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

Análise da maturidade em gestão de riscos no MP: proposição e aplicação de um instrumento de avaliação orientado aos processos de TI

Bruno Fassheber Novais

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

Orientadora
Prof.ª Dr.ª Ana Carla Bittencourt Reis

Brasília
2016

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

FN935a

Fassheber Novais, Bruno
Análise da maturidade em gestão de riscos no MP: proposição e aplicação de um instrumento de avaliação orientado aos processos de TI / Bruno Fassheber Novais; orientador Ana Carla Bittencourt Reis. -- Brasília, 2016.
123 p.

Dissertação (Mestrado - Mestrado Profissional em Computação Aplicada) -- Universidade de Brasília, 2016.

1. Riscos. 2. Modelo de Maturidade. 3. ISO 31000. 4. Governança de TI. I. Carla Bittencourt Reis, Ana, orient. II. Título.

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

Análise da maturidade em gestão de riscos no MP: proposição e aplicação de um instrumento de avaliação orientado aos processos de TI

Bruno Fassheber Novais

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

Prof.ª Dr.ª Ana Carla Bittencourt Reis (Orientadora)
EPR/UnB

Prof. Dr. Clóvis Neumann
EPR/UnB

Dr. Sérgio Assis Rodrigues
Universidade Federal do Rio de Janeiro

Prof. Dr. Marcelo Ladeira
Coordenador do Programa de Pós-graduação em Computação Aplicada

Brasília, 13 de julho de 2016

Dedicatória

Aos meus filhos pela paciência e compreensão e a minha querida esposa Jeane Duarte que sempre me confortou e incentivou em todos os momentos com bastante carinho e amor, dedico-lhes essa conquista com gratidão.

Agradecimentos

Agradeço primeiramente a Deus, por ter me dado esta oportunidade de crescimento profissional e pessoal. Agradeço ainda aos meus pais, Alonso Novais Ferro *in memoriam* e Ione Fassheber Novais, pela educação dada ao longo dos anos. À minha esposa Jeane Rocha Duarte pela paciência, compreensão e estímulo durante o curso. Ao Sr, Eduardo Cesar Soares Gomes, Diretor de TI do Ministério do Planejamento, por acreditar e incentivar este projeto. Ao meu chefe, Marco Fragoso, pelo apoio e compreensão. Ao colega Orlando Oliveira dos Santos, pelos inúmeros conselhos e palavras de encorajamento. Agradeço ainda a todos os colegas do curso que de alguma forma me apoiaram, sendo eles professores e alunos. Um agradecimento especial a minha orientadora Prof.ª Dr.ª Ana Carla Bittencourt Reis, pela confiança, paciência e capacidade que me trouxe até o fim desta jornada.

Resumo

Muitas organizações estão engajadas na adoção de abordagens consistentes e holísticas para a Gestão de Riscos. O aprimoramento da Gestão de Riscos nas instituições públicas se deve, inclusive, pela atuação recente dos órgãos de controle, quando intensificaram ações de auditoria voltadas para riscos. Um fator relevante para o sucesso da Gestão de Riscos é a obtenção, pela organização, de uma avaliação dos processos nos quais serão tratados os riscos. Para atender a falta de um instrumento de avaliação em Gestão de Riscos para o setor público é proposto o desenvolvimento de um Instrumento de Avaliação da Maturidade em Gestão de Riscos (IAMGR) orientado aos processos de Tecnologia da Informação (TI), baseado no processo de Gestão de Riscos da Norma ISO 31000:2009. A abordagem da pesquisa é "Qualitativa". Quanto à estratégia de pesquisa, foi utilizada a "Pesquisa-Ação", pois há a proposição do instrumento e a sua aplicação no Ministério do Planejamento, Desenvolvimento e Gestão (MP). Já as técnicas utilizadas para a coleta de dados foram: revisão bibliográfica, análise documental e técnica Delphi. O IAMGR é voltado para o setor público brasileiro e pode ser aplicado em qualquer instituição independente do tamanho e do estágio de maturidade em Gestão de Riscos, considerando os processos tratados no instrumento. Os níveis de maturidade propostos vão desde as organizações totalmente imaturas na área de riscos, até as que se encontram em estágio avançado de maturidade. Uma ferramenta automatizada foi desenvolvida para aplicação do instrumento, facilitando a autoavaliação. Com o intuito de validar o instrumento, foi feita uma aplicação na Diretoria de Tecnologia de Informação (DTI) do MP. Como resultado foram identificados os níveis de maturidade em Gestão de Riscos de 11 (onze) processos de TI, sendo que o nível de maturidade em gestão de riscos alcançado pelo órgão foi "Vulnerável". Com isso, conclui-se que a organização não tem, ainda, uma metodologia de gestão de riscos estável e organizada e não há nenhuma evidência de que a gestão de riscos atual possa apoiar a tomada de decisão. A DTI do MP afirma que o uso do IAMGR fortaleceu a cultura de riscos no órgão e tem contribuído para o aprimoramento da governança de TI.

Palavras-chave: Riscos, Modelo de Maturidade, ISO 31000, Governança de TI

Abstract

Many organizations are engaged in the adoption of consistent approaches and holistic for Risk Management. The improvement of risk management in public institutions whether even the recent actions of regulatory agencies, when intensified audit of actions for risk. An important factor for success Management Risks is to obtain, by the organization, an evaluation of the processes which will be treated risks. To meet the lack of an evaluation instrument in Management Risks to the public sector is proposed the development of an Assessment Tool Maturity in Risk Management, named as IAMGR, oriented to technology processes Information based on the risk management process of ISO 31000: 2009. The Research approach is "qualitative". As the search strategy was used "Action Research", because there is the instrument of the proposal and its implementation in the Ministry of Planning, Development and Management (MP). As for the techniques used for collection Data were: literature review, document analysis and Delphi technique. The IAMGR It is facing the Brazilian public sector and can be applied in any institution regardless of size and maturity stage in risk management, considering the cases dealt with in the instrument. The proposed maturity levels ranging from Immature organizations fully in risk area, to those found in stage advanced maturity. An automated tool has been developed for application instrument, facilitating self-assessment. In order to validate the instrument, It was made an application to the Directorate of Information Technology (DTI) of the MP. As result maturity levels have been identified in Risk Management 11 (eleven) IT processes, and the level of maturity in risk management achieved by the body It was "vulnerable". Thus, it is concluded that the organization has also a methodology stable and organized risk management and there is no evidence that the management current risks to support decision making. The DTI-MP states that the use of IAMGR strengthened risk culture in the body and has contributed to the improvement IT governance.

Keywords: Risk, Maturity Model, ISO 31000, IT Governance

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

APF Administração Pública Federal. 1–4, 8, 30, 44

CGSTI Contratação e Gestão de Soluções de TI. ix, xi, xii, 44, 47, 52, 57, 59, 99, 100, 103, 106

CGU Controladoria Geral da União. 1

COBIT *Control Objectives for Information and related Technology.* viii, xii, 1, 12, 27, 29, 30, 41, 45–49, 52, 86

COSO *Committee of Sponsoring Organizations of the Treadway Comission.* x, 8, 21

DTI Diretoria de Tecnologia de Informação. v, 4, 5, 36, 80–83, 95, 99, 102, 106, 108

FCTI Funcionamento dos Comitês de TI. viii, xi, xii, 44, 45, 49, 56, 59, 88, 89, 102, 103

GESPUBLICA Programa Nacional de Gestão Pública e Desburocratização. 8, 45, 53, 54, 83

GPeTI Gestão de Pessoal de TI. ix, xi, xii, 44, 47, 51, 57, 59, 97, 98, 103

GPTI Gerenciamento de Projetos de TI. viii, xi, xii, 44, 46, 50, 57, 58, 91, 92, 102, 103

GSTI Gerenciamento de Serviços de TI. viii, xi, xii, 44, 46, 50, 57, 58, 93, 94, 102, 103

IAMGR Instrumento de Avaliação da Maturidade em Gestão de Riscos. v, ix, 5, 6, 34–36, 40, 42, 43, 52–55, 60, 61, 68, 69, 73, 76, 81, 83, 91, 103, 106, 107

IBGC Instituto Brasileiro de Governança Corporativa. 12

IN Instrução Normativa. 47, 52, 99, 100

ITIL *Information Technology Infrastructure Library.* 46, 93, 95

MDTI Monitoração do Desempenho da TI. ix, xi, xii, 44, 48, 52, 58, 59, 100–103

MEGP Modelo de Excelência em Gestão Pública. 53

MP Ministério do Planejamento, Desenvolvimento e Gestão. v, xiii, 2–6, 34–36, 44, 47, 52, 55, 75, 77–83, 86, 88, 90, 95, 99–101, 103, 108

OTI Orçamentário de TI. viii, xi, xii, 44, 46, 49, 56, 58, 89, 103

PEI Planejamento Estratégico Institucional. viii, x, xii, 44, 45, 48, 49, 56, 58, 83–85, 103

PES Processo de Entrega de Solução. 90, 91

PETI Planejamento Estratégico de TI. viii, xi, xii, 44, 45, 49, 56, 58, 81, 86, 87, 103

PMBOK Guia do Conjunto de Conhecimentos em Gerenciamento de Projetos. 7, 30, 46, 50, 91, 92, 110

PNQ Prêmio Nacional de Qualidade. xii, 53, 54, 59, 60

POSIC Política de Segurança da Informação e Comunicação. 97

PS Processo de Software. viii, xi, xii, 44, 46, 50, 56, 58, 90, 91, 102, 103

SI Segurança da Informação. viii, xi, xii, 44, 46, 51, 57, 59, 95, 96, 103

SISP Sistema de Administração dos Recursos de Tecnologia da Informação. 3, 36, 47, 79, 99, 108

STI Secretaria de Tecnologia de Informação. 3, 36, 47, 79, 99, 100, 108

TCU Tribunal de Contas da União. vii, 1–3, 12, 25, 30, 36, 44–48, 53, 54, 60, 66

TI Tecnologia da Informação. v, 1–5, 11–13, 16, 25–27, 29, 36, 44, 45, 48–50, 52, 55, 69, 75, 80–83, 88, 90–93, 95, 97, 102, 107, 108

Capítulo 1

Introdução

1.1 Contextualização

Ao longo das últimas décadas, o setor público, de um modo geral, tem sofrido grande pressão para melhorar seu desempenho na governança de Tecnologia da Informação (TI), por meio do poder de fiscalização exercido pelos órgãos de controle externo: Tribunal de Contas da União (TCU) e Controladoria Geral da União (CGU), o que tem levado muitas organizações a buscarem as melhores práticas no mercado [48].

Com o objetivo de induzir a melhoria da governança de TI na Administração Pública Federal (APF), o TCU criou um índice, por meio do Acórdão 2.308/2010-TCU-Plenário [47], que busca refletir, de forma geral, a situação de governança de TI de cada organização avaliada, denominado de índice de Governança de TI - iGovTI. É realizado bienalmente um levantamento de informações da Governança de TI nos órgãos sob sua jurisdição, que tem como objetivo subsidiar o controle e o aperfeiçoamento da governança da TI na APF, com vistas à garantia de que a TI agrega valor ao negócio institucional de cada unidade jurisdicionada, com riscos mitigados e aceitáveis [48].

A Governança de TI é de responsabilidade da autoridade máxima do órgão e é parte integral da Governança Corporativa. Ela é formada pela liderança, estruturas organizacionais e processos que garantem que a área de TI sustenta e melhora a estratégia e objetivos da organização [26]. Sendo assim, a Governança de TI está voltada ao reconhecimento do valor da TI para o Negócio, fazendo com que sua implantação, seu entendimento e o gerenciamento dos riscos que envolvem a tecnologia da informação, possam ser explorados a fim de colaborar para a organização e controle das atividades internas a fim de garantir a melhoria continua dos serviços prestados e efetividade estratégica da corporação.

Autores como Giampaoli [22], Bakry e Bin-Abbas [9] descrevem o *Control Objectives for Information and related Technology* (COBIT) como o principal norteador para alcançar a Governança de TI. Além disso, o TCU utiliza este guia de boas práticas nas auditorias

sobre o tema. Cabe destacar que este guia apresenta a Gestão de Riscos como um dos focos da governança de TI.

Com uma abordagem mais específica, o TCU incluiu, no seu Plano Estratégico do Tribunal – PET 2011 – 2015 [31], um objetivo voltado para "Intensificar ações que promovam a melhoria da gestão de riscos e controles internos da Administração Pública".

Dessa forma, a gestão de riscos de TI é entendida como fator crítico de sucesso para que a organização atinja seus objetivos [22]. No entanto, somente isto não é suficiente. Faz-se necessário conhecer o quão eficiente está sendo o processo de gestão de riscos em uma organização [4]. Essa eficiência do processo de gestão de riscos é denominada como maturidade em gestão de riscos [4].

A seguir será apresentada a análise de contexto realizada com base nas orientações da Norma ISO 31000 [16], o qual define contexto como: definição dos parâmetros externos e internos a serem levados em consideração ao gerenciar riscos, e estabelecimento do escopo e critérios de riscos.

No caso do contexto externo, o TCU realizou, em 2013, um levantamento para avaliar a maturidade da gestão de riscos na APF Indireta e identificou um baixo nível de maturidade do processo em gestão de riscos, inclusive indicou possível negligência quanto à sua importância [49]. Tal levantamento incluiu 65 entidades e permitiu constatar que apenas 21,5% dessas entidades participantes apresentam nível de maturidade aprimorado ou avançado, enquanto 53,8% encontram-se nos estágios inicial e básico.

Já no contexto interno, o Ministério do Planejamento, Desenvolvimento e Gestão (MP) recebeu duas recomendações do TCU em auditoria realizada no ano de 2012. A primeira recomendação foi que o órgão estabeleça e normatize a obrigatoriedade de a Alta Administração implantar uma estrutura de controles internos mediante a definição de atividades de controle em todos os níveis da organização para mitigar os riscos de suas atividades, envolvendo atividades relacionadas a TI. Já a segunda recomendação foi para criar ações voltadas à disseminação de metodologia de gestão de riscos nos órgãos do Poder Executivo, com a finalidade de desenvolver instrumentos de avaliação da maturidade de gestão de riscos apropriados a esse segmento da administração [48].

O TCU é categórico quando afirma que a sua pretensão ao mensurar o grau de maturidade de cada entidade em gestão de riscos, é fornecer aos gestores informações sobre os possíveis pontos de melhoria nessa área, bem como acompanhar sua evolução ao longo do tempo [48].

1.2 Motivação

A importância em estabelecer a gestão de riscos é evidenciada por ações como, por exemplo, atividades de controle para mitigar os riscos nos processos envolvendo a área de TI, os quais foram proferidos pelo TCU ao MP. O Acórdão 1.233/2012-TCU [48] cita o estabelecimento e a normatização de atividades de controle para mitigar os riscos em processos de TI. Para tanto, o TCU indicou os processos de TI, fornecendo um direcionamento claro na atuação dos órgãos de controle. Além disso, o fato de um órgão da APF receber uma recomendação de um órgão de controle, como o TCU, significa que ele fica obrigado a cumprir a determinação, podendo inclusive ser penalizado por crime de responsabilidade.

Com o intuito de atender às recomendações de órgão de controle, o Ministério do Planejamento, Desenvolvimento e Gestão (MP) formalizou no seu Plano Diretor de Tecnologia da Informação [37] ações voltadas para a institucionalização de processos, como por exemplo: unificar o processo de gestão de solicitações de TI no MP; estruturar o processo de medição de serviços de TI; mapear os processos de serviços de TI; implantar modelo de governança integrada de TI; estruturar o escritório de projetos de TI do MP; implantar processos de gestão do orçamento de TI; implantar procedimento de inventário de ativos de informação; implantar os processos de gestão de configuração, mudanças e incidentes do MP [37]. Vale destacar as ações: implementar e aperfeiçoar o processo de Gestão de Riscos do MP; e instituir processo de compartilhamento das boas práticas de TI do MP com os órgãos do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP).

O MP tem um papel central de orientação do Poder Executivo na área de planejamento e gestão. Acrescenta-se ao papel do MP a atuação como Órgão Central do SISP, por meio da Secretaria de Tecnologia de Informação (STI), na normatização, gestão e coordenação das ações voltadas a TI.

O SISP foi instituído pelo Decreto n. 1.048 de 21 de janeiro de 1994 e atualizado pelo Decreto n. 7.579 de 11 de outubro de 2011. O SISP considera Recursos de Tecnologia da Informação como um conjunto formado pelos bens e serviços de tecnologia da informação que constituem a infraestrutura tecnológica de suporte automatizado ao ciclo da informação, que envolve as atividades de produção, coleta, tratamento, armazenamento, transmissão, recepção, comunicação e disseminação da informação.

Considerando que os processos de TI elencados pelo TCU são de observância nas diversas auditorias realizadas e que o instrumento proposto fornece uma visão do grau de maturidade em gestão de riscos, propõe-se a disponibilização do instrumento à STI a fim de diagnosticar a gestão de riscos dos órgãos sob sua jurisdição.

As diversas ações de institucionalização de processos de TI e a falta de uma estrutura de riscos institucionalizada no MP demonstra uma baixa maturidade em Gestão de Riscos

de TI no órgão [49]. Acredita-se ainda que, por meio da utilização do Instrumento de Avaliação da Maturidade em Gestão de Riscos, a cultura de riscos na organização seja fortalecida.

1.3 Justificativa

A Diretoria de Tecnologia de Informação (DTI) é a área responsável pela TI no MP, inclusive das unidades espalhadas pelo território nacional. A partir do Decreto n. 7.799 de 12 de setembro de 2012, que designou que a DTI passasse a ser vinculada diretamente à Secretaria Executiva houve um fortalecimento da TI na APF. Entre as competências da DTI, destacam-se:

- Planejar, coordenar e controlar as atividades relacionadas à tecnologia da informação no Ministério, efetuadas diretamente ou por meio da contratação de serviços de terceiros;
- Estabelecer padrões, instrumentos e metodologias próprias para o desenvolvimento das atividades da Diretoria;
- Propor a escolha e implementação de metodologias, sistemas, plataformas e bases tecnológicas a serem adotadas pelo Ministério.

Encontra-se em fase de implantação no MP, a ação que implementa e aperfeiçoa o processo de Gestão de Riscos. No final de 2014 a parceria firmada com a Universidade de Brasília (UnB) entregou a metodologia de gestão de riscos ao MP, que, desde então, vem sendo internalizado por meio de um projeto piloto, especificamente em um sistema de uso transversal.

No entanto, apesar de seus esforços, a maturidade em gestão de riscos no órgão ainda é baixa [49]. A falta de um referencial teórico em gestão de riscos e a ausência de controles na implementação dos processos de TI podem levar a unidade entregar um produto sem uma devida análise dos riscos envolvidos [49].

A DTI deseja conhecer o grau de maturidade em gestão de riscos de cada processo de TI, os quais servirão de insumo para tomada de decisão por parte do Gestor de TI, porém atualmente não há um modelo voltado para a Administração Pública.

1.4 Objetivos

1.4.1 Objetivo Geral

O objetivo geral do trabalho é o desenvolvimento de um Instrumento de Avaliação da Maturidade em Gestão de Riscos (IAMGR) orientado aos processos de TI e a identificação do grau de maturidade em Gestão de Riscos no MP.

1.4.2 Objetivos Específicos

1. Identificar os principais normativos que os órgãos de controle levam em consideração na avaliação dos processos de TI, por meio da pesquisa documental, em especial dos relatórios de auditorias;
2. Identificar as questões observadas pelos órgãos de controle em cada processo de TI elencado neste trabalho;
3. Definir um fluxograma para desenvolvimento de um instrumento de avaliação da maturidade em gestão de riscos;
4. Elaborar uma ferramenta para avaliação da maturidade em gestão de riscos; e
5. Aplicar o instrumento proposto na Diretoria de Tecnologia de Informação (DTI) do MP, identificando o grau de maturidade em gestão de riscos, especificamente relacionados aos processos de TI.

1.5 Metodologia de Desenvolvimento do Trabalho

A abordagem da pesquisa é Qualitativa. Gunther [23] reconheceu que diversos atores definem a "pesquisa qualitativa"como uma ciência baseada em textos, ou seja, a coleta de dados produz textos, que nas diferentes técnicas analíticas, são interpretados hermeneuticamente.

A pesquisa qualitativa se dá pelo fato do método não se limitar a um determinado pano de fundo teórico, além de propiciar a análise de pontos de vista subjetivos, coletados com entrevistas semiestruturadas.

Quanto à estratégia de pesquisa, este trabalho se encaixa como “Pesquisa-Ação”, pois há a proposição do instrumento de avaliação e a sua aplicação no MP. Tripp [53] conceitua a pesquisa-ação como toda tentativa continuada, sistemática e empiricamente fundamentada de aprimorar a prática.

As técnicas a serem utilizadas para a coleta de dados são: revisão bibliográfica, análise documental e técnica Delphi.

A seguir será apresentada a organização do trabalho.

1.6 Organização do Trabalho

O trabalho está dividido em seis capítulos. O primeiro capítulo apresenta a contextualização, a motivação, a justificativa e os objetivos do trabalho. O segundo, mostra os principais conceitos em relação ao tema do trabalho. Já o terceiro, trata da revisão de literatura que visa identificar o "estado da arte" em relação a modelo de maturidade em gestão de riscos. O quarto capítulo demonstra o desenvolvimento do Instrumento de Avaliação da Maturidade em Gestão de Riscos. A aplicação do Instrumento no MP está descrita no quinto capítulo. Por fim, o último capítulo apresenta as conclusões sobre o trabalho.

Capítulo 2

Base Conceitual

2.1 Riscos

A Norma ISO Guia 73 [15] que institui o vocabulário da Gestão de Riscos define o termo Risco como “o efeito da incerteza nos objetivos”. A referida norma ainda classifica o efeito como um desvio em relação ao esperado que pode ser positivo ou negativo.

O Instituto Brasileiro de Governança Corporativa (IBGC) [26] entende risco como possibilidade de algo não dar certo, mas seu conceito atual envolve a quantificação e qualificação da incerteza, tanto no que diz respeito às perdas como aos ganhos [26].

No Guia do Conjunto de Conhecimentos em Gerenciamento de Projetos (PMBOK), o termo riscos é definido como um evento ou condição incerta que, se ocorrer, terá um efeito positivo ou negativo sobre pelo menos um objetivo do projeto [13].

Observa-se que o termo "risco"pode ter duas faces: a negativa (perda, dano, perigo) e a positiva (potencial impacto positivo, oportunidade de aumento do faturamento, do lucro e do retorno). O risco positivo também é chamado de Oportunidade [13].

Os riscos podem ter maior ou menor grau de impacto e probabilidade de ocorrência. Os riscos com alta probabilidade e/ou alto impacto devem ter um acompanhamento especial, já os riscos com baixa probabilidade e/ou impacto não necessitam de um acompanhamento tão próximo. Esta priorização se faz necessária para garantir a efetiva gestão de riscos [16].

2.2 Gestão de Riscos

A Norma ISO Guia 73 [15] define o termo Gestão de Riscos como “atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos”. Segundo o PMI [13], a Gestão de Riscos inclui os processos de planejamento, identificação, análise, planejamento de respostas e controle de riscos. Os objetivos da Gestão de Riscos são: aumentar a

probabilidade e o impacto dos eventos positivos; e reduzir a probabilidade e o impacto dos eventos negativos.

Para Kriouile e Elmaallan [19] a Gestão de Riscos é uma disciplina indispensável para qualquer organização no alcance de seus objetivos. Também pode ser definido como um processo contínuo de antecipação de problemas, sendo uma parte importante da gestão que é aplicada durante toda a vida de um projeto para antecipar e mitigar, de forma efetiva, os riscos com impactos críticos no projeto [30].

O ERM (*Enterprise Risk Management*) é um modelo de gerenciamento de riscos corporativos desenvolvido pelo *Committee of Sponsoring Organizations of the Treadway Comission* (COSO) com a finalidade de proporcionar as diretrizes para a evolução e aprimoramento do gerenciamento de riscos, servindo de base para que uma organização possa determinar se o gerenciamento de riscos está sendo eficaz, ou ao contrário, o que necessita para se tornar eficaz. Parte-se do princípio que a Gestão de Riscos é "um processo, efetuado pelo conselho de administração ou outro pessoal de uma entidade, aplicado na determinação de estratégias e em toda a organização, desenvolvido para identificar eventos potenciais que possam afetar a entidade e gerenciar riscos para que se limitem a seu apetite, para fornecer uma avaliação razoável do alcance dos objetivos da entidade" [39].

Nota-se que na literatura há diversas definições para o termo "Gestão de Riscos", porém verifica-se que há um consenso comum no seu significado, inclusive na esfera governamental, quando define a Gestão de Riscos como uma aplicação de princípios e processos para identificação e avaliação de riscos ao planejamento, à implementação e ao controle das respostas aos riscos [38]. Caso os riscos não sejam adequadamente gerenciados, a organização acaba tomando riscos que não foram analisados adequadamente e, portanto, desconhece.

O Programa Nacional de Gestão Pública e Desburocratização (GESPUBLICA) possui a finalidade de fortalecer a gestão pública, por meio do desenvolvimento de ações de apoio técnico aos órgãos e entidades da APF, a fim de mobilizar, preparar e motivar para a atuação em prol da inovação e da melhoria da gestão [38]. O GESPUBLICA esclarece que os riscos devem ser gerenciados em três níveis: estratégico, programas, projetos e atividades [38].

- Nível Estratégico: é neste nível onde se dá o contrato político do Governo com a sociedade e é estabelecida a coerência do seu programa de Governo. Decisões neste nível envolvem a formulação dos objetivos estratégicos e as prioridades para a alocação de recursos públicos em alinhamento com as políticas públicas.

- Nível Programa: neste nível encontram-se as decisões de implementação e gerenciamento de programas temáticos previstos no nível estratégico, por meio dos quais são executadas as politicas e as ações prioritárias de Governo.

- Nível Projetos e Atividades: neste nível encontram-se os projetos que contribuirão para o atingimento dos objetivos dos Programas, e as atividades relativas aos processos finalísticos.

As lideranças em todos os níveis da organização devem estar conscientes, capacitadas e motivadas com relação à relevância da Gestão de Riscos nos três níveis, que são interdependentes. Para isso, deve seguir um processo de Gestão de Riscos [38].

Conceitualmente, a gestão de risco privilegia o alcance de resultados em qualquer modelo (setores público e privado, nacional e internacional) [49].

2.3 Processo em Gestão de Riscos

A Norma ISO 31000 [16] estabelece princípios, estrutura e um processo de gestão do risco no sentido amplo. Pode ser utilizada por qualquer organização, independentemente do tamanho, atividade ou setor. Essa norma pode ajudar as organizações a aumentar a probabilidade de alcançar objetivos propostos, melhorar a identificação de oportunidades e ameaças, bem como a alocar e utilizar os recursos para a gestão de riscos. As organizações que a utilizam podem comparar as suas práticas de gestão de risco com uma referência reconhecida internacionalmente, proporcionando bons princípios de gestão eficaz e administração corporativa [16].

Um conceito importante que a Norma ISO 31000 [16] referencia é o "Processo de Gestão de Riscos", sendo de suma importância para o desenvolvimento deste trabalho. Esta norma é um dos principais *frameworks* e padrões de gerenciamento de riscos [54].

Ferreira et al. [20] realizaram um estudo detalhado e compararam o processo de gestão de riscos da Norma ISO 31000 [16] e do Guia padrão de Gerenciamento de Projetos [13], concluindo pela semelhança dos processos de gestão de riscos para ambas metodologias.

O processo de gestão de riscos da Norma ISO 31000 [16] é descrito da seguinte forma: aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de: comunicação e consulta; estabelecimento do contexto; identificação de riscos; análise de riscos; avaliação de riscos; tratamento de riscos; e monitoramento e análise crítica dos riscos (Figura 2.1).

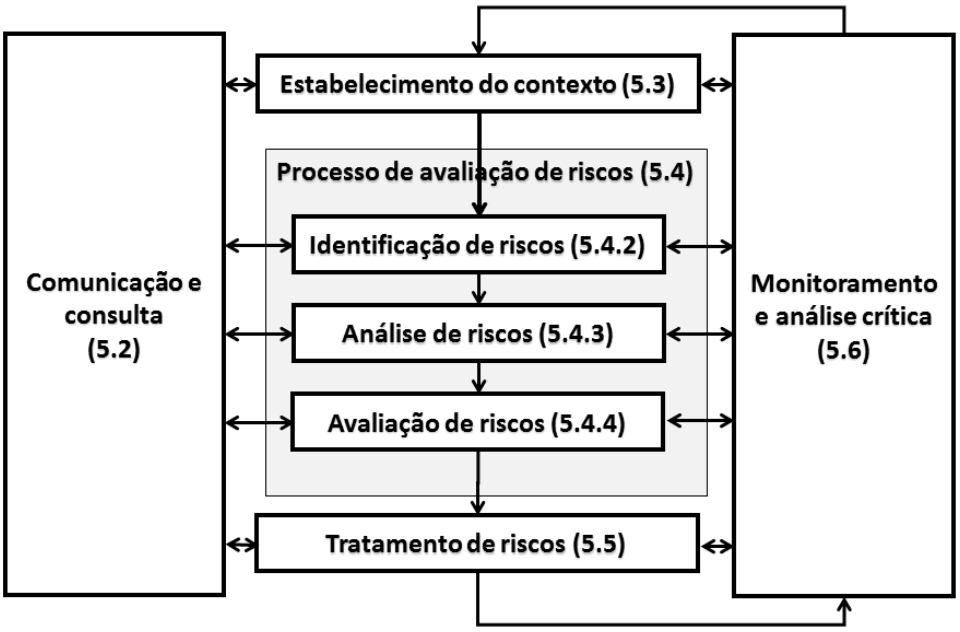


Figura 2.1: Processo de Gestão de Riscos. Fonte: [16]

Uma breve descrição das etapas do processo de gestão de riscos (Figura 2.1), segundo a referida norma está descrita abaixo:

- Comunicação e consulta: acontece durante todas as fases do processo da gestão de riscos, e deve ser a base das decisões do que deve ser feito, quais as razões e que ações devem ser tomadas. Convém que sejam abordadas questões relacionadas com risco, suas causas, consequências e medidas que estão sendo tomadas, bem como assegurar os interesses das partes interessadas, para que sejam compreendidas e consideradas [20];
- Estabelecimento de contexto: definição dos parâmetros externos e internos a serem levados em consideração ao se efetuar o gerenciamento de riscos, e estabelecimento do escopo e dos critérios de risco para a política de sua gestão [16]:
  - Contexto externo: ambiente externo no qual a organização busca atingir seus objetivos;
  - Contexto interno: ambiente interno no qual a organização busca atingir seus objetivos.
- Processo de avaliação de riscos: processo global de identificação, análise e avaliação dos riscos [16]:
  - Identificação dos riscos: a organização deve identificar as fontes, impactos e eventos (incluindo mudanças nas circunstâncias); e suas causas e consequências

potenciais. O objetivo é gerar uma lista abrangente de riscos que possam criar aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos;

  - Análise de riscos: envolve compreensão, apreciação das causas e as fontes dos riscos, suas consequências positivas e negativas, e a probabilidade que essas consequências possam ocorrer, além de prover ações para avaliar as decisões sobre a necessidade dos riscos serem tratados, sobre as estratégias e métodos mais adequados para o tratamento de riscos. A análise do risco pode ser qualitativa, quantitativa, ou a combinação destas.
  - Avaliação de riscos: processo de comparação dos resultados da análise de riscos com os critérios de risco para determinar se o risco e/ou sua magnitude é aceitável ou tolerável.

