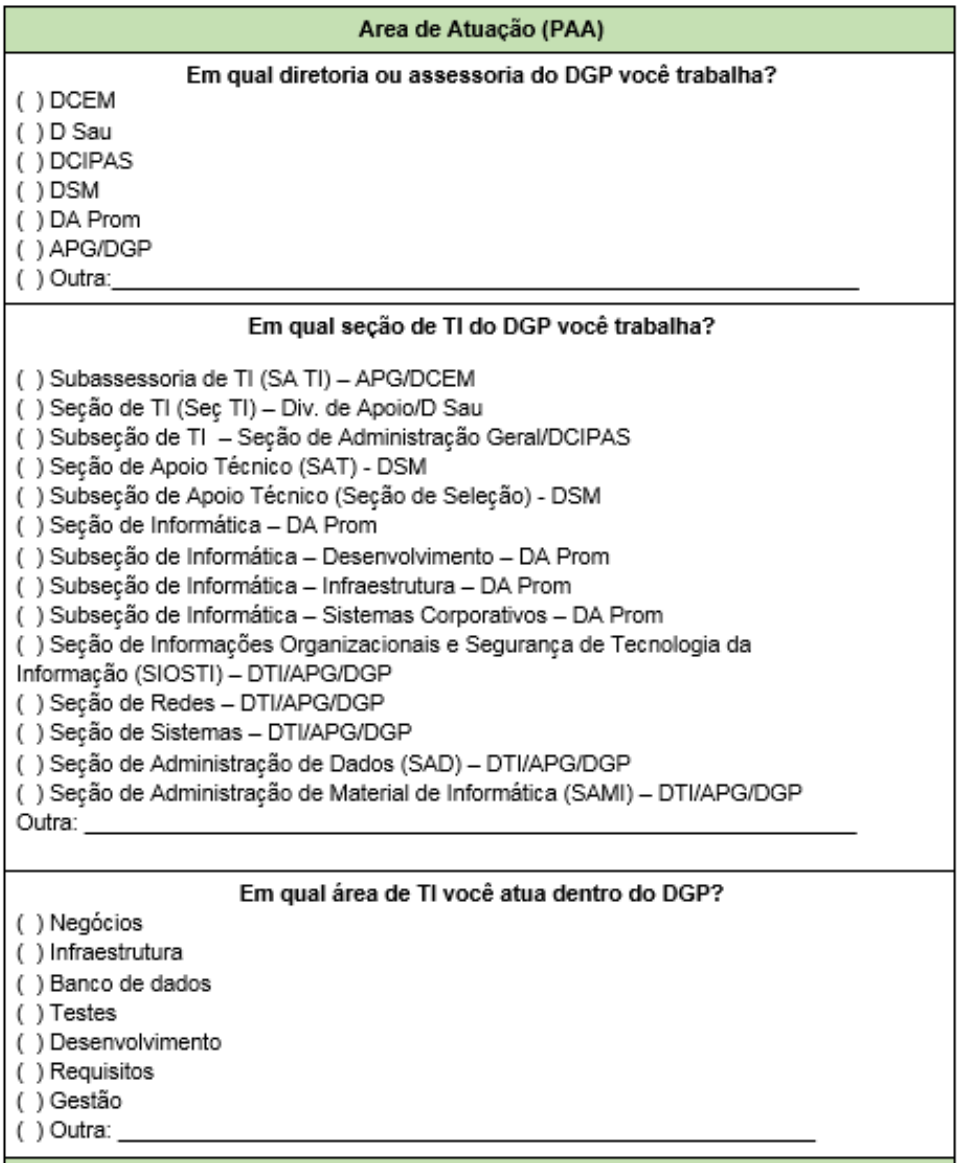
Figura A.1: Estrutura Organizacional de TI do DGP
Elaborado pelo autor com base nos regimentos internos da organização [73].

Apêndice B

Questionário de Perfil de Profissional de TI

Este instrumento faz parte da coleta de dados para o diagnóstico de TI, e tem como objetivo auxiliar no entendimento do perfil do profissional de TI do DGP, levantando informações sobre áreas de atuação (negócios, requisitos, programação, gestão, testes, etc.) e o conhecimento das tecnologias que dominam para realizar a comparação com as principais tecnologias utilizadas nos sistemas do DGP.