- Tratamento de riscos: processo para modificar os riscos e a implementação de ações, quer para aumentar a probabilidade e o impacto dos riscos positivos e/ou ações para minimizar a probabilidade de riscos negativos. Este tratamento é selecionado e documentado e mesmo após o tratamento de riscos, há extensão do risco residual que deverá também ser documentado, monitorado, e analisado criticamente, e quando apropriado, deve ser dado tratamento adicional. Os planos de ação para o tratamento, em geral podem ser: a) evitar o risco ao se decidir não iniciar ou descontinuar a atividade que dá origem ao risco; b) remoção da fonte de risco; c) alteração da probabilidade e das consequências; e d) redução da probabilidade de ocorrer [20].
- Monitoramento e Analise crítica: quanto ao monitoramento, deve ser verificada a situação de forma contínua, a fim de garantir que os controles sejam eficazes e eficientes [16]. Na Análise Crítica é realizada atividade para determinar a adequação, suficiência e eficácia do assunto em questão para atingir os objetivos estabelecidos [16].

A forma que o processo de gerenciamento de riscos está implantado na organização e sua aderência às melhores práticas de mercado define o nível de maturidade que a organização se encontra [4].

2.4 Governança Corporativa e Governança de TI

Governança de TI não existe de forma isolada. Pelo contrário, é parte da Governança Corporativa, mas tendo como foco particular a área de TI [42]. Dessa forma, antes de apresentar o conceito de Governança de TI, se faz necessário apresentar de forma sucinta o conceito de Governança Corporativa.

Para o Instituto Brasileiro de Governança Corporativa (IBGC), Governança Corporativa é o sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo as práticas e os relacionamentos entre proprietários, conselho de administração, diretoria e órgãos de controle [26]. No setor público, por sua vez, a governança caracteriza-se pela capacidade de implementar políticas públicas, sendo este o retorno efetivo das ações do Governo para a sociedade [3]. Em outras palavras, é a capacidade de prestar serviços a sociedade de forma efetiva [3].

Dada a definição de Governança Corporativa é possível levantar o alicerce teórico da Governança de TI. De acordo com o ISACA [6] a Governança de TI é de responsabilidade da alta administração, na liderança, nas estruturas organizacionais e nos processos que garantem que a TI da empresa sustente e estenda as estratégias e objetivos da organização. Os autores Pereira e Silva [42] compilaram uma série de definições sobre este tema, sendo que a primeira delas remete ao ano de 1994: "a Governança de TI define as responsabilidades pelas funções de TI", concluindo pela convergência dos seguintes pontos: utilizada para tomada de decisão, possui como objetivo o alinhamento entre TI e o negócio e gera valor para a organização.

A norma ISO 38500 [17] define a Governança de TI como um sistema pelo qual o uso atual e futuro da TI são dirigidos e controlados. Significa avaliar e direcionar o uso da TI para dar suporte à organização e monitorar seu uso para realizar planos. Inclui a estratégia e as políticas de uso da TI dentro da organização.

Nessa mesma linha, o TCU, por meio do Acórdão 2.308 [47], define a Governança de TI como um conjunto estruturado de políticas, normas, métodos e procedimentos destinados a permitir à alta administração e aos executivos o planejamento, a direção e o controle da utilização atual e futura de TI.

A Governança de TI pode ser direcionada pelo *Control Objectives for Information and related Technology* (COBIT) [22]. O COBIT é um guia de boas práticas de gestão de TI apresentado como um padrão (o item 3.3.6 descreve o COBIT em maiores detalhes). Os quatro domínios do COBIT (Planejar e Organizar; Adquirir e Implementar; Entregar e Suportar; e Monitorar e Avaliar) apoiam diretamente as cinco áreas focos da Governança de TI. Destaca-se ainda que o COBIT é o principal norteador que aponta para onde se deve seguir para alcançar a Governança de TI. A Figura 2.2 resume as principais dimensões focalizadas pela Governança de TI [6]:

Figura 2.2: Os cinco focos da Governança de TI. Fonte: [6]

Cada área foco tem um objetivo principal que pode ser descrito como se segue. O "Alinhamento Estratégico" assegura o alinhamento dos planos da TI com os de negócio e alinha a operação e as entregas da TI com as operações da organização. A "Entrega de Valor" assegura que os benefícios previstos pela TI estão realmente sendo gerados, dentre eles a otimização de custos e outros valores intrínsecos que a TI pode proporcionar. Já a "Gestão de Riscos" permite que a organização reconheça todos os riscos (e oportunidades) derivados da TI para o negócio e que decida e tenha planos para mitigá-los na medida em que julgue necessário. Por sua vez, a "Gestão de Recursos" assegura a gestão dos recursos mais importantes para TI: recursos humanos e recursos tecnológicos (informações, infraestrutura, aplicações), promove a valorização do conhecimento e da infraestrutura. Por fim, a "Mensuração de Desempenho" acompanha e monitora a implementação da estratégia, consumação de projetos, uso dos recursos e entrega dos serviços quanto à sua contribuição para as estratégias e objetivos do negócio, utilizando-se não apenas de critérios financeiros [6].

Como pode ser observado o tema Gestão de Riscos de TI integra a Governança de TI e é um item promissor de auditorias pelos órgãos de controle. Risco de TI é o risco de negócio associado ao uso, gerenciamento, operação, suporte, inovação, influência ou adoção de TI para efetuar os negócios da organização [6].

2.5 Maturidade e Modelos de Maturidade

O conceito de maturidade de uma organização foi definido por De Bruin et al. [12] como uma medida para avaliar a capacidade da organização em relação a certa disciplina. Para os autores, a maturidade está relacionada a processo, de forma genérica, e os Modelos de Maturidade são ferramentas muito úteis para avaliação desses processos. Além de identificação de processos-chave e planejamento de quais processos priorizarem.

Segundo a Norma ISO 15504-3 [18], a maturidade organizacional é "uma expressão do grau no qual uma organização implementa consistentemente processos em um escopo definido, os quais contribuem para o atendimento de seus objetivos de negócios (correntes ou projetados)". A referida norma ainda recomenda a aplicação de um modelo de avaliação da maturidade em dois contextos: o de melhoria de processo e o de determinação de capacidade de processo. Além disso, indica a importância da autoavaliação para o aprimoramento do processo.

Kohlegger et al. [34] mencionam que um modelo de maturidade representa conceitualmente fases de aprimoramento da capacidade quantitativa ou qualitativa de um processo específico, a fim de avaliar seus avanços em relação ao estágio anterior.

O uso de um modelo de maturidade permite que uma organização tenha seus métodos e processos avaliados de acordo com as boas práticas de mercado e com um conjunto de parâmetros estabelecidos [2]. Além disso, esclarece que a maturidade é indicada pela atribuição de um "Nível de Maturidade" em particular.

A avaliação da organização geralmente ocorre pela aplicação de um questionário no qual um grupo de pessoas, previamente selecionadas, respondem as questões estabelecidas pelo modelo. Um cálculo irá definir o nível de maturidade que o órgão se encontra para um determinado processo [8].

Becker et al. [8] destacam que não é relevante questionar quando a entidade atingirá o nível mais alto, mas sim quanto esforço e atenção a organização está disposta a ceder. Nessa mesma linha, Introna et al. [32] reconhecem que o nível ótimo de maturidade é reconhecido como o nível que entrega os objetivos estratégicos da organização de maneira mais efetiva e eficaz, não necessariamente correspondendo ao nível mais alto da escala definida.

Com isso, conclui-se que é preciso considerar o estágio atual da organização e entender suas limitações e lacunas em relação a um estágio futuro desejado [8].

Os modelos de maturidade existentes podem ser diferenciados de acordo com vários aspectos, relacionados com a forma como as organizações utilizam. Esses aspectos incluem [32]:

- Estrutura do Modelo: contínuo ou por etapas;
- Metodologia de análise: a forma como o objetivo é verificado;
- Referência às normas internacionais;
- Modo de avaliação: procedimentos técnicos, por meio do qual a avaliação é operacionalmente realizada (incluindo autoavaliação);
- Resultados da avaliação: os elementos-chave para compreender os pontos fortes e fracos da organização;
- Guia de melhoria: a presença mais ou menos explícita e estruturada de instruções específicas para a melhoria da organização.

Kriouile e Elmaallam [19] concluem que as organizações que querem se proteger e se desenvolver, devem implementar um processo eficaz de gestão de riscos, submetendo-o a uma avaliação periódica por meio de um modelo de maturidade apropriado.

Capítulo 3

Revisão de Literatura

Uma revisão literária em relação aos modelos de maturidade é de suma importância para identificar o estado da arte relacionado ao tema deste trabalho. Inicia-se o estudo em modelos de maturidade com aplicações gerais, passando por modelos de maturidade em gestão de riscos até identificar modelos de maturidade em gestão de riscos de TI.

Pesquisas demonstram que diversos modelos de maturidade têm sido propostos [12]. Observa-se também que as publicações constantes de proposição de novos modelos são, geralmente, baseadas em um modelo já existente com um adicional aplicado de forma arbitrária [8]. Os autores ainda mencionam que é raro identificar nos modelos propostos atividades de revisão, melhorias ou validações nos instrumentos. Isso tem ocasionando a obsolescência dos modelos de maturidade, pois condições mudam, a tecnologia evolui, e as pesquisas científicas surgem diariamente com propostas inovadoras.

3.1 Modelos de Maturidade com aplicações gerais

A indústria de energia conta com alguns modelos de maturidade para gerenciamento de energia. Introna et al. [32] propõem um Modelo de Maturidade para Gerenciamento de Energia acessível via Web de forma rápida, efetiva e autônoma. O nível de maturidade é obtido pela resposta a um questionário de 40 itens. O EMMM (*Energy Management Maturity Model*) é um modelo de maturidade em gerenciamento de energia. O EMMM possui cinco níveis de maturidade e cinco dimensões. Além disso, este modelo propõe a aderência à norma ABNT ISO 50001:2011 que certifica a existência de um sistema de gestão energética otimizado para o uso correto da energia em qualquer ambiente. Nesta mesma linha, Antunes et al. [1], também propõem um modelo de maturidade para a Gestão de Energia que consiste em várias atividades de gerenciamento de energia, derivadas de diversos guias de gestão de energia, estudos de caso e artigos científicos. Também foram definidos cinco níveis de maturidade. Há uma avaliação detalhada da

norma ABNT ISO 50001, a qual demonstra que praticamente todos os requisitos deste padrão da indústria foram cobertos.

Na área de *software* Raza et al. [46] apresentam um modelo de maturidade para projetos de código aberto que relaciona o grau de coordenação entre projetos de código aberto e o seus aspectos de usabilidade. O instrumento de medição do modelo contém fatores que examinam as perspectivas dos usuários do sistema, dos desenvolvedores, dos colaboradores e da indústria. O modelo apresenta 5 níveis de maturidade: Preliminar, Reconhecido, Definido, Agilizado e Institucionalizado. Os fatores de usabilidade foram agrupados em quatro dimensões que incluem "Usabilidade da Metodologia", "estratégia de projeto", "Avaliação"' e "Documentação". A dimensão de "Metodologia" incorpora as necessidades dos usuários, como: feedback do usuário e usabilidade do sistema. A dimensão "Projeto" também é focada no usuário do sistema e leva em consideração a compreensibilidade, apreensibilidade, operacionalidade e atratividade que o sistema apresenta. A dimensão "Avaliação" engloba os resultados dos testes: relatório de bugs e Teste de Usabilidade. Por fim, a dimensão "Documentação"engloba o manual do administrador do sistema, do usuário, *help-online*, guia rápido, entre outros.

3.2 Modelos de Maturidade em Gestão de Riscos

Na revisão de literatura foi possível identificar a existência de modelos de maturidade relacionados às indústrias, como por exemplo, o modelo de Batenburg et al. [7] que se aplica para utilização em 91 hospitais dos Países Baixos. Em seu trabalho intitulado "Um modelo de maturidade de Governança, Riscos e Conformidade (GRC) em hospitais" são elencadas quatorze dimensões e cinco níveis de maturidade. O modelo de maturidade pode guiar hospitais para melhorar a sua maturidade relacionada a GRC, sendo que o uso do modelo não é necessariamente a mesma para cada hospital. Um hospital pode usar o modelo para melhorar sua maturidade em GRC de uma forma evolutiva ou revolucionária, como por exemplo, buscando sair do segundo para o terceiro nível, ou por mudanças mais radicais, quando um ou dois níveis de maturidade são ignorados.

O protótipo de um sistema denominado, (RMM - *Risk Management Maturity*, [33]), proposto para projetos de construção civil em grande escala, utiliza o método de análise multicritério *Analytic Network Process* (ANP) para medir a eficácia global do gerenciamento de risco em relação aos principais fatores de risco. São quatro níveis de maturidade e dez dimensões, sendo seis relacionadas ao gerenciamento de processos e quatro à organização.

Rae et al. [45] apresentam um modelo de maturidade para Avaliação Quantitativa de Riscos (QRA), o qual abrange potenciais falhas discutidas na literatura sobre QRA.

O modelo proposto fornece uma maneira de priorizar o desenvolvimento de processos de QRA dentro de uma organização. Foram definidos quatro níveis de maturidade. O nível de maturidade é dado por possíveis falhas em cada nível. Estas imperfeições foram agrupadas em dezenove categorias e distribuídas para os níveis de maturidade. Todas as possíveis lacunas foram abrangidas na avaliação quantitativa de riscos [45].

3.2.1 CMMI - Modelo Integrado de Maturidade e de Capacidade

O CMMI (*Capability Maturity Model Integration*) é um modelo de maturidade para melhoria de processo de software. Seu objetivo é auxiliar as organizações na melhoria de seus processos de desenvolvimento e manutenção de produtos e serviços, por meio das melhores práticas associadas a atividades, que cobrem o ciclo de vida do produto desde a concepção até a entrega e manutenção [30].

O CMMI surgiu para combinar outros CMMs (*Capability Maturity Model*) existentes. Sua estrutura fornece os elementos essenciais de um processo efetivo, cobrindo várias disciplinas e traçando um caminho de melhoria evolutiva do processo. A fim de desenvolver e manter produtos e serviços de qualidade, o modelo foi desenvolvido a partir de três dimensões críticas nas quais as organizações devem se concentrar: pessoas; procedimentos e métodos; ferramentas e equipamentos [30]. A coesão entre essas três dimensões é feita por meio dos processos de negócio da organização, que fornecem os elementos necessários para a otimização de recursos, maximização da produtividade e maior competitividade.

O CMMI oferece duas abordagens distintas, Contínua e por Estágios. A abordagem Contínua permite à organização melhorar de forma incremental os processos correspondentes a uma ou mais áreas de processo individualmente selecionadas pela organização. Já a abordagem por Estágios permite que as organizações melhorem um conjunto de processos interrelacionados, tratando sucessivos conjuntos de áreas de processos de forma incremental [30].

Para a representação contínua, utiliza-se o termo “nível de capacidade” e para a representação por estágios “nível de maturidade” [30]. A Figura 3.1 demonstra uma comparação entre os níveis de capacidade e maturidade do CMMI.

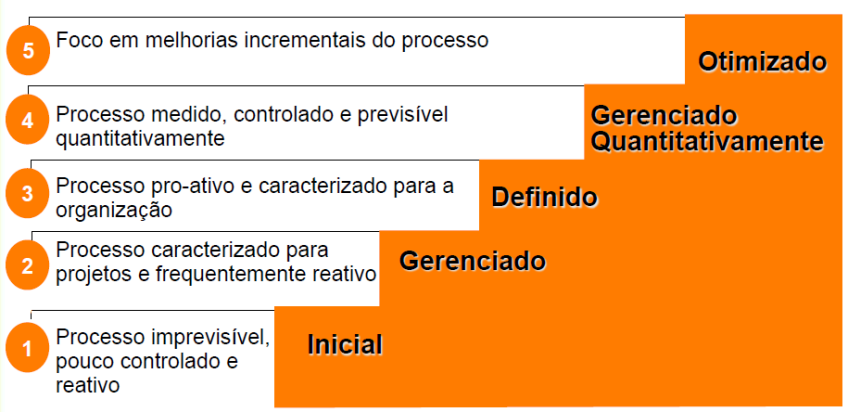


Figura 3.1: Níveis de maturidade e capacidade do CMMI. Fonte: [30]

Para a progressão entre os níveis de maturidade o CMMI define um conjunto de práticas específicas e genéricas associadas às "áreas de processo". Para se alcançar um nível, todos os requisitos do nível anterior devem ter sido cumpridos [30].

A "área de processo" pode ser definida como "conjunto de práticas relacionadas em uma área que, quando implementadas conjuntamente, satisfazem a um conjunto de metas consideradas importantes para a realização de melhorias naquela área" [30].

A gestão de riscos é uma das vinte e quatro áreas do processo do CMMI-SVC (*CMMI for Service*), sendo esta a área de processo selecionada para o estudo comparativo. Segundo o CMMI-SVC o objetivo desta área de processo é fornecer subsídios para identificar potenciais problemas antes que ocorram, de forma que atividades de tratamento de riscos possam ser planejadas e colocadas em prática quando necessário (no longo da vida do produto ou do projeto) para mitigar impactos indesejáveis que comprometam a realização dos objetivos [30].

3.2.2 ERM - Gerenciamento de Riscos Corporativos

A implementação da estrutura do ERM (*Enterprise Risk Management*), suporta e melhora a consciência sobre os riscos em todos os níveis, desde o nível estratégico ao operacional, conforme observa-se na matriz tridimensional, representada na Figura 3.2:

Figura 3.2: Matriz de relacionamento ERM. Fonte: [39]

A estrutura da matriz tridimensional sugere um relacionamento entre os objetivos da organização, os componentes do gerenciamento de riscos corporativos e as unidades de uma organização [39].

O ERM tem por finalidade [39]:

- Alinhar o apetite a risco com a estratégia adotada – os administradores avaliam o apetite a risco da organização ao analisar as estratégias, definindo os objetivos a elas relacionados e desenvolvendo mecanismos para gerenciar esses riscos.
- Fortalecer as decisões em resposta aos riscos – o gerenciamento de riscos corporativos possibilita o rigor na identificação e na seleção de alternativas de respostas aos riscos - como evitar, reduzir, compartilhar e aceitar os riscos.
- Reduzir as surpresas e prejuízos operacionais – as organizações adquirem melhor capacidade para identificar eventos em potencial e estabelecer respostas a estes, reduzindo surpresas e custos ou prejuízos associados.
- Identificar e administrar riscos múltiplos e entre empreendimentos – toda organização enfrenta uma gama de riscos que podem afetar diferentes áreas da organização. A gestão de riscos corporativos possibilita uma resposta eficaz a impactos inter-relacionados e, também, respostas integradas aos diversos riscos.
- Aproveitar oportunidades – pelo fato de considerar todos os eventos em potencial, a organização posiciona-se para identificar e aproveitar as oportunidades de forma proativa.

- Otimizar o capital – a obtenção de informações adequadas a respeito de riscos possibilita à administração conduzir uma avaliação eficaz das necessidades de capital como um todo e aprimorar a alocação desse capital.

O ERM não possui um modelo de maturidade nato [39]. Embora hajam organizações privadas interessadas no estudo e desenvolvimento de modelos de maturidade utilizando o seu padrão [4]. Como é o caso da empresa Protiviti [28], que desenvolveu um modelo de maturidade para determinar a necessidade de melhorias no gerenciamento de riscos. Esse modelo possui cinco estágios que vai do inicial ao otimizado [28]. Os atributos e o método de realização de cada nível de maturidade estão descritos na Figura 3.3.

Figura 3.3: Níveis de maturidade COSO-ERM. Fonte: [28]

O modelo de maturidade desenvolvido pela empresa Protiviti, denominado como COSO-ERM, se baseia em dois modelos: CMMI e o próprio ERM.

3.2.3 RMM - Modelo de Maturidade de Riscos

Um dos primeiros modelos de maturidade de Gestão de Riscos foi criado por Hillson [24], o RMM (*Risk Maturity Model*). Esse modelo tornou-se referência para vários outros modelos criados. Esse modelo mensura a maturidade de riscos em quatro níveis, conforme Figura 3.4. As dimensões envolvidas são: cultura, processo, experiência e aplicação.

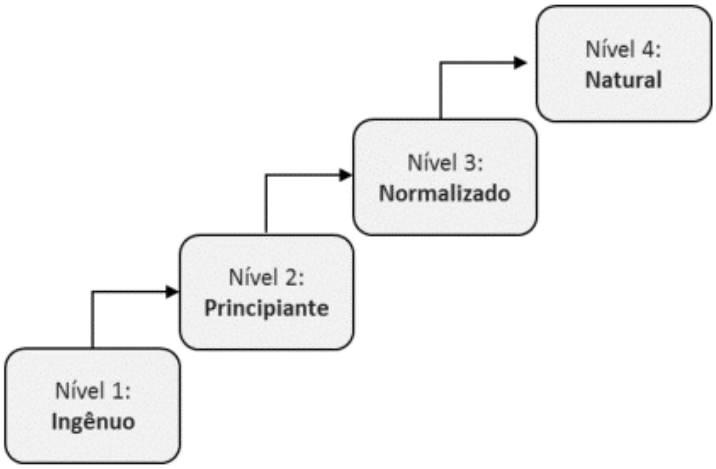


Figura 3.4: Níveis de maturidade RMM. Fonte: [24]

Segundo o próprio autor, reconhece-se que algumas organizações podem não se encaixar perfeitamente nessas categorias, mas os níveis propostos pelo modelo são suficientemente diferentes para acomodar a maioria das organizações de forma não ambígua [24].

O RMM permite medir a maturidade do risco a partir das quatro áreas (cultura, processo, experiência e aplicação) descritas na Tabela 3.1. A transição entre níveis se dá a partir do relacionamento dos atributos dessas áreas com os níveis [24].

Tabela 3.1: Relacionamento entre níveis e áreas do modelo RMM. Fonte: [24]

	Nível 1 Ingênuo	**Nível 2 Principiante**	**Nível 3 Normalizado**	**Nível 4 Natural**
Definição	Desconhecem a necessidade de gerenciamento de risco. Não existe uma abordagem estruturada para lidar com a incerteza. Processo de gestão reativo e repetitivo, Pouca ou nenhuma tentativa de aprender com o passado ou se preparar para o futuro.	Experiência com gestão de riscos por intermédio de um pequeno número de indivíduos. Nenhuma abordagem genérica estruturada localmente. Consciência dos benefícios potenciais da gestão de risco, mas aplicação ineficaz e sem ganho pleno de benefícios.	Gerenciamento de riscos construído em processos de negócios rotineiros. Gerenciamento de riscos implementado na maioria ou todos os projetos. Processos genéricos de riscos formalizados. Benefícios entendidos em todos os níveis da organização, embora nem sempre sejam consistentemente alcançados.	Cultura na consciência em risco com uma abordagem proativa do gerenciamento do risco em todos os aspectos do negócio, Uso ativo das informações sobre riscos para melhorar os processos de negócio e ganhar vantagem competitiva. Ênfase no gerenciamento de oportunidades (riscos positivos).
Cultura	Sem consciência do risco. Resistente/relutante em mudar. Tendência a continuar com processo existente.	Processo de risco pode ser visto como uma sobrecarga adicional com benefícios variáveis. Gerenciamento do risco empregado somente em projetos selecionados.	Aceitação da política de gestão de riscos. Benefícios reconhecidos e esperados. reparado para comprometer recursos a fim de colher ganhos.	Compromisso com a gestão de riscos de cima para baixo (da liderança, por exemplo). Gestão de riscos proativa encorajada e recompensada.
Processo	Não há um processo formal.	Não há um processo genérico formal, embora alguns métodos formais específicos possam estar em uso.	Processo genérico aplicado à maioria dos projetos. Processo formal incorporado ao sistema de qualidade. Alocação de ativos e gestão dos orçamentos de risco em todos os níveis. Necessidade limitada de apoio externo.	Processos de negócio baseados em risco. "Gestão Total de Risco"transversal a todo o negócio. Atualização regular e frequente dos processos. Métrica das rotinas de risco com comentários consistentes com a melhoria.
Experiência	Não entendimento dos princípios de risco ou linguagem.	Limitado a indivíduos que tiveram um treinamento pequeno ou informal.	Especialistas locais, formalmente treinados em habilidades básicas. Desenvolvimento de processos específicos e ferramentas.	Toda a equipe está consciente dos riscos e usando habilidades básicas. Aprendizagem por meio da experiência como parte do processo. Treinamentos externos regulares para aprimorar habilidades.
Aplicação	Não há aplicativos estruturados. Não há recursos dedicados. Não existe ferramentas de risco.	Aplicação inconsistente. Disponibilidade variável de pessoal. coleção ad hoc de ferramentas e métodos.	Rotina e aplicativos consistentes para todos os projetos e recursos entregues. Conjunto integrado de ferramentas e métodos.	Segunda natureza, aplicada para todas as atividades. Relatórios de riscos-base para a tomada de decisão. Estado da arte em ferramentas e métodos.

Segundo Hillson [24], o RMM permite que: as organizações referenciem a sua capacidade de riscos em quatro níveis de maturidade, a fim de identificar o que precisa ser feito para melhorar e desenvolver a sua capacidade de gerenciar risco. O uso do RMM também vai permitir diagnosticar a situação atual, e ajudar no desenvolvimento de estratégias específicas para o progresso de uma implementação eficaz [24].

O próximo tópico apresenta a evolução do modelo RMM, o RMMM.

3.2.4 RMMM - Modelo de Maturidade em Gestão de Riscos

Hopkinson [25] apresenta uma adaptação do modelo RMM para o processo de gerenciamento de riscos de um projeto, denominado RMMM (*Risk Management Maturity Model*), onde os riscos são avaliados a partir de seis perspectivas: projeto das partes interessadas, identificação de riscos, análise de risco, respostas aos riscos, gerenciamento de projetos e cultura de gestão de risco.

O RMMM permite uma avaliação global da capacidade de gerenciamento do risco de um projeto a partir da comparação das seis perspectivas, conforme Figura 3.5 que evidencia aquela que apresenta o maior risco [25].

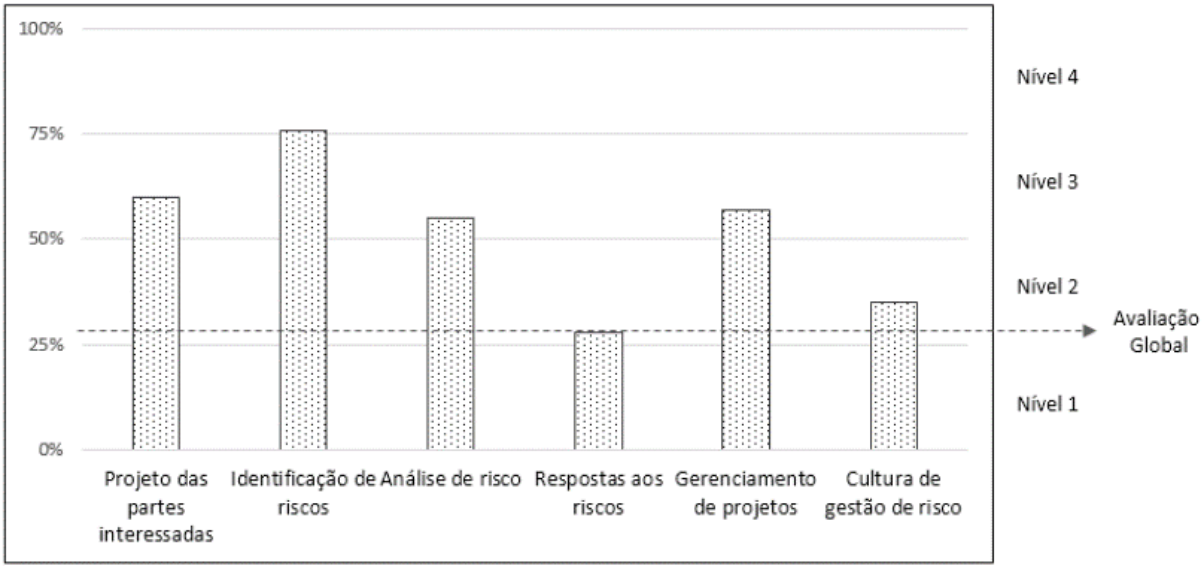


Figura 3.5: Exemplo de aplicação do modelo RMMM. Fonte: [25]

No exemplo acima é possível observar a avaliação de cada uma das perspectivas do modelo, onde a perspectiva "resposta aos riscos" define o estágio atual.

3.3 Modelos de Maturidade em Gestão de Riscos de TI

Modelos de maturidade têm sido cada vez mais utilizados por gestores de TI para autoavaliação e podem prover uma abordagem comum para que profissionais de TI e de controle entendam e acordem sobre prioridades e áreas que exijam maior atenção. [29].

3.3.1 Modelo de Maturidade do TCU

O modelo proposto e utilizado pelo TCU na avaliação de 65 Entidades da Administração Pública Indireta [49] baseou-se principalmente no modelo de avaliação da gestão de riscos desenvolvido pelo governo britânico, com adaptações vindas dos modelos ERM [28] e norma ISO 31000 [16]. O modelo possui cinco níveis de maturidade e quatro dimensões avaliativas: Ambiente de Gestão de Riscos, Processos de Gestão de Riscos, Gestão de Riscos em Parcerias e Resultados. Sendo três destas dimensões subdividida em três níveis cada. No relatório ficou evidenciado que a aplicação do questionário proposto de gestão de riscos na Administração Direta não seria prudente, tendo em vista o baixo grau de conhecimento do tema por parte dos gestores públicos. Optou-se assim, pela aplicação nas Entidades da Administração Indireta, julgadas como organizações com a gestão de riscos mais evoluída e de conhecimento geral. As dimensões receberam pesos fixos após a aplicação da técnica *Analytic Hierarchy Process* - AHP [10] aplicada às respostas dadas por oito especialistas do TCU a comparações duas a duas da importância relativa das quatro dimensões do modelo. A técnica AHP presta-se a facilitar a tomada de decisão por meio da hierarquização de opções com base na opinião de um grupo de pessoas acerca dos atributos de cada opção.

3.3.2 Ferramenta *Risk IT*

Kriouile e Elmaallam [19] propuseram a ferramenta Risk IT (*Maturity Model of RISK IT Framework*), a qual define três domínios de risco: governança de riscos, avaliação de riscos e resposta a riscos. Cada domínio tem um modelo de maturidade alto nível e um modelo de maturidade detalhado. O modelo de maturidade de alto nível oferece seis níveis de 0 a 5: 0 – inexistente; 1 - inicial/*ad hoc*; 2 - repetível, mas intuitivo; 3 - processo definido; 4 - gerenciado e mensurado; e 5 – otimizado. Já o modelo detalhado foi construído em torno dos seguintes atributos: aumentar a sensibilização e comunicação; responsabilidades e imputabilidade; definição dos objetivos e as medidas associadas; política, normas e procedimentos; habilidades e expertises; e ferramentas e automação.

3.3.3 Ferramenta *IT Score*

Gartner é uma empresa de consultoria fundada em 1979 por Gideon Gartner. Trata-se de uma das maiores empresas de auditoria, avaliação e análise de mercado em todo o mundo, que geram dados e números que influenciam tomadas de decisões importantes em vários pontos do globo, no que se trata de investimentos e desenvolvimento de novas soluções de TI.

Em 2014, a Gartner propôs a ferramenta "*IT Score*" para Gestores de TI e Executivos com o intuito de avaliar a maturidade das organizações de TI (governança corporativa) [27]. São cinco níveis progressivos de maturidade (Figura 3.6) e cinco dimensões (Pessoas; Práticas e Processos de PPM – *Program and Project Management*; Valor e Gestão Financeira; Tecnologia; e Relacionamentos).

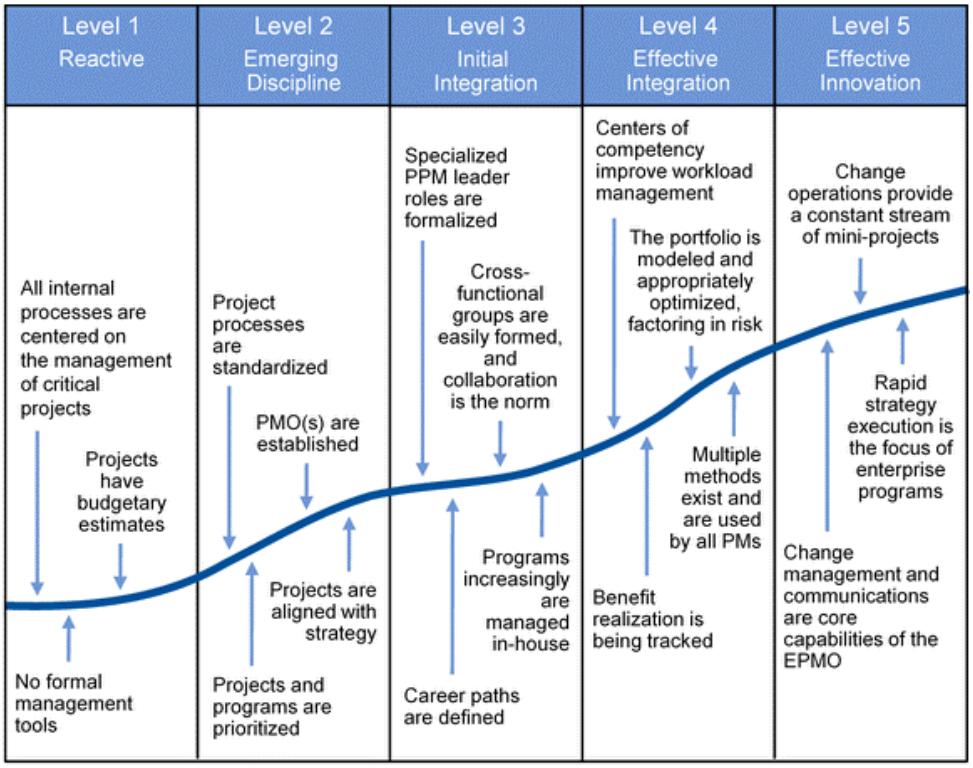


Figura 3.6: Cinco níveis de maturidade do modelo da Gartner. Fonte: [27]

Observa-se que cada dimensão tem sua própria escala de maturidade e constrói cumulativamente na maturidade a partir do nível anterior. O modelo é estático não havendo nenhuma distinção na aplicação para o mercado privado e público.

3.3.4 COBIT - Objetivo de Controle para Tecnologia da Informação e Áreas Relacionadas

O *Control Objectives for Information and related Technology* (COBIT) foi desenvolvido pelo ISACF - *The Information Systems Audit and Control Foundation*, em 2006. Posteriormente, o COBIT passou a ser mantido pelo *IT Governance Institute* (ITGI) que fornece boas práticas por meio de uma estrutura lógica e gerenciável para garantir que a área de TI suporte adequadamente os objetivos de negócio da instituição [29].

O COBIT consiste em três modelos para o controle e gerenciamento da tecnologia da informação: Modelo de Processo (*framework*); Modelo de Governança de TI e Modelo de Maturidade.

Para que as organizações possam aperfeiçoar o uso dos recursos de TI, os dirigentes precisam entender o estágio atual da sua arquitetura de TI a fim de identificar qual caminho deverá seguir. Assim, o COBIT busca um alinhamento entre os objetivos de negócios e os objetivos de TI da organização, por meio de modelos de maturidade e métricas que possam medir sua eficácia e identificar responsabilidades dos donos de processos de negócios e de TI [4].

A versão 4.1 do COBIT trabalha ainda com o conceito de "áreas de foco", que pode ser entendido como tópicos os quais os dirigentes precisam estar atentos. Dentre as cinco áreas de foco existentes esta a área de gestão de riscos [6].

O COBIT 4.1 provê um modelo constituído por 34 processos, agrupados em 4 domínios inter-relacionados que se alinham as áreas responsáveis por planejar, construir, executar e monitorar, de forma a prover uma visão total da área de TI [6].

O domínio "Planejar e Organizar" (PO) cobre os aspectos referentes às ações estratégias e táticas necessárias para a TI contribuir para o alcance dos objetivos do negócio. O domínio "Adquirir e Implementar" (AI) se preocupa com as soluções de TI que precisam ser desenvolvidas, adquiridas ou implementadas para integração aos processos dos negócios necessários para a execução das estratégias de TI. O domínio "Entregar e Suportar" (DS), refere-se a entrega e gerenciamento dos serviços solicitados. Por fim, o domínio "Monitorar e Avaliar" (ME) diz respeito a avaliação dos processos a fim de assegurar a qualidade e a aderência aos requisitos de controle.

A Tabela 3.2 descreve os quatro domínios do COBIT 4.1 e seus respectivos processos:

Tabela 3.2: Domínios e processos do COBIT 4.1. Fonte: [6]

Planejar e Organizar	PO1	Definir um plano estrategico de TI
	PO2	Definir a arquitetura de informação
	PO3	Determinar o direcionamento tecnológico
	PO4	Definir os processos, organização e relacionamentos de TI
	PO5	Gerenciar o investimento em TI
	PO6	Comunicar as diretrizes e expectativas da diretoria
	PO7	Gerenciar os recursos humanos de TI
	PO8	Gerenciar a qualidade
	PO9	Avaliar e gerenciar os riscos de TI
	PO10	Gerenciar projetos
Adquirir e Implementar	AI1	Identificar soluções
	AI2	Adquirir e manter software de aplicativo
	AI3	Adquirir e manter infraestrutura de tecnologia
	AI4	Habilitar operação e uso
	AI5	Adquirir recursos de TI
	AI6	Gerenciar mudanças
	AI7	Instalar e homologar soluções e mudanças
Entregar e Suportar	DS1	Definir e gerenciar níveis de serviço
	DS2	Gerenciar serviços de terceiros
	DS3	Gerenciar capacidade e desempenho
	DS4	Assegurar continuidade de serviços
	DS5	Assegurar a segurança dos serviços
	DS6	Identificar e alocar custos
	DS7	Educar e treinar usuários
	DS8	Gerenciar a central de serviço e os incidentes
	DS9	Gerenciar a configuração
	DS10	Gerenciar os problemas
	DS11	Gerenciar os dados
	DS12	Gerenciar o ambiente físico
	DS13	Gerenciar as operações
Monitorar e Avaliar	ME1	Monitorar e avaliar o desempenho
	ME2	Monitorar e avaliar os controles internos
	ME3	Assegurar a conformidade com requisitos externos
	ME4	Prover a governança de TI

Observa-se que o domínio "Planejar e Organizar" é constituído por dez processos, sendo um deles o processo "Avaliar e Gerenciar os Riscos de TI". Os processos do COBIT estão descritos de forma a se alinhar aos objetivos de TI que suportam os objetivos de negócio da instituição.

Devido ao escopo deste trabalho de maturidade em gestão de riscos de TI será considerado para o desenvolvimento do trabalho, apenas o processo P09 - Avaliar e Gerenciar os Riscos de TI. Segundo o ISACA [6] o processo Avaliar e Gerenciar os Riscos de TI (P09) visa: Criar e manter uma estrutura de gestão de risco. Esta estrutura documenta um nível comum e acordado de riscos de TI, estratégias de mitigação e riscos residuais. Qualquer impacto em potencial nos objetivos da empresa causado por um evento não planejado deve ser identificado, analisado e avaliado. Estratégias de mitigação de risco devem ser adotadas para minimizar o risco residual a níveis aceitáveis. O resultado da avaliação deve ser entendido pelas partes interessadas e expresso em termos financeiros para permitir que as partes interessadas alinhem o risco a níveis de tolerância aceitáveis.

Há um conjunto de seis controles gerenciais que devem ser considerados pela área de TI na implementação do processo P09, conforme Tabela 3.3, de forma a prover uma razoável garantia de que os objetivos de negócio possam ser atingidos e que eventos indesejáveis possam ser prevenidos, ou ainda detectados e corrigidos [6].

Tabela 3.3: Controles gerenciais do processo P09 do COBIT 4.1. Fonte: [6]

Processo	**Descrição**
PO9.1	Alinhamento da gestão de riscos de TI e de negócios
PO9.2	Estabelecimento de contexto de riscos
PO9.3	Identificação de eventos
PO9.4	Avaliação de risco
PO9.5	Resposta em risco
PO9.6	Manutenção e monitoramento do plano de ação de risco

O Modelo de Maturidade do COBIT 4.1 é composto por critérios de avaliação dos processos. Seu objetivo é auxiliar os gestores na tomada de decisão, relacionando os processos de TI considerados estratégicos para o negócio da organização, ou seja, a maturidade é avaliada por processo [6].

Existem seis níveis de maturidade para o COBIT 4.1, de complexidade crescente [6]:

- Inexistente: falta absoluta de elementos reconhecíveis no processo;
- Inicial (*ad hoc*): reconhece-se, ainda que caso a caso, o interesse de tratar da necessidade;

- Repetível: procedimentos similares seguidos por pessoas distintas para o mesmo tipo de atividade;
- Definido: procedimentos padronizados e documentados comunicados por meio de treinamento;
- Gerenciado: é possível monitorar e medir a conformidade com os procedimentos; e
- Otimizado: processo automatizado baseado nas melhores práticas.

A aplicação do modelo de maturidade permite que a organização faça um diagnóstico de seus processos, identifique seu estágio atual de desenvolvimento em relação à posição desejável e implemente medidas que assegurem o alcance das metas propostas. Permite, também, que a organização identifique o nível de maturidade em que ela se encontra em comparação com outras organizações da sua categoria e com os padrões internacionais [6].

Em 2012 foi lançada nova versão do Framework COBIT, o COBIT 5, com profundas mudanças, inclusive no que tange ao modelo de maturidade do COBIT. O modelo de maturidade do COBIT 5 se baseia na Norma ISO 15504 [14] que é detalhada no item 3.4. Ele utiliza novos conceitos em sua estrutura, apresentados como princípios e capacitadores. Apesar de continuar com seis níveis de maturidade o novo modelo de maturidade do COBIT 5 vai do "processo incompleto" ao "processo em otimização". Nesta nova versão um nível de capacidade só pode ser alcançado quando todos os atributos do nível anterior tiverem sido concluídos [5].

O foco do COBIT 5 é a governança de TI, pois ele alinha as estruturas e os padrões mais recentes e relevantes utilizados nas empresas, ou seja, trata de um integrador global das estruturas de governança e gerenciamento:

- Corporativos: ERM [39], Norma ISO/IEC 31000 [16];
- Relacionados à TI: ISO/IEC 38500 [17], PMBOK [13], CMMI [30]

Embora a versão mais recente do COBIT seja a 5, lançada em 2012, esta ainda não é amplamente adotada pelo mercado, papel ocupado pela versão 4.1 do modelo, lançada por sua vez em 2007. Não por acaso, o TCU, órgão de controle na esfera pública federal, quando realiza levantamentos acerca da Governança de TI, tem utilizado como referência normativa a versão 4.1 do COBIT, conforme análise documental realizada em recentes relatórios de Auditorias realizadas pelo órgão na APF([50]; [51]; [52]). Portanto, alinhada com o mercado e com o cenário público nacional, esta pesquisa adota como referência o COBIT 4.1 [6].

3.3.5 ISR3M - Modelo de Maturidade em Gestão de Riscos de Sistemas de Informações

O ISR3M (*Information System Risk Management Maturity Model*) é um modelo de maturidade de gestão de risco que tem como objetivo atender a necessidade de avaliação, controle e melhoria da gestão de riscos no âmbito de Sistemas de Informações (SI). O modelo proposto por Maallam e Kriouile [35] possui cinco níveis de maturidade de 1 a 5 e as dimensões são os elementos da área de SI: participantes, informações, tecnologia, processos, produtos e serviços, clientes, infraestrutura, meio ambiente e estratégia. O ISR3M é baseado na abordagem da Norma ISO 31000 [16], inclusive nas atividades de gestão de riscos previstas na Norma (Figura 2.1).

Para Kriouile e Maallam [35] o modelo proposto é de fácil implementação e cumpre as melhores práticas de gestão de risco. O modelo ISR3M está estruturado em dois formatos. O primeiro formato avalia os elementos de SI no âmbito da gestão de riscos. O segundo, representa os aspectos em que essas atividades são avaliadas, ou seja, verifica a adoção de práticas relacionadas ao desenvolvimento de software.

A avaliação de maturidade é feita de acordo com a arquitetura “da área de foco". A escolha pontual permite uma abordagem mais sofisticada do que modelos abrangentes. Dessa forma, ela define pequenos passos evolutivos, tornando assim mais fácil a melhoria, menos arriscada e menos onerosa. O objetivo a ser alcançado fica mais claro e evidente para os *stakeholders*. A escolha também se justifica, tendo em conta a interdependência dos objetivos de controle, que é uma característica importante do negócio de gestão de riscos [35].

Kriouile e Maallam [35] definiram as áreas de avaliação (eixos) dos elementos principais para o desenvolvimento de software: (1) de infraestrutura, (2) estratégia, (3) ambiente, (4) tecnologia, (5) Informações, (6) participantes, (7) processo, (8) produtos e (9) clientes. Além disso, foi necessário definir também os elementos de avaliação de cada um dos eixos, os quais foram identificados por meio de pesquisa literária e *frameworks* de *software* reconhecidos internacionalmente. Já as áreas adotadas para o modelo ISR3M foram as atividades de gestão de risco da Norma ABNT ISO 31000 [16].

Para a proposição do instrumento de avaliação da maturidade em gestão de riscos, objetivo principal deste trabalho, também foi necessário uma pesquisa sobre as metodologias para elaboração de um Modelo de Maturidade que será detalhado a seguir.

3.4 Metodologias para elaboração de um Modelo de Maturidade

A norma ABNT NBR ISO/IEC 15504-3 [18], define a estrutura e condições para uma avaliação de maturidade organizacional a partir da avaliação da capacidade de processo [18]. A norma descreve os requisitos para:

- Construir modelos de maturidade organizacional;
- Realizar uma avaliação de maturidade organizacional; e
- Verificar conformidade das avaliações de maturidade organizacional.

A escala de maturidade da norma ABNT ISO/IEC 15504-4 está descrita na Figura 3.7:

Figura 3.7: Níveis de Maturidade ISO/IEC 15504. Fonte: [14]

A escala de maturidade possui seis níveis, onde sua estrutura de medição fornece para a avaliação de capacidade de um processo e uma representação crescente, que vai do "incompleto" ao "em otimização" [14].

A medição da capacidade é feita com base em um conjunto de atributos de processo, que define um escala de pontuação, podendo ser: não atingido, parcialmente atingido, amplamente atingido e completamente atingido. Para alcançar um nível de maturidade todos os processos daquele nível e do anterior devem ser alcançados [14].

Autores como Pöppelbuss e Röglinger [44] e Becker et al. [8] realizaram estudos sobre princípios comuns a serem respeitados na elaboração de modelos de maturidade. Pöppelbuss e Röglinger [44] apresentam os requisitos de qualidade esperados e desejados em um modelo de maturidade: validade, confiabilidade, eficiência, fundamentação empírica, suporte de ferramentas de software, padronização, flexibilidade, adaptabilidade, aplicabilidade de *benchmarking*, certificação, divulgação do potencial de melhoria e evidência de correlação entre a adoção do modelo e o desempenho esperado. Já Becker et al. [8] estabeleceram um conjunto de requisitos para o desenvolvimento de modelos de maturidade:

- R1 - Comparação com modelos de maturidade existentes: a necessidade de desenvolvimento de um modelo de maturidade deve ser fundamentada por uma comparação com os modelos existentes. O novo modelo pode ser resultado da ausência de modelos para um determinado domínio ou uma melhoria de um modelo já existente;
- R2 - Desenvolvimento Iterativo: modelos de maturidade devem ser desenvolvidos iterativamente, passo a passo;
- R3 - Avaliação: todos os princípios e premissas para o desenvolvimento de um modelo de maturidade, tais como a qualidade, utilidade e eficácia devem ser avaliadas iterativamente;
- R4 - Desenvolvimento Multimetodológico: o desenvolvimento de modelos de maturidade deve empregar uma variedade de métodos de pesquisa, cuja utilização deve ser bem fundamentada;
- R5 - Identificação da Relevância do Problema: a relevância da solução do problema proposto pelo modelo de maturidade para pesquisadores e/ou profissionais deve ser demonstrada;
- R6 - Definição do Problema: o domínio de aplicação do modelo de maturidade, bem como as condições de sua aplicação e os benefícios pretendidos, devem ser demonstrados antes da concepção;
- R7 - Apresentação Objetiva dos Resultados: a apresentação do modelo de maturidade deve ser orientada pelas condições de sua aplicação e as necessidades de seus usuários; e
- R8 - Documentação Científica: o processo de concepção do modelo de maturidade deve ser documentado em detalhes, considerando cada etapa do processo, as partes envolvidas, os métodos aplicados e os resultados.

A partir destes requisitos, os autores Becker et al. [8] propõem ainda uma sequência lógica de aplicação deles: R5 – R6 – R1 – R2 – R4 – R7 – R3 – R8.

Os trabalhos relacionados neste item foram levados em consideração para o desenvolvimento do instrumento de avaliação da maturidade em gestão de riscos, objeto do próximo capítulo.

Capítulo 4

Desenvolvimento do IAMGR

O desenvolvimento do instrumento de avaliação da maturidade é realizada com base em referenciais teóricos sobre o tema. Para isso, foram observadas as boas práticas para elaboração de um modelo de maturidade, bem como os modelos de maturidade detalhados no Capítulo anterior. O objetivo deste Capítulo é apresentar o passo a passo para o desenvolvimento do Instrumento de Avaliação da Maturidade em Gestão de Riscos (IAMGR).

Com base na metodologia para elaboração de um modelo de maturidade proposto por Becker et al. [8] e do contexto que o MP está inserido foi descrito o fluxograma para elaboração do IAMGR que consiste em cinco etapas, conforme Figura 4.1.

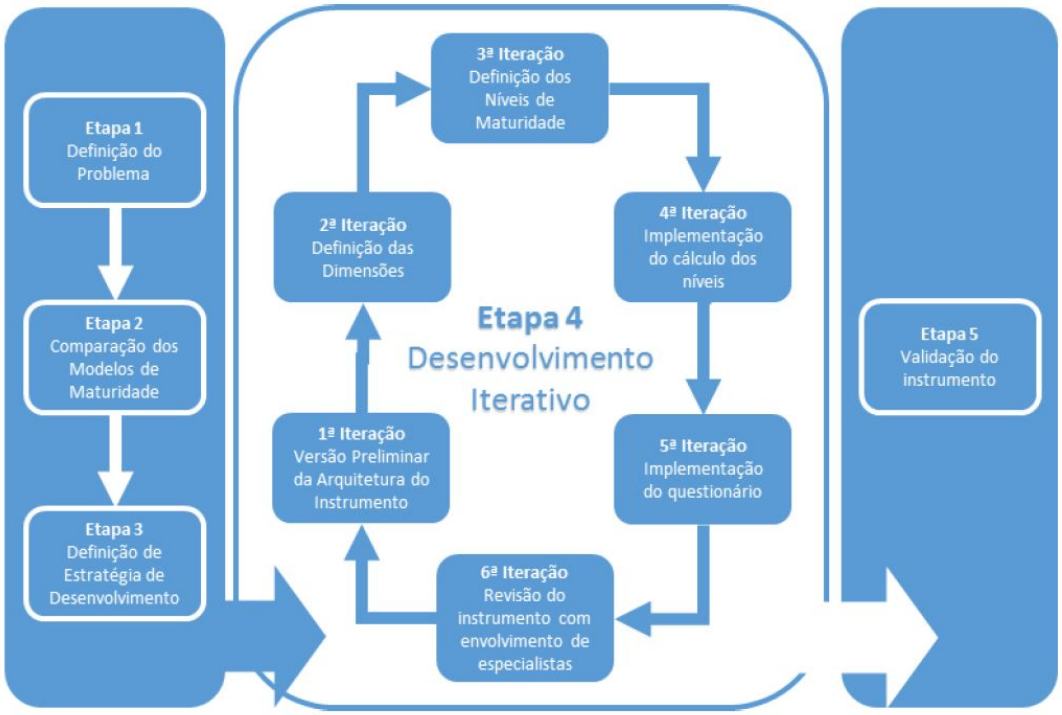


Figura 4.1: Fluxograma para elaboração do IAMGR. Fonte: adaptado de [8]

As cinco etapas para o desenvolvimento do IAMGR são descritas de forma sucinta como:

1. **Definição do problema**: essa seção é responsável por demonstrar a relevância da solução do problema proposto para os usuários do instrumento, determinando assim, o domínio de aplicação do instrumento, bem como as condições para a sua aplicação e os benefícios pretendidos.
2. **Comparação dos modelos de maturidade**: esta etapa é responsável pela comparação dos modelos de maturidade que estão relacionados ao contexto deste trabalho com o intuito de verificar o "estado da arte" sobre o tema e extrair destes modelos o que for relevante;
3. **Definição da estratégia de desenvolvimento do IAMGR**: etapa responsável pela definição de "como" será desenvolvido o IAMGR:
4. **Desenvolvimento iterativo**: etapa que trata especificamente do desenvolvimento do instrumento composta por seis iterações. Indo da definição da arquitetura preliminar do instrumento, definição das dimensões e dos níveis de maturidade, implementação do cálculo dos níveis, elaboração do questionário até a revisão do instrumento com envolvimento de especialistas;
5. **Validação do instrumento**: a última etapa consiste na validação do IAMGR que se deu, por meio da aplicação do instrumento, no ambiente do MP. A apresentação e análise dos resultados ao Gestor de TI do órgão contribui para a validação do IAMGR.

A principal alteração do modelo proposto por Becker et al. [8] foi a unificação das atividades "Concepção de transferência e validação"e "Implementação de meios de transferência"na "implementação do questionário", pois apresentam objetivos similares e relacionados com o desenvolvimento de uma ferramenta. Dessa forma, a concepção e a implementação da ferramenta foi inserida na etapa de implementação do questionário e a validação ocorre na iteração seguinte envolvendo especialistas na validação da ferramenta. Além disso, a referida atividade foi inserida na etapa 4 - Desenvolvimento iterativo, devido à necessidade de revisão em conjunto com os demais requisitos do instrumento.

As seções seguintes detalham cada etapa do desenvolvimento do IAMGR proposto neste trabalho.

4.1 Definição do Problema

A relevância da solução do problema proposto é demonstrada na disponibilização de um instrumento de avaliação da maturidade em gestão de riscos orientado aos principais processos de TI e voltado para a entidade pública.

Esse instrumento atende duas recomendações do TCU emanadas ao MP. A primeira é o desenvolvimento de instrumentos de avaliação da maturidade de gestão de riscos. E a segunda, que prevê a definição de atividades de controle para mitigar riscos das atividades relacionadas de TI [48].

O IAMGR pode ser utilizado como uma ferramenta de autoavaliação. O uso do instrumento pela Diretoria de Tecnologia de Informação (DTI), unidade de TI do MP, visa possibilitar uma avaliação da maturidade em gestão de riscos nos processos de TI, identificando os processos críticos e auxiliando na tomada de decisão pelo gestor de TI do MP.

Além disso, o uso do IAMGR nos órgãos sob jurisdição do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) garante à Secretaria de Tecnologia de Informação (STI) uma avaliação padronizada da maturidade em gestão de riscos de diversas entidades públicas, contribuindo assim para alinhar as iniciativas de Tecnologia da Informação e Comunicação (TIC) às estratégias do governo federal, caso seja utilizado.

O contato com o tema "riscos" em conjunto com os processos de TI fornecido pelo IAMGR possibilita um aumento da maturidade em gestão de riscos e, secundariamente, a governança de TI.

O IAMGR aplica-se em qualquer organização pública que queira conhecer o seu grau de maturidade em gestão de riscos nos processos de TI especificados no item 4.4.1.1, pág. 66, que totalizam onze processos. Sabe-se que nem todos os onze processos se aplicam em todas as entidades, com isso o instrumento foi elaborado prevendo tais possibilidades. Em relação às condições de aplicação do instrumento é importante que a entidade identifique a área de TI para o fornecimento de informações. Dessa forma, o questionário é respondido pela autoridade máxima de TI do órgão que deve ser julgado com imparcialidade, inserindo as evidências, sempre que possível.

Os benefícios esperados deste instrumento são:

- Conhecer o nível de maturidade em gestão de riscos de cada processo de TI do órgão;
- Fomentar a cultura de riscos na instituição;
- Definir um instrumento de avaliação mais adequado para a realidade do órgão; e

- Contribuir para a melhoria da gestão de riscos no órgão e, de forma secundária, da governança de TI.

4.2 Comparação dos modelos de maturidade

O segundo passo para elaboração de um instrumento de avaliação consiste em comparar os modelos de maturidade. Com base na revisão de literatura foi elaborado um quadro comparativo dos modelos que estão relacionados ao contexto deste trabalho (Tabela 4.1).

Tabela 4.1: Quadro comparativo dos Modelos de Maturidade em Gestão de Riscos

Modelos	**Base**	**Descrição das Dimensões**	**Descrição dos Níveis**	**Documentação**
RMM [24]	HILLSON	Cultura: Processo; Experiência; Aplicação.	Ingênuo; Principiante; Normalizado; e Natural	Um dos primeiros modelos de maturidade em gestão de riscos criados, sendo constantemente atualizados. Modelo é base para diversos novos modelos, além de inúmeras citações.
RMMM [25]	RMM	Cultura: Processo; Experiência; Aplicação	Projeto das partes interessadas; Identificação de riscos; Análise de risco; Respostas aos riscos; Gerenciamento de projetos; Cultura de gestão de risco.	Modelo baseado na obra do Hilsson com alguns artigos publicados.

Tabela 4.1: Quadro comparativo dos Modelos de Maturidade em Gestão de Riscos

Risk IT [19]	ISO 31000	Infraestrutura; Estratégia; Ambiente; Tecnologia; Informação; Participantes; Processo de negócio; Produtos e serviços; Clientes	Inexistente; Inicial/ad hoc; Repetível, mas intuitivo; Processo definido; Gerenciado e mensurado; e Otimizado.	Artigos publicado sem congressos e revistas internacionais. Autores amplamente citados.
ERM [28]	COSO	Não explícito	Inicial; Repetitivo; Definido; Gerenciado; Otimizando.	O ERM desenvolvido pelo COSO, não deixa claro em sua documentação a proposta de um modelo de maturidade. Após consulta a área mantenedora foi esclarecido que não há no modelo um modelo de maturidade.
COBIT [6]	CMM e Especialistas	Framework COBIT 4.1 provê um modelo constituído por 34 processos,	Inexistente; Inicial (ad hoc); Repetível; Definido; Gerenciado; Otimizado.	Amplo material divulgado pela mantenedora e vários artigos científicos mencionando o modelo
CMMI [30]	Especialista	Pessoas; Procedimentos e métodos; Ferramentas e equipamentos.	Inicial; Gerenciado; Definido; Quantitativamente gerenciado; Otimização	Amplo material divulgado pela mantenedora e vários artigos científicos mencionando o modelo

Tabela 4.1: Quadro comparativo dos Modelos de Maturidade em Gestão de Riscos

Modelo de Maturidade do TCU [49]	COSO, Tesouro Britânico e a Norma ABNT ISO31000:2009	Ambiente de Gestão de Riscos; Processos de Gestão de Riscos; Gestão de Riscos em Parcerias; Resultados	Inicial; Básico; Intermediário; Aprimorado; Avançado.	Relatório de auditoria em nível de detalhamento satisfatório, inclusive com o detalhamento sobre a construção do modelo. Observa-se que algumas partes não são publicadas. Ex.: questionário
NBR ISO 15504-3 [18]	Especialistas	Não explícito	Incompleto; Executado; Gerenciado; Estabelecido; Previsível; Em otimização.	As normas da família ISO15504 são mantidas pela ABNT e podem ser adquiridas por aproximadamente R$ 150,00 cada. As normas vigentes são: 15504-1,15504-3 e 15504-4. Elas são normas de 2008 e ainda não passaram por nenhuma revisão.
ISR3M [35]	ISO	Especialista	Nível 1; Nível 2: Nível 3; Nível 4; Nível 5.	Modelo de Maturidade baseado na abordagem da ISO31000 e as 5 atividades principais: (1) Comunicação, (2) Estabelecimento do contexto, (3) Avaliação do risco, (4) Tratamento do risco e (5) Monitoramento e Revisão

Um item de suma importância para a comparação dos modelos é a documentação. Becker et al. [8] esclarecem que somente os modelos de maturidade que apresentam uma documentação detalhada tornam viável tal comparação. Dessa forma, no comparativo dos modelos foram considerados somente os modelos que apresentaram uma documentação mínima de implantação.

Apesar de terem sido referenciados diversos modelos de maturidade com aplicações gerais (item 3.1), o fato de não constarem no quadro comparativo não significa que não foram utilizados no desenvolvimento do instrumento. Becker et al. [8] citam que a análise de modelos fora do contexto original não se perde, pois valerá como incentivos por modificações do modelo.

Os Modelos de Maturidade elencados na Tabela 4.1 são considerados como referência e foram utilizados como base para a proposição do instrumento, objeto desse estudo, subsidiando assim a definição da estratégia de desenvolvimento do instrumento.

4.3 Definição da estratégia de desenvolvimento do IAMGR

Este passo consiste em definir a Estratégia de desenvolvimento do instrumento, ou seja, apresentar "como" o IAMGR é desenvolvido.

Antes de definir a estratégia, se faz necessário definir a diretriz do modelo. Becker et al. [8] propõem as seguintes opções de diretrizes:

- Criação de um modelo totalmente novo - inovador;
- Implementação de melhorias de um modelo existente;
- Combinação de vários modelos em um modelo;
- Transferência de estruturas ou conteúdos de modelos existentes para uma nova aplicação.

No caso deste trabalho, a diretriz definida é a combinação de vários modelos em um único modelo, pois foram observados pontos relevantes em cada modelo, conforme detalhado abaixo:

- O primeiro ponto observado é a nomenclatura utilizada para os níveis de maturidade do RMM [24]: ingênuo, principiante, normalizado e natural. Araújo [4] definiu como critério de seleção de modelo de maturidade a nomenclatura dos níveis de

maturidade, evidenciando que o nome deve ser suficientemente claro, ou seja, auto-explicativo. Nessa mesma linha, De Bruin et al. [12] reforçam que os níveis devem ser nomeados com rótulos curtos e que deem uma clara indicação do propósito do nível. Alguns Modelos de Maturidade apresentam apenas um número indicando a sua maturidade que, geralmente, vão de 0 a 5, onde "0" é o nível inicial e o "5" o último nível da maturidade.

- O RMMM [25] insere atividades voltadas aos riscos como níveis de maturidade (projeto das partes interessadas, identificação de riscos, análise de risco, respostas aos riscos, gerenciamento de projetos e cultura de gestão de risco).
- A ferramenta Risk IT [19] se baseia na ISO 31000 que entrelaça controles específicos (políticas, procedimentos, práticas, estruturas organizacionais) com cada atividade do processo de gerenciamento de riscos da Norma. Nessa mesma linha, o modelo ISR3M proposto por Maallam e Kriouile [35], é baseado na abordagem da Norma ISO 31000 [16], em especial nas atividades principais da norma.
- O COBIT [6] utiliza o conceito de controles, especificamente no processo P09 – "Avaliar e Gerenciar os Riscos de TI" que define seis controles gerenciais que devem ser considerados pela área de TI na implementação do processo (Tabela 3.3), de forma a prover uma razoável garantia de que os objetivos de negócio possam ser atingidos e que eventos indesejáveis possam ser prevenidos, ou ainda detectados e corrigidos.
- O modelo do TCU [49] foi criado com base em um modelo voltado para a aplicação no governo e utiliza a norma ISO 31000 [16] e o ERM [39] como referências. A estrutura das dimensões do modelo possui um viés de governo e demonstra aderência nas orientações da gestão pública de excelência.
- A proposta de Maallam e Kriouile [35] que apresentaram um modelo genérico e efetivo, denominado como ISR3M (*Information System Risk Management Maturity Model*), também é interessante, pois eles demonstraram a viabilidade na utilização dos processos de gestão de riscos da norma ISO 31000 [16] com a estrutura utilizada na área de sistemas de informações.