B.1 Área de Atuação



Area de Atuação (PAA)

Em qual diretoria ou assessoria do DGP você trabalha?

( ) DCEM
( ) D Sau
( ) DCIPAS
( ) DSM
( ) DA Prom
( ) APG/DGP
( ) Outra:_____

Em qual seção de TI do DGP você trabalha?

( ) Subassessoria de TI (SA TI) – APG/DCEM
( ) Seção de TI (Seç TI) – Div. de Apoio/D Sau
( ) Subseção de TI – Seção de Administração Geral/DCIPAS
( ) Seção de Apoio Técnico (SAT) - DSM
( ) Subseção de Apoio Técnico (Seção de Seleção) - DSM
( ) Seção de Informática – DA Prom
( ) Subseção de Informática – Desenvolvimento – DA Prom
( ) Subseção de Informática – Infraestrutura – DA Prom
( ) Subseção de Informática – Sistemas Corporativos – DA Prom
( ) Seção de Informações Organizacionais e Segurança de Tecnologia da Informação (SIOSTI) – DTI/APG/DGP
( ) Seção de Redes – DTI/APG/DGP
( ) Seção de Sistemas – DTI/APG/DGP
( ) Seção de Administração de Dados (SAD) – DTI/APG/DGP
( ) Seção de Administração de Material de Informática (SAMI) – DTI/APG/DGP
Outra: _____

Em qual área de TI você atua dentro do DGP?

( ) Negócios
( ) Infraestrutura
( ) Banco de dados
( ) Testes
( ) Desenvolvimento
( ) Requisitos
( ) Gestão
( ) Outra: _____

Figura B.1: Área de Atuação
Fonte: Elaborado pelo autor.

B.2 Experiência

Experiência (PE)
Há quanto tempo você trabalha na TI do DGP? ( ) Menos de 1 ano ( ) 1 a 3 anos ( ) 3 a 5 anos ( ) 5 a 7 anos ( ) Mais de 7 anos
Você já trabalhou em outras unidades de TI do Exército? ( ) Não ( ) Sim Se sim, qual(is)? _____ _____
Se a resposta da PE2 foi sim, você trabalhou durante quanto tempo em outras unidades de TI do Exército? ( ) Menos de 1 ano ( ) 1 a 3 anos ( ) 3 a 5 anos ( ) 5 a 7 anos ( ) Mais de 7 anos
Você já programou em alguma linguagem de programação? ( ) Não ( ) Sim
Se a resposta da PE4 foi sim, durante quanto tempo você programou nessa(s) linguagem(ns) de programação? ( ) Menos de 1 ano ( ) 1 a 3 anos ( ) 3 a 5 anos ( ) 5 a 7 anos ( ) Mais de 7 anos
Você já trabalhou com algum framework de linguagem de programação? ( ) Não ( ) Sim
Se a resposta da PE6 foi sim, durante quanto tempo você trabalhou com esse(s) framework(s)? ( ) Menos de 1 ano ( ) 1 a 3 anos ( ) 3 a 5 anos ( ) 5 a 7 anos ( ) Mais de 7 anos
Você já trabalhou com alguma ferramenta de banco de dados? ( ) Não ( ) Sim
Se a resposta da PE8 foi sim, durante quanto tempo você trabalhou com essa(s) ferramenta(s) de banco de dados? ( ) Menos de 1 ano ( ) 1 a 3 anos ( ) 3 a 5 anos ( ) 5 a 7 anos ( ) Mais de 7 anos

Figura B.2: Experiência
Fonte: Elaborado pelo autor.

B.3 Conhecimento Técnico

1. Em quais linguagens de programação você possui conhecimento? Nível básico, intermediário, avançado? Possui certificação?
2. Em quais *frameworks* de linguagem de programação você possui conhecimento?
3. Em quais Sistemas de Gerenciamento de Banco de Dados (SGBD) você possui conhecimento?
4. Em quais métodos de desenvolvimento de software você possui conhecimento?
5. Em quais *frameworks* de Governança de TI você possui conhecimento?
6. Em quais modelos de gestão de riscos você possui conhecimento?