A Estratégia de Desenvolvimento do instrumento proposto prevê relacionar os processos de Gestão de Riscos da Norma ISO 31000:2009 [16] com cada processo de TI elencado pelo TCU [48]. Criando assim um instrumento de avaliação da maturidade em gestão de riscos orientado aos processos de TI.

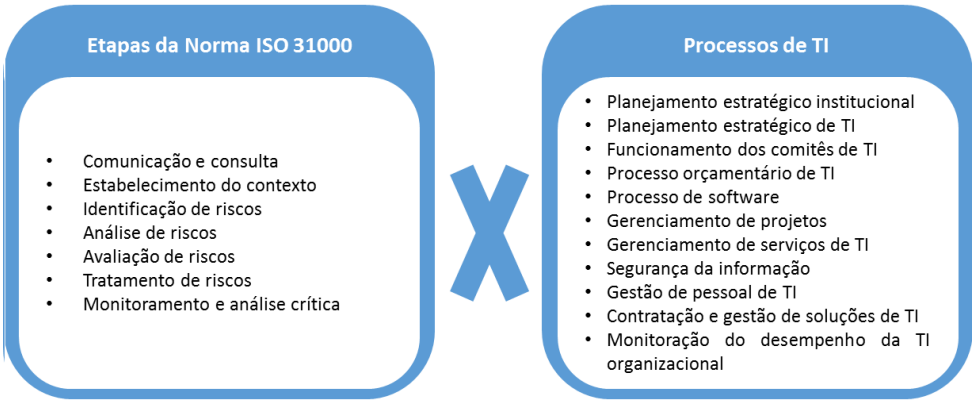


Figura 4.2: Estratégia de desenvolvimento do IAMGR

Os modelos: IS3RM [35], Risk IT [19] e RMMM [25] foram utilizados como base para a definição da estratégia de desenvolvimento do IAMGR, pois eles entrelaçam as atividades da gestão de gestão de riscos aos contextos dos modelos de maturidade: sistemas de informação, riscos de TI e de Projeto, respectivamente.

Definida a estratégia de desenvolvimento do IAMGR, a próxima seção apresenta o desenvolvimento do instrumento que se dá de forma iterativa.

4.4 Desenvolvimento Iterativo

Um modelo de maturidade deve ser desenvolvido de forma repetitiva, possibilitando que a proposta seja: projetada, refinada, avaliada e, se necessário, melhorada [41]. No contexto de um modelo de maturidade, significa que ele seja construído etapa por etapa [8]. O instrumento proposto contém seis iterações na 4ª etapa - Desenvolvimento Iterativo, indo da estrutura inicial até a revisão do instrumento com envolvimento de especialistas, conforme Figura 4.3.

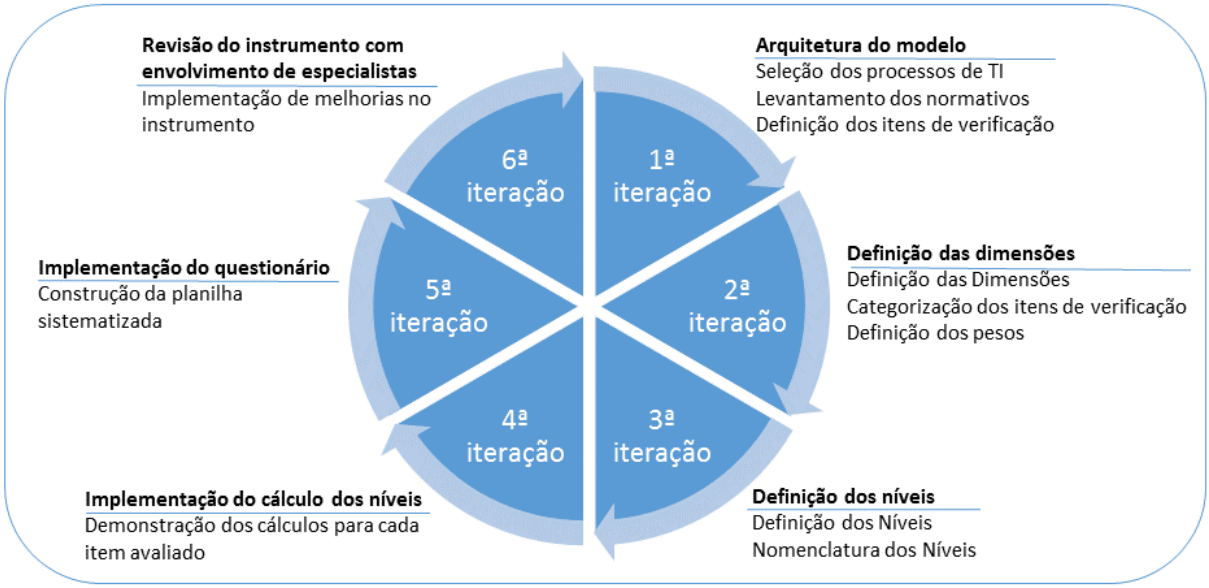


Figura 4.3: Iterações da etapa Desenvolvimento Iterativo

Os objetivos de cada iteração são apresentados a seguir:

- 1ª Iteração: definir a versão preliminar da arquitetura do instrumento. Para isso, se faz necessário a seleção dos processos de TI, a identificação dos normativos que orientam cada processo de TI, viabilizando a identificação dos itens de verificação dos respectivos processos;
- 2ª Iteração: definir as dimensões, categorizando os itens de verificação. Além disso, apresentar uma proposta de pesos para cada dimensão;
- 3ª Iteração: definir os níveis de maturidade e sua nomenclatura.
- 4ª Iteração: demonstrar os cálculos aplicados para cada item de avaliação, definindo o intervalo de pontuação de cada nível;
- 5ª Iteração: desenvolver a ferramenta de coleta de informações, por meio de questionários, disponibilizando os resultados da aplicação do instrumento;
- 6ª Iteração: revisar o instrumento com envolvimento de especialistas.

Os próximos itens apresentam o detalhamento das seis iterações, sendo que a 1ª iteração apresenta a estrutura inicial do IAMGR.

4.4.1 Desenvolvimento da 1ª Iteração

A estrutura básica do instrumento leva em consideração os onze processos de TI elencados na Auditoria do TCU realizada no MP [48], conforme Tabela 4.23.

Tabela 4.2: Processos de TI

Processos de TI
Planejamento Estratégico Institucional (PEI)
Planejamento Estratégico de TI (PETI)
Funcionamento dos Comitês de TI (FCTI)
Orçamentário de TI (OTI)
Processo de Software (PS)
Gerenciamento de Projetos de TI (GPTI)
Gerenciamento de Serviços de TI (GSTI)
Segurança da Informação (SI)
Gestão de Pessoal de TI (GPeTI)
Contratação e Gestão de Soluções de TI (CGSTI)
Monitoração do Desempenho da TI (MDTI)

Sabe-se que cada processo possui um conjunto de normativos legais e/ou melhores práticas que orientam a APF na busca de uma maior governança e gestão em TI.

Como o objetivo foi verificar qual é o instrumento legal que os Órgãos de Controle adotam numa auditoria inserida no contexto de riscos de TI, foi necessário uma análise documental no Relatório de Auditoria que culminou no Acórdão 1.233/2012 - TCU [48]. Essa análise é chamada de Mapeamento de Processos.

Para o mapeamento dos processos é primordial a execução de três passos: seleção dos processos de TI, levantamento dos normativos e a identificação dos itens de verificação.

Passo 1: seleção dos processos de TI

Esse passo consiste na seleção dos processos de TI. Considerando que os processos de TI elencados pelo Órgão de Controle são críticos e de comum aplicação nos diversos órgãos da APF, foi definido o mapeamento dos onze processos.

Passo 2: levantamento dos normativos

O passo seguinte objetiva identificar os documentos de referência (regramentos, regulamentos, normas ou guias de melhores práticas). Cada processo de TI possui um ou mais documentos de referência. Por meio da pesquisa documental nos relatórios de auditoria

foi possível levantar os documentos que o TCU considera como referência para cada processo de TI. A seguir são relacionados os documentos de referência levantados para cada processo.

1. **Planejamento Estratégico Institucional (PEI)**

   O PEI tem como o principal regulamento orientador o Programa Nacional de Gestão Pública e Desburocratização (GESPUBLICA). O Programa foi instituído pelo Decreto n. 5.378, de 23 de fevereiro de 2005, que demonstra o resultado da evolução histórica de diversas iniciativas do Governo Federal para a promoção da gestão pública de excelência, visando a contribuir para a qualidade dos serviços públicos prestados ao cidadão e para o aumento da competitividade do país [36] .

   Visto como uma política pública fundamentada em um modelo de gestão específico, o GESPUBLICA tem como principais características o fato de ser essencialmente público: orientado ao cidadão e respeitando os princípios constitucionais da impessoalidade, da legalidade, da moralidade, da publicidade e da eficiência; de ser contemporâneo; alinhados ao estado da arte da gestão; de estar voltado para a disposição de resultados para a sociedade; com impactos na melhoria da qualidade de vida e na geração do bem comum; e de ser federativo, ou seja, com aplicação a toda a administração pública, em todos os poderes e esferas do governo [48].

2. **Planejamento Estratégico de TI (PETI)**

   O PETI tem como principal norteador o modelo COBIT [6], conhecido como COBIT 4.1, em especial do processo PO1 – Planejamento Estratégico de TI. O planejamento estratégico de TI é requerido para gerenciar e direcionar todos os recursos da TI em linha com as estratégias e prioridades do negócio. A função da TI e os *stakeholder's* do negócio são responsáveis para assegurar que um valor otimizado é realizado por meio dos portfólios dos projetos e serviços. O plano estratégico deve aumentar a compreensão das partes interessadas chaves em relação das oportunidades e limites da TI, avaliar o desempenho atual e esclarecer o nível de investimentos requeridos [6].

   A estratégia e as prioridades do negócio devem ser refletidas nos portfolios e executadas por meio dos planos táticos da TI, os quais estabeleçam objetivos concisos, planos e tarefas compreendidas e aceitos pelo negócio e pela TI [48].

3. **Funcionamento dos Comitês de TI (FCTI)**

   O FCTI também é guiado pelo modelo COBIT [48]. Um comitê estratégico de TI tem como funções básicas assegurar que a governança de TI seja adequadamente tratada, aconselhar a direção estratégica de TI e revisar os grandes investimentos,

conforme preceitua o processo PO4.2 - Comitê Estratégico de TI [6]. Já um comitê de direção de TI (PO4.3) tem como atribuições típicas priorizar os investimentos de TI em alinhamento com a estratégia e as prioridades do negócio da instituição, acompanhar o status dos projetos e resolver conflitos por recursos e monitorar os níveis de serviço e as melhorias implantadas na organização [6].

4. **Orçamentário de TI (OTI)**

   O OTI também tem como principal norteador o COBIT [48], espera-se que os entes elaborem suas propostas (planejamento do orçamento) com base nas ações que efetivamente pretendem realizar, alinhadas aos objetivos de negócio (PO5.3), e que mantenham o acompanhamento da sua execução, de forma a saber precisamente quanto foi gasto onde e qual a disponibilidade para gastos futuros (PO5.4).

5. **Processo de Software (PS)**

   A norma ISO/IEC 15504-3 [18], também conhecida como SPICE, é a norma ISO que define processo de desenvolvimento de software. O TCU [48] cita que esta norma é reconhecida internacionalmente, inclusive sendo utilizada como referência para outros modelos, como: COBIT 5 [5] e CMMI [30].

6. **Gerenciamento de Projetos de TI (GPTI)**

   O Guia do Conjunto de Conhecimentos em Gerenciamento de Projetos (PMBOK) [13] é a consolidação dos conhecimentos em gerenciamento de projeto. O PMBOK completo inclui práticas tradicionais que são amplamente aplicadas, bem como, práticas inovadoras que estão surgindo na profissão, e as que têm um consenso generalizado sobre o seu valor e utilidade [48].

7. **Gerenciamento de Serviços de TI (GSTI)**

   A sigla ITIL, que vem de *Information Technology Infrastructure Library*, traduzido para a língua portuguesa, fica algo como Biblioteca de Infraestrutura de Tecnologia da Informação é o guia utilizado pelo TCU como referência para o gerenciamento de serviços de TI. O ITIL é uma biblioteca, ou seja, um conjunto de livros que reúne as melhores práticas em gerenciamento de serviços de TI [48]. O órgão que criou o ITIL e o mantêm é o OGC - *Office of Government Commerce*.

8. **Segurança da Informação (SI)**

   A SI não está restrita apenas a sistemas computacionais, informações eletrônicas ou qualquer outra forma mecânica de armazenamento. Ela está relacionada com a proteção existente ou necessária sobre dados, informações ou documentos que possuem valor para alguém ou uma organização [48].

Dada a importância estratégica em controlar e garantir a proteção da informação e, manter e zelar pela integridade e sigilo dos dados corporativos foram identificadas a Norma complementar n. 1/2008 do Gabinete de Segurança Institucional da Presidência da República GSI/PR e o conjunto e normas da ABNT ISO 27000, em especial a ISO 27002 e ISO 27005.

9. **Gestão de Pessoal de TI (GPeTI)**

   Para a efetiva Gestão de Pessoal de TI foi levado em consideração o Decreto n. 5.707/2006 que define a Política e as Diretrizes para o Desenvolvimento de Pessoal da administração pública federal direta, em especial aos arts. 2º e 5º, bem como a sua regulamentação pela Portaria MP 208/2006 [48].

   Observa-se ainda que outras referências são utilizadas pelo o TCU para a Gestão de pessoal de TI, como: encontrar dentro de um setor de TI uma estrutura formal (PO4.5), com papéis e suas responsabilidades formalmente definidos (PO4.6), em que os papéis sensíveis encontrem-se com responsáveis formalmente designados (PO4.13), ambos processos estão positivados no modelo do COBIT [6]. Ademais o órgão de controle cita que é necessário que os responsáveis pela gestão da TI das organizações sejam integrantes do quadro da organização, conforme Decreto-Lei n. 200/1967 no seu art. 10, § 7º.

10. **Contratação e Gestão de Soluções de TI (CGSTI)**

    A IN MP/SLTI n. 4, de 11 de setembro de 2014, foi editada pela Secretaria de Logística e Tecnologia da Informação – SLTI, atualmente denominada como Secretaria de Tecnologia de Informação (STI) e dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) do Poder Executivo Federal. Tem como principal objetivo elevar a possibilidade de sucesso das aquisições de soluções de TI, bem como de reduzir o desperdício dos recursos financeiros aplicados.

    Esse modelo é resultante da compilação de normativos que se encontravam esparso em regulamentos diversos, além de englobar boas práticas reconhecidas pelo mercado e entendimentos jurisprudenciais relacionados ao tema, e publicados até a edição da referida norma [48]. A aplicação da IN 4/2014 é obrigatória para os órgãos e entidades da administração pública federal direta, autárquica e fundacional, e recomendável para os demais órgãos e entidades de toda a Administração, inclusive a Estadual e Municipal.

11. **Monitoração do Desempenho da TI (MDTI)**

    A MDTI tem como referência também o COBIT 4.1, em especial o processo de operacional PO1.4 – Plano estratégico e o processo de medição ME1.1 – Abordagem de monitoramento. Tendo como objetivo principal o estabelecimento de objetivos, indicadores e metas para a gestão de TI, o que já deveria estar no Plano Diretor de TI [48].

    Com a identificação dos documentos de referência de cada processo, torna-se possível a identificação dos itens de verificação. O passo seguinte detalha esta análise realizada.

Passo 3: definição dos itens de verificação

O último passo dessa iteração é responsável por identificar os "itens de verificação", ou seja, os pontos observados pelo órgão de controle em cada processo. Com a execução dos passos anteriores foi possível identificar para cada processo as evidências coletadas pelo TCU, evidenciando assim os "Itens de verificação". Os quadros seguintes listam os itens de verificação por processos.

Tabela 4.3: Itens de verificação do processo Planejamento Estratégico Institucional (PEI)

Processo	**Código**	**Itens de verificação**
PEI	PEI01	Existe a elaboração, com participação de representantes dos diversos setores da organização, de um documento que materialize o PEI de longo prazo, contemplando,pelo menos, objetivos, indicadores e metas para a organização?
	PEI02	Existe a aprovação, pela mais alta autoridade da organização, do PEI?
	PEI03	O PEI é desdobrado pelas unidades executoras?
	PEI04	Existe a divulgação do PEI para conhecimento dos cidadãos brasileiros, exceto nos aspectos formalmente declarados sigilosos ou restritos?
	PEI05	Existe o acompanhamento periódico do alcance das metas estabelecidas, para correção de desvios?
	PEI06	Existe a divulgação interna e externa do alcance das metas, ou dos motivos de não as ter alcançado?

Tabela 4.4: Itens de verificação do processo Planejamento Estratégico de TI (PETI)

Processo	**Código**	**Itens de verificação**
PETI	PETI01	O PETI é publicado formalmente?
	PETI02	A elaboração do PETI é feita com a participação das áreas de negócio, da Alta Administração e da TI?
	PETI03	O PETI é elaborado com métodos e técnicas indicadas no COBIT 4.1, em especial do processo PO1 – Planejamento Estratégico de TI?
	PETI04	O PETI é desdobrado pelas diversas áreas executoras em plano de médio e curto prazo?
	PETI05	Existe a divulgação do PETI?
	PETI06	Existe a avaliação periódica do PETI?
	PETI07	O PETI está alinhado com o Planejamento Estratégico Institucional (PEI)?

Tabela 4.5: Itens de verificação do processo Funcionamento dos Comitês de TI (FCTI)

Processo	**Código**	**Itens de verificação**
FCTI	FCTI01	A organização possui comitês de TI vigentes e implementados com base no modelo COBIT 4.1, em especial do processo PO4.2 - Comitê Estratégico de TI
	FCTI02	Existe a descrição do Funcionamento dos Comitês de TI?
	FCTI03	Há indicação da composição dos representantes da área de negócio e de TI?
	FCTI04	O Funcionamento dos Comitês de TI é realizado periodicamente?

Tabela 4.6: Itens de verificação do processo Orçamentário de TI (OTI)

Processo	**Código**	**Itens de verificação**
OTI	OTI01	É feita a previsão de orçamento de TI na LOA?
	OTI02	Existe uma proposta orçamentária de TI feita com base nas estimativas de custos das atividades que pretendem executar alinhadas aos objetivos do negócio da organização?
	OTI03	É realizado um acompanhamento ao longo do exercício financeiro dos gastos efetuados especificamente com TI?

Tabela 4.7: Itens de verificação do Processo de Software (PS)

Processo	**Código**	**Itens de verificação**
PS	PS01	Existe a definição do Processo de Software com base na Norma ISO/IEC 15504-3?
	PS02	O Processo de Software é formalizado?
	PS03	Existe a divulgação do Processo de Software?
	PS04	O Processo de Software sofre uma avaliação periódica?

Tabela 4.8: Itens de verificação do processo Gerenciamento de Projetos de TI (GPTI)

Processo	**Código**	**Itens de verificação**
GPTI	GPTI01	O processo de gerenciamento de projetos de TI é baseado no guia do Conjunto de Conhecimentos em Gerenciamento de Projetos, conhecido como PMBOK?
	GPTI02	O processo de gerenciamento de projeto de TI está formalizado?
	GPTI03	O processo de gerenciamento de projeto de TI foi divulgado?
	GPTI04	O processo de gerenciamento de projeto de TI é avaliado periodicamente?

Tabela 4.9: Itens de verificação do processo Gerenciamento de Serviços de TI (GSTI)

Processo	**Código**	**Itens de verificação**
GSTI	GSTI01	A gestão de serviços da TI possui um catálogo de serviços normatizado?
	GSTI02	Existe algum plano da continuidade dos serviços de TI já implantado?
	GSTI03	Existe um processo de gerenciamento de configuração e ativos normatizado?
	GSTI04	Existe um processo de gerenciamento de incidentes normatizado?
	GSTI05	Existe um processo de gerenciamento de mudanças normatizado?
	GSTI06	A gestão de serviços de TI possui um processo de gerenciamento da liberação e implantação normatizado?
	GSTI07	A gestão de serviços de TI possui um processo de gerenciamento de problemas normatizado?

Tabela 4.10: Itens de verificação do processo Segurança da Informação (SI)

Processo	**Código**	**Itens de verificação**
SI	SI01	Foi definido um responsável pela segurança da informação?
	SI02	O funcionamento do comitê de segurança de informação possui uma descrição?
	SI03	A política de segurança da informação é publicada formalmente?
	SI04	Existe uma equipe de tratamento e resposta a incidentes em redes computacionais formalizada?
	SI05	Existe um inventário de ativos de informação normatizado?
	SI06	A classificação da informação é normatizada?
	SI07	A gestão de riscos de segurança da informação está normatizada?

Tabela 4.11: Itens de verificação do processo Gestão de Pessoal de TI (GPeTI)

Processo	**Código**	**Itens de verificação**
GPeTI	GPeTI01	O plano anual de capacitação institucionalizado existe?
	GPeTI02	Existe um plano anual de capacitação que contempla a área de gestão de TI?
	GPeTI03	Existe um programa de capacitação em governança e em gestão de TI?
	GPeTI04	É feita uma forma de avaliação do quadro do pessoal de TI?
	GPeTI05	Metas de desempenho do pessoal de TI são adotadas?
	GPeTI06	É realizada uma avaliação periódica de desempenho do pessoal de TI?
	GPeTI07	Há algum benefício financeiro para instituição em função do desempenho alcançado pelo pessoal de TI?

Tabela 4.12: Itens de verificação do processo Contratação e Gestão de Soluções de TI (CGSTI)

Processo	**Código**	**Itens de verificação**
CGSTI	CGSTI01	O órgão realiza as contratações de soluções de TI de acordo com a Instrução Normativa n. 04/2010 da SLTI-MP?
	CGSTI02	Existem controles que promovam o cumprimento da IN4?
	CGSTI03	Existem controles que promovam a regularização da gestão contratual?

Tabela 4.13: Itens de verificação do processo Monitoração do Desempenho da TI (MDTI)

Processo	**Código**	**Itens de verificação**
MDTI	MDTI01	São estabelecidos objetivos, indicadores e metas para gestão de TI com base no COBIT 4.1, em especiais os processos de operação PO1.4 – Plano estratégico e o de medição ME1.1 - Abordagem de monitoramento?
	MDTI02	A gestão de TI é monitorada por meio de relatórios gerenciais?
	MDTI03	A avaliação da gestão de TI é realizada?
	MDTI04	O acompanhamento periódico do alcance das metas estabelecidas para correção de desvios é feita?
	MDTI05	A unidade de auditoria interna do órgão apoia a realização das 3 últimas tarefas acima?

A arquitetura do IAMGR prevê que cada "Item de verificação" de um processo de TI específico seja avaliado quanto aos processos de gerenciamento de riscos (Figura 2.1) da norma ISO 31000 [16], contribuindo assim para o cumprimento das etapas previstas nos documentos de referência em conjunto com a análise efetiva de riscos. Entende-se que se esta diretriz é realizada de forma simultânea, este instrumento guia a organização para um aprimoramento da maturidade tanto na governança de TI como na gestão de riscos.

Dessa forma, o IAMGR pode ser aplicado em um único processo de TI, em alguns ou em todos os onze processos de TI. Ou seja, pode ser avaliada a maturidade em gestão de riscos de um processo específico ou do conjunto deles.

4.4.2 Desenvolvimento da 2ª Iteração

Esta seção analisa os "Itens de Verificação" com o intuito de definir as dimensões propostas no IAMGR.

Desenvolvimento das Dimensões

A segunda iteração prevê a definição das dimensões do instrumento proposto. Para tanto são considerados os modelos do TCU [49] e IS3RM [35], além dos programas de excelência de gestão: o Programa Nacional de Gestão Pública e Desburocratização (GESPUBLICA) [38] com atuação no governo e o Prêmio Nacional de Qualidade (PNQ) [11] com atuação na iniciativa privada.

O GESPUBLICA tem como principais características o fato de ser essencialmente público – orientado ao cidadão e respeitando os princípios constitucionais da impessoalidade, da legalidade, da moralidade, da publicidade e da eficiência –, de ser contemporâneo – alinhado ao estado da arte da gestão –, de estar voltado para a disposição de resultados para a sociedade – com impactos na melhoria da qualidade de vida e na geração do bem comum – e de ser federativo – com aplicação a toda a administração pública, em todos os poderes e esferas do governo [38].

Por sua vez, o Modelo de Excelência em Gestão Pública (MEGP) representa a principal referência a ser seguida pelas instituições públicas que desejam aprimorar constantemente seus níveis de gestão. Como todo modelo de gestão, o MEGP contém diretrizes expressas em seus critérios de excelência gerencial (liderança, estratégias e planos, cidadãos, sociedade, informação e conhecimento, pessoas, processos e resultados).

A Fundação Nacional da Qualidade [11] é um centro brasileiro de estudo, debate e irradiação de conhecimento sobre excelência em gestão. Criada em 1991, a FNQ é uma instituição sem fins lucrativos, fundada por 39 organizações, privadas e públicas, cujo objetivo é disseminar amplamente os Fundamentos e os Critérios de Excelência em Gestão para organizações de todos os setores e portes, contribuindo para o aperfeiçoamento da gestão, o aumento da competitividade das organizações e, consequentemente, para a melhoria da qualidade de vida do povo brasileiro. O Prêmio Nacional da Qualidade (PNQ) é utilizado para promover a melhoria da qualidade da gestão e o aumento da competitividade das organizações. Por isso, o PNQ é considerado o maior reconhecimento à excelência na gestão das organizações sediadas no Brasil [11]. Oliveira e Martins [40] reforçam que o PNQ é a representação de esforços de alguns países para melhorar a reputação internacional no âmbito da qualidade, além de reconhecer as organizações que são referências em excelência da gestão no Brasil.

As categorias do GESPUBLICA são: liderança, estratégias e planos, cidadãos, sociedade, informações e conhecimento, pessoas e processos [38].

A Tabela 4.14 apresenta um comparativo das dimensões dos modelos relacionados acima.

Tabela 4.14: Comparação das dimensões de modelos de referência

IS3RM [35]	**TCU** [49]	**GESPUBLICA** [38]	**PNQ** [11]
Infraestrutura	Ambiente	Liderança	Liderança
Estratégia	Processo	Estratégias e planos	Estratégias e planos
Ambiente	Parcerias	Cidadãos	Clientes
Informação		Informações e conhecimento	Informações e conhecimento
Participantes		Pessoas	Pessoas
Processos		Processos	Processos
Produtos		Resultados	Resultados
Produtos			
Clientes			

As dimensões enumeradas na Tabela 4.14 apresentam um alto grau de similaridade e são úteis para a definição das dimensões do instrumento.

Tomando como base as categorias do GESPUBLICA [38], do PNQ [11] e o contexto que o IAMGR está inserido, foram definidas as cinco dimensões fundamentais do IAMGR (Figura 4.4), aderentes aos programas de excelência de gestão: GESPUBLICA [38] e PNQ [11] e aos modelos de maturidade do TCU [49] e do IS3RM [35].

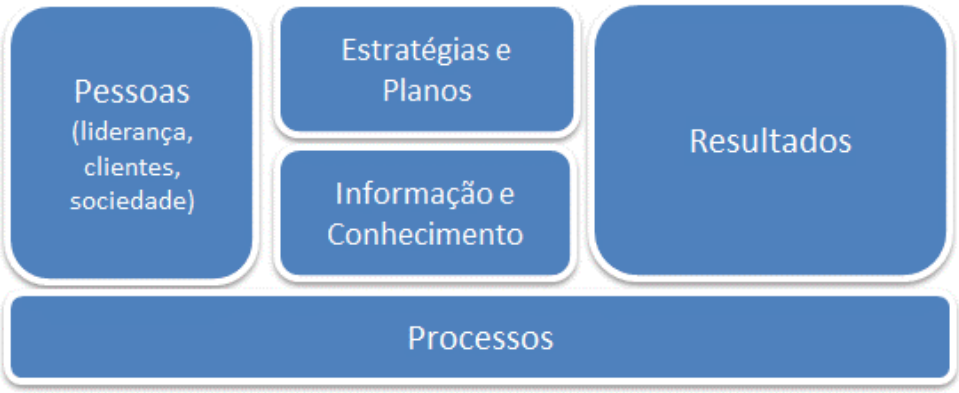


Figura 4.4: Dimensões do IAMGR

As dimensões são descritas da seguinte forma:

- **Pessoas**: esta divisão agrupa os recursos humanos responsáveis pela execução das atividades, bem como as que relacionam com a organização, podendo ser: sociedade, clientes e os líderes. A norma ISO 31000 [16] indica que estes aspectos devem ser levados em consideração para melhorar a sua maturidade na gestão de riscos.
- **Estratégias e Planos**: processos gerenciais relativos à concepção e a execução das estratégias, inclusive aqueles referentes ao estabelecimento de metas e ao acompanhamento de planos necessários para o êxito das estratégias [11].
- **Informação e Conhecimento**: as informações da organização e o conhecimento são ativos intangíveis geradores de diferenciais competitivos [11].
- **Processos**: processos gerenciais relativos aos da organização, tratando separadamente os de TI.
- **Resultados**: as entregas da TI quando agrega valor aos resultados organizacionais são consideradas para o instrumento proposto.

Categorização dos itens de verificação

Uma vez definida as cinco dimensões do IAMGR, foi realizada entrevista com especialistas para categorizar cada item de verificação. O método consistiu em aplicar um questionário para três especialistas, sendo um deles o Diretor de TI do MP com mais de 20 anos de experiência em gestão de TI, um Coordenador-Geral de Governança de TI do setor público com mais 10 anos na área e um especialista em TI também com 10 anos de experiência.

Durante a fase de preparação do questionário foi elaborada uma planilha listando todos os itens de verificação mapeados agrupando-os pelos processos de TI. A planilha permite que cada item de verificação seja categorizado a uma das cinco dimensões do IAMGR.

Antes da aplicação do questionário foi realizada reunião com a participação dos três especialistas para esclarecer o objetivo do questionário. Após alguns esclarecimentos, a planilha foi enviada para cada especialista.

De posse das planilhas respondidas observou-se que houve alguns pontos divergentes. Sendo assim, foi necessário realizar uma reunião de alinhamento com os especialistas. Nesta ocasião, os pontos divergentes foram debatidos e o grupo entrou em consenso, conforme Tabela 4.15.

Tabela 4.15: Identificação das dimensões dos itens de verificação

Processos	**Itens**	**Dimensão**
Planejamento Estratégico Institucional (PEI)	PEI01	Estratégias e Planos
	PEI02	Estratégias e Planos
	PEI03	Estratégias e Planos
	PEI04	Pessoas
	PEI05	Resultados
	PEI06	Resultados
Planejamento Estratégico de TI (PETI)	PETI01	Estratégias e Planos
	PETI02	Estratégias e Planos
	PETI03	Processos
	PETI04	Estratégias e Planos
	PETI05	Informação e Conhecimento
	PETI06	Resultados
	PETI07	Estratégias e Planos
Funcionamento dos Comitês de TI (FCTI)	FCTI01	Processos
	FCTI02	Processos
	FCTI03	Pessoas
	FCTI04	Resultados
Orçamentário de TI (OTI)	OTI01	Processos
	OTI02	Processos
	OTI03	Resultados
Processo de Software (PS)	PS01	Processos
	PS02	Processos
	PS03	Informação e conhecimento
	PS04	Resultados

Tabela 4.15: Identificação das dimensões dos itens de verificação

Gerenciamento de Projetos de TI (GPTI)	GPTI01	Processos
	GPTI02	Processos
	GPTI03	Informação e conhecimento
	GPTI04	Resultados
Gerenciamento de Serviços de TI (GSTI)	GSTI01	Processos
	GSTI02	Estratégias e Planos
	GSTI03	Processos
	GSTI04	Processos
	GSTI05	Processos
	GSTI06	Processos
	GSTI07	Processos
Segurança da Informação (SI)	SI01	Pessoas
	SI02	Processos
	SI03	Estratégias e Planos
	SI04	Processos
	SI05	Processos
	SI06	Processos
	SI07	Processos
Gestão de Pessoal de TI (GPeTI)	GPeTI01	Estratégias e Planos
	GPeTI02	Processos
	GPeTI03	Processos
	GPeTI04	Resultados
	GPeTI05	Resultados
	GPeTI06	Resultados
	GPeTI07	Resultados
Contratação e Gestão de Soluções de TI (CGSTI)	CGSTI01	Processos
	CGSTI02	Processos
	CGSTI03	Processos

Tabela 4.15: Identificação das dimensões dos itens de verificação

Monitoração do Desempenho da TI (MDTI)	MDTI01	Resultados
	MDTI02	Processos
	MDTI03	Resultados
	MDTI04	Resultados
	MDTI05	Processos

Com o intuito de apresentar uma tabela mais enxuta, foi referenciado apenas os códigos dos itens de verificação, sendo que a descrição destes itens estão dispostos na Tabela 4.3 à Tabela 4.13.

A seguir, é apresentada de forma resumida a relação dos processos de TI, suas respectivas dimensões e a quantidade de itens de verificação (Tabela 4.16).

Tabela 4.16: Relação das dimensões dos processos de TI

Processos de TI e Dimensões	**Qtde. de itens de verificação**
Planejamento Estratégico Institucional (PEI)	**6**
Resultados	2
Estratégias e planos	3
Pessoas (Liderança, Clientes, Sociedade e Pessoas)	1
Planejamento Estratégico de TI (PETI)	**7**
Processos	1
Resultados	1
Estratégias e Planos	4
Informação e conhecimento	1
Orçamentário de TI (OTI)	**3**
Processos	2
Resultados	1
Processo de Software (PS)	**4**
Processos	2
Resultados	1
Informação e conhecimento	1
Gerenciamento de Projetos de TI (GPTI)	**4**
Processos	2
Resultados	1
Informação e conhecimento	1
Gerenciamento de Serviços de TI (GSTI)	**7**
Processos	6
Resultados	1

Segurança da Informação (SI)	**7**
Processos	5
Estratégias e planos	1
Pessoas (Liderança, Clientes, Sociedade e Pessoas)	1
Gestão de Pessoal de TI (GPeTI)	**7**
Processos	2
Resultados	4
Estratégias e planos	1
Contratação e Gestão de Soluções de TI (CGSTI)	**3**
Processos	3
Monitoração do Desempenho da TI (MDTI)	**5**
Processos	2
Resultados	3
Funcionamento dos Comitês de TI (FCTI)	**4**
Processos	2
Resultados	1
Pessoas (Liderança, Clientes, Sociedade e Pessoas)	1

As dimensões podem ter pesos diferenciados como é o caso dos critérios do PNQ. Sendo assim, a próxima seção apresenta os pesos para as dimensões definidas do IAMGR.

Definição dos pesos das Dimensões

O Modelo de Excelência da Gestão (MEG) previsto no PNQ pontua os critérios de excelência para avaliação do grau de maturidade da gestão. A escala de pontuação compreende o intervalo de 0 (zero) a 1.000 (mil). Cada critério possui um valor máximo, conforme Tabela 4.17. Esse criterioso processo de avaliação submete a organização uma profunda análise de sua gestão, que é efetuada por avaliadores treinados e capacitados pela FNQ, guiados por um rigoroso código de ética. Ao final do processo, a empresa obtém um amplo Diagnóstico de Maturidade da Gestão (DMG), com comentários que sinalizam os pontos fortes e as oportunidades de melhoria, assim como os eixos potencializadores e fragilizadores da gestão. Vale ressaltar que a distribuição de pontos advém de comparações realizadas com modelos similares adotados por outros países. [11].

Tabela 4.17: Distribuição de pontos do PNQ. Fonte: [11]

Critérios do PNQ	**Pontos do PNQ**
1 - Liderança	110
2 - Estratégias e Planos	60
3 - Clientes	60
4 - Sociedade	60
5 - Informação e Conhecimento	60
6 - Pessoas	90
7 - Processos	110
8 - Resultados	450

Considerando uma equivalência com as dimensões definidas para o instrumento proposto, é possível atribuir os pesos das dimensões do IAMGR, conforme Tabela 4.18.

Tabela 4.18: Distribuição dos pontos e pesos do IAMGR

Dimensões do IAMGR	**Pontos do IAMGR**	**Pesos do IAMGR**
Pessoas (Liderança, Clientes, Sociedade e Pessoas)	320	32%
Estratégias e Planos	60	6%
Informação e Conhecimento	60	6%
Processos	110	11%
Resultados	450	45%

A próxima seção apresenta os níveis de maturidade do Instrumento de Avaliação da Maturidade em Gestão de Riscos (IAMGR).

4.4.3 Desenvolvimento da 3ª Iteração

Esta iteração prevê a identificação dos níveis de maturidade do IAMGR.

O IAMGR é estruturado em estágios e apresenta 5 níveis de maturidade. Para a nomenclatura dos níveis foram utilizados termos intuitivos, conforme preconiza Araújo [4]. Para definir a quantidade de níveis de maturidade foi levada em consideração a proposta de Pöppelbuß e Röglinger [44], que considera ideal os modelos que tenha de quatro e seis níveis. Sendo assim, o IAMGR possui cinco níveis de maturidade (Vulnerável, Reativo, Complacente, Proativo e Otimizado). Estes níveis de maturidade foram definidos considerando os onze processos auditáveis pelo TCU. Para cada nível de maturidade foi identificada uma ou duas características principais, conforme descrito na Figura 4.5.

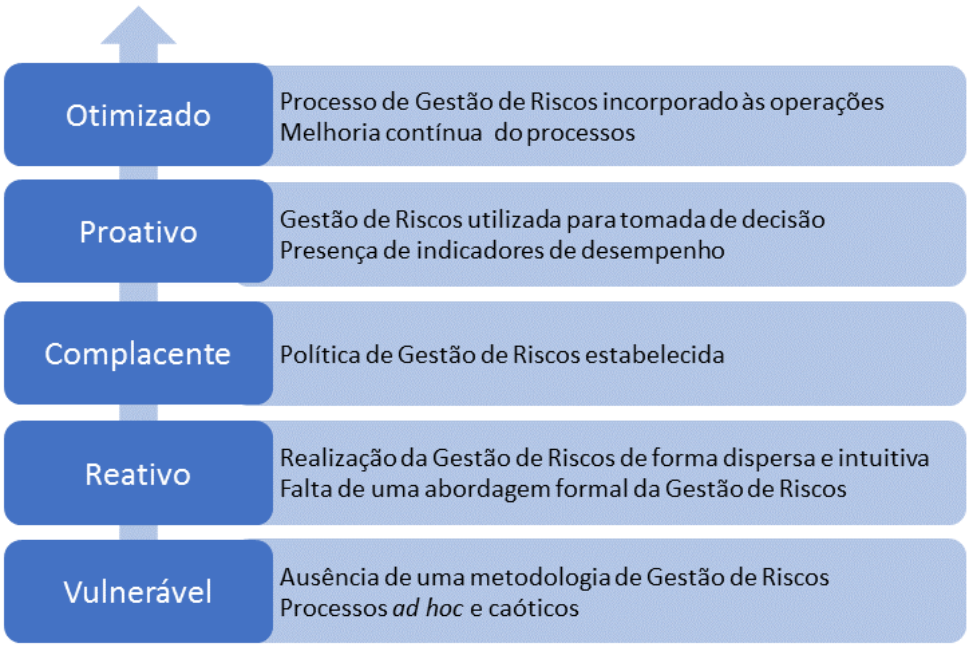


Figura 4.5: Níveis de Maturidade do IAMGR

As Tabelas 4.19 a 4.21 apresentam a descrição detalhada dos níveis de maturidade do IAMGR.

Tabela 4.19: Descrição dos níveis de maturidade do IAMGR

Nível	**Descrição**
Vulnerável	A organização não tem um conhecimento básico sobre o processo de gestão de riscos ou tem o conhecimento, porém ainda não o implementa. Indica que a organização não tem, ainda, uma metodologia de gestão de riscos estável e organizada. Neste nível, não há nenhuma evidência de que a gestão de riscos possa apoiar a tomada de decisão. Nesse nível de maturidade os processos são geralmente *ad hoc* e caóticos. O sucesso nessas organizações depende da competência e heroísmo dos seus funcionários e não ao uso de processos estruturados.

Tabela 4.20: Descrição dos níveis de maturidade do IAMGR - continuação

Nível	Descrição
Reativo	A entidade tem um bom conhecimento sobre o processo de Gestão de Riscos, porém apenas determinadas pessoas detêm esse conhecimento, que ainda não foi difundido por todo o setor. São estas pessoas que realizam a gestão de riscos na empresa de forma dispersa e intuitiva, ou seja, nenhuma abordagem formal foi desenvolvida para a gestão de riscos. A adoção de um processo de gestão de riscos ajuda a garantir que práticas existentes sejam utilizadas em momentos de estresse. Quando essas práticas são adotadas, os projetos decorrem (e são gerenciados) de acordo com o planejamento inicial.
Complacente	A empresa adota um padrão para os processos de gestão de riscos com o uso de uma metodologia. Essa metodologia pode ter sido desenvolvida, com base na ISO 31000 [16] ou a empresa adotou uma metodologia já existente no mercado. A organização desenvolveu uma política de Gestão de Riscos, que está disponível e, pelo menos, uma equipe recebeu treinamento para sua utilização. A empresa tem definido, de forma sistemática, como identificar, analisar e tratar riscos, bem como estimar o valor do impacto e da probabilidade em função das escalas previamente definidas, seja de forma quantitativa ou qualitativa. Muitas vezes o critério de aceitação do risco, bem como o cálculo do Risco Residual, também estão bem definidos. A organização possui uma metodologia e esta é publicada e melhorada periodicamente.
Proativo	O processo de Gestão de Riscos da organização é auditado e sua avaliação é utilizada pela direção para tomada de decisão. O conhecimento é amplo por parte de toda a equipe em relação ao processo de gestão de riscos. Organizações neste nível conseguem indicadores de desempenho para o processo de gestão de riscos. Subprocessos são selecionados conforme a importância na performance total do processo. Esses subprocessos selecionados são controlados usando técnicas estatísticas e quantitativas.

Tabela 4.21: Descrição dos níveis de maturidade do IAMGR - continuação

Nível	Descrição
Otimizado	O órgão atingiu um nível de excelência, pois consegue estimar de forma precisa os riscos, impactos e probabilidades de seus processos, assim elimina desperdícios, falhas e retrabalhos, conseguindo níveis elevados de eficácia. A organização se torna mais efetiva no controle de desempenho e mais previsível, pois a diferença entre os resultados desejados e os resultados reais atingidos é quase nula. A entidade consegue refinar os seus processos e os controles do processo de gestão de riscos já estão incorporados às operações. Neste nível de maturidade, o foco é o contínuo progresso do desempenho dos processos, por meio da introdução de melhorias de inovação tecnológica e incremental. Objetivos de melhoria quantitativa dos processos para a organização são estabelecidos, continuamente revisados, refletindo as mudanças nos objetivos da organização, e usando critérios de melhoria na gerência de processos. Os efeitos da melhoria da revisão dos processos são medidos e acompanhados, utilizando-se processos de melhoria de qualidade. Os processos definidos e o conjunto de processos padrões da organização são alvos de melhoria de métricas.

O estágio Vulnerável se refere ao estágio inicial que pode ser, por exemplo, caracterizado por uma organização com pouca ou nenhuma capacidade em gestão de risco. Em contraste, o estágio mais alto, Otimizado, representa o conceito de total maturidade. Avançar de um extremo ao outro envolve um progresso contínuo e incremental no que se refere às capacidades da organização.

A distinção entre os níveis Reativo e Complacente é o escopo dos padrões e a descrição dos processos e procedimentos. No nível Reativo, os padrões e a descrição de processos e procedimentos podem ser bem diferentes em cada instância específica do processo (por exemplo, em um projeto particular). No nível Complacente, os padrões e a descrição de processos e procedimentos para o projeto são guiados pelo conjunto de padrões de processos da organização. Como resultado, os processos realizados por meio da organização são consistentes, exceto pelas diferenças permitidas pelos guias. Ou seja, no nível Complacente, processos são geralmente descritos com mais detalhes e com mais rigor do que no nível Reativo. No nível Complacente, processos são gerenciados mais proativamente.

Entre o nível de maturidade Complacente e Proativo, a principal distinção é a previsibilidade do desempenho do processo. No nível Proativo, o desempenho do processo é

controlado usando técnicas estatísticas e quantitativas, e é previsível quantitativamente. No nível Complacente, os processos são somente previsíveis qualitativamente.

Já nos níveis Proativo e Otimizado, a diferença é o tipo de variação do processo. No nível Proativo, o interesse é verificar as causas especiais de variação de processo e fornecer resultados estatísticos. Já no nível Otimizado, o foco são as causas comuns de variação de processo e a introdução de mudanças de modo a melhorar a performance do processo, atingindo objetivos quantitativos.

É desejável que o último nível englobe a inovação e o monitoramento constante das práticas, para que isso sustente a filosofia Kaizen de melhoria contínua.

O nível ótimo de maturidade é reconhecido como o nível que entrega os objetivos estratégicos da organização de maneira mais efetiva e eficaz, não necessariamente correspondendo ao nível mais alto da escala definida [32].

4.4.4 Desenvolvimento da 4ª Iteração

Essa seção é responsável pela implementação do cálculo dos níveis de maturidade. Cada processo é avaliado por dois critérios: quanto ao nível de adoção dos itens de verificação e quanto à avaliação das etapas da ISO 31000 [16].

Primeiro critério: nível de adoção do item de verificação

O primeiro critério é o nível de adoção dos itens de verificação. O instrumento permite que apenas uma das cinco opções de adoção do item de verificação possa ser selecionada, conforme Tabela 4.22.

Tabela 4.22: Escala de respostas para os níveis de adoção dos itens de verificação

Nível de adoção do item da verificação	**Definição**
Não se aplica	A organização entende que o processo não se aplica à sua realidade, apresentando a justificativa no campo "Comentários" ao final do questionário.
Não adota	A organização ainda não adota o processo, bem como não iniciou planejamento para adotá-lo.
Iniciou plano para adotá-la	A organização ainda não adota o processo, mas iniciou ou concluiu planejamento visando adotá-lo, o que se evidencia por meio de documentos formais (planos, atas de reunião, estudos preliminares, etc).
Adota parcialmente	A organização iniciou a adoção do processo, que ainda não está completamente implementado, conforme planejamento realizado; ou o processo não é executado uniformemente em toda a organização. Há, pelo menos, uma instância de execução do processo e os artefatos produzidos são evidências dessa execução.
Adota integralmente	A organização adota integralmente o processo apresentado, de modo uniforme, o que se evidencia em documentação específica ou por meio do(s) produto(s) ou artefato(s) resultante(s) de sua execução.

Essas opções de respostas são pontuadas de 0 a 4, conforme Tabela 4.23. Como só há uma resposta possível, então a Nota Final do Critério 1 (NFC1) é a atribuição da pontuação recebida para o item de verificação.

Tabela 4.23: Pontuação do nível de adoção para um item de verificação

Nível de adoção do item de verificação	**Pontos**
Não se aplica	0
Não adota	1
Iniciou plano para adotá-la	2
Adota parcialmente	3
Adota integralmente	4

As escalas utilizadas nesse critério são adotadas pelo TCU e justificam-se pelas respostas mais representativas, o não nivelamento por baixo das instituições e um menor peso para a formalização [47]. Por outro lado, traz dificuldades como a possibilidade de práticas em que a escala não se aplica (práticas binárias), e a dificuldade para definir a fronteira entre o que é parcial e o que é integral [47].

Segundo critério: avaliação das etapas da ISO 31000 [16]

O segundo critério de avaliação da prática se refere às etapas da ISO 31000 [16] que foram mencionadas neste trabalho na Figura 4.3. Neste momento, questiona-se para cada item de verificação se foi observado cada um dos processos de gestão de riscos positivados na referida Norma. As opções de resposta foram baseadas no sistema de mensuração do modelo CMMI [30], descritas na Tabela 4.24.

Tabela 4.24: Escala de respostas para a aplicabilidade dos processos de gestão de riscos para o item de verificação

Opções de resposta	**Significado**
Nenhuma	Muito pouca ou nenhuma aplicabilidade da atividade de gestão de riscos no item de verificação.
Muito pouca	A organização apoia a intenção, mas na prática a aplicabilidade da atividade de gestão de riscos no item de verificação ainda é pouca.
Alguma	Concordam certamente com a intenção, mas a aplicabilidade da atividade de gestão de riscos no item de verificação é limitada.
Boa	A administração apoia completamente a intenção, mas há conformidade parcial na aplicabilidade da atividade de gestão de riscos no item de verificação.
Completa	Conformidade absoluta com a aplicabilidade da atividade de gestão de riscos no item de verificação– na intenção e na prática – em todos os momentos.

A Tabela 4.25 apresenta uma escala de pontuação para cada opção de resposta. Ressalta-se que as sete etapas do processo de gestão de riscos são avaliadas para cada item de verificação.

Tabela 4.25: Pesos das opções de respostas para a aplicabilidade dos processos de gestão de riscos aos itens de verificação.

Opções de resposta	**Pontos**
Nenhuma	1
Muito pouca	2
Alguma	3
Boa	4
Completa	5

Além disso, cada processo da gestão de riscos da ISO 31000 [16] possui um peso que quantifica seu impacto em relação à aplicabilidade do processo. Gaffo e De Barros [21] propuseram pesos para cada processo de gestão de riscos, conforme Tabela 4.26.

Tabela 4.26: Pesos dos Processos de gestão de riscos.

Processos de gestão de riscos	**Pesos**
Comunicação e Consulta	1
Estabelecimento de contexto	4
Identificação de riscos	3
Análise de riscos	1
Avaliação de riscos	2
Tratamento de Riscos	1
Monitoramento e análise crítica	2

A pontuação parcial desse critério se dá pela multiplicação do peso da etapa com o peso da resposta. A nota final do critério 2 (NFC2) será a soma dos pontos obtidos de cada etapa da Norma ISO 31000 [16], conforme fórmula abaixo.

$$NFC_2 = \frac{(ETP_1 \cdot P_1) + (ETP_2 \cdot P_2) + ... + (ETP_7 * P_7)}{100}, \tag{4.1}$$

NFC_2 = nota final do critério dois; ETP_i = ponto obtido da opção de resposta, onde i = 1 a 7 que correspondem; as quantidades de etapas da norma P_i = peso da respectiva etapa.

Cálculo da pontuação final

A nota de cada item de verificação (NIV) se dá pela multiplicação dos pontos obtidos pelo primeiro critério (NFC1) com a pontuação final do segundo critério (NFC2).

$$NIV = NFC_1 \cdot NFC_2 \tag{4.2}$$

O cálculo da nota final do processo (NFP) é obtido pela média ponderada dos valores alcançados por cada item de verificação. A necessidade de utilizar a média ponderada justifica-se pelo fato de cada item de verificação estar classificado numa dimensão específica (Tabela 4.15), o qual possui um peso associado (Tabela 4.18). Destaca-se que neste cálculo é desconsiderado o item de verificação que recebe nota “0” (zero), ou seja, retira do cálculo o item de verificação que foi respondido como "Não se aplica!"para o critério “Nível de adoção do item de verificação”. A fórmula abaixo apresenta o cálculo da pontuação final de cada processo de TI.

$$NFP = \frac{\sum NIV_i \cdot P_i}{\sum P_j} \tag{4.3}$$

NFP = nota final do processo Capítulo 4 - Elaboração do IAMGR 90;

PIV_i = Pontuação do Item de Verificação, onde “i” corresponde as notas obtidas pelos itens de verificação;

P_i = pesos das dimensões dos itens de verificação;

A pontuação máxima alcançada para cada processo avaliado é de 2,40. Para identificar o nível de maturidade do processo de TI, o IAMGR utiliza uma distribuição uniforme da pontuação máxima nos cinco níveis previsto no referido instrumento, conforme Tabela 4.27.

Tabela 4.27: Faixa de pontos para cada nível de maturidade

Margem	**Nivel de Maturidade**
0,01-0,48	Vulnerável
0,49-0,96	Reativo
0,97-1,44	Complacente
1,45-1,92	Proativo
1,93-2,40	Otimizado

O IAMGR indica o nível de maturidade para cada processo de TI, sendo que o nível de maturidade em gestão de riscos do órgão é dado pelo menor nível alcançado entre os processos avaliados.

4.4.5 Desenvolvimento da 5ª Iteração

Essa iteração visa à implementação do questionário. O desenvolvimento de uma planilha sistematizada, elaborada no Microsoft Excel, possibilita a avaliação do nível de maturidade em gestão de riscos para ser utilizada pelo gestor de TI, especificamente nos processos de TI enumerados neste trabalho. A planilha é composta por seis abas:

- Instruções de Uso
- Cartões de Resposta
- Pontuação
- Resultado
- Questionário Conf.
- Banco de Dados

A aba "Instruções de Uso" é a aba inicial do IAMGR e tem como objetivo orientar o usuário/respondente na utilização do questionário. Procurou-se elaborar as instruções de forma com que elas fossem esclarecedoras, simples e objetiva. O painel de instruções pode ser visualizado na Figura 4.6.

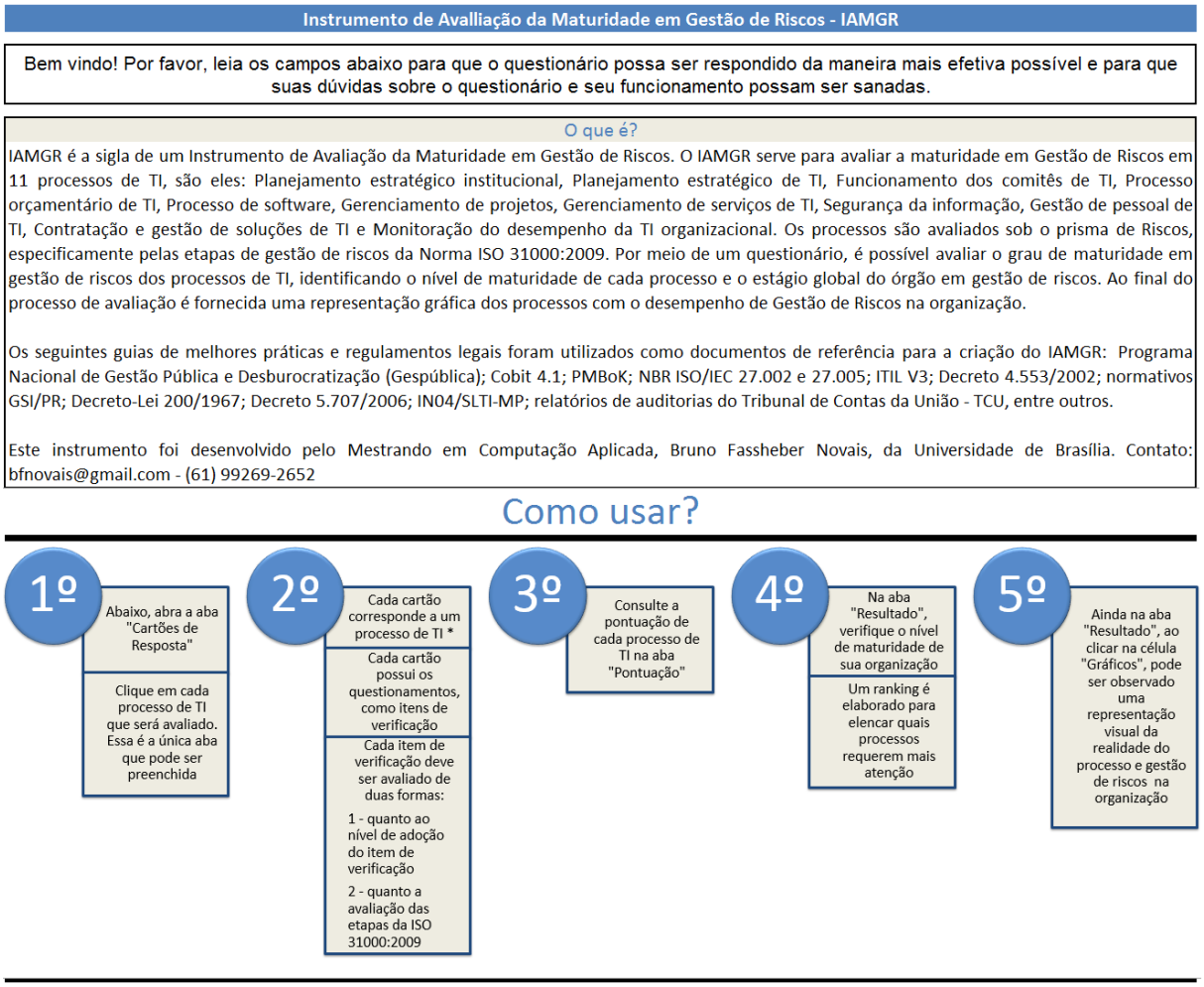


Figura 4.6: Aba "Instruções de Uso"do IAMGR

A aba “Cartões de Resposta” é a única aba do IAMGR que deve e pode ser preenchida. Foi criada uma tela inicial (Figura 4.7) para que o usuário visualize os onze processos de TI, ao clicar no processo abre-se o cartão de resposta com os respectivos itens de verificação. Todos os cartões de resposta seguem o mesmo modelo e padrão, diferenciando-se apenas nas cores e na quantidade de itens. Todos os cartões de resposta podem ser encontrados no Apêndice A deste trabalho.

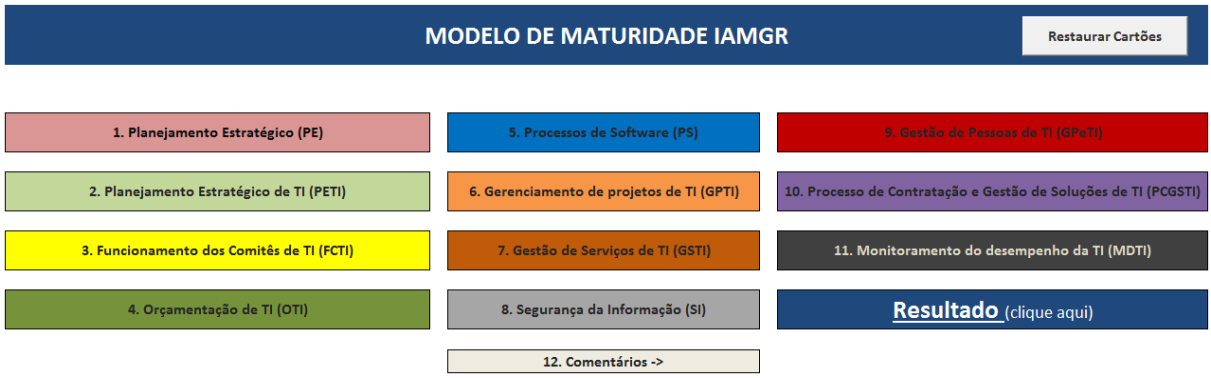
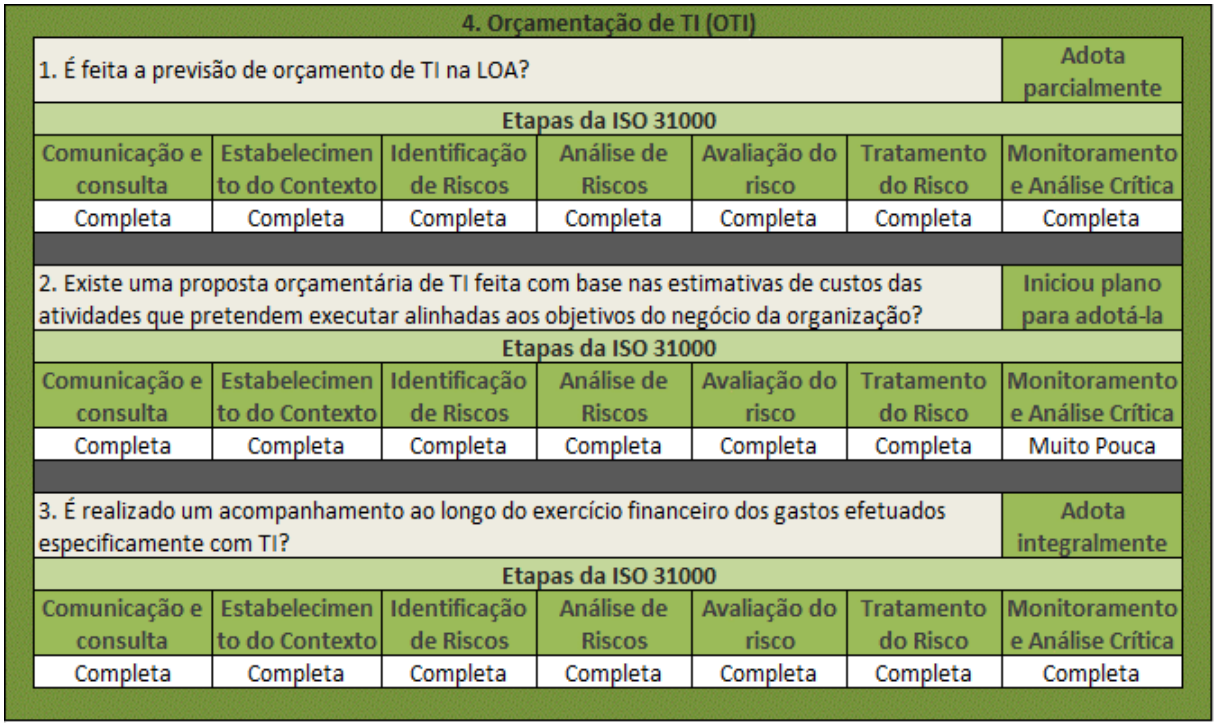


Figura 4.7: Tela inicial de acesso aos "Cartões de resposta"

Dentro do cartão de resposta, é possível visualizar os itens de verificação, os quais são avaliados por dois critérios, conforme exposto no item 4.4.4.

O primeiro critério é o nível de adoção do item de verificação, que pode ser utilizado selecionando uma das cinco diferentes escolhas (não se aplica, não adota, iniciou plano para adotá-la, adota parcialmente e adota integralmente), conforme Tabela 4.20. Já o segundo critério de avaliação do item de verificação se refere às etapas da ISO 31000 [16], apresentadas na Figura 2.1. As sete etapas são avaliadas ao clicar na célula imediatamente abaixo à etapa, uma lista com cinco opções são exibidas: nenhuma, muito pouca, alguma, boa e completa.

A Figura 4.8 exemplifica um Cartão de Resposta do processo "Orçamento de TI" com a avaliação dos critérios referenciados acima e que são aplicados para todos os demais cartões de resposta.



4. Orçamentação de TI (OTI)						
1. É feita a previsão de orçamento de TI na LOA?						Adota parcialmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Completa	Completa	Completa	Completa	Completa	Completa	Completa
2. Existe uma proposta orçamentária de TI feita com base nas estimativas de custos das atividades que pretendem executar alinhadas aos objetivos do negócio da organização?						Iniciou plano para adotá-la
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Completa	Completa	Completa	Completa	Completa	Completa	Muito Pouca
3. É realizado um acompanhamento ao longo do exercício financeiro dos gastos efetuados especificamente com TI?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Completa	Completa	Completa	Completa	Completa	Completa	Completa

Figura 4.8: Cartão de resposta do processo

A aba “Pontuação”, que impossibilita qualquer preenchimento, é simplesmente uma agregação de todos os cálculos realizados, demonstrando a pontuação de cada item de verificação e a pontuação final do processo. As pontuações obtidas nos cartões de resposta são automaticamente repassadas aos cartões de pontuação. A Figura 4.9 exemplifica o processo de pontuação de um processo específico.

Orçamentação de TI	
1. É feita a previsão de orçamento de TI na LOA?	1,8
2. Existe uma proposta orçamentária de TI feita com base nas estimativas de custos das atividades que pretendem executar alinhadas aos objetivos do negócio da organização?	1,08
3. É realizado um acompanhamento ao longo do exercício financeiro dos gastos efetuados especificamente com TI?	2,4
Pontuação:	2,08

Figura 4.9: Cartão de pontuação do processo

A planilha conta com algumas abas que são utilizadas subsidiariamente, criadas a fim de permitir parametrizar e automatizar a planilha, não havendo interação com o usuário. São elas: “Banco de Dados” e “Questionários Conf.”. Esta conta com os itens de verificação já categorizados pelas Dimensões do IAMGR, além da indicação dos pesos das dimensões, permitindo alterar a descrição textual dos itens de verificação, a dimensão associada e os pesos das dimensões. A aba “Banco de Dados” é oculta e foi elaborada para dar suporte

aos cálculos e operações realizados pelo sistema. A principal função dela é parametrizar os pesos das etapas da ISO 31000 [16], a pontuação das opções de respostas para o primeiro e segundo critério, bem como os intervalos de pontuação para cada nível de maturidade do IAMGR, além de calcular o resultado e disponibilizar graficamente na aba "Resultado".

Na aba "Resultado", a pontuação obtida em cada processo é exibida e na célula imediatamente abaixo da pontuação, o nível de maturidade de cada processo é informado, conforme intervalo de pontuação detalhado na Tabela 4.25.

Ao final, o IAMGR informa o nível de maturidade final em Gestão de Riscos no órgão. O nível de maturidade final é estabelecido pelo menor nível de maturidade obtido na avaliação dos processos de TI.

Uma análise gráfica também é fornecida na aba "Resultado". O primeiro gráfico (Figura 4.10) elenca em ordem decrescente de pontuação os processos de TI. Dessa forma, os gestores conseguem identificar de maneira mais visual e em ordem de prioridade quais são os processos que requerem mais atenção para que o nível de maturidade final possa ser elevado.

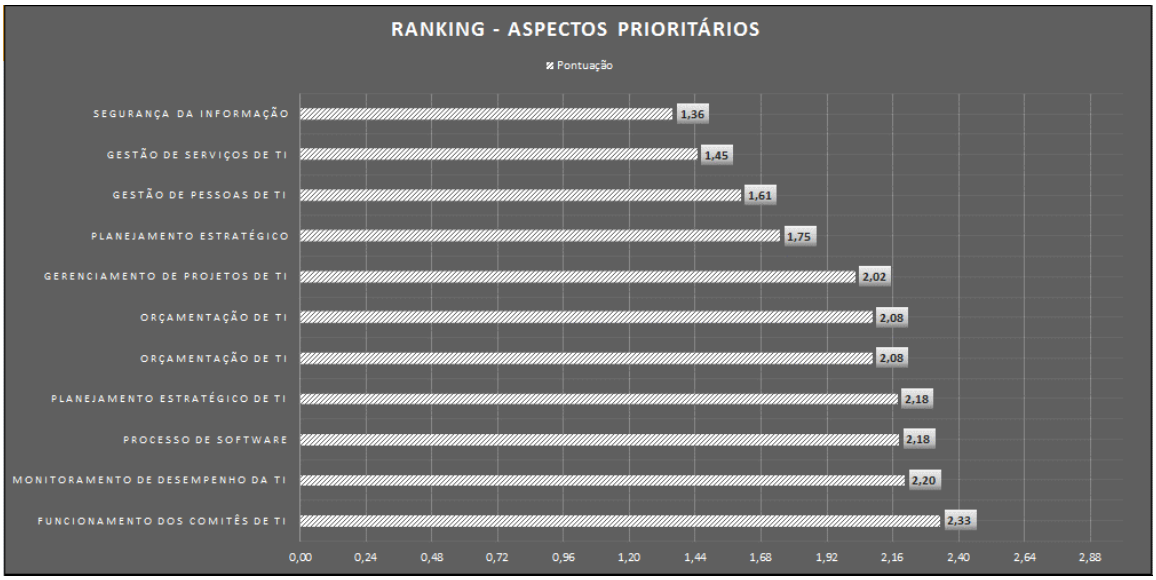


Figura 4.10: Exemplo do gráfico *Ranking* do IAMGR

Outros dois gráficos compõem a análise gráfica da aba "Resultado". Um gráfico de radar (Figura 4.11) traz outra forma de representação visual da pontuação obtida por cada um dos processos de TI.

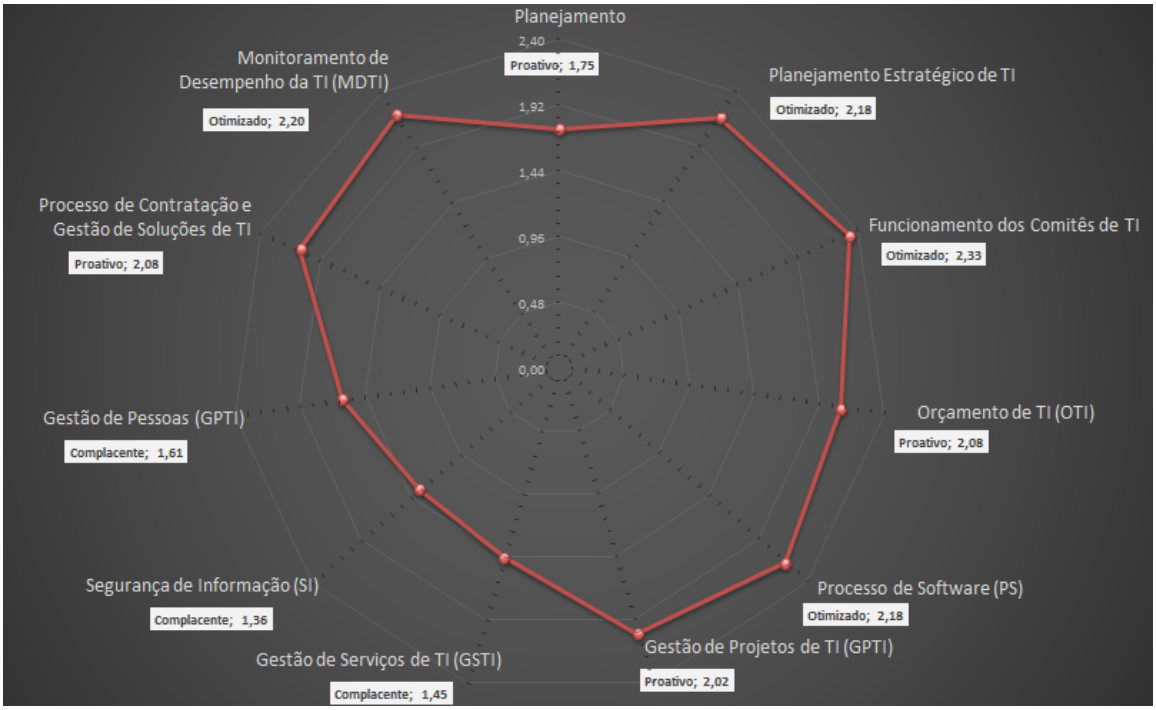


Figura 4.11: Exemplo de gráfico Radar do IAMGR

Um gráfico de Barras (Figura 4.12) também é apresentado com o mesmo intuito do Gráfico Radar.

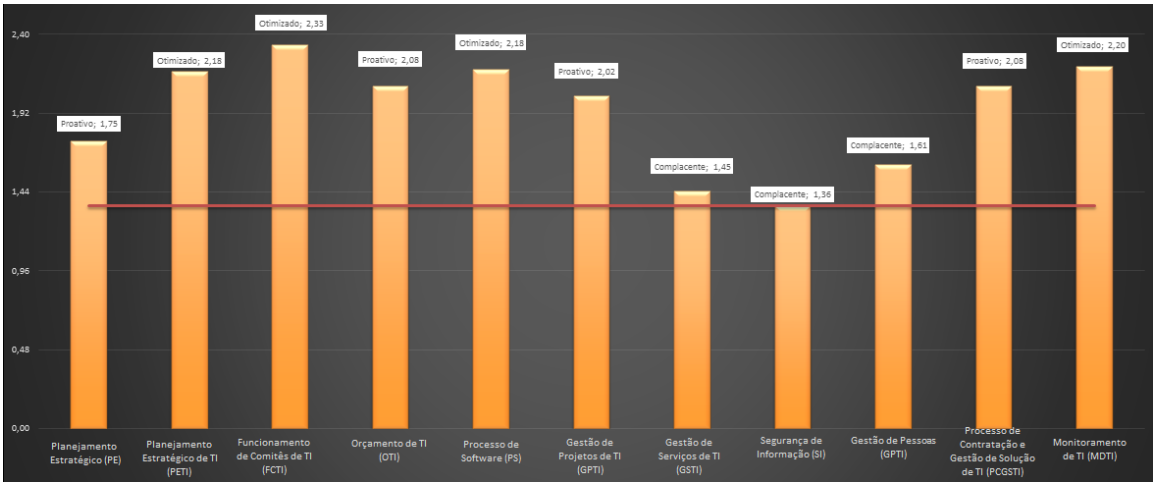


Figura 4.12: Exemplo de gráfico de Barras do IAMGR

Com o objetivo de facilitar o uso da planilha, foram adotados os seguintes critérios de usabilidade:

- A tela principal enumera os onze processos de TI;
- Botão de navegação entre os processos (Cartão anterior, Próximo cartão ou Voltar a tela principal) e gráficos (Ranking, Radar e Barra;

- Botão para restaurar o questionário;
- Flag que sinaliza se o cartão já foi ou não respondido;
- Campo de comentários por processo de TI;
- Utilização de dados parametrizados;
  - Pontuação das opções de resposta do NFC1
  - Pontuação das opções de resposta do NFC2
  - Pesos dos processos de Gestão de Riscos
  - Enquadramento dos itens de verificação com as dimensões
  - Pesos das dimensões
  - Pesos das etapas da ISO 31000 [16]
- Mensagens de alerta/erros:
  - Caso o respondente esqueça-se de selecionar uma opção para alguma etapa da ISO 31000 [16], o sistema avisa o usuário automaticamente com a seguinte mensagem no campo respondente à Pontuação: "Verifique se todos os itens acima foram respondidos!".

Para um diagnóstico real e eficaz sobre o desempenho do processo de Gestão de Risco, é importante que o questionário seja respondido de maneira imparcial e de acordo com a realidade da organização, e não com o que se espera que seja realizado.

4.4.6 Desenvolvimento da 6ª Iteração

O envolvimento de especialistas na revisão do instrumento possibilitou verificar itens que possam ter passado despercebidos nas iterações anteriores. Além disso, verificou-se que houve um grande interesse por partes dos gestores na utilização do instrumento para conhecimento do seu nível de maturidade em gestão de riscos nos processos de TI em seus respectivos órgãos.

Ao todo, houve interesse de quatro gestores de TI de órgãos externos ao MP como: Advocacia Geral da União - AGU, Conselho Administrativo de Defesa Econômica – CADE, Empresa Brasil de Comunicação – EBC e Ministério da Previdência Social – MPS. Além disso, as secretarias do Patrimônio da União e de Tecnologia da Informação, ambas do Ministério do Planejamento, também demonstraram interesse na planilha e fizeram suas contribuições.

A revisão da planilha pelos interessados possibilitou ajustes nos seguintes aspectos:

- Alterações no layout para tornar o instrumento de fácil manuseio;
- Alterações no texto tornando-o conciso e claro, evitando assim, dupla interpretação;
- Retirada de termos genéricos nas perguntas, como por exemplo: maior, menor, melhor. Tornando o instrumento mais direto e objetivo;
- Validação dos cálculos da planilha;
- Verificação e aprimoramento na distribuição de pontos para cada nível de maturidade do IAMGR.

4.5 Validação do Instrumento

A validação, correspondente a etapa 5 do fluxograma para elaboração do IAMGR, apresentado na Figura 4.1, está detalhada na aplicação, conforme capítulo a seguir.

Capítulo 5

Estudo de Caso: Aplicação do IAMGR no MP

5.1 Conhecendo o MP

O Ministério do Planejamento, Desenvolvimento e Gestão (MP), órgão da Administração Pública Federal Direta, possui a seguinte Missão [36]:

"Planejar e coordenar as políticas de gestão da administração pública federal, para fortalecer as capacidades do Estado para promoção do desenvolvimento sustentável e do aprimoramento da entrega de resultados ao cidadão."

E as seguintes visões de futuro:

- Ser reconhecido pela excelência e competência na gestão pública e por uma administração moderna, transparente e eficiente;
- Ser a organização de excelência na gestão dos recursos públicos federais;
- Promoção do cumprimento do Plano Plurianual com participação da sociedade e diálogo com os planos de desenvolvimento de longo prazo;
- Melhoria permanente na entrega de serviços e atendimento das necessidades da sociedade;
- Coordenação de ações de infraestrutura, logística e social que sustenta o crescimento e a competitividade do país alcançada a partir da formulação e monitoramento dos planos coordenados pelo MP;
- Desenvolvimento de modelos e instrumentos de governança e gestão que melhoram a capacidade de atuação dos órgãos;

- Modernização dos sistemas estruturantes de governo (planejamento, orçamento, pessoal, administração de recursos da informação, de logística e organização administrativa);
- Formulação de diretrizes, coordenação e definição de critérios de governança corporativa das empresas estatais federais;
- Realização de estudos e pesquisas para acompanhamento da conjuntura socioeconômica e gestão dos sistemas cartográficos e estatísticos nacionais.

O MP é um órgão complexo que possui na sua estrutura organizacional diversas Secretarias com finalidades distintas. Para um melhor entendimento da função do MP, a Figura 5.1 representa a Cadeia de Valor do MP. Porter [43] conceitua a Cadeia de Valor como um conjunto de atividades desempenhadas por uma organização.

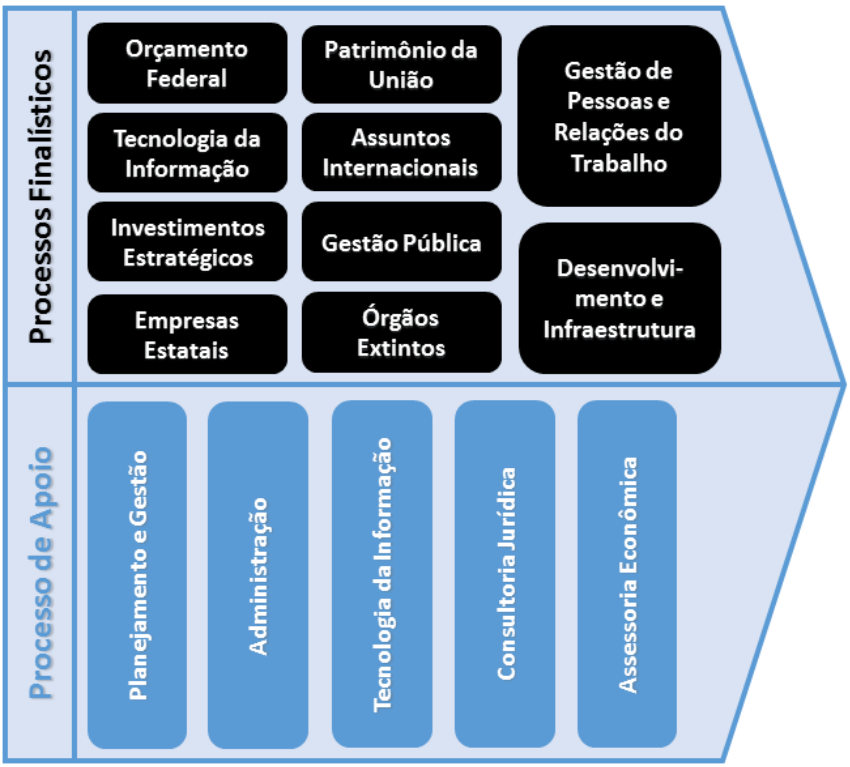


Figura 5.1: Cadeia de Valor do MP

Além disso, o órgão é responsável por alguns dos principais sistemas do Governo Federal [36], tais como:

- O Sistema de Planejamento e Orçamento Federal compreende as atividades de elaboração, acompanhamento e avaliação de planos, programas e orçamentos, e de realização de estudos e pesquisas socioeconômicas. Sistema tem por finalidade formular

o planejamento estratégico nacional, os planos nacionais, setoriais e regionais de desenvolvimento econômico e social e o plano plurianual, as diretrizes orçamentárias e os orçamentos anuais. Também destina-se a gerenciar o processo de planejamento e orçamento federal e promover a articulação com os Estados, o Distrito Federal e os Municípios, visando a compatibilização de normas e tarefas afins aos diversos Sistemas, nos planos federal, estadual, distrital e municipal. A ferramenta utilizada é o Sistema Integrado de Planejamento e Orçamento (SIOP).

- O Sistema de Pessoal Civil da Administração Federal (SIPEC) possui como funções básicas de Administração de Pessoal: Classificação e Redistribuição de Cargos e Empregos; recrutamento e Seleção; Cadastro e Lotação; Aperfeiçoamento; e Legislação de Pessoal. O suporte a estas atividades é realizado por meio do Sistema Integrado de Administração de Recursos Humanos – SIAPE (sendo substituído pelo SIGEPE). Além disso, a fonte oficial de informações sobre a estrutura organizacional dos órgãos do Poder Executivo – Administração Direta, Autarquias e Fundações são mantidas pelo Sistema de Informações Organizacionais do Governo Federal (SIORG).

- O Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) organiza sob a forma de sistema o planejamento, a coordenação, a organização, a operação, o controle e a supervisão dos recursos de tecnologia da informação dos órgãos e entidades da administração pública federal direta, autárquica e fundacional, em articulação com os demais sistemas utilizados direta e indiretamente na gestão da informação pública federal. Tendo a Secretaria de Tecnologia de Informação (STI) como órgão central.

- O Sistema de Serviços Gerais (SISG) organiza as atividades de administração de edifícios públicos e imóveis residenciais, material, transporte, comunicações administrativas e documentação. Compete ao MP, como órgão central, o gerenciamento e expedição de normas complementares. Esta administração é realizada pelo Sistema Integrado de Administração dos Serviços Gerais (SIASG).

- O Sistema Integrado de Administração Patrimonial (SIAPA) consiste em uma ferramenta de apoio à administração do patrimônio imobiliário da União, especificamente dos seus imóveis dominiais.

  O Sistema de Gestão de Convênios e Contratos de Repasse (SICONV) é uma ferramenta eletrônica que reúne e processa informações sobre as transferências de recursos do Governo Federal para órgãos públicos e privados sem fins lucrativos. Esse repasse acontece por meio de contratos e convênios destinados à execução de programas, projetos e ações de interesse comum.

- O Sistema de Informações das Estatais (SIEST) trata da elaboração do Plano de Dispêndios Globais (PDG) das empresas estatais para o exercício financeiro subsequente. Ele acompanha a execução e revisão do PDG para o exercício financeiro vigente e fornece informações para o Balanço Geral da União. Cuida ainda da manutenção de informações cadastrais (perfil das estatais), contábeis (endividamento, plano de contas, balanço patrimonial) e econômicofinanceiras (política de aplicações) das empresas.

Observa-se o foco estratégico que é dado ao MP e a grande responsabilidade na condução de políticas públicas. Ressalta-se também a importância da TI nos processos de negócios definidos acima.

Segundo o Decreto 8.578, de 26 de novembro de 2015, o MP tem a seguinte estrutura organizacional (Figura 5.2).

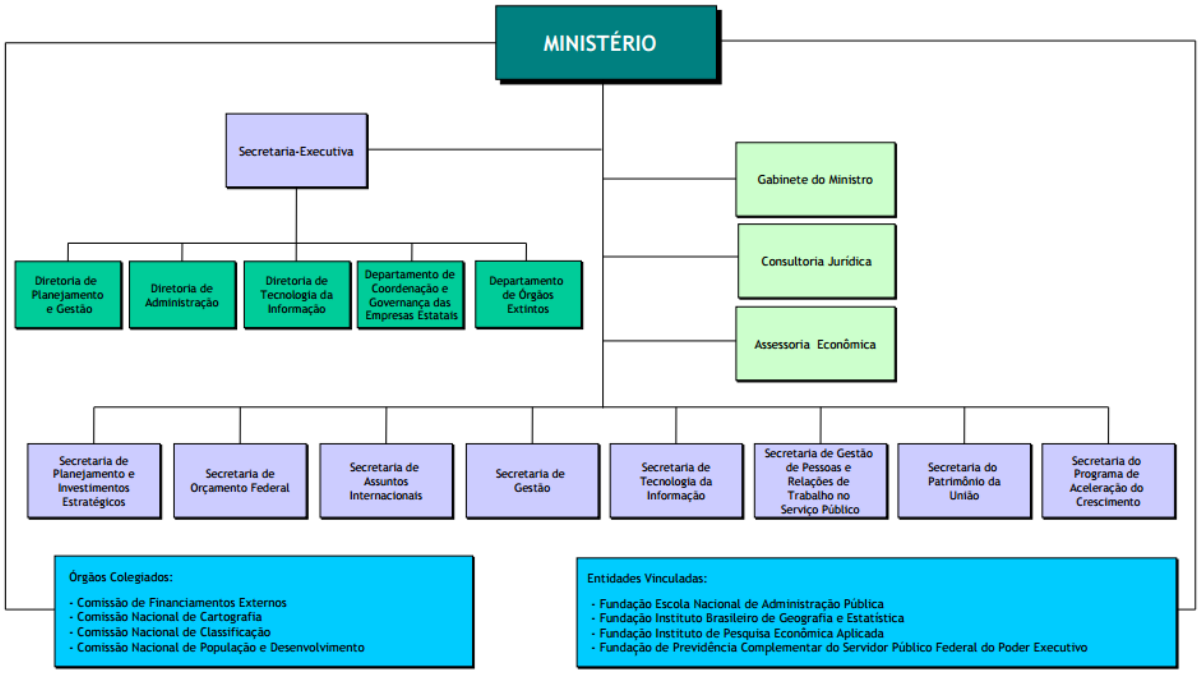


Figura 5.2: Organograma do MP. Fonte: [36]

O referido Decreto define a estrutura da Diretoria de Tecnologia de Informação (DTI), sendo composta pela Coordenação-Geral de Governança de TI, Coordenação-Geral de Sistemas e Coordenação-Geral de Serviços de TI.

No Planejamento Estratégico de TI (PETI) do MP foram estabelecidas a missão e a visão da TI, conforme descrito a seguir [36]:

- Missão da TI: Prover soluções e serviços de TI para as unidades do Ministério do Planejamento, Desenvolvimento e Gestão, a fim de alcançar seus objetivos institucionais com o foco na satisfação do público usuário.
- Visão da TI: Ser referência em gestão de TI na Administração Pública Federal.

Importa ressaltar que tanto o Plano Estratégico Institucional como o Planejamento Estratégico de TI estão sendo revisados e possuem processos abertos para prorrogação da vigência de cada plano para o fim de 2016. De toda sorte, encontra-se em andamento no MP dois grupos de trabalho com o objetivo de elaborar, implantar e publicar os novos planos até o fim do corrente ano.

5.2 Etapas de aplicação do Estudo de Caso

Para a efetiva aplicação do IAMGR na DTI foram propostas quatro atividades, conforme Figura 5.3. Com isso, buscou-se garantir o envolvimento e o comprometimento dos gestores de TI da unidade nas respostas dadas.

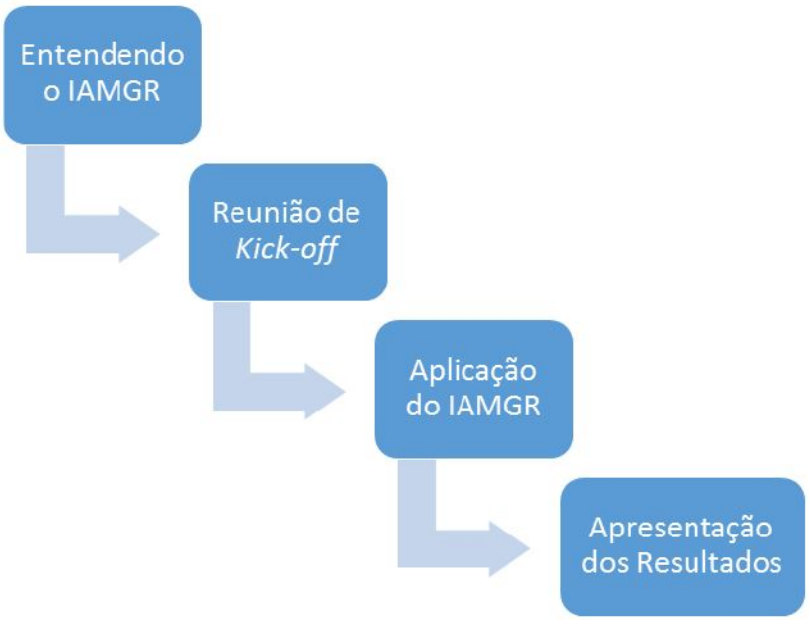


Figura 5.3: Etapas de aplicação do IAMGR

As etapas da aplicação do Estudo de Caso podem ser descritas como:

- Entendendo o IAMGR: distribuição de materiais sobre a Proposta de Avaliação para Leitura-Prévia do respondente, no caso da DTI, o Diretor de TI.
- Reunião de Kick-Off: apresentação da forma de avaliação e do levantamento de dados; estabelecimento da expectativa do respondente quanto ao nível de maturidade.
- Aplicação do IAMGR: analisar a completude e conformidade das informações levantadas com a proposta de avaliação; analisar o correto registro das informações levantadas; utilizar a planilha proposta e analisar os resultados alcançados.
- Apresentação dos Resultados: apresentação dos resultados; comparar a expectativa do respondente quanto ao nível de maturidade e o resultado encontrado com a aplicação do IAMGR.

A execução desses passos foi suficiente para aplicar o instrumento na Diretoria de Tecnologia de Informação (DTI) do Ministério do Planejamento, Desenvolvimento e Gestão (MP), além de analisar os resultados alcançados.

5.3 Apuração do método aplicado (Resultados)

Como o desenvolvimento do instrumento foi feito em alinhamento com os gestores de TI da unidade, a fase de entendimento do IAMGR foi simplificada, pois eles já tiveram contato com o Instrumento desde a fase de elaboração. De qualquer forma, houve o alinhamento dos objetivos e das expectativas em relação a este trabalho antes de apresentar o questionário (planilha do IAMGR). O questionário foi debatido com os gestores da unidade.

A reunião de Kick-off foi realizada e nesta oportunidade foram repassados os objetivos deste trabalho, bem como explicado o uso da planilha IAMGR. Foram repassados os processos de TI a serem avaliados e definiu-se que como o modelo preconiza que seja preenchido pela autoridade máxima de TI, o Diretor TI, Sr. Eduardo Cesar Soares Gomes, seria o respondente da pesquisa, sem prejuízo às considerações feitas pelos demais gestores na reunião do colegiado. A partir daí, foi levantada a percepção do respondente quanto ao nível de maturidade em gestão de riscos nos onze processos de TI, o sentimento relatado é que o nível de maturidade do órgão esteja entre Vulnerável e Reativo, sendo que alguns processos apresentam um nível de maturidade maior outros não.

Durante a fase de levantamento das informações foram sanadas algumas dúvidas sobre o IAMGR para que fosse dado prosseguimento a pesquisa. Em geral, os questionamentos eram sobre a relação dos itens de verificação com as etapas da ISO 31000 [16]. Essa

dificuldade pode ter surgido devido a falta de conhecimento em relação aos riscos. Depois que o autor citou alguns exemplos ficou mais claro para o respondente o que se pretendia com aquela questão específica. A pesquisa foi concluída com as respostas para todos os onze processos do IAMGR em menos de 2 horas.

Na apresentação dos resultados para os demais gestores de TI foram demonstrados os resultados alcançados. Neste momento, os envolvidos fizeram uma reflexão sobre o que não está sendo atendido, já que são itens considerados importantes para a governança de TI e que deveria ser observados. O detalhamento abaixo dos processos apresenta os resultados alcançados e as considerações feitas pelos responsáveis.

O processo de Planejamento Estratégico Institucional foi o primeiro questionário a ser respondido. Após uma nova orientação quanto a avaliação das etapas da norma ISO 31000 [16], foram respondidos todos os processos, por meio dos cartões de respostas.

5.3.1 Aplicação do instrumento no processo de Planejamento Estratégico Institucional (PEI)

O Programa Nacional de Gestão Pública e Desburocratização (GESPUBLICA) orienta que os órgãos avaliem periodicamente os seus planejamentos [38]. No caso do MP, cumpre esclarecer que durante a aplicação do questionário estava sendo conduzido pela alta administração do órgão o projeto de elaboração do novo PEI com o envolvimento da DTI.

Quanto ao nível de adoção das práticas (Figura 5.4), os itens de 1 a 4 foram avaliados e classificados como “Adota integralmente”, ou seja, a organização adota integralmente os referidos itens de verificação, evidenciado no próprio plano. Já os itens 5 (acompanhamento periódico) e 6 (divulgação interna e externa do alcance das metas) foram classificados como “Parcial”, devido o acompanhamento periódico do alcance das metas e a divulgação não serem realizados, de forma uniforme, em toda a organização.

Em relação ao processo de gestão de riscos, ficou evidenciado no item 1 (elaboração do PEI com envolvimento das áreas) que as etapas de Identificação, Análise de Avaliação dos Riscos é limitada, ou seja, essas atividades ocorrem de forma isolada, sem seguir um processo de riscos e não havendo qualquer atividade em relação a documentação. Para as etapas de comunicação, contexto, tratamento e monitoramento do risco as atividades de gestão de riscos são ainda mais tímidas, ou seja, poucas atividades são executadas. Os itens 2 (aprovação do PEI) e 3 (desdobramento do PEI) apresentam uma pequena evolução dos processos de gestão de riscos, passando de “muito pouco” para “limitada”, exceto os processos de tratamento e de monitoramento. Nos itens 3 a 6 percebe-se pouca aplicabilidade das atividades de gestão de riscos, apesar da organização apoiar as práticas.

Numa análise qualitativa da aplicação das etapas da Norma ISO 31000 [16] no respectivo processo, nota-se que as etapas de Comunicação e de Contexto alcançaram um índice de aproximadamente 67% com pouca aplicabilidade da atividade de gestão de riscos. O restante (33%) apresentaram um nível um pouco melhor, mas não alcança um nível adequado ainda. Já as atividades básicas da gestão de riscos (identificação, análise e avaliação dos riscos) atingiram uma média de 50% para a aplicação limitada das atividades de gestão de riscos e os outros 50% percebe-se pouca atividade de gestão de riscos. As atividades de Tratamento e de Monitoramento atingiram um nível de 100% com pouca aplicabilidade das atividades de gestão de riscos para os 6 itens de verificação do processo PEI, alcançando o nível de maturidade "**Reativo**".

1. Existe a elaboração, com participação de representantes dos diversos setores da organização, de um documento que materialize o Plano Estratégico Institucional de longo prazo, contemplando, pelo menos, objetivos, indicadores e metas para a organização?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Alguma	Alguma	Alguma	Muito Pouca	Muito Pouca
2. Existe a aprovação, pela mais alta autoridade da organização, do Plano Estratégico Institucional?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Alguma	Alguma	Alguma	Alguma	Alguma	Muito Pouca	Muito Pouca
3. O Plano Estratégico Institucional é desdobrado pelas unidades executoras?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Alguma	Alguma	Alguma	Alguma	Alguma	Muito Pouca	Muito Pouca
4. Existe a divulgação do Planejamento Estratégico Institucional para conhecimento dos cidadãos brasileiros, exceto nos aspectos formalmente declarados sigilosos ou restritos?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca
5. Existe o acompanhamento periódico do alcance das metas estabelecidas, para correção de desvios?						Adota parcialmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca
6. Existe a divulgação interna e externa do alcance das metas, ou dos motivos de não as ter alcançado?						Adota parcialmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca

Figura 5.4: Resultado da aplicação no processo Planejamento Estratégico Institucional (PEI)

Segundo relato do respondente, o atual processo de elaboração do PEI passou por mudanças recentes com o envolvimento das áreas. Destaca-se as oficinas realizadas com as áreas de negócio que geraram oportunidades para identificação de alguns riscos.

5.3.2 Aplicação do instrumento no processo de Planejamento Estratégico de TI (PETI)

Encontra-se em andamento no MP o projeto de elaboração do novo Planejamento Estratégico de TI (PETI). Neste projeto, o líder do projeto é a mesma unidade responsável por responder este questionário, ou seja, a TI.

Observa-se que o nível de adoção dos itens de verificação foram respondidos como "Adota integralmente" (Figura 5.5), apenas o item 3 (utilização de métodos e técnicas do COBIT 4.1) foi classificado como parcial. Isso se deve ao fato de que na elaboração do PETI foram utilizados alguns métodos e técnicas, e não todas as ferramentas.

Quanto a análise das etapas da ISO 31000 [16], nota-se que a organização apoia a intenção, mas na prática a aplicabilidade das atividades de gestão de riscos nos itens de verificação ainda são poucas. O item 6 (avaliação periódica do PETI) destaca-se pela total ausência de comunicação e monitoramento dos riscos. Para os itens 1 (publicação do PETI) e 2 (elaboração com envolvimento de áreas) percebe-se uma atividade um pouco maior nos processos de análise e avaliação dos riscos.

Analisando as atividades de "Comunicação", "Estabelecimento do Contexto", "Identificação", "Tratamento" e "Monitoramento", percebe-se que em 100% dos casos a aplicabilidade dessas atividades são poucas no processo PETI. Nas atividades de "Análise" e "Avaliação de riscos", há uma pequena melhora em 28% dos casos com alguma aplicabilidade, porém o restante 72% permanece com pouca aplicabilidade. Dessa forma, o processo PETI atingiu o nível de maturidade "**Reativo**".

1. O Planejamento Estratégico de TI é publicado formalmente?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Alguma	Alguma	Muito Pouca	Muito Pouca

2. A elaboração do Planejamento Estratégico de TI é feita com a participação das áreas de negócio, da Alta Administração e da TI?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Alguma	Alguma	Muito Pouca	Muito Pouca

3. O Planejamento Estratégico de TI é elaborado com métodos e técnicas indicadas no Cobit 4.1, em especial do processo PO1 – Planejamento Estratégico de TI?						Adota parcialmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca

4. O Planejamento Estratégico de TI é desdobrado pelas diversas áreas executoras em plano de médio e curto prazo?						Adota parcialmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca

5. Existe a divulgação do Planejamento Estratégico de TI?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca

6. Existe a avaliação periódica do Planejamento Estratégico de TI?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Nenhum	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Nenhum

7. O Planejamento Estratégico de TI está alinhado com o Plano Estratégico Institucional?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca

Figura 5.5: Resultado da aplicação no processo de Planejamento Estratégico de TI (PETI)

O projeto de elaboração do novo PETI está previsto para ser concluído no primeiro semestre de 2016. Impulsionado pela crise econômica vivenciada pelo País, gestores de TI estão engajados em definir novos objetivos estratégicos que visam a otimização dos gastos de TI, levando a organização analisar novos modelos de serviços de TI.

5.3.3 Aplicação do instrumento no processo de Funcionamento dos Comitês de TI (FCTI)

Os quatro itens de verificação do processo de Funcionamento dos Comitês de TI estão adotados integralmente no MP (Figura 5.6). Isso se deve ao fato do próprio MP emitir normas de boas práticas sobre o tema, demonstrando a sua aderência em relação às boas práticas de governança e aos critérios adotados pelos órgãos de controle.

Por outro lado, os processos de gestão de riscos são praticamente negligenciados, quando se evidencia a baixíssima aplicabilidade das atividades de gestão de riscos, atingindo o nível **Reativo** para o processo FCTI.

1. A organização possui comitês de TI vigentes e implementados com base no modelo Cobit 4.1, em especial do processo PO4.2 - Comitê Estratégico de TI						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca
2. Existe a descrição do funcionamento dos comitês de TI?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca
3. Há indicação da composição dos representantes da área de negócio e de TI?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca
4. O funcionamento dos comitês de TI é realizado periodicamente?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca

Figura 5.6: Resultado da aplicação no processo Funcionamento dos Comitês de TI (FCTI)

Há uma nova proposta de funcionamento do Funcionamento dos Comitês de TI que visa transformá-lo em um comitê deliberativo. O atual comitê funcionaria no plano tático/operacional e seria considerado um subcomitê que levaria os assuntos críticos para o nível estratégico.

5.3.4 Aplicação do instrumento no processo Orçamentário de TI (OTI)

Os três itens de verificação do processo Orçamentário de TI (OTI) são práticas que a organização reconhece a sua importância, porém apenas o item 1 (Orçamento de TI na LOA) é adotado integralmente (Figura 5.7). Os itens 2 (proposta baseada nos objetivos do negócio) e 3 (acompanhamento dos gastos de TI) são adotados parcialmente, pois não estão completamente implementadas.

Em relação as atividades de riscos, percebe-se uma evolução em relação ao processo anterior. Neste caso, há evidências de que as atividades de riscos são executadas em todas as etapas da ISO 31000 [16], sendo que 95% dos casos a aplicabilidade das atividades de gestão de riscos são limitadas. Destaca-se a atividade "Tratamento do Risco" com a aplicabilidade adequada para o item 1 (Previsão de orçamento de TI na LOA). Assim o processo OTI alcançou o nível de maturidade "**Complacente**".

1. É feita a previsão de orçamento de TI na LOA?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Alguma	Alguma	Alguma	Alguma	Alguma	Boa	Alguma
2. Existe uma proposta orçamentária de TI feita com base nas estimativas de custos das atividades que pretendem executar alinhadas aos objetivos do negócio da organização?						Adota parcialmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Alguma	Alguma	Alguma	Alguma	Alguma	Alguma	Alguma
3. É realizado um acompanhamento ao longo do exercício financeiro dos gastos efetuados especificamente com TI?						Adota parcialmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Alguma	Alguma	Alguma	Alguma	Alguma	Alguma	Alguma

Figura 5.7: Resultado da aplicação no processo Orçamentário de TI (OTI)

Em recente execução do processo OTI, foram realizadas reuniões específicas para identificar, analisar, avaliar e tratar riscos, além da realização de treinamentos em gestão de riscos para alguns recursos humanos do MP. Nesse processo específico fica demonstrado um nível de maturidade maior.

5.3.5 Aplicação do instrumento no Processo de Software (PS)

A unidade de TI preconiza as boas práticas em gestão de TI e adota integralmente as práticas de "Definição do processo - item 1" e de "formalização do processo de software - item 2", conforme Figura 5.8. A "Divulgação do processo - item 3" e a "Avaliação periódica - item 4" são adotadas parcialmente. Foi constatada que a divulgação do processo só ocorre na equipe interna, sendo que a Norma ISO 15504-3 estabelece uma ampla divulgação. Já a avaliação periódica é realizada de forma *ad hoc*, faltando um normativo que descreva o processo de avaliação e revisão.

Quanto a avaliação das etapas da ISO 31000 [16], constata-se que há pouca atividade relacionada a riscos, alcançando o nível de maturidade "**Reativo**" para o processo PS. O processo de desenvolvimento de software do MP, denominado Processo de Entrega de Solução (PES), não prevê atividades de gestão de riscos embarcadas. Geralmente, a equipe só se envolve depois que os riscos são concretizados e se tornam um problema, ou seja, há uma atuação reativa do órgão.

1. Existe a definição do Processo de Software com base na Norma ISO/IEC 15504-3?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca
2. O Processo de Software é formalizado?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca
3. Existe a divulgação do Processo de Software?						Adota parcialmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca
4. O Processo de Software sofre uma avaliação periódica?						Adota parcialmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca

Figura 5.8: Resultado da aplicação no Processo Processo de Software (PS)

O envolvimento do time de mantenedores do PES na aplicação do IAMGR possibilitou que o grupo chegasse à conclusão da importância da gestão de riscos, bem como comprovar a sua ausência, concluindo pela necessidade de evolução do PES para incorporar o tema "riscos".

5.3.6 Aplicação do instrumento no processo de Gerenciamento de Projetos de TI (GPTI)

A organização implantou uma unidade responsável pelo portfólio de projetos de TI e o processo de gerenciamento de projetos de TI que foi definido está totalmente aderente ao PMBOK. Dessa forma, o item 1 é Adotado integralmente (Figura 5.9). Quanto à Formalização (item 2) e à Divulgação (item 3), o órgão está aguardando o amadurecimento do processo para formalizar e divulgar um processo estável que agregue valor aos projetos, sendo classificadas como "Iniciou plano para adotá-la". A Avaliação periódica (item 4)

é adotada parcialmente, pois falta o normativo que estabelece a periodicidade. Hoje é realizada de forma *ad hoc*.

Em relação à gestão de riscos, observa-se uma aplicabilidade maior no item "Processo de gerenciamento de projetos aderente ao PMBOK", item 1. Isso se deve ao fato do PMBOK incorporar as boas práticas de gestão de riscos. Para os demais itens, percebem-se raras atividades de gestão de riscos. Quando ocorre são dispersas e isoladas. Com isso, o processo GPTI atingiu o nível "**Reativo**".

1. O processo de gerenciamento de projetos de TI é baseado no guia do Conjunto de Conhecimentos em Gerenciamento de Projetos, conhecido como PMBOK?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Alguma	Alguma	Alguma	Alguma	Alguma	Alguma	Muito Pouca
2. O processo de gerenciamento de projeto de TI está formalizado?						Iniciou plano para adotá-la
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca
3. O processo de gerenciamento de projeto de TI foi divulgado?						Iniciou plano para adotá-la
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca
4. O processo de gerenciamento de projeto de TI é avaliado periodicamente?						Adota parcialmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca

Figura 5.9: Resultado da aplicação no processo Gerenciamento de Projetos de TI (GPTI)

A metodologia de gestão de projetos de TI está em fase de implantação e foi, recentemente, revisada pela Universidade de Brasília - UnB, por meio de um Termo de Cooperação. A organização optou por coloca-la em prática antes da normatização, adotando uma metodologia mais simples devido ao grau de maturidade em gestão de projetos do órgão.

5.3.7 Aplicação do instrumento no processo de Gerenciamento de Serviços de TI (GSTI)

A adoção do primeiro item (gestão de serviços TI possui catálogo de serviços normatizado) é parcial, devido a manutenção do catálogo não estar normatizada (Figura 5.10), apesar dos esforços da unidade de TI em mantê-lo sempre atualizado. Os demais itens são reconhecidos como importantes para a organização, porém ainda não os implementam. O Termo de Cooperação celebrado com a UnB possibilitou que o órgão planejasse a implantação das boas práticas em gestão de serviços de TI, são elas: plano de continuidade (item 2) e os processos de gerenciamento de configuração e ativos (item 3), de incidentes (item 4), de mudanças (item 5), da liberação e implantação (item 6) e de problemas (item 7). Todos esses itens foram apontados pela UnB como críticos, com base na Biblioteca de Boas Práticas em Gestão de Serviços de ITIL. Sendo assim, os itens de verificação foram classificados como "Iniciou plano para adotar" para o critério de aplicabilidade.

Para as etapas da ISO 31000 [16], o órgão reconhece pouca atividade de gestão de riscos em todos os itens de verificação do processo GSTI, alcançando o nível de maturidade "**Reativo**".

1. A gestão de serviços da TI possui um catálogo de serviços normatizado?						Adota parcialmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca
2. Existe algum plano da continuidade dos serviços de TI já implantado?						Iniciou plano para adotá-la
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca
3. Existe um processo de gerenciamento de configuração e ativos normatizado?						Iniciou plano para adotá-la
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca
4. Existe um processo de gerenciamento de incidentes normatizado?						Iniciou plano para adotá-la
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca
5. Existe um processo de gerenciamento de mudanças normatizado?						Iniciou plano para adotá-la
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca
6. A gestão de serviços de TI possui um processo de gerenciamento da liberação e implantação normatizado?						Iniciou plano para adotá-la
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca
7. A gestão de serviços de TI possui um processo de gerenciamento de problemas normatizado?						Iniciou plano para adotá-la
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca

Figura 5.10: Resultado da aplicação no processo Gerenciamento de Serviços de TI (GSTI)

A unidade de TI reconhece que os processos de gerenciamentos de serviços propostos pela ITIL são inovadores, porém devido a complexidade e completude dos processos de gestão de serviços de TI o órgão enfrenta dificuldades na sua implantação.

5.3.8 Aplicação do instrumento no processo de Segurança da Informação (SI)

Os níveis de adoção dos itens de verificação são dispersos, ou seja, há itens que se aplicam totalmente e outros que não são adotados (Figura 5.11). Os itens "Responsável pela Segurança da Informação (item 1)", "Funcionamento dos Comitês de TI (item 2)", "Política de Segurança da Informação (item 3)" e "Equipe de tratamento e resposta a incidentes (item 4)" são adotados integralmente. Além disso, foi evidenciada a falta do inventário de ativos de informação (item 5), sendo classificada como "Não adota". O item 6 (Classificação da Informação) é adotado parcialmente, devido o normativo estar desatualizado. Quanto ao item 7 (gestão de riscos de segurança da informação), o termo de cooperação celebrado com a UnB previa a entrega da metodologia de gestão de riscos para segurança da informação, porém após pesquisas científicas e análise da DTI do MP-, optou-se por implantar uma metodologia de gestão de riscos corporativos com foco nos processos de negócio.

Em relação às etapas da ISO 31000 [16], observa-se que os itens que foram classificados como "Adota integralmente" possuem uma aplicação limitada das atividades de gestão de riscos. Já os itens que estão em fase de implantação, tais como: "não adota", "iniciou plano para adotar" ou "adota parcialmente" apresentaram pouca ou nenhuma atividade de risco.

O processo SI tem a Norma ISO 27000 como o seu principal norteador. Como esta norma possui a gestão de riscos embutida é possível que ela contribuiu para que o processo SI atingisse o nível de maturidade "**Complacente**".

1. Foi definido um responsável pela segurança da informação?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Alguma	Alguma	Alguma	Alguma	Alguma	Alguma	Alguma
2. O funcionamento do comitê de segurança de informação possui uma descrição?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Alguma	Alguma	Alguma	Alguma	Alguma	Alguma	Muito Pouca
3. A política de segurança da informação é publicada formalmente?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Alguma	Alguma	Alguma	Alguma	Alguma	Alguma	Alguma
4. Existe uma equipe de tratamento e resposta a incidentes em redes computacionais formalizada?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Alguma	Alguma	Alguma	Alguma	Alguma	Alguma	Alguma
5. Existe um inventário de ativos de informação normatizado?						Não adota
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Nenhum	Nenhum	Muito Pouca	Muito Pouca	Nenhum	Muito Pouca	Nenhum
6. A classificação da informação é normatizada?						Adota parcialmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca
7. A gestão de riscos de segurança da informação está normatizada?						Iniciou plano para adotá-la
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca

Figura 5.11: Resultado da aplicação no processo Segurança da Informação (SI)

Encontra-se em fase de aprovação pela Secretaria-Executiva do MP a nova Política de Segurança da Informação e Comunicação (POSIC), tendo como foco principal a gestão de riscos. A discussão gerada para elaboração dessa política elevou o conhecimento em gestão de riscos pelos colaboradores, contribuindo para o aculturamento do tema "riscos".

5.3.9 Aplicação do instrumento no processo Gestão de Pessoal de TI (GPeTI)

O processo de gestão de pessoal de TI (GPeTI) deve ser tratado com muito cuidado, pois os servidores públicos são regidos por estatuto próprio e a sua capacitação pode ou não estar vinculado a sua promoção/progressão na carreira.

Os itens 1 (Institucionalização do plano de capacitação), 2 (plano de capacitação com TI), 3 (capacitação em governança e em gestão de TI e 5 (metas de desempenho) foram classificados como “Adota parcialmente”, conforme Figura 5.12. No caso do item 1, ressalta-se que o plano de capacitação existe, porém necessita ser revisto. Em relação ao item 2, o atual plano de capacitação não atende todas as frentes da TI. Para o item 3, a capacitação em governança e em gestão de TI é realizada para um cargo específico de TI. Para os demais cargos o treinamento é optativo e livre. Em relação ao item 5, a unidade de TI do órgão iniciou plano para definir metas para o pessoal de TI.

A adoção integral dos itens de verificação ocorre nos itens 4 (avaliação do pessoal de TI) e 6 (avaliação periódica do desempenho do pessoal de TI). O núcleo de gestão de pessoal de TI do órgão implementa esses tipos de avaliações de forma periódica, submetendo todos os analistas em TI ao processo de avaliação. O item 7 foi classificado como “Não se aplica”, devido não haver um benefício financeiro para instituição em função do desempenho do pessoal da TI. Um exemplo de aplicação seria o recebimento de uma comissão pelos auditores da Receita Federal no caso de houver devolução de dinheiro aos cofres públicos.

Percebe-se que atividades de gestão de riscos no processo GPeTI são raras. Dessa forma, o referido processo encontra-se no nível de maturidade “**Reativo**”. Vale esclarecer que o item 7 não foi avaliado, pois o item não se aplica no órgão.

9. Gestão de Pessoas de TI (GPeTI)						
1. O plano anual de capacitação institucionalizado existe?						Adota parcialmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca
2. Existe um plano anual de capacitação que contempla a área de gestão de TI?						Adota parcialmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca
3. Existe um programa de capacitação em governança e em gestão de TI?						Adota parcialmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca
4. É feita uma forma de avaliação do quadro do pessoal de TI?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca
5. Metas de desempenho do pessoal de TI são adotadas?						Adota parcialmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca
6. É realizada uma avaliação periódica de desempenho do pessoal de TI?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca
7. Há algum benefício financeiro para instituição em função do desempenho alcançado pelo pessoal de TI?						Não se aplica
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Nenhum	Nenhum	Nenhum	Nenhum	Nenhum	Nenhum	Nenhum

Figura 5.12: Resultado da aplicação no processo Gestão de Pessoal de TI (GPeTI)

A unidade de TI do órgão definiu um processo de avaliação periódica das Funções Comissionadas Técnicas (FCT) que estão sob responsabilidade da DTI. A cada seis meses o comitê formado por gestores da unidade se reúne para discutir e definir os candidatos que devem receber a FCT, possibilitando que a meritocracia seja aplicada no serviço público.

5.3.10 Aplicação do instrumento no processo de Contratação e Gestão de Soluções de TI (CGSTI)

O processo de Contratação e Gestão de Soluções de TI (CGSTI) adota integralmente os itens 1 (Utilização da IN4/2010) e 2 (Controles para IN4), impulsionado pelo próprio MP que é responsável pela criação da Instrução Normativa n. 04/2010 da STI-MP que regulamenta a contratação de solução de TI nos órgãos do SISP. Já o item 3 (controles para gestão contratual) foi classificado como "Adota parcialmente", pois o processo de gestão de contratos de TI foi implantado somente em uma unidade do órgão (Figura 5.13).

Quanto a avaliação do processo de gestão de riscos, percebe-se que há atividades de gestão de riscos em todas as etapas. Vale destacar, que o item 1 (Aderência do processo de contratação de solução de TI à IN04/2010/STI-MP) apresenta um bom nível de maturidade para as etapas "Estabelecimento do contexto" e "Identificação" porque estão previstas na Instrução Normativa n. 04/2010/STI-MP. Por outro lado, a execução das atividades "Tratamento do Risco" e "Monitoramento e Análise Crítica" ainda são tímidas. Mesmo assim o processo CGSTI alcançou o nível de maturidade "**Complacente**".

1. O órgão realiza as contratações de soluções de TI de acordo com a Instrução Normativa n. 04/2010 da SLTI-MP?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Alguma	Boa	Boa	Alguma	Alguma	Muito Pouca	Muito Pouca
2. Existem controles que promovam o cumprimento da IN4?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Alguma	Alguma	Alguma	Alguma	Alguma	Alguma	Alguma
3. Existem controles que promovam a regularização da gestão contratual?						Adota parcialmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Alguma	Alguma	Alguma	Alguma	Alguma	Alguma	Alguma

Figura 5.13: Resultado da aplicação no processo Contratação e Gestão de Soluções de TI (CGSTI)

A proposição de alteração da Instrução Normativa n. 04/2010-STI-MP com a inclusão de atividade de tratamento e monitoramento dos riscos podem viabilizar o aprimoramento da gestão de riscos no órgão e, especificamente, para o processo de CGSTI. Dessa forma, os riscos seriam cobertos nas três fases: planejamento da contratação, seleção de fornecedor e gestão de contratos de TI.

5.3.11 Aplicação do instrumento no processo de Monitoração do Desempenho da TI (MDTI)

O órgão considera que faz a gestão de TI, porém a avaliação da gestão ainda é tímida dentro do órgão. Os itens 1 (Definição de indicadores, objetivos e metas para a gestão) e 2 (Gestão da TI monitorada) foram classificados como "Iniciou plano para adotá-la", pois encontra-se em andamento na unidade esforço entre a direção e os gestores para definir os indicadores, os objetivos e as metas para a gestão da TI (Figura 5.14). O monitoramento da gestão da TI (item 2) também foi classificada como "Iniciou plano para adotá-la". Atualmente relatórios gerenciais são entregues sob demanda ao Diretor.

Quanto ao item 3 (avaliação da gestão de TI) que foi classificado como "Adota parcialmente", foi relatado que o titular da unidade realiza a avaliação da gestão de TI de forma contínua para os detentores de cargos de chefia, porém não há um processo formalizado

nem um padrão estabelecido. Já os itens 4 (acompanhamento das metas) e 5 (uso da auditoria interna) não são adotados pelo MP, apesar de serem considerados críticos.

Em relação ao processo de gestão de riscos, percebe-se pouca aplicabilidade das atividades de gestão de riscos nos itens 1 ao 3. Nos itens 4 e 5 as atividades de gestão de riscos são inexistentes. Dessa forma, o processo MDTI alcançou o nível de maturidade em gestão de riscos "**Vulnerável**", o mais baixo dentre os processos avaliados.

1. São estabelecidos objetivos, indicadores e metas para gestão de TI?						**Iniciou plano para adotá-la**
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca
2. A gestão de TI é monitorada por meio de relatórios gerenciais?						**Iniciou plano para adotá-la**
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca
3. A avaliação da gestão de TI é realizada?						**Adota parcialmente**
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca
4. O acompanhamento periódico do alcance das metas estabelecidas para correção de desvios é feita?						**Não adota**
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Nenhum	Nenhum	Nenhum	Nenhum	Nenhum	Nenhum	Nenhum
5. A utilização de auditoria interna comum dos mecanismos para apoiar a realização das 3 ultimas tarefas acima é realizado?						**Não adota**
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Nenhum	Nenhum	Nenhum	Nenhum	Nenhum	Nenhum	Nenhum

Figura 5.14: Resultado da aplicação no processo de Monitoração do Desempenho da TI (MDTI)

O entrevistado relatou que a governança de TI do órgão melhorou muito nos últimos anos, porém a recente inclusão do projeto "Aprimorar a governança de TI" no Plano Estratégico de TI evidencia que ainda há muito a ser feito em relação ao tema.

5.4 Resultados Alcançados

O nível de maturidade em gestão de riscos alcançado na DTI foi **Vulnerável** (Tabela 5.1), ou seja, a organização não tem um conhecimento básico sobre o processo de gestão de riscos ou tem o conhecimento, porém ainda não o implementa. Indica que a organização não tem, ainda, uma metodologia de gestão de riscos estável e organizada. Neste nível, não há nenhuma evidência que a gestão de riscos possa apoiar a tomada de decisão.

Dos 11 processos avaliados, 3 processos atingiram o nível **Complacente**, devido a adoção das práticas de gestão de riscos nos normativos que regulam cada processo. As equipes envolvidas com orçamento, contratação de solução de TI e segurança da informação estão treinadas para identificar, analisar e tratar riscos, bem como estimar o valor do impacto e da probabilidade em função das escalas previamente definidas, seja de forma quantitativa ou qualitativa. Sabe-se que a Política de Gestão de Riscos do órgão está em vias de ser publicada.

A maioria dos processos, 7 ao todo, alcançaram o nível **Reativo**, ou seja, as pessoas envolvidas com planejamentos estratégicos (institucional e TI), comitês de TI, software, gerenciamento de projetos, gestão de serviços de TI e gestão de pessoas têm um bom conhecimento sobre o processo de Gestão de Riscos, porém ainda não foi propagado por todo o setor. Essas pessoas realizam a gestão de riscos de forma dispersa e intuitiva. Já o processo Monitoração do Desempenho da TI alcançou o menor índice, **Vulnerável**, sendo responsável pelo nível alcançado pela organização. Destaca-se que o resultado alcançado com a aplicação da planilha se demonstrou coerente com o sentimento inicial relatado pelo titular da área.

Percebe-se ainda que o processo Funcionamento dos Comitês de TI está na última faixa de pontuação do nível Reativo, podendo facilmente ascender para o próximo nível (Complacente).

Já os processos de Gerenciamento de Projetos de TI, Gerenciamento de Serviços de TI, Processo de Software e Monitoração do Desempenho da TI apresentaram os índices mais baixos, o que preocupa os gestores da área uma vez que esses processos são o núcleo da TI.

Tabela 5.1: Níveis de maturidade dos processos de TI no MP

Processos	**Pontuação Alcançada**	**Nível de Maturidade**
Planejamento Estratégico Institucional (PEI)	0,85	Reativo
Planejamento Estratégico de TI (PETI)	0,87	Reativo
Funcionamento dos Comitês de TI (FCTI)	0,96	Reativo
Orçamentário de TI (OTI)	1,15	Complacente
Processo de Software (PS)	0,79	Reativo
Gerenciamento de Projetos de TI (GPTI)	0,76	Reativo
Gerenciamento de Serviços de TI (GSTI)	0,52	Reativo
Segurança da Informação (SI)	1,08	Complacente
Gestão de Pessoal de TI (GPeTI)	0,85	Reativo
Contratação e Gestão de Soluções de TI (CGSTI)	1,15	Complacente
Monitoração do Desempenho da TI (MDTI)	**0,28 (menor)**	**Vulnerável**

O IAMGR disponibiliza três formas de representação gráfica para os resultados alcançados, são eles:

- *Ranking*: lista os processos de TI por ordem de pontuação, do menor para o maior. Possibilita que os processos mais críticos apareçam no topo da lista.

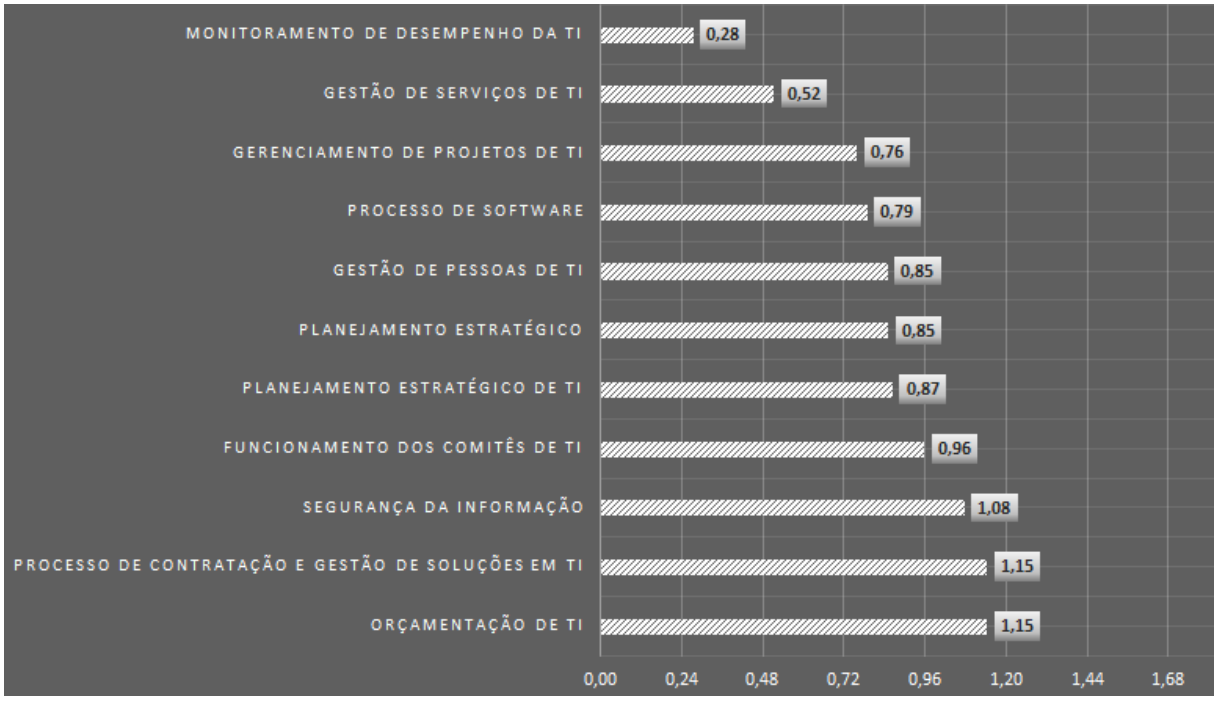


Figura 5.15: Gráfico de Ranking com a pontuação alcançado pelo MP

- Barras: este tipo de representação utiliza barras verticais para comparar o nível de maturidade em gestão de riscos dos processos avaliados. A linha horizontal indica o processo que obteve o nível de maturidade mais baixo com a aplicação do instrumento proposto neste trabalho.

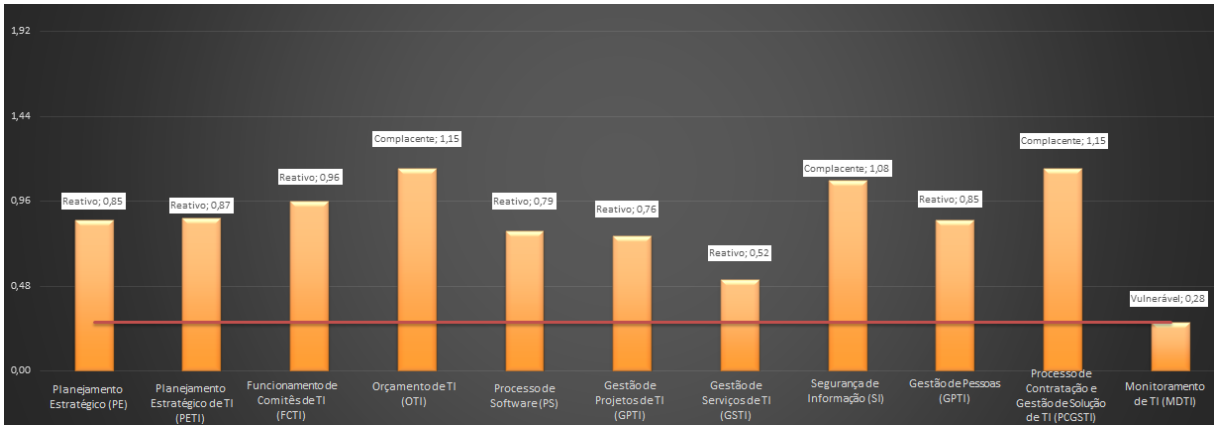


Figura 5.16: Gráfico de barras do resultado alcançado pelo MP

- Radar: este tipo de gráfico plota os valores e os níveis de maturidade alcançados de cada processo ao longo de um eixo separado que inicia no centro do gráfico e termina no anel externo (processo).

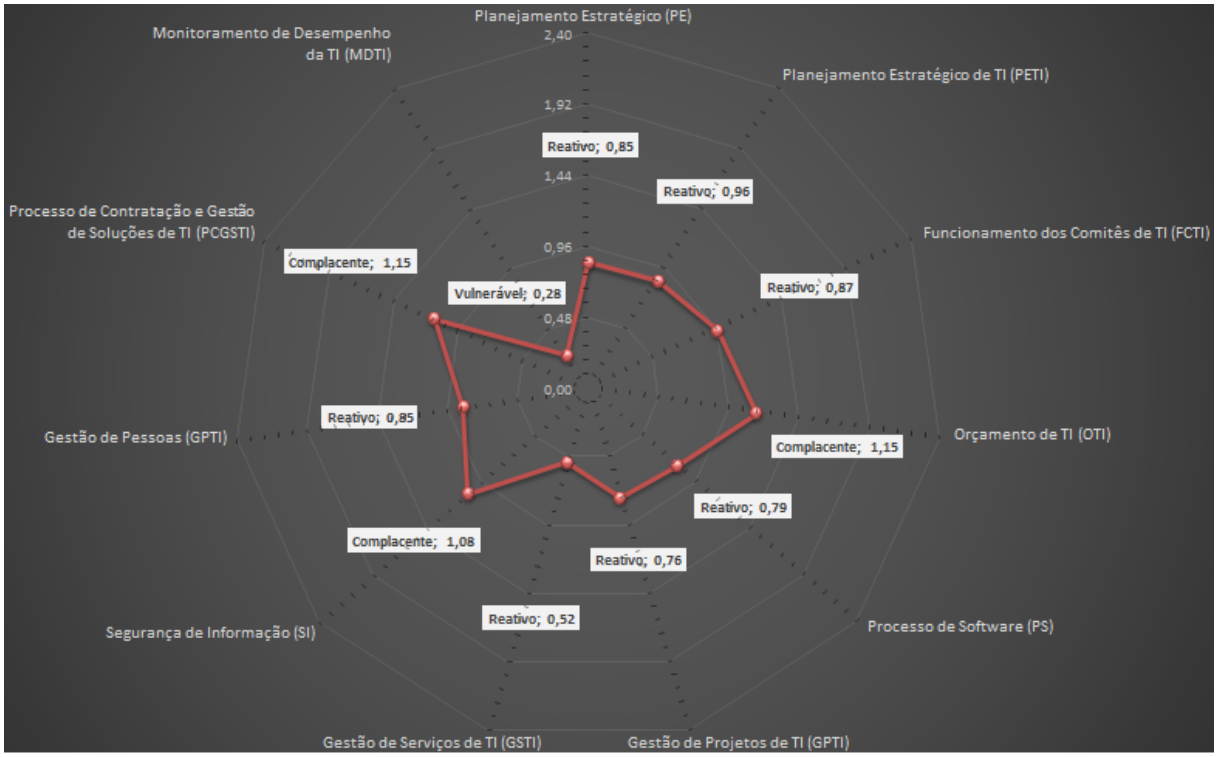


Figura 5.17: Gráfico Radar do resultado alcançado pelo MP

Pela análise gráfica é possível identificar os processos críticos e tomar alguma ação. Nesse estudo, se o dirigente tiver interesse em alavancar a maturidade do órgão deve ser priorizado o processo "Monitoramento do Desempenho da TI". Caso haja evolução nas práticas de gestão de riscos nesse processo é possível que o nível de maturidade do órgão seja Reativo.

A análise dos dados permite identificar as oportunidades de melhoria para a organização que se encontra no nível **Vulnerável**, visando à institucionalização da gestão de riscos. São elas:

- Obter o envolvimento ativo da alta administração com a institucionalização da gestão de riscos, divulgando a política corporativa de gestão de riscos;
- Instituir a capacitação regular de gestores para lidar com riscos;
- Orientar e estimular os servidores a encaminhar assuntos relacionados a risco às instâncias decisórias adequadas; e
- Estruturar e operacionalizar as etapas de identificação, análise, avaliação tratamento, monitoramento e comunicação de riscos.

Os dados mostram que há bastante espaço para que a gestão de riscos possa ser estruturada e fortalecida no órgão.

5.5 Análise do IAMGR

Percebeu-se que para utilização do IAMGR se faz necessário um alinhamento inicial dos conceitos envolvidos na gestão de riscos para que não haja dúvida quanto ao que se pretende. Uma noção básica em gestão de riscos por parte do respondente torna a pesquisa mais fácil de responder.

No caso específico, o Diretor de TI demonstrou amplo conhecimento em riscos, atuando de forma neutra e imparcial, o que facilitou a aplicação do instrumento. Percebeu-se também que ele conhece os processos avaliados. Assim não foi necessário discutir os processos avaliados nem os itens de verificação. Foi notório que a cada item de verificação avaliado se via uma preocupação no sentido do que podia ser melhorado. Nesse momento não analisava apenas o víeis de riscos, e sim, as boas práticas de governança que devem ser seguidas.

Foi relatado pelo respondente que uma possível restrição de uso do IAMGR poderá ser na dificuldade em visualizar o viés da gestão de riscos nos itens de verificação. Foi explicado ao titular que esse sentimento é causado normalmente pela baixa maturidade em gestão de riscos, ou seja, ausência da cultura de riscos no órgão. Acredita-se que com uma noção básica sobre gerenciamento de riscos e a identificação de um risco para cada item de verificação ajudaria no entendimento da relação dos itens com as etapas da ISO 31000 [16]. Percebeu-se também que quando o tema "riscos" está incorporado na unidade torna-se a aplicação do instrumento ainda mais fácil. Esta foi a percepção depois da avaliação de um processo considerado mais maduro, por exemplo, o processo Contratação e Gestão de Soluções de TI (CGSTI). Ao todo, foram gastas duas horas para aplicar o IAMGR na DTI, incluindo o tempo utilizado para exemplificar alguns riscos nos itens de verificação.

Foi identificada a necessidade de alguns ajustes nos cartões de respostas a fim de tornar as questões mais claras. Em relação aos requisitos implementados, não foi identificado qualquer problema em relação aos dados coletados. Um dos pontos fortes citado pelo respondente é relacionado aos cálculos, uma vez que a pontuação alcançada de cada processo apresentou uma variação, mas manteve o estágio de maturidade no mesmo nível. Essa questão foi analisada e na percepção do respondente o nível de maturidade não deveria mudar mesmo, já que o sentimento dele é que o processo não está em outro nível de maturidade. Com isso, foi validada a distribuição de pontos dos níveis de maturidade.

Capítulo 6

Conclusão

6.1 Considerações Finais

Este trabalho de pesquisa foi iniciado com um estudo comparativo entre os diversos modelos de maturidade, avaliando desde os modelos genéricos, passando por *frameworks* tradicionais, para então, atingir os modelos específicos de riscos. Na pesquisa bibliográfica foi possível identificar as características de cada modelo, as semelhanças e as inovações.

O levantamento dos normativos que os órgãos de controle levam em consideração na avaliação dos processos de TI, por meio da análise dos relatórios de auditorias, possibilitou identificar as questões observadas pelos órgãos de controle em cada um dos 11 processos de TI elencados neste trabalho, permitindo que, de forma secundária, seja possível verificar a aderência dos órgãos nas boas práticas em governança de TI.

De forma inovadora, o fluxograma para desenvolvimento de modelo de avaliação da maturidade proposto neste trabalho permite a sua aplicação em ambientes diversos ao tema estudado, podendo ser utilizado como apoio ou referência para trabalhos correlatos.

A partir do fluxograma proposto, foi elaborado o Instrumento de Avaliação da Maturidade em Gestão de Riscos, denominado como IAMGR. O instrumento prevê a aplicação em 11 (onze) processos de TI que são avaliados por meio dos itens de verificação que, por sua vez, estão relacionados com as 7 (sete) etapas da Norma ISO 31000 [16], tornando o IAMGR uma ferramenta de análise da maturidade em gestão de riscos para o setor público.

O IAMGR foi elaborado por meio de uma planilha eletrônica no software Microsoft Excel®. A ferramenta foi distribuída internamente para alguns servidores do órgão e para algumas entidades externas, as quais tiveram conhecimento deste trabalho e demonstraram interesse em colaborar com a pesquisa. Esse compartilhamento contribuiu para avaliação do instrumento e validação dos cálculos e da usabilidade. A ferramenta foi automatizada para apresentar os resultados de forma imediata e sem risco de erros. Ela é

composta por um tutorial sobre o instrumento, onze cartões de respostas que possibilitam a inserção de dados pelo respondente e uma seção com os resultados alcançados. Também foi prevista a possibilidade de inovação da ferramenta, por isso um conjunto de campos foram parametrizados. Além da demonstração da pontuação alcançada em cada processo de TI, a ferramenta apresentada o resultado de forma gráfica, sendo utilizados três tipos de gráficos: *Ranking*, Barras e Radar.

A validação do instrumento ocorreu na Diretoria de Tecnologia de Informação do Ministério do Planejamento, Desenvolvimento e Gestão (DTI/MP) que foi respondida pela autoridade máxima da unidade. A avaliação do Diretor de Tecnologia da Informação demonstrou que é viável a utilização do instrumento e que os requisitos estão corretamente definidos.

Outra possibilidade é a disponibilização do IAMGR à STI com a devida normatização do uso do instrumento pelos órgãos do SISP, permitindo que seja traçado um panorama da gestão de riscos nas entidades respondentes, subsidiando à STI de informações para a tomada de decisão em relação ao tema.

De uma forma geral, a aplicação do IAMGR permitiu identificar o nível de maturidade em gestão de riscos nos onze processos de TI na DTI, além de fornecer uma visão clara dos pontos críticos de cada processo, subsidiando o tomador de decisão de informações.

Os gestores de TI, que foram envolvidos neste trabalho, mencionaram as principais dificuldades à implantação de processos de gestão de riscos no MP, como a falta de aculturamento em gestão de riscos (evidenciada pela necessidade de incorporar atividades de análise de riscos às suas atividades cotidianas) e a ausência de estrutura dedicada à gestão de riscos (matriz de responsabilidade).

6.2 Recomendações para trabalhos futuros

Como sugestões para trabalhos futuros, citam-se:

- Construção de um *software* de avaliação da maturidade em gestão de riscos, baseada na planilha criada neste trabalho. Esse sistema pode evoluir para realizar a gestão dos riscos dos órgãos sob jurisdição do SISP;
- Desenvolvimento de outras versões do IAMGR incorporando outros processos de TI, além dos 11 (onze) utilizados;
- Validação dos pesos atribuídos para cada etapa da norma ISO 31000, proposto por Gaffo e De Barros [21], desenvolvendo um modelo de inferência dos pesos; e
- Desenvolvimento de um modelo para ponderação dos cinco níveis de maturidade do IAMGR.

Referências

[1] Carreira P. da Silva M.M. Antunes, P. Towards an energy management maturity model. http://dx.doi.org/10.1016/j.enpol.2014.06.011. 16

[2] APMG-International. O que é um modelo de maturidade e quais as razões para utilizá-lo? http://www.apmginternational.com/br/consultoria/modelo-maturidade.aspx, 2015. 14

[3] Araújo. A conceituação de governabilidade e governança, da sua relação entre si e com o conjunto da reforma do estado e do seu aparelho. *ENAP*, 2002. 12

[4] M. Araújo. Análise de maturidade da gestão de riscos de ti na fiocruz: definição e aplicação de instrumento de avaliação e especificação de requisitos para um sistema computacional. *UnB*, 2014. 2, 11, 21, 27, 40, 60

[5] ISACA Information Systems Audit e Control Association. Control objectives for information and related technology - cobit 5: Um modelo corporativo para a governança e gestão de ti da organização. 30, 46

[6] ISACA Information Systems Audit e Control Association. Control objectives for information and related technology - cobit 4.1: Governance it., 2007. x, xii, 12, 13, 27, 28, 29, 30, 38, 41, 45, 46, 47

[7] Neppelenbroek M. Shahim A. Batenburg, R. A maturity model for governance, risk management and compliance in hospitals. journal of hospital administration 3. 10.5430/jha.v3n4p43. 17

[8] Knackstedt R. Pöppelbuss s D.-W.I.J. Becker, J. Developing maturity models for it management. page 213 – 222, 2009. x, 14, 16, 32, 33, 34, 35, 40, 42

[9] Bakry S.H. Bin-Abbas, H. *Assessment of IT governance in organizations: A simple integrated approach.* 2014. 1

[10] G. Coyle. *The Analytic Hierarchy Process.* 2004. 25

[11] FNQ Fundação Nacional da Qualidade. Prêmio nacional de qualidade - pnq. http://www.fnq.org.br/avalie-se/pnq. xii, 53, 54, 55, 59, 60

[12] Freeze R. Kaulkarni U.-Rosemann M. De Bruin, T. Understanding the main phases of developing a maturity assessment model, in: Campbell, b., underwood, j., bunker, d. (eds.). 2005. 14, 16, 41

[13] PMI Instituto de Gerenciamento de Projetos. *Guia do PMBOK: um Guia do Conjunto de Conhecimentos em Gerenciamento de Projetos*. 5ª. Edição, 2013. 7, 9, 30, 46

[14] ABNT Associação Brasileira de Normas Técnica. Nbr iso 15504-4:2008 – avaliação de processos – parte 4: Orientação no uso para melhoria do processo e determinação da potencialidade do processo, 2008b. x, 30, 32

[15] ABNT Associação Brasileira de Normas Técnica. Abnt iso guia 73:2009 - gestão de riscos - vocabulário, 2009a. 7

[16] ABNT Associação Brasileira de Normas Técnica. Nbr iso/iec 31000:2009 - gestão de riscos corporativos – princípios e diretrizes, 2009b. x, 2, 7, 9, 10, 11, 25, 30, 31, 41, 52, 55, 62, 64, 66, 67, 71, 73, 75, 82, 83, 84, 86, 89, 90, 93, 95, 106, 107

[17] ABNT Associação Brasileira de Normas Técnica. Nbr iso/iec 38500:2009 - governança corporativa de tecnologia da informação, 2009c. 12, 30

[18] ABNT Associação Brasileira de Normas Técnicas. Nbr iso 15504-3:2008 – parte 3: Orientações para realização de uma avaliação, 2008a. 14, 32, 39, 46

[19] Kriouile A. Elmaallam, M. Towards a model of maturity for is risk management. *International Journal of Computer Science and Information Technology (IJCSIT)*, 3, 2012. 8, 15, 25, 38, 41, 42

[20] Almeida J. de O.R. de Leão P.R.C. Silva N.P.G. Ferreira, B.A. de A. Gestão de riscos em projetos: Uma análise comparativa da norma iso 31000 e o guia pmbok®. pages 46–72, 2012. 9, 10, 11

[21] De Barros R.M. Gaffo, F.H. *Metodologia para Avaliar o Grau de Maturidade em Gestão de Riscos*. Universidade Estadual de Londrina (UEL), 2013. 67, 108

[22] R.Z. Giampaoli, 2010. 1, 2, 12

[23] Hartmut Gunther. Pesquisa qualitativa versus pesquisa quantitativa: Esta É a questão? *Psicologia: Teoria e Pesquisa*, 22:201 – 209, 08 2006. 5

[24] D.A. Hillson. Towards a risk maturity model. *The International Journal of Project and Business Risk Management*, 1:35–45, 1997. x, xii, 22, 23, 24, 37, 40

[25] M.M. Hopkinson. The project risk maturity model: Measuring and improving risk management capability. 2012. x, 24, 37, 41, 42

[26] "Instituto Brasileiro de Governança Corporativa" IBGC. Itscore overview for program and portfolio management. `http://www.ibgc.org.br/inter.php?id=18161/governanca-corporativa.`, 2015. 1, 7, 12

[27] Gartner Inc. Itscore overview for program and portfolio management. `https://www.gartner.com/doc/2837917/itscore-overview-programportfolio-management`, 2014. x, 26

[28] Protiviti Inc. Guide to enterprise risk management – frequently asked questions. http://www.protiviti.com/en-US/Documents/Resource-Guides/ProtivitiERM_FAQGuide.pdf, 2006. x, 21, 25, 38

[29] ITGI IT Governance Institute. Itscore overview for program and portfolio management. http://www.itgi.org/, 2015. 25, 27

[30] SEI Software Engineering Institute. Modelo integrado de maturidade e de capacidade - CMMI. https://www.sei.cmu.edu/cmmi/, 2010. x, 8, 18, 19, 30, 38, 46, 66

[31] SEI Software Engineering Institute. Plano estratégico do tribunal (PET) - 2011/2015, 2015. 2

[32] Cesarotti V. Benedetti M. Biagiotti S. Rotunno R. Introna, V. Energy management maturity model: an organizational tool to foster the continuous reduction of energy consumption in companies. *Journal of Cleaner Production*, 83:108–117, 2014. 14, 16, 64

[33] Ni X. Chen Z. Hong B. Chen Y. Yang F. Lin C. Jia, G. Measuring the maturity of risk management in large-scale construction projects. *Automation in Construction*, 34:56 – 66, 2013. 17

[34] Maier R. Thalmann S. Kohlegger, M. Understanding maturity models results of a structured content analysis proceedings of i-know '09 and isemantics '09. 2009. 14

[35] Kriouile A. Maallam, M. El. Development of the isr3m model for is risk management evaluation using the focus area structure according to the mmdpis generic process. transactions on machine learning and artificial intelligence 2. 31, 39, 41, 42, 53, 54

[36] G.F. MP. Planejamento estratégico 2012 - 2015. http://www.planejamento.gov.br/secretarias/upload/Arquivos/publicacao/planejamento_estrategico/130314_planejamento_estrategico.pdf, 2015a. x, 45, 77, 78, 80, 81

[37] G.F. MP. Plano diretor de tecnologia da informação – pdti 2014/2015 - edição revisada. http://www.planejamento.gov.br/secretarias/upload/Arquivos/sec_exec/131224_pdti_mp.pdf/view, 2015b. 3

[38] G.F. MP. Plano diretor de tecnologia da informação – peti. http://www.gespublica.gov.br/, 2015c. 8, 9, 53, 54, 83

[39] COSO The Committee of Sponsoring Organizations of the Treadway. Gerenciamento de riscos corporativos: Estrutura integrada. http://www.coso.org/Publications/erm/COSO_ERM_ExecutiveSummary_Portuguese.pdf, 2007. x, 8, 20, 21, 30, 41

[40] Martins R.A. Oliveira, G.T. de. Efeitos da adoção do modelo do prêmio nacional da qualidade na medição de desempenho: estudos de caso em empresas ganhadoras do prêmio. *Gestão e Produção*, 2008. 53

[41] Tuunanen T. Rothenberger M.A. Chatterjee S. Peffers, K. A design science research methodology for information systems research. *Journal of management information systems*, 2007. 42

[42] Silva M.M. Pereira, R. IT governance implementation: The determinant factors. communications of the IBIMA, 2012. 11, 12

[43] M.E PORTER. *What makes a useful maturity model? a framework of general design principles for maturity models and its demonstration in business process management.* 2011. 78

[44] Röglinger M. Pöppelbuss, J. *Vantagem competitiva.* Rio de Janeiro: Campus, 1990. 32, 60

[45] Alexander R. McDermid J. Rae, A. Fixing the cracks in the crystal ball: A maturity model for quantitative risk assessment. *Reliability Engineering and System Safety*, 2014. 17, 18

[46] Capretz L.F. Ahmed F. Raza, A. An open source usability maturity model (OS-UMM). *Computers in Human Behavior*, 2012. 17

[47] TCU. Avaliar se a gestão e o uso da tecnologia da informação estão de acordo com a legislação e aderentes às boas práticas de governança de TI. (auditoria no. acórdão 2308/2010 - TCU - plenário), 2010. 1, 12, 66

[48] TCU. Agregar os resultados de todas as fiscalizações previstas, de modo a sintetizar os achados e conclusões sobre a gestão e uso de ti na administração pública federal (APF). (auditoria no. acórdão 1.233/2012 – plenário TCU), 2012. 1, 2, 3, 36, 41, 44, 45, 46, 47, 48

[49] TCU. Elaborar indicador que reflita o grau de maturidade dos órgãos e entidades públicos em relação à gestão de riscos e aos controles internos (auditoria no. acórdão 2.467/2013 - plenário TCU), 2013. 2, 4, 9, 25, 39, 41, 53, 54

[50] TCU. Avaliar a implementação dos controles de TI informados pela empresa brasileira de infraestrutura aeroportuária - infraero em resposta ao levantamento doperfil de governança de TI realizado em 2012 (auditoria no. acórdão 0.755/2014 - plenário TCU), 2014a. 30

[51] TCU. Avaliar a implementação dos controles de TI informados pelo ministério da educação (MEC) em resposta ao levantamento do perfil de governança de ti realizado em 2012 (auditoria no. acórdão 1.015/2014 - plenário TCU), 2014b. 30

[52] TCU. Avaliar a implementação dos controles informados pela eletrobrás termonuclear S.A. (eletronuclear) em resposta ao levantamento do perfil de governança de ti realizado em 2012 (auditoria no. acórdão 1.684/2014 - plenário TCU), 2014c. 30

[53] D. Tripp. Pesquisa-ação: uma introdução metodológica. *Educação e Pesquisa, São Paulo*, 31, 2005. 5

[54] Bianchin L.A. Lunardi R.C. Granville L.Z. Gaspary L.P. Bartolini C. Wickboldt, J.A. A framework for risk assessment based on analysis of historical information of workflow execution in it systems. *Computer Networks*, 55, 2011. 9

Apêndice A

Cartões de Resposta

Os processos de TI levados em consideração na elaboração do IAMGR foram materializados em onze cartões de resposta.

1. É feita a previsão de orçamento de TI na LOA?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Alguma	Alguma	Alguma	Alguma	Alguma	Boa	Alguma

2. Existe uma proposta orçamentária de TI feita com base nas estimativas de custos das atividades que pretendem executar alinhadas aos objetivos do negócio da organização?						Adota parcialmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Alguma	Alguma	Alguma	Alguma	Alguma	Alguma	Alguma

3. É realizado um acompanhamento ao longo do exercício financeiro dos gastos efetuados especificamente com TI?						Adota parcialmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Alguma	Alguma	Alguma	Alguma	Alguma	Alguma	Alguma

1. Existe a definição do Processo de Software com base na Norma ISO/IEC 15504-3?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca

2. O Processo de Software é formalizado?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca

3. Existe a divulgação do Processo de Software?						Adota parcialmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca

4. O Processo de Software sofre uma avaliação periódica?						Adota parcialmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca

3. Funcionamento dos Comitês de TI (FCTI)

1. A instituição formal dos comitês de TI é realizada?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	**Estabelecimento do Contexto**	**Identificação de Riscos**	**Análise de Riscos**	**Avaliação do risco**	**Tratamento do Risco**	**Monitoramento e Análise Crítica**
Completa	Completa	Completa	Completa	Completa	Completa	Completa

2. Existe a descrição do funcionamento dos comitês de TI?						Adota parcialmente
Etapas da ISO 31000						
Comunicação e consulta	**Estabelecimento do Contexto**	**Identificação de Riscos**	**Análise de Riscos**	**Avaliação do risco**	**Tratamento do Risco**	**Monitoramento e Análise Crítica**
Completa	Completa	Completa	Completa	Completa	Completa	Completa

3. A indicação da composição dos representantes da área de negócio e de TI é feita?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	**Estabelecimento do Contexto**	**Identificação de Riscos**	**Análise de Riscos**	**Avaliação do risco**	**Tratamento do Risco**	**Monitoramento e Análise Crítica**
Completa	Completa	Completa	Completa	Completa	Completa	Completa

4. O funcionamento dos comitês de TI é realizado periodicamente?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	**Estabelecimento do Contexto**	**Identificação de Riscos**	**Análise de Riscos**	**Avaliação do risco**	**Tratamento do Risco**	**Monitoramento e Análise Crítica**
Completa	Completa	Completa	Completa	Completa	Completa	Completa

4. Orçamentação de TI (OTI)						
1. É feita a previsão de orçamento de TI na LOA?						Adota parcialmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Completa	Completa	Completa	Completa	Completa	Completa	Completa
2. Existe uma proposta orçamentária de TI feita com base nas estimativas de custos das atividades que pretendem executar alinhadas aos objetivos do negócio da organização?						Iniciou plano para adotá-la
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Completa	Completa	Completa	Completa	Completa	Completa	Muito Pouca
3. É realizado um acompanhamento ao longo do exercício financeiro dos gastos efetuados especificamente com TI?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Completa	Completa	Completa	Completa	Completa	Completa	Completa

5. Processo de Software (PS)						
1. Existe a definição dos processos de software com base nas melhores práticas de mercado?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca
2. O processo de software é formalizado?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Completa	Completa	Completa	Completa	Completa	Completa	Completa
3. Existe a divulgação do processo de software?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Completa	Completa	Completa	Completa	Completa	Completa	Completa
4. O processo de Software sofre uma avaliação periódica?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Completa	Completa	Completa	Completa	Completa	Completa	Completa

6. Gerenciamento de projetos de TI (GPTI)						
1. O processo de gerenciamento de projetos de TI é baseado nas melhores práticas?						Não adota
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Completa	Completa	Completa	Completa	Completa	Completa	Completa
2. O processo de gerenciamento de TI está formalizado?						Não se aplica
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Completa	Completa	Completa	Completa	Completa	Completa	Completa
3. O gerenciamento do projeto de TI foi divulgado?						Adota parcialmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Completa	Completa	Completa	Completa	Completa	Completa	Completa
4. O gerenciamento de projeto de TI é avaliado periodicamente?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Completa	Completa	Completa	Completa	Completa	Completa	Completa

7. Gestão de Serviços de TI (GSTI)						
1. A gestão de serviços da TI possui um catálogo de serviços normatizado?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Completa	Completa	Completa	Completa	Completa	Completa	Completa
2. Existe algum plano da continuidade dos serviços de TI já implantado?						Adota parcialmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Completa	Completa	Completa	Completa	Completa	Completa	Completa
3. Existe gerenciamento de configuração e ativos normatizado?						Iniciou plano para adotá-la
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Completa	Completa	Completa	Completa	Completa	Completa	Completa
4. Existe gerenciamento de incidentes normatizado?						Não adota
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Completa	Completa	Completa	Completa	Completa	Completa	Completa
5. Existe gerenciamento de mudanças normatizado?						Não se aplica
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Completa	Completa	Completa	Completa	Completa	Completa	Completa
6. A gestão de serviços de TI possui gerenciamento da liberação e implantação normatizado?						Não adota
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Completa	Completa	Alguma	Nenhum	Muito Pouca	Completa	Completa
7. A gestão de serviços de TI possui gerenciamento de problemas normatizado?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Completa	Completa	Boa	Completa	Completa	Completa	Completa

8. Segurança da Informação (SI)						
1. Foi definido um responsável pela segurança da informação?						Não adota
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Completa	Completa	Completa	Completa	Completa	Completa	Completa
2. O funcionamento do comitê de segurança de informação possui uma descrição?						Não se aplica
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Completa	Completa	Completa	Completa	Completa	Completa	Completa
3. A política de segurança da informação é publicada formalmente?						Iniciou plano para adotá-la
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Completa	Completa	Completa	Muito Pouca	Muito Pouca	Muito Pouca	Muito Pouca
4. Existe uma equipe de tratamento e resposta a incidentes em redes computacionais formalizada?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Completa	Completa	Completa	Completa	Muito Pouca	Muito Pouca	Muito Pouca
5. Existe um inventário de ativos de informação normatizado?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Completa	Completa	Completa	Completa	Completa	Boa	Completa
6. A classificação da informação é normatizada?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Completa	Completa	Completa	Completa	Completa	Completa	Completa
7. A gestão de riscos de segurança da informação está normatizada?						Não se aplica
Etapas da ISO 31000						

9. Gestão de Pessoas de TI (GPTI)						
1. O plano anual de capacitação institucionalizado existe?						Não se aplica
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Completa	Completa	Completa	Completa	Completa	Completa	Completa
2. Existe um plano anual de capacitação que contempla a área de gestão de TI?						Não adota
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Completa	Completa	Completa	Completa	Completa	Completa	Completa
3. Existe um programa de capacitação em governança e em gestão de TI?						Iniciou plano para adotá-la
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Completa	Completa	Completa	Completa	Completa	Completa	Completa
4. É feita uma forma de avaliação do quadro do pessoal de TI?						Adota parcialmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Nenhum	Nenhum	Nenhum	Nenhum	Nenhum	Nenhum	Nenhum
5. Metas de desempenho do pessoal de TI são adotadas?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento e Análise Crítica
Completa	Completa	Completa	Completa	Completa	Completa	Completa
6. É realizada uma avaliação periódica de desempenho do pessoal de TI?						Não se aplica
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento Análise Crítica
Completa	Completa	Completa	Completa	Completa	Completa	Completa
7. Em função do desempenho alcançado pelo pessoal de TI apresenta algum benefício financeiro?						Adota integralmente
Etapas da ISO 31000						
Comunicação e consulta	Estabelecimento do Contexto	Identificação de Riscos	Análise de Riscos	Avaliação do risco	Tratamento do Risco	Monitoramento Análise Crítica
Completa	Completa	Completa	Completa	Completa	Completa	Completa

10. Processo de Contratação e Gestão de Soluções de TI (PCGSTI)

1. O órgão realiza as contratações de soluções de TI de acordo com a IN04/SLTI-MP?						**Não se aplica**
Etapas da ISO 31000						
Comunicação e consulta	**Estabelecimento do Contexto**	**Identificação de Riscos**	**Análise de Riscos**	**Avaliação do risco**	**Tratamento do Risco**	**Monitoramento e Análise Crítica**
Completa	Completa	Completa	Completa	Completa	Completa	Completa

2. Existem controles que promovam o cumprimento da IN4?						**Não adota**
Etapas da ISO 31000						
Comunicação e consulta	**Estabelecimento do Contexto**	**Identificação de Riscos**	**Análise de Riscos**	**Avaliação do risco**	**Tratamento do Risco**	**Monitoramento e Análise Crítica**
Completa	Completa	Completa	Completa	Completa	Completa	Completa

3. Existem controles que promovam a regularização da gestão contratual?						**Adota integralmente**
Etapas da ISO 31000						
Comunicação e consulta	**Estabelecimento do Contexto**	**Identificação de Riscos**	**Análise de Riscos**	**Avaliação do risco**	**Tratamento do Risco**	**Monitoramento e Análise Crítica**
Completa	Completa	Completa	Completa	Completa	Completa	Completa

11. Monitoramento do desempenho da TI						
1. São estabelecidos objetivos, indicadores e metas para gestão de TI?						**Adota integralmente**
Etapas da ISO 31000						
Comunicação e consulta	**Estabelecimento do Contexto**	**Identificação de Riscos**	**Análise de Riscos**	**Avaliação do risco**	**Tratamento do Risco**	**Monitoramento e Análise Crítica**
Completa	Completa	Completa	Completa	Completa	Completa	Completa
2. A gestão de TI é monitorada por meio de relatórios gerenciais?						**Adota parcialmente**
Etapas da ISO 31000						
Comunicação e consulta	**Estabelecimento do Contexto**	**Identificação de Riscos**	**Análise de Riscos**	**Avaliação do risco**	**Tratamento do Risco**	**Monitoramento e Análise Crítica**
Completa	Completa	Completa	Completa	Completa	Completa	Completa
3. A avaliação da gestão de TI é realizada?						**Não adota**
Etapas da ISO 31000						
Comunicação e consulta	**Estabelecimento do Contexto**	**Identificação de Riscos**	**Análise de Riscos**	**Avaliação do risco**	**Tratamento do Risco**	**Monitoramento e Análise Crítica**
Completa	Completa	Completa	Completa	Completa	Completa	Completa
4. O acompanhamento periódico do alcance das metas estabelecidas para correção de desvios é feita?						**Não se aplica**
Etapas da ISO 31000						
Comunicação e consulta	**Estabelecimento do Contexto**	**Identificação de Riscos**	**Análise de Riscos**	**Avaliação do risco**	**Tratamento do Risco**	**Monitoramento e Análise Crítica**
Completa	Completa	Completa	Completa	Completa	Completa	Completa
5. A utilização de auditoria interna comum dos mecanismos para apoiar a realização das 3 ultimas tarefas acima é realizado?						**Adota integralmente**
Etapas da ISO 31000						
Comunicação e consulta	**Estabelecimento do Contexto**	**Identificação de Riscos**	**Análise de Riscos**	**Avaliação do risco**	**Tratamento do Risco**	**Monitoramento e Análise Crítica**
Completa	Completa	Completa	Completa	Completa	Completa	Completa