B.4 Formação

1. Qual a sua patente na Organização militar?
2. Quais cursos de TI você já realizou?
3. Quais cursos de TI dentro da Organização Militar você já realizou?
4. Qual curso de graduação concluiu?
5. Possui pós-graduação lato-senso (especialização)?
6. Possui pós-graduação stricto-senso (mestrado e doutorado)?
7. Qual a sua forma de ingresso na Organização Militar?

Apêndice C

Lista de ameaças

- FR01 - Distribuição incorreta de recursos alocados para o projeto, prejudicando o andamento das atividades da organização e dos projetos.
- FR02 - Utilização de recursos em atividades e insumos que não agregam valor à organização, aos seus projetos e aos produtos desenvolvidos.
- FR03 - Definição indevida de prioridades, ou seja, identificação incorreta de necessidades, fazendo com que componentes prioritários sejam desenvolvidos tardiamente e que tarefas sejam acompanhadas de forma incorreta.
- FR04 - Descumprimento do orçamento. O montante financeiro previsto para a conclusão do projeto ou entrega do produto tende a ser ultrapassado.
- FR05 - Descumprimento de prazo. O tempo previsto para a conclusão do projeto ou entrega do produto tende a ser desobedecido.
- FR06 - Desestabilização do projeto. Atividades e tarefas do projeto não são executadas conforme o planejado.
- FR07 - Problemas no acompanhamento do Projeto. Dificuldades no acompanhamento da execução das atividades e tarefas do projeto.
- FR08 - Definição imprópria de papéis e responsabilidades.
- FR09 - Insatisfação do Cliente. Produto não atende às expectativas e necessidades do cliente.
- FR10 - Interesses divergentes dentro da organização.
- FR11 - Problemas de comunicação entre os interessados. Comunicação ineficiente entre os interessados no projeto, gerando inconsistências, consumindo recursos dos projetos e dificultando o trabalho colaborativo.

- FR12 - Conflito entre os participantes da organização ou do projeto.
- FR13 - Falta de alinhamento da organização à implantação de processos de software.
- FR14 - Equipes diferentes de desenvolvimento não quererem executar o processo da mesma forma.
- FR15 - Resistência das equipes desenvolvedoras em utilizar o processo.
- FR16 - Processo com baixa eficiência. Problemas técnicos na execução do processo consomem mais recursos para a realização das tarefas e o desenvolvimento do produto.
- FR17 - Retrabalho inútil. Despender tempo em atividades que serão refeitas ou executar ou executar o mesmo trabalho mais de uma vez, indicando um ponto de desperdício de recursos.
- FR18 - Falta de metodologia/processo de desenvolvimento.
- FR19 - Existência de requisitos incompletos, inconsistentes, inválidos, incorretos ou não verificáveis que impedem a correta implementação.
- FR20 - Requisitos mudam com frequência.
- FR21 - Escopo e os objetivos do projeto mudam constantemente.
- FR22 - Os requisitos são mal entendidos.
- FR23 - Falha em obter comprometimento do cliente / fornecedores de requisitos.
- FR24 - Implementação do produto não atende aos projetos do produto. Inconsistência entre o que foi projetado e o que foi desenvolvido pelo projeto.
- FR25 - Limitações técnicas. Barreiras técnicas no desenvolvimento do sistema que limitam algumas das funcionalidades ou até mesmo tornando impossível a realização de sua definição primária.
- FR26 - Utilização de Ferramentas impróprias.
- FR27 - Perda de controle sobre os itens de configuração modificados. Alterações nos itens de configuração (ambiente de desenvolvimento, versões de artefatos, baselines) acontecem de forma desestruturada.
- FR28 - Falha de Software. Código ineficaz, fora de especificação, incompatível com outros módulos de software ou hardware, ou falhas provocadas por parâmetros configurados indevidamente.
- FR29 - Baixa qualidade dos produtos desenvolvidos.

- FR30 - Dificuldade de integração dos componentes do software.
- FR31 - Ineficiência na implementação ou controle de solicitações de mudança.
- FR32 - Baixa manutenabilidade dos produtos gerados no desenvolvimento do software.
- FR33 - A aplicação do software é obsoleta. Por exemplo: tecnologia antiga, com má documentação, de manutenção custosa, difícil de entender, não integrada na atual arquitetura